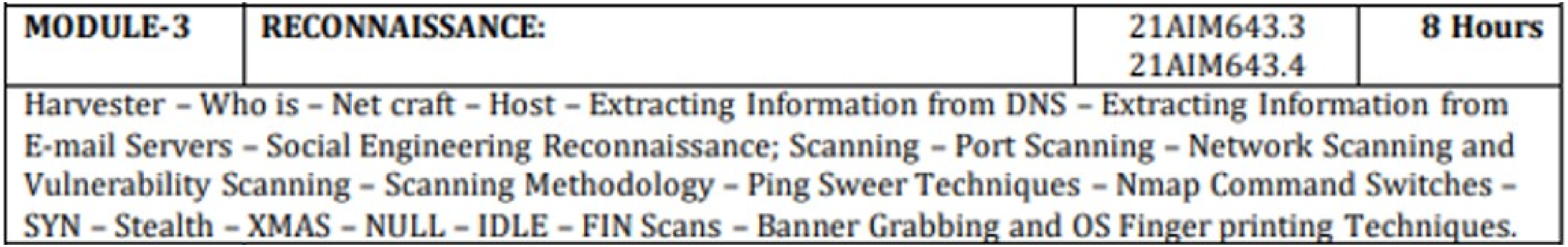
MODULE III

Shashi KS



MODULE-3	RECONNAISSANCE:	21AIM643.3 21AIM643.4	8 Hours
Harvester – Who is – Net craft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches – SYN – Stealth – XMAS – NULL – IDLE – FIN Scans – Banner Grabbing and OS Finger printing Techniques.			

COURSE CODE: 21AIM643
COURSE NAME: CYBER SECURITY
FACULTY NAME: K.S.SHASHIKALA

Textbook for reference for this module

Shashi KS

Chapter 2 – “The basics of hacking and penetration testing” , 2nd edition

By Patrick Engebretson, Elsevier 2013 edition

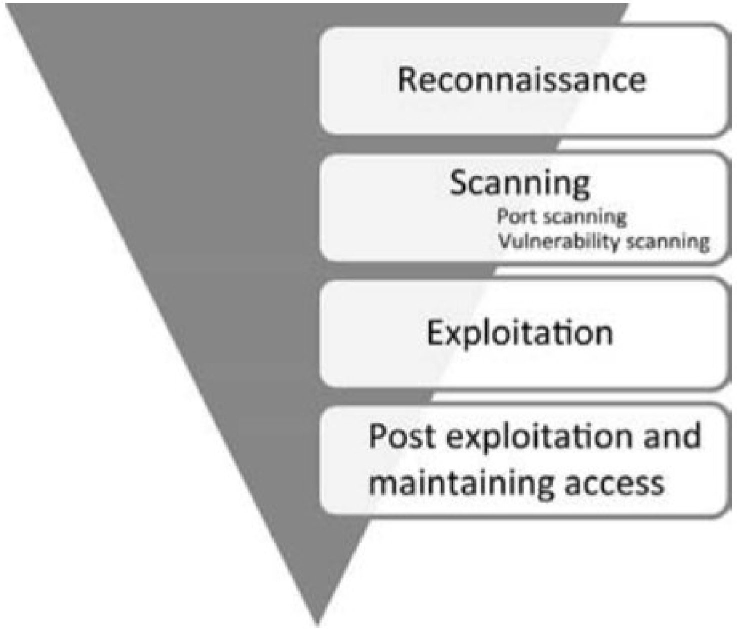
Penetration testing

Shashi KS

A penetration test, or "pen test," **is a security test that launches a mock cyberattack to find vulnerabilities in a computer system. Penetration testing and hacking are a means of securing systems.**

The overall process of penetration testing can be broken down into a series of steps or phases. When put together, these steps form a comprehensive methodology for completing a penetration test.

This methodology usually contains between four phases, **Reconnaissance, Scanning, Exploitation, and Post Exploitation**



ZERO ENTRY HACKING PENETRATION TESTING METHODOLOGY

STEPS IN PENETRATION TESTING

Shashi KS

The first step in any penetration test is **“reconnaissance”**. This phase deals with **information gathering** about the target. The more information you collect on your target, the more likely you are to succeed in later steps

Regardless of the information you had to begin with, after completing indepth reconnaissance **you should have a list of target IP addresses that can be scanned.**

The second step in our methodology can be broken out into two distinct activities. The first activity we conduct is port **scanning.**

Vulnerability scanning

Shashi KS

Port scanning results in having a **list of open ports and potential service running on each of the targets**. The second activity in the scanning phase is vulnerability scanning. Vulnerability scanning is the process of locating and **identifying specific weaknesses in the software and services of our targets.**

Exploitation phase:

Once we know exactly what ports are open, what services are running on those ports, and what vulnerabilities are associated with those services, we can begin to attack our target.

Exploitation can involve lots of different **techniques, tools, and code.**

Reconnaissance

Shashi KS

Reconnaissance" phase deals with **information gathering** about the target. The goal of reconnaissance is to collect as much information as possible on your target

Active reconnaissance includes **interacting directly with the** target. During this process, the target **may record our IP address and log our activity. This has a higher likelihood of being detected i**f we are attempting to perform a PT in a stealth fashion.

Passive reconnaissance makes use of the vast amount of information available on the web. When we are conducting passive reconnaissance, we are not interacting directly with the target and as such, **the target has no way of knowing, recording, or logging our activity.**

At this point in the penetration test, no detail should be overlooked regardless of how innocuous it may seem. While you are gathering information, it is important to **keep your data in a central location. Whenever possible, it is helpful to keep the information in electronic format. This allows for quick and accurate searches later on. Digital records can be easily sorted, edited, copied, imported, pruned, and mined.**

THE HARVESTER: DISCOVERING AND LEVERAGING E-MAIL ADDRESSES

Shashi KS

- ✓ An excellent tool to use **in reconnaissance is the Harvester.**

- ✓ The Harvester is a simple but highly effective Python script written by **Christian Martorella at Edge Security.**

- ✓ This tool allows us to quickly and accurately **catalog both e-mail addresses and subdomains that are directly related to our target.**

- ✓ It is important to always use **the latest version of the Harvester** as many search engines regularly update and change their systems. Even subtle changes to a search engine’s behavior can render automated tools ineffective. In some cases, search engines will actually filter the results before returning information to you.

- ✓ Many search engines also employ throttling techniques that will attempt to prevent you from running automated searches. The Harvester can be used to search **Google, Bing, and PGP servers for e-mails, hosts, and subdomains. It can also search LinkedIn for user names.**

How to access the Harvester

Shashi KS

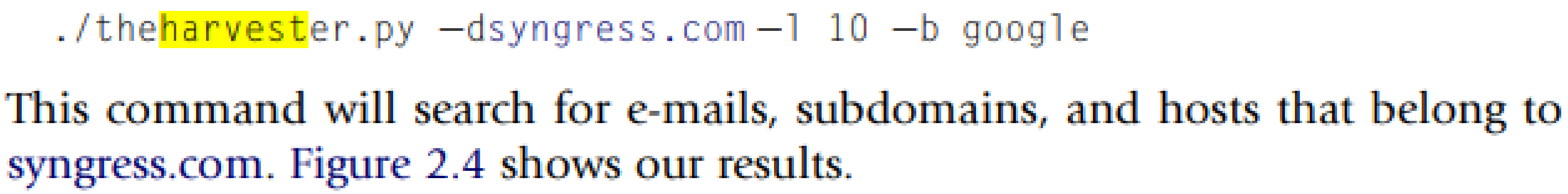
The Harvester is built into **Kali.** The quickest way to access the Harvester is to open a terminal window and issue the command:

theharvester.

If you need the full path to the program and you are using Kali, the Harvester (and nearly all other tools) can be found in the **/usr/bin/ directory.**

However, one major advantage to Kali is that you no longer need to specify the full path to run these tools. Simply opening the terminal and entering the tool's start command will invoke it. For example, to run the harvester, open a terminal and issuing the following command: **theharvester**

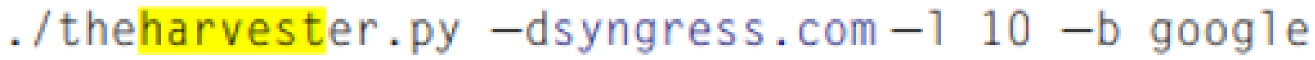
You could also issue the full path to run the program: **/usr/bin/theharvester**
Be sure you are in theHarvester folder and run the following command:



```
./theharvester.py –dsyngress.com –l 10 –b google
```

This command will search for e-mails, subdomains, and hosts that belong to syngress.com. Figure 2.4 shows our results.

Analyzing the command



```
./theharvester.py –dsyngress.com –l 10 –b google
```

Shashi KS

- "./theHarvester.py" is used to invoke the tool.

- A lowercase "-d" is used to specify the **target domain.**

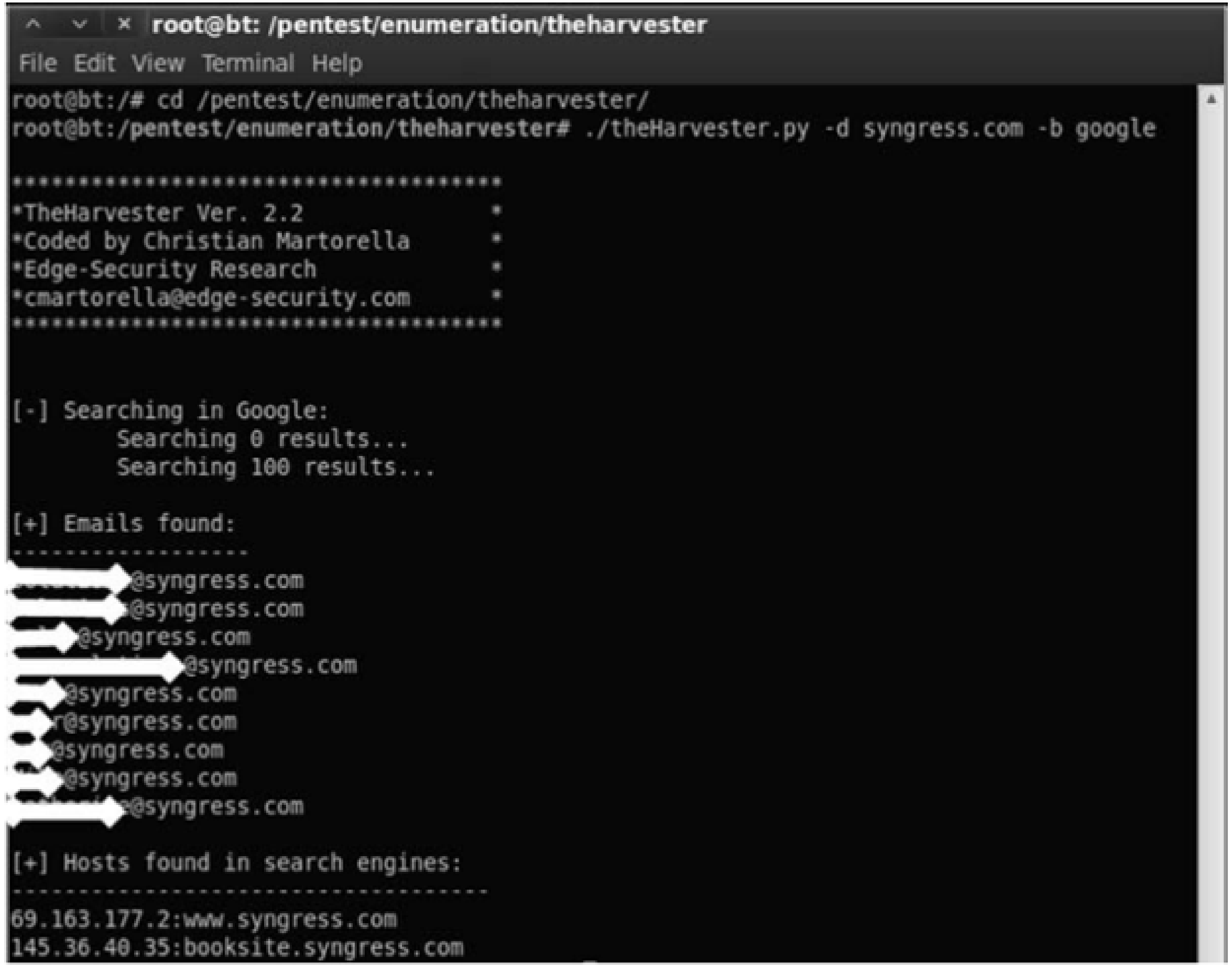
- A lowercase "-l" (that is an L not an 1) is used to **limit the number of results** returned to us.
- In this case, the tool was instructed to return only 10 results.

- The **"-b" is used to specify** what public repository we want to search.

- We can choose from a wide variety including **Google, Bing, PGP, LinkedIn,etc.**
- For this example, we chose to search using Google.

- If you are not sure which data source to use for your search, you can also use the **-b all** switch to simultaneously search all the repositories that the Harvester can use.

Discussing the results of Harvestor tool



root@bt: /pentest/enumeration/theharvester
File Edit View Terminal Help

```
root@bt:/# cd /pentest/enumeration/theharvester/
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d syngress.com -b google

*************************************
*TheHarvester Ver. 2.2              *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...

[+] Emails found:
------------------
[redacted]@syngress.com
[redacted]@syngress.com
[redacted]@syngress.com
[redacted]@syngress.com
[redacted]@syngress.com
[redacted]r@syngress.com
[redacted]@syngress.com
[redacted]@syngress.com
[redacted]e@syngress.com

[+] Hosts found in search engines:
------------------------------------
69.163.177.2:www.syngress.com
145.36.40.35:booksite.syngress.com
```

FIGURE 2.4
Output of the Harvester.

Shashi KS

The Harvester was effective in locating several e-mail addresses that could be of value to us.

The e-mail addresses in the screenshot have been obfuscated.

The Harvester was also successful in finding **two subdomains.**

Both **"booksite.syngress.com" and "www.syngress.com" need to be fully recon'd.**

We simply add these new domains to our target list and begin the reconnaissance process again.

WHOIS

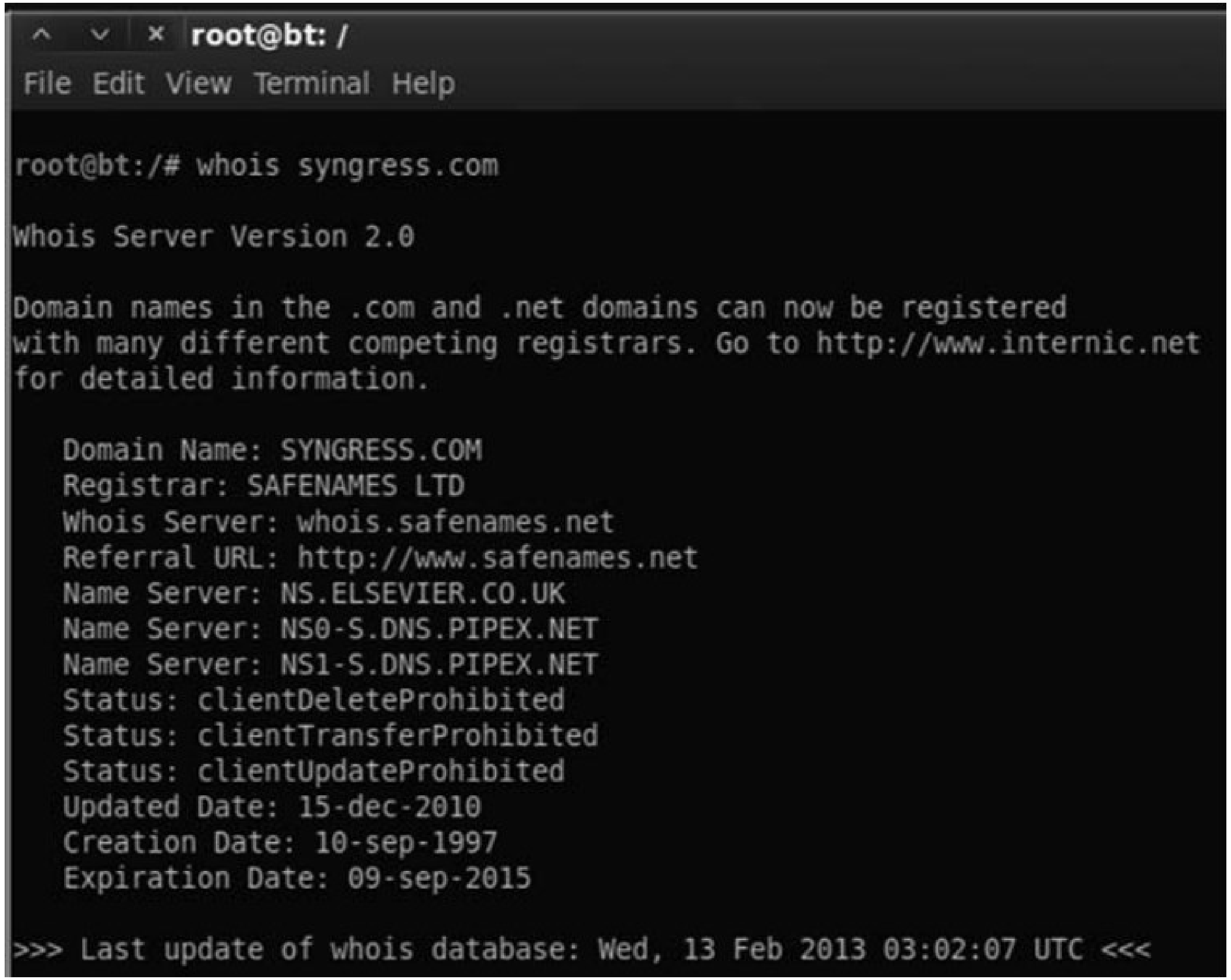
Shashi KS

- A very simple but effective means for collecting additional information about our target is Whois.

- The Whois service allows us to access specific information about our target including the **IP addresses or host names of the** company’s Domain Name Systems (DNS) servers and **contact information which usually contains an address and a phone number.**

Whois is built into the **Linux OS**. The simplest way to use this service is to open a terminal and enter the following command:

```
whois  target_domain
```



```
root@bt:/# whois syngress.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SYNGRESS.COM
   Registrar: SAFENAMES LTD
   Whois Server: whois.safenames.net
   Referral URL: http://www.safenames.net
   Name Server: NS.ELSEVIER.CO.UK
   Name Server: NS0-S.DNS.PIPEX.NET
   Name Server: NS1-S.DNS.PIPEX.NET
   Status: clientDeleteProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 15-dec-2010
   Creation Date: 10-sep-1997
   Expiration Date: 09-sep-2015

>>> Last update of whois database: Wed, 13 Feb 2013 03:02:07 UTC <<<
```

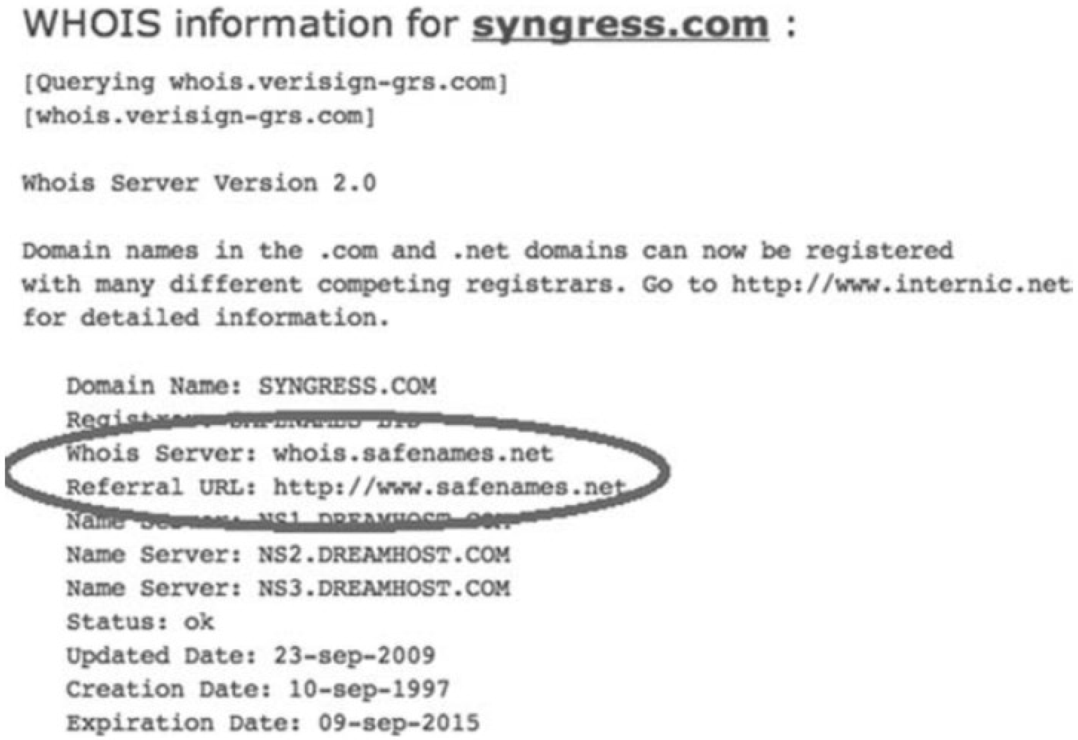
FIGURE 2.5
Partial output from a Whois query.

Shashi KS

whois server

Sometimes, the output will not provide many details. We can often access these **additional details by querying the specific whois server** listed in the output of our original search.

Figure 2.7 shows an example of this.



WHOIS information for syngress.com :

```
[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SYNGRESS.COM
   Registrar: SAFENAMES LTD
   Whois Server: whois.safenames.net
   Referral URL: http://www.safenames.net
   Name Server: NS1.DREAMHOST.COM
   Name Server: NS2.DREAMHOST.COM
   Name Server: NS3.DREAMHOST.COM
   Status: ok
   Updated Date: 23-sep-2009
   Creation Date: 10-sep-1997
   Expiration Date: 09-sep-2015
```

FIGURE 2.7
Whois output showing where to go for additional details.

When available, we can conduct a further Whois search by following the link provided in the “Referral URL:” field.

We may have to search the web page for a link to their Whois service.

By using **Safename’s Whois service, we can extract a significantly larger amount of information**

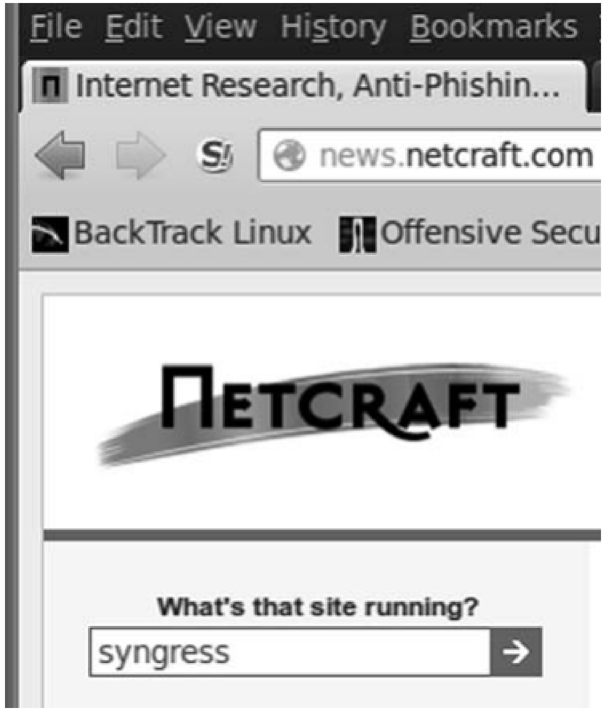
NETCRAFT

Shashi KS

Another great source of information is Netcraft.

Their site can be visited at http:// **news.netcraft.com.**

Start by searching for your target in the "What's that site Running?" textbox as shown in Figure


File Edit View History Bookmarks
Internet Research, Anti-Phishin...
news.netcraft.com
BackTrack Linux
Offensive Secu
NETCRAFT
What's that site running?
syngress

NETCRAFT search option

- Netcraft will return **any websites it is aware of that contain your search words.**

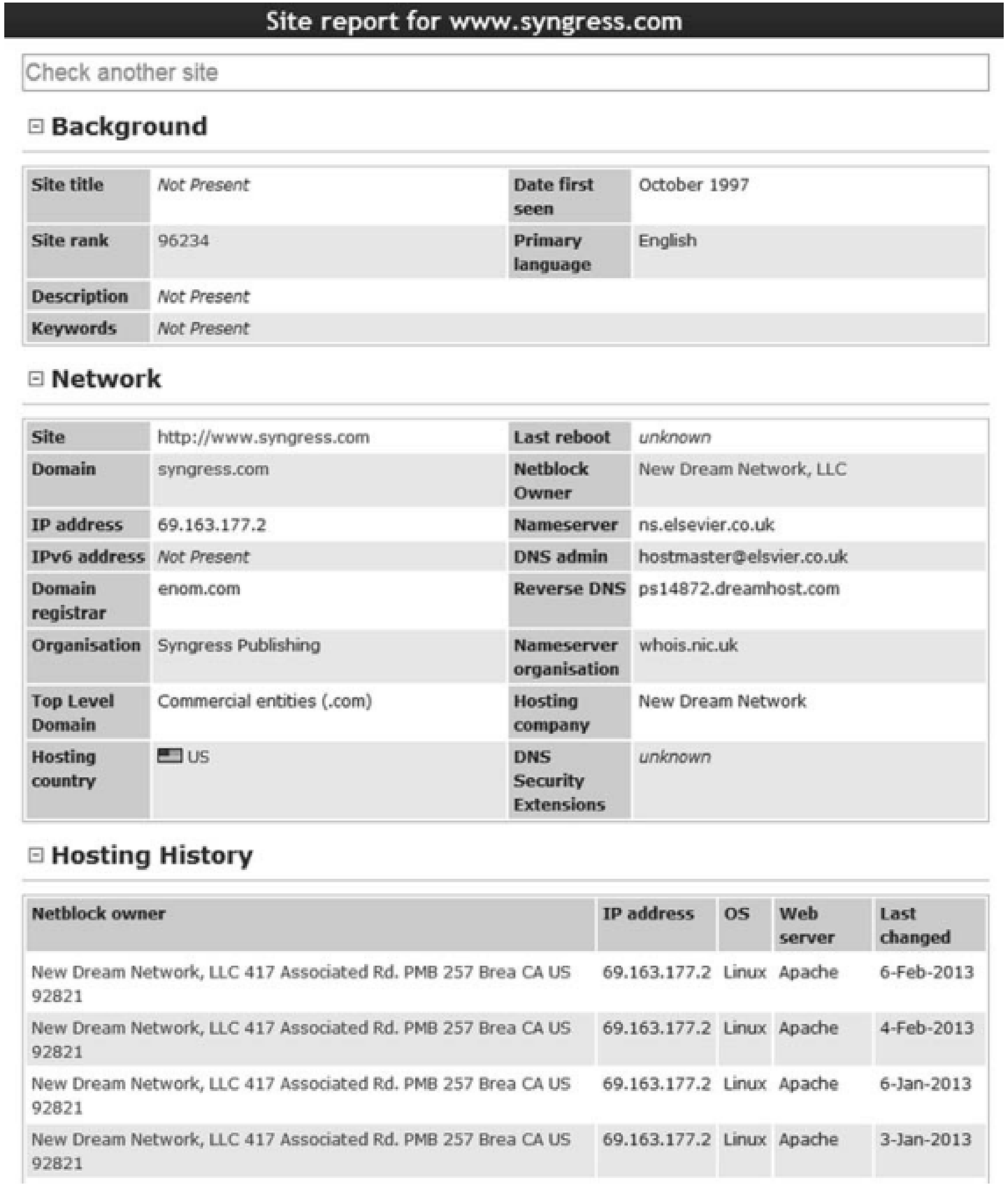
- In our example, we are presented with three sites: **syngress.com, www.syngress.com, and booksite.syngress.com.** If any of these sites have escaped our previous searches, it is important to add them to our potential target list. The returned results page will allow us to click on a “Site Report”.

- Viewing the site report should provide us with some valuable information

- The site report provides us with some great information about our target including the **IP address and OS of the web server as well as the DNS server**. Once again all this information should be cataloged and recorded.

Shashi KS

SITE REPORT



Site report for www.syngress.com

Check another site

⊟ Background

Site title	*Not Present*	**Date first seen**	October 1997
Site rank	96234	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

⊟ Network

Site	http://www.syngress.com	**Last reboot**	*unknown*
Domain	syngress.com	**Netblock Owner**	New Dream Network, LLC
IP address	69.163.177.2	**Nameserver**	ns.elsevier.co.uk
IPv6 address	*Not Present*	**DNS admin**	hostmaster@elsvier.co.uk
Domain registrar	enom.com	**Reverse DNS**	ps14872.dreamhost.com
Organisation	Syngress Publishing	**Nameserver organisation**	whois.nic.uk
Top Level Domain	Commercial entities (.com)	**Hosting company**	New Dream Network
Hosting country	US	**DNS Security Extensions**	*unknown*

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last changed
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	6-Feb-2013
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	4-Feb-2013
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	6-Jan-2013
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	3-Jan-2013

HOST

- Sometimes, reconnaissance efforts will result in host names rather than IP addresses. When this occurs, we can use the “**host” tool to perform a translation of host names to IP addresses .**

- The host tool is **built into most Linux systems** including Kali.

  We can access it by opening a terminal and typing:

```
host target_hostname
```

HOST TOOL EXAMPLE

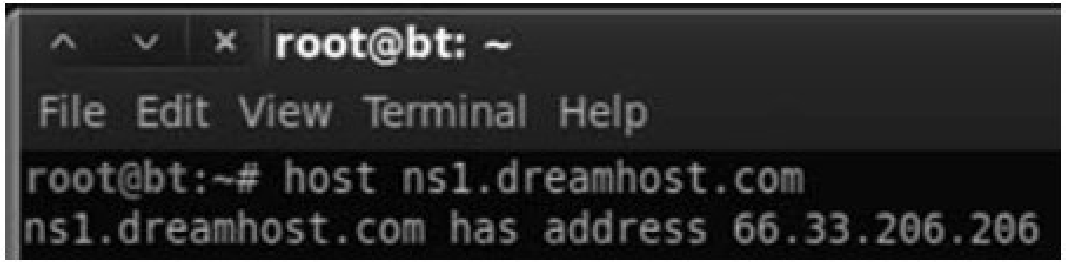
Shashi KS

Suppose in our previous searches, we uncovered a DNS server with the host name **“ns1.dreamhost.com”.**

To translate this into an IP address, we would enter the following command in a terminal:

host ns1.dreamhost.com

Figure 2.10 shows the result of this tool.



```
root@bt:~# host ns1.dreamhost.com
ns1.dreamhost.com has address 66.33.206.206
```

FIGURE 2.10
Host command output.

Host command to translate IP addresses into host names.

Shashi KS

- The host command can also be used in reverse. It can be used to **translate IP addresses into host names.**

- To perform this task, **simply enter host IP_address**. Using the “-a” switch will provide you with **verbose output and possibly reveal additional information about your target.**

- Reviewing the “host” documentation and help files can be done by issuing the “**man host” command** in a terminal window. This help file will allow you to become familiar with the various options that can be used to provide additional functionality to the “host” tool.

EXTRACTING INFORMATION FROM DNS

Shashi KS

DNS servers are an excellent target for hackers and penetration testers. They usually contain information that is considered highly valuable to attackers.

DNS is a core component of both our **local networks and the Internet**. Among other things, DNS is responsible for the process of **translating domain names to IP addresses.**

As humans, it is much easier for us to remember “google.com” rather than http://74.125.95.105.

However, machines prefer the reverse. DNS serves as the middle man to perform this translation process

Remember one of the key elements of information gathering is to collect IP addresses that belong to the target. In terms of reconnaissance, **gaining full access to a company’s DNS server is like finding a blueprint to the organization. The blueprint contains a full listing of internal IP addresses and host names that belong to our target.**

ZONE TRANSFER

Suppose we have a list of DNS IP addresses that belong to or (serve our target) we can begin the process of interrogating DNS to extract information

Shashi KS

- One of our first tasks when interacting with a target DNS is to attempt **a zone transfer.**
- DNS servers contain a series of records that match up the IP address and host name for all the devices that the servers are aware of.
- Many **networks deploy multiple DNS servers** for the sake of redundancy or load balancing. As a result, DNS servers need a way to share information. This “sharing” process occurs through the use of a **zone transfer.**
- During a zone transfer, also commonly referred to as **AXFR**, one DNS server will send all the host-to-IP mappings it contains to another DNS server.
- This process allows multiple DNS servers to stay in sync.
- Even if we are unsuccessful in performing a zone transfer, we should still spend time investigating any DNS servers that fall within our authorized scope.

Tools that can be used to interact with DNS

Shashi KS

Tools to examine DNS are:

- **nslookup**
- **dig**
- **Fierce**

NSLOOKUP

- nslookup is a tool **that can be used to query DNS servers and potentially obtain records about the various hosts of which it is aware.**
- nslookup is built into many versions of **Linux** including Kali and is even available for **Windows**.

USING NSLOOKUP

Shashi KS

- ✓ nslookup is a tool that can be run in **interactive mode**. This simply means we will first invoke the program and then feed it the particular switches we need to make it function properly.

- ✓ We begin using nslookup by opening a terminal and entering: **nslookup**

- ✓ By issuing the “nslookup” command, we start the nslookup tool from the OS.

- ✓ After typing “nslookup” and hitting enter, **your usual “#” prompt will be replaced with a “>” prompt.**
- ✓ At this point, you can enter the additional information required for nslookup to function.

Feeding commands to nslookup

Shashi KS

- We begin feeding commands to nslookup by entering the “server” keyword and an IP address of the DNS server you want to query.

Example:

server 8.8.8.8

- nslookup will simply accept the command and present you with another “>” prompt. Next, we specify the type of record we are looking for.

- During the reconnaissance process, there are many types of DNS record types that you maybe interested in.

- If you are looking for general information, you should set the type to any by using the keyword “any”:

set type = any

COMBINING HOST AND NSLOOKUP

If you are looking for specific information from the DNS server such as the **IP address of the mail server that handles e-mail for the target organization, you would use the**

set type =mx.

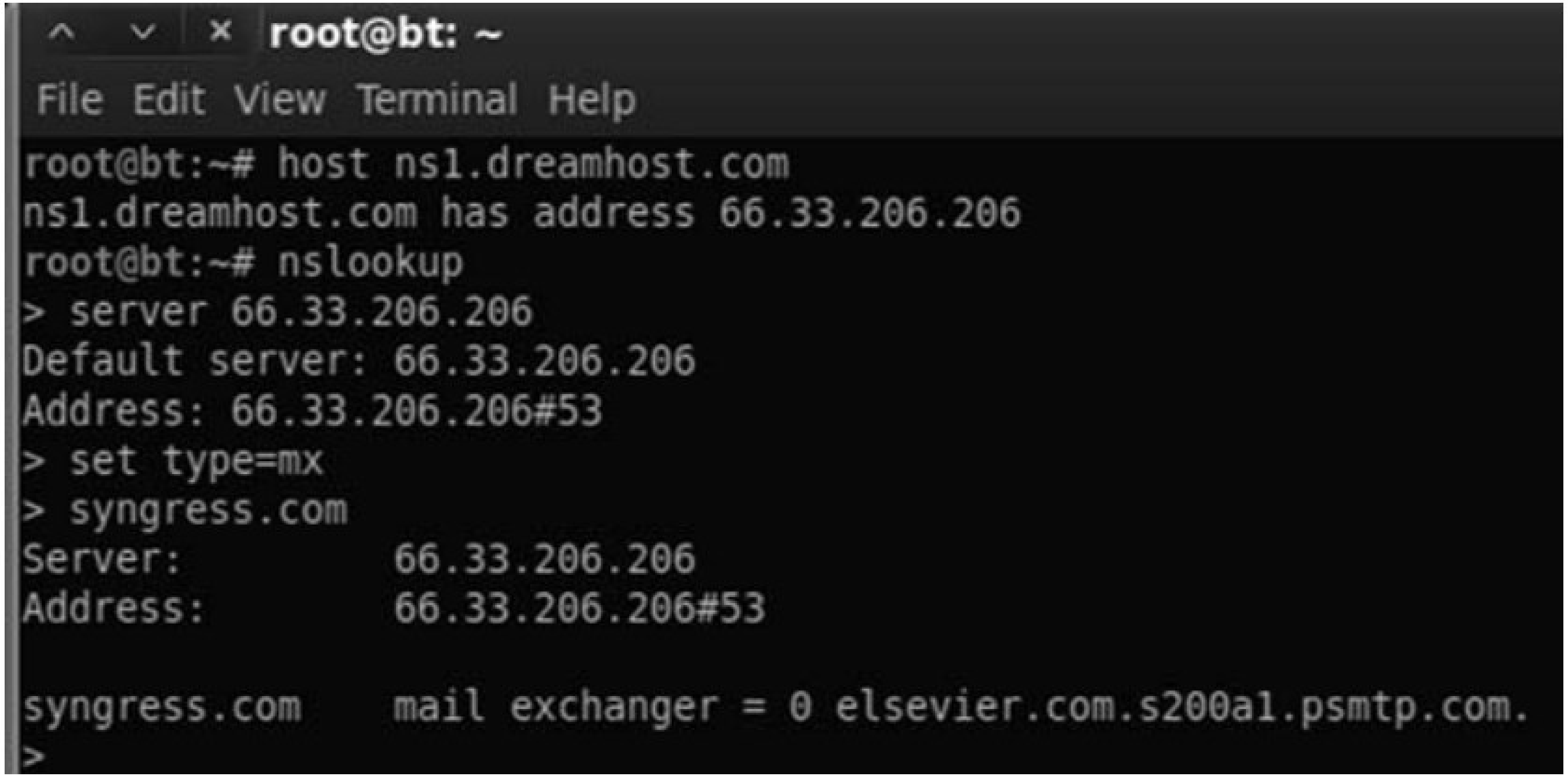
Example:

Suppose you wanted to know what mail server is used to handle the e-mail for Syngress.

We can use **the host tool** to quickly determine what IP address is associated with **ns1.dreamhost.com**.

With this information in hand, we can use **nslookup to query DNS and find mail server for Syngress.**

Figure 2.11 shows an example of this process; **the name of the e-mail server has been highlighted (in the bottom right of the screenshot) and now needs to be added to our potential target list.**



```
root@bt:~# host ns1.dreamhost.com
ns1.dreamhost.com has address 66.33.206.206
root@bt:~# nslookup
> server 66.33.206.206
Default server: 66.33.206.206
Address: 66.33.206.206#53
> set type=mx
> syngress.com
Server:         66.33.206.206
Address:        66.33.206.206#53

syngress.com    mail exchanger = 0 elsevier.com.s200a1.psmtp.com.
>
```

FIGURE 2.11
Combining host and nslookup to determine the address of our target's e-mail server (MX record).

DIG

Shashi KS

- ❑ Another great tool for extracting information from DNS is “dig”.

- ❑ To work with dig, we simply open a terminal and enter the following command:

```
dig @target_ip
```

- ❑ The “target_ip” will be replaced with the actual IP address of your target.

- ❑ Among other things, **dig makes it very simple to attempt a zone transfer. Recall that a zone transfer is used to pull multiple records from a DNS server.**

- ❑ In some cases, a zone transfer can result in the target DNS server sending all the records it contains. **This is especially valuable if your target does not distinguish between internal and external IPs when conducting a zone transfer.**
- ❑ We can attempt a zone transfer with dig by using the **“-t AXFR” switch.**

DIG - EXAMPLE

Shashi KS

If we wanted to attempt a zone transfer against a fictitious DNS server with an IP address of 192.168.1.23 and a domain name of “example.com”, we would issue the following command in a terminal window:

```
dig @192.168.1.23example.com -t   AXFR
```

If zone transfers are allowed and **not restricted,** you will be presented with a listing of host and IP addresses from the target DNS server that relate to your target domain.

FIERCE: WHAT TO DO WHEN ZONE TRANSFERS FAIL

Shashi KS

In Kali, you can find **Fierce in the /usr/bin/ directory**.

Once again, you can simply open a terminal and issue the "fierce" command (along with the required switches) or you can move into the /usr/bin/ directory.

To run Fierce from the /usr/bin directory, you will need to open a terminal and issuing the following command:

```
cd  /usr/bin/fierce
```

Running fierce tool

Shashi KS

- ❑ Inside the Fierce directory, you can run the tool by executing the **fierce.pl script** and utilizing the -dns switch followed by your target domain.

```
./fierce.pl  -dns trustedsec.com
```

- ❑ The "./" in front of the tool name is required and **tells Linux to execute the file in the local directory**.

- ❑ The script will begin by attempting to complete a zone transfer from the specified domain.

- ❑ In the event the process fails, **Fierce will attempt to brute-force host names by sending a series of queries to the target DNS server.** This can be an extremely effective method for uncovering additional targets.

- ❑ The general idea is that if Dave owns "trustedsec.com" (which he does, please do not scan or interrogate), he may also own **support.trustedsec.com, citrix.trustedsec.com, print.trustedsec.com, or many others.**

EXTRACTING INFORMATION FROM E-MAIL SERVERS

Shashi KS

- E-mail servers can provide a wealth of information for hackers and penetration testers. In many ways, e-mail is like a revolving door to your target's organization.

- Assuming your target is hosting their own e-mail server, this is often a great place to attack. It is important to remember, "You can't block what you must let in."

- In other words, **for e-mail to function properly, external traffic must pass through your border devices like routers and firewalls, to an internal machine, typically somewhere inside your protected networks**

We can often gather significant pieces of information by interacting directly with the e-mail sever.

One of the first things to do when attempting to recon an e-mail server is to send an e-mail to the organization with an **empty .bat file or a nonmalicious .exe file like calc.exe.**

In this case, the goal is to **send a message to the target e-mail server inside the organization in the hope of having the e-mail server inspect, and then reject the message.**

Extracting information about the target e-mail server

- Once the rejected message is returned back to us, we can attempt to extract information about the target e-mail server.

- In many cases, the body of the message will include a precanned write-up explaining that the server does not accept e-mails with potentially dangerous extensions. This message often indicates the specific vendor and version of antivirus that was used to scan the e-mail.

- Having a return message from a target e-mail server also allows us to inspect the headers of the e-mail.

- Inspecting the Internet headers will often allow us to extract some basic information about the e-mail server, including IP addresses and the specific software versions or brand of e-mail server running.

- Knowing the IP address and software versions can be incredibly useful when we move into the exploitation phase (Step 3).

SOCIAL ENGINEERING

Shashi KS

Social engineering is one of the most simple and effective means for gathering information about a target.

Social engineering is the process of exploiting the “human” weakness that is inherent in every organization. When utilizing social engineering, the attacker’s goal is to get an employee to divulge some information that should be kept confidential.

EXAMPLE

Let us assume you are conducting a penetration test on an organization. During your early reconnaissance, you discover an e-mail address for one of the company’s sales people.

You understand that sales people are highly likely to return product inquiry e-mails. As a result, you sent an e-mail from an anonymous address feigning interest in a particular product.

In reality, you did not care about the product. The real purpose of sending the e-mail is to get a reply from the sales person so you can review the e-mail headers contained in the response. This process will allow you to gather additional information about the company’s internal e-mail servers.

Suppose our salesman’s name is Ben Owned.
(we found this information during our reconnaissance of the company website and in the signature of his e-mail response).

Let us assume that in this example, when you sent the employee the product inquiry e-mail, you received an automatic reply with the notification that Ben Owned was “currently out of the office travelling overseas” and “would be gone for two weeks with only limited e-mail access.

A classic example of social engineering would be to impersonate Ben Owned and call the target company’s tech support number asking for help resetting your password because you are overseas and cannot access your web mail. If you are lucky, the tech support people will believe your story and reset the password.

Assuming they use the same password, you now have access to Ben Owned’s e-mail and other network resources like VPN for remote access, or FTP for uploading sales figures and customer orders.

If you are conducting social engineering over the phone, it can be extremely helpful to have detailed and well-written notes in case you are asked about some obscure detail.

Another example of social engineering is to leave USB thumb drives or compact discs (CDs) at the target organization. The thumb drives should be distributed to several locations in or near the organization.

In this example though, the thumb drive or CD is preloaded with a self-executing backdoor program that automatically launches when the drive is inserted into the computer.

The backdoor is capable of bypassing the company firewall and will dial home to the attacker’s computer, leaving the target exposed and giving the attacker a clear channel into the organization.

SCANNING

Shashi KS

One of the final steps in reconnaissance was to create a list of IP addresses that both belonged to the target and that we were authorized to attack. This list is the key to transitioning from step 1(Reconnaissance) to step 2(scanning).

In step 1 (Reconnaissance), we mapped our gathered information to attackable IP addresses. In step 2(scanning), we will map IP addresses to open ports and services.

Each service, connection, or route to another network provides a potential foothold for an attacker. Scanning is the **process of identifying live systems and the services that exist on those systems.**

Scanning methodology can be broken down into into four distinct phases:

Shashi KS

1. Determining if a system is alive with ping packets.

This is the process of determining whether a target system is turned on and capable of communicating or interacting with our machine. This step is the least reliable and we should always continue with steps 2-4 regardless of the outcome of this test

A **ping** is a special type of network packet called an **Internet Control Message Protocol (ICMP) packet.**

Pings work by sending a particular type of network traffic, called an ICMP echo request packet, to a specific interface on a computer or network device.

If the device (and the attached network card) that received the ping packet is turned on and not restricted from responding, the receiving machine will respond back to the originating machine with an **echo reply packet**.

Pings tell us if a host is alive and accepting traffic, total time it took for the packet to travel to the target and return.

Pings also report traffic loss that can be used to gauge the reliability of a network connection.
To run ping from your Linux machine, open a terminal and issue the command:

```
ping target_ip
```

Replace the “target_ip” portion of the command with the actual IP address or hostname of the machine you are trying to ping.

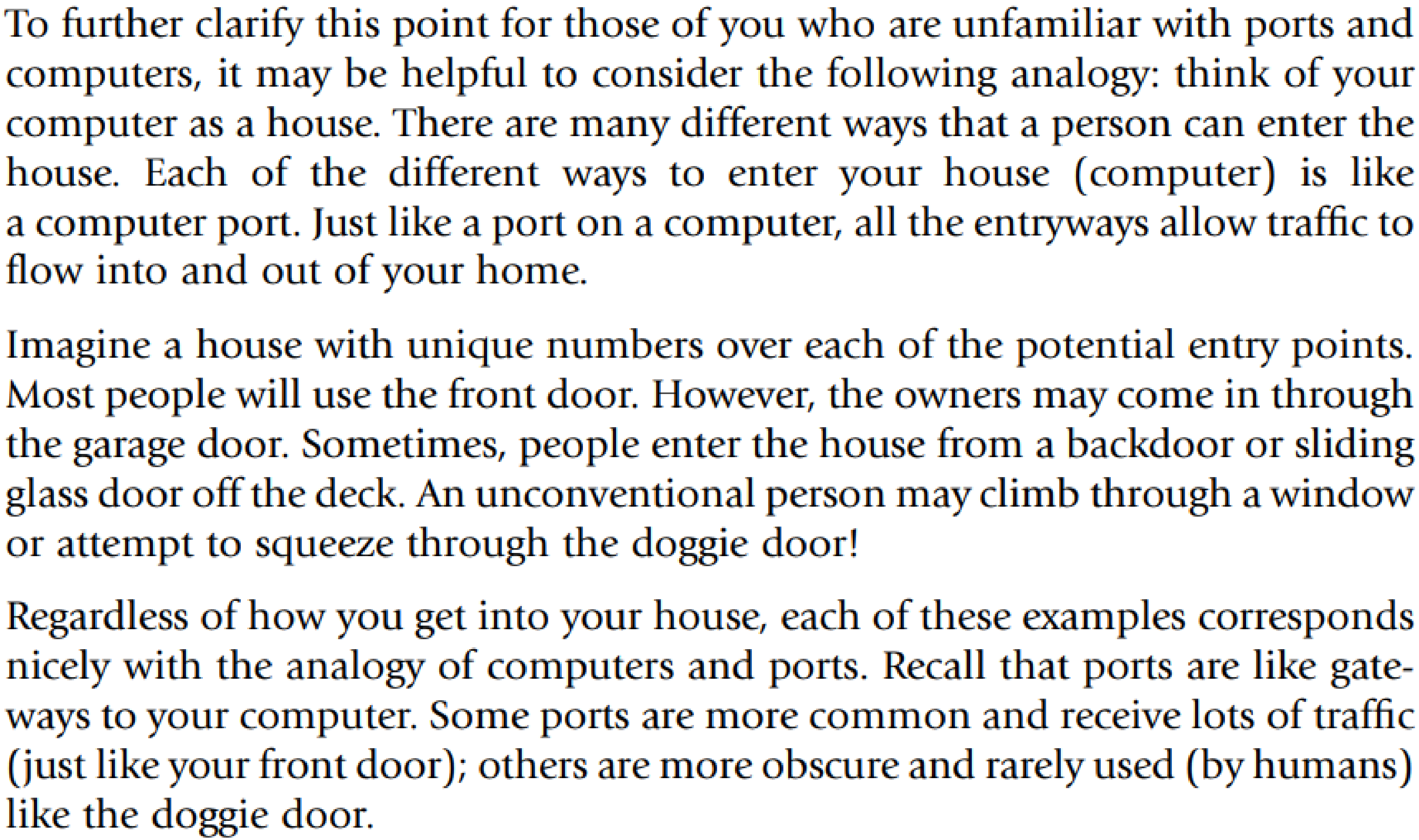
Shashi KS

2. **Port scanning the system with Nmap**.

This is the process of identifying the specific ports and services running a particular host. Ports provide a way or location for software, services, and networks to communicate with hardware like a computer. A port is a data connection that allows a computer to exchange information with other computers, software, or devices. Once computers were connected to a network, ports provide an efficient means for computers to communicate with each other. The use of multiple ports allows for simultaneous communication without the need to wait.

ANALOGY EXAMPLE FOR THE CONCEPT OF PORTS

Shashi KS



To further clarify this point for those of you who are unfamiliar with ports and computers, it may be helpful to consider the following analogy: think of your computer as a house. There are many different ways that a person can enter the house. Each of the different ways to enter your house (computer) is like a computer port. Just like a port on a computer, all the entryways allow traffic to flow into and out of your home.

Imagine a house with unique numbers over each of the potential entry points. Most people will use the front door. However, the owners may come in through the garage door. Sometimes, people enter the house from a backdoor or sliding glass door off the deck. An unconventional person may climb through a window or attempt to squeeze through the doggie door!

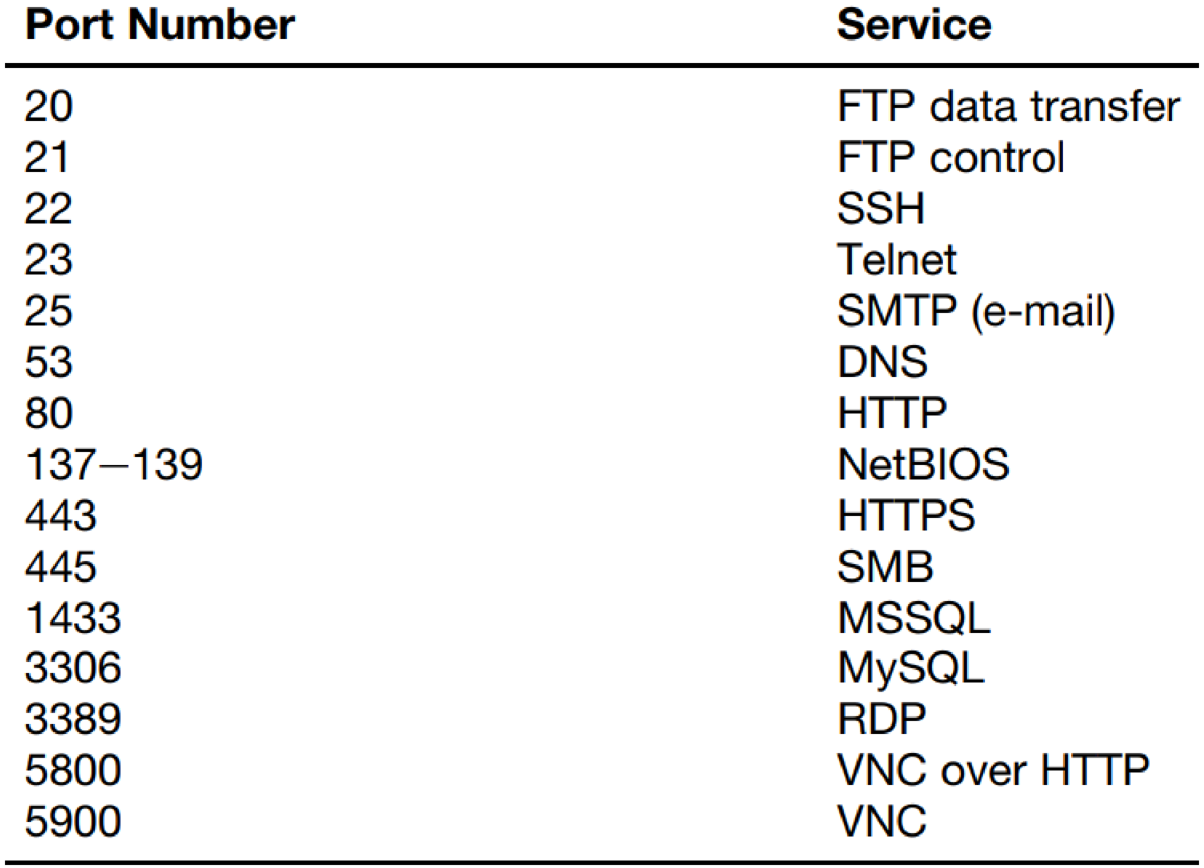
Regardless of how you get into your house, each of these examples corresponds nicely with the analogy of computers and ports. Recall that ports are like gateways to your computer. Some ports are more common and receive lots of traffic (just like your front door); others are more obscure and rarely used (by humans) like the doggie door.

Shashi KS

Common Port Numbers and Their Corresponding Service

Many common network services run on standard port numbers and can give attackers an indication as to the function of the target system.

Table 3.1 provides a list of common ports and their corresponding services.



Port Number	Service
20	FTP data transfer
21	FTP control
22	SSH
23	Telnet
25	SMTP (e-mail)
53	DNS
80	HTTP
137–139	NetBIOS
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
3389	RDP
5800	VNC over HTTP
5900	VNC

Port scanning

Shashi KS

The goal of port scanning is to identify which ports are open and determine what services are available on our target system.
A service is a specific job or task that the computer performs like e-mail, file transfer protocol (FTP), printing, or providing web pages.

For example if we find that port 80 is open, we can attempt a connection to the port and get specific information about the web server that is listening on that port.

There are a total of 65,536 (0-65,535) ports on every computer.

Ports can be **either transmission control protocol (TCP) or user datagram protocol (UDP**) depending on the service utilizing the port or nature of the communication occurring on the port. We scan computers to see what ports are in use or open. This gives us a better picture of the purpose of the machine, which, in turn, gives us a better idea about how to attack the box

Nmap

Shashi KS

Nmap is one tool used to conduct port scanning.

Nmap was written by Gordon “Fyodor” Lyon and is available for free from www.insecure.org.

It is built into many of today’s Linux distributions including Kali.

Although it is possible to run Nmap from a graphical user interface (GUI), we are going to focus on using the terminal to run our port scans

When we conduct a port scan, our tool will literally create a packet and send it to each designated port on the machine. The goal is to determine what kind of a response we get from the target port. Different types of port scans can produce different results. It is important to understand the type of scan you are running as well as the expected output of that scan.

USING NMAP TO PERFORM A TCP CONNECT SCAN

Shashi KS

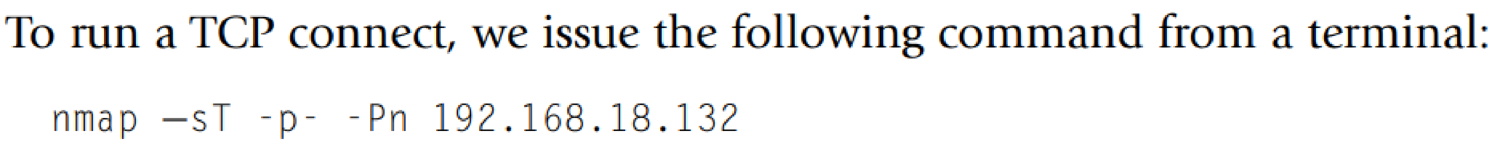
TCP Connect scan is often considered the most basic and stable of all the port scans because Nmap attempts to complete the three-way handshake on each port specified in the Nmap command

If you do not specify a specific port range, Nmap will scan the 1000 most common ports. Unless you are in a great hurry, it is always recommended to scan all ports, not just the 1000 most common. The reason is that oftentimes crafty administrators will attempt to obscure a service by running it on a nonstandard port. You can scan all the ports by specifying “-p-” when running Nmap.

Using the “-Pn” switch with every Nmap scan is also recommended. Utilizing the “-Pn” switch will cause Nmap to disable host discovery and force the tool to scan every system as if it were alive. This is extremely useful for discovering additional systems and ports that otherwise may be missed.

RUNNING A TCP CONNECT SCAN

Shashi KS



To run a TCP connect, we issue the following command from a terminal:

```
nmap –sT -p- -Pn 192.168.18.132
```

The first word “nmap” causes the Nmap port scanner to start.

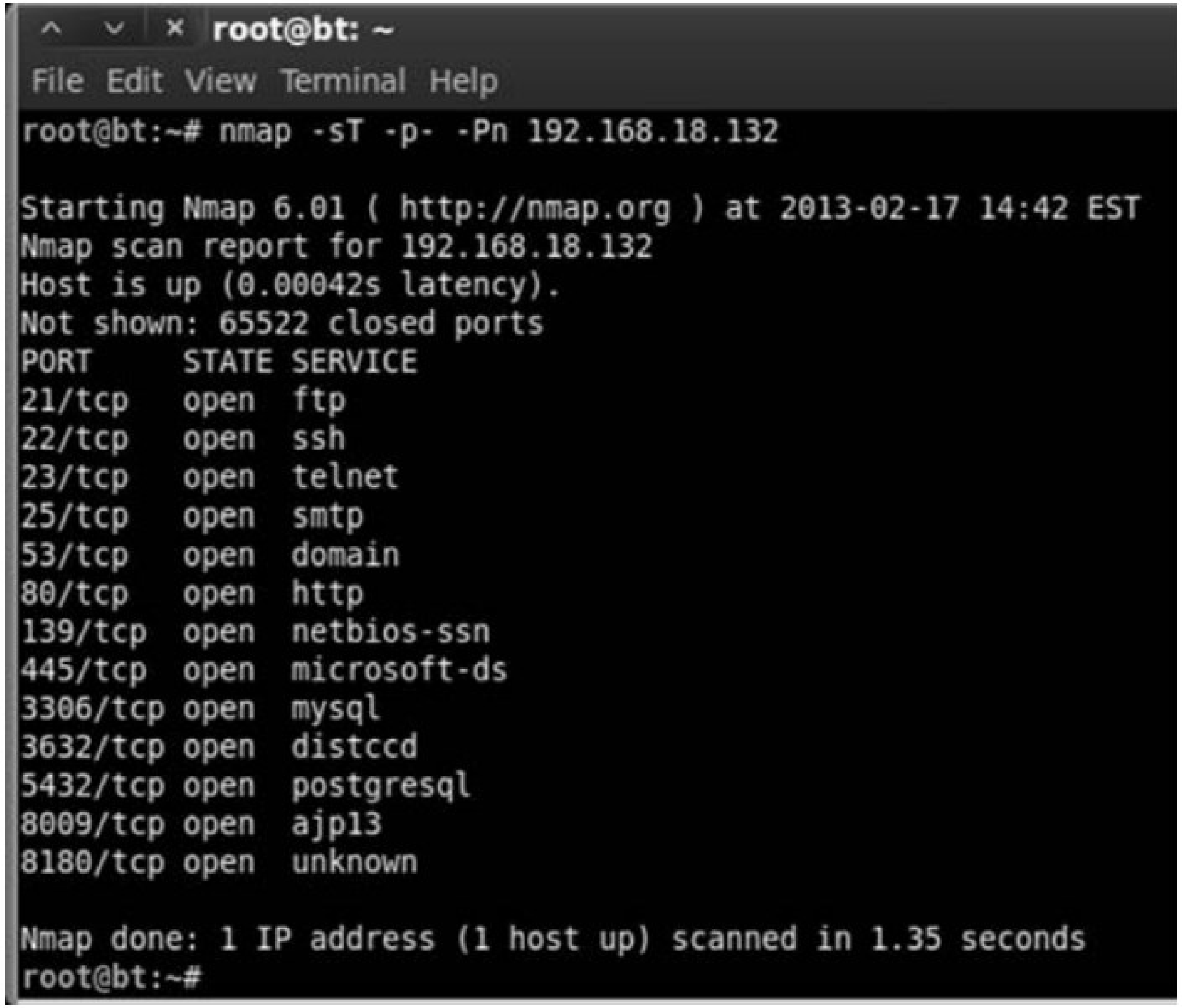
The second command “-sT” tells Nmap to run a TCP Connect scan.

The “-s” is used to tell Nmap what kind of scan we want to run. The “-T” in the “-sT” is used to run a scan type of TCP Connect.

We use the “-p-” to tell Nmap to scan all the ports not just the default 1000.

We use the “-Pn” switch to skip the host discovery phase and scan all the addresses as if the system were alive and responding to ping requests.

Finally, we specify the target IP address; obviously, your target’s IP address will be different from the one shown in the screenshot!
Figure 3.2 shows the TCP Connect Nmap scan and the output that was received when run against the Metasploitable target.



```
root@bt:~# nmap -sT -p- -Pn 192.168.18.132

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-17 14:42 EST
Nmap scan report for 192.168.18.132
Host is up (0.00042s latency).
Not shown: 65522 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
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
root@bt:~#
```

FIGURE 3.2
TCP connect scans and results.

Shashi KS

USING NMAP TO PERFORM AN SYN SCAN

The SYN Scan is arguably the most popular , default Nmap scan.

If you run the Nmap command without specifying a scan type (using the -s switch), Nmap will use the SYN scan by default.

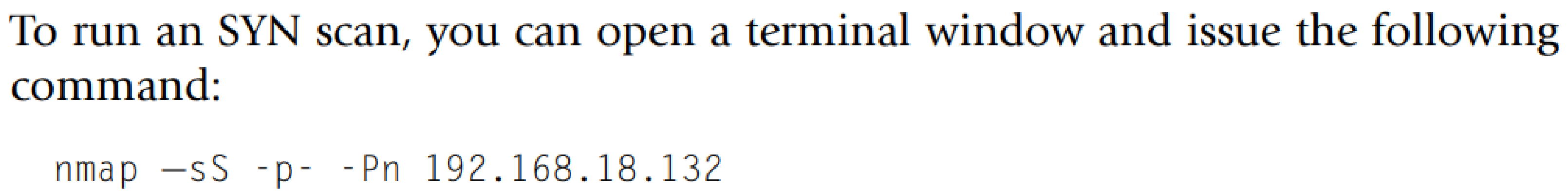
Aside from the fact that the SYN scan is the default choice, it is also popular because it is faster than the TCP connect scan and yet remains quite safe, with little chance of (Denial of Service) or crashing the target system. SYN scans are faster because rather than completing the entire three-way handshake, it only completes the first two steps of the process.

In an SYN scan, the scanning machine sends an SYN packet to the target and the target responds with an SYN/ACK (assuming the port is in use and not filtered) .

However, at this point, rather than sending the traditional ACK packet, the scanning machine sends an RST (reset) packet to the target.

The reset packet tells the target machine to disregard any previous packets and close the connection between the two machines.

The speed advantage of the SYN scan over the TCP Connect scan comes from the fact that there are fewer packets sent between the hosts when using an SYN scan rather than a TCP Connect scan.



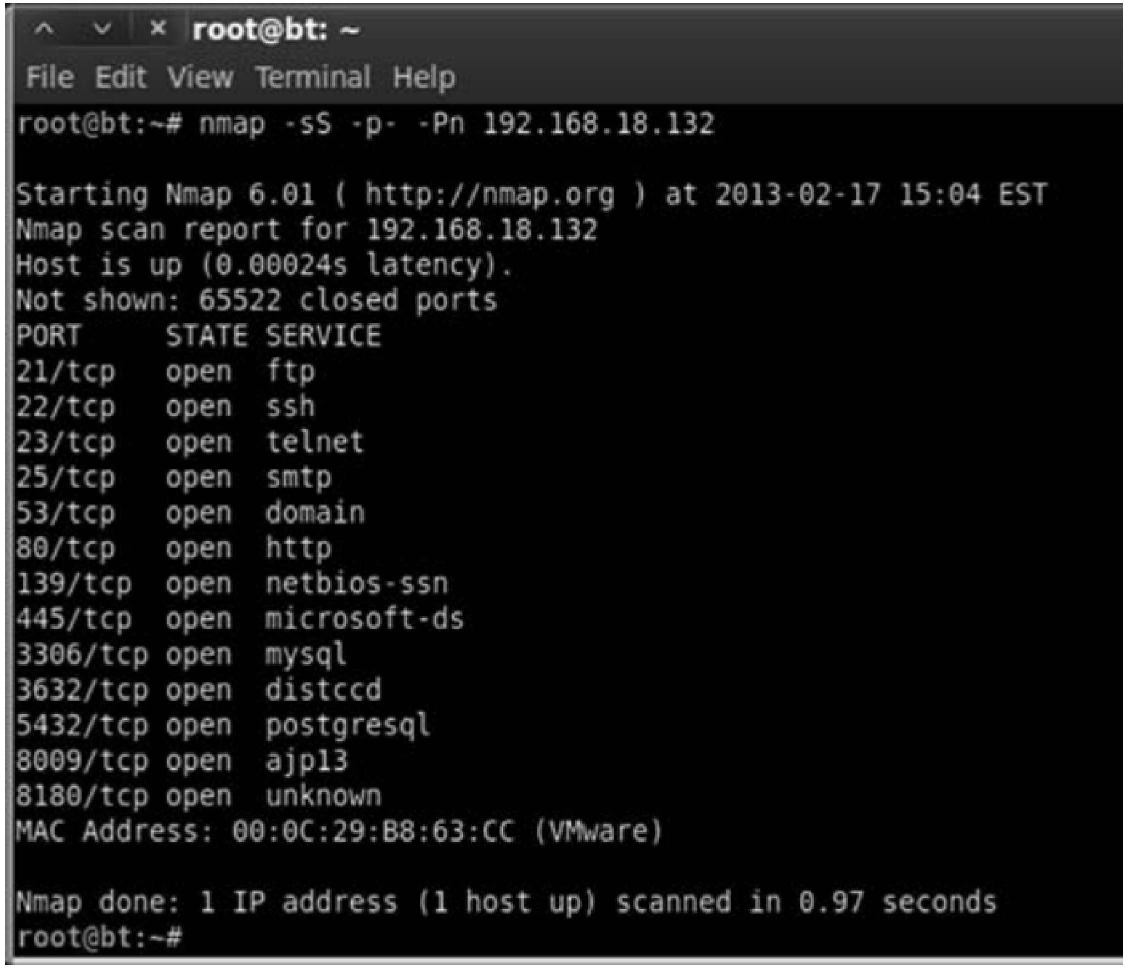
To run an SYN scan, you can open a terminal window and issue the following command:

```
nmap —sS -p- -Pn 192.168.18.132
```

This instructs Nmap to run an SYN scan rather than a TCP Connect scan.

Output of an SYN scan against our target.

Shashi KS



```
root@bt:~# nmap -sS -p- -Pn 192.168.18.132

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-17 15:04 EST
Nmap scan report for 192.168.18.132
Host is up (0.00024s latency).
Not shown: 65522 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
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B8:63:CC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
root@bt:~#
```

SYN SCAN AND OUR RESULTS

3. Leveraging the **Nmap scripting engine (NSE) to further interrogate the target.**

Shashi KS

Step 3 leverages the NSE to further interrogate and verify our earlier findings.

The NSE is a tremendously powerful and simple tool, which extends the power and flexibility of Nmap. It gives hackers and penetration testers the ability to use precanned or custom scripts, which can be used to verify findings, discover new processes and vulnerabilities, and automate many penetration testing techniques.

the NSE provides Nmap with an entirely new skill set and dimension. The NSE is a powerful addition to the classic tool that transforms its functionality and capability well beyond its traditional port scanning duties

NSE allows Nmap to complete a variety of tasks including vulnerability scanning, advanced network discovery, detection of backdoors, and in some cases even perform exploitation! The NSE community is a very active and open group. New scripts and capabilities are being constantly added.

The NSE divides the scripts by category. The current categories include auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln.
Each category can be further broken down into individual scripts that perform a particular function.
A hacker or penetration tester can run a single script or the entire category (which includes multiple scripts).

You can find the most recent and up-to-date NSE information at http://nmap.org/nsedoc/

In order to invoke the NSE, we use "`--script`" argument followed by the category or script name and the target IP address as shown below:

```
nmap --script banner 192.168.18.132
```

The "banner" script is an extension of Nmap that creates a connection to a TCP port and prints any output sent from the target system to the local terminal. This can be extremely helpful in identifying unrecognized services on obscure ports.

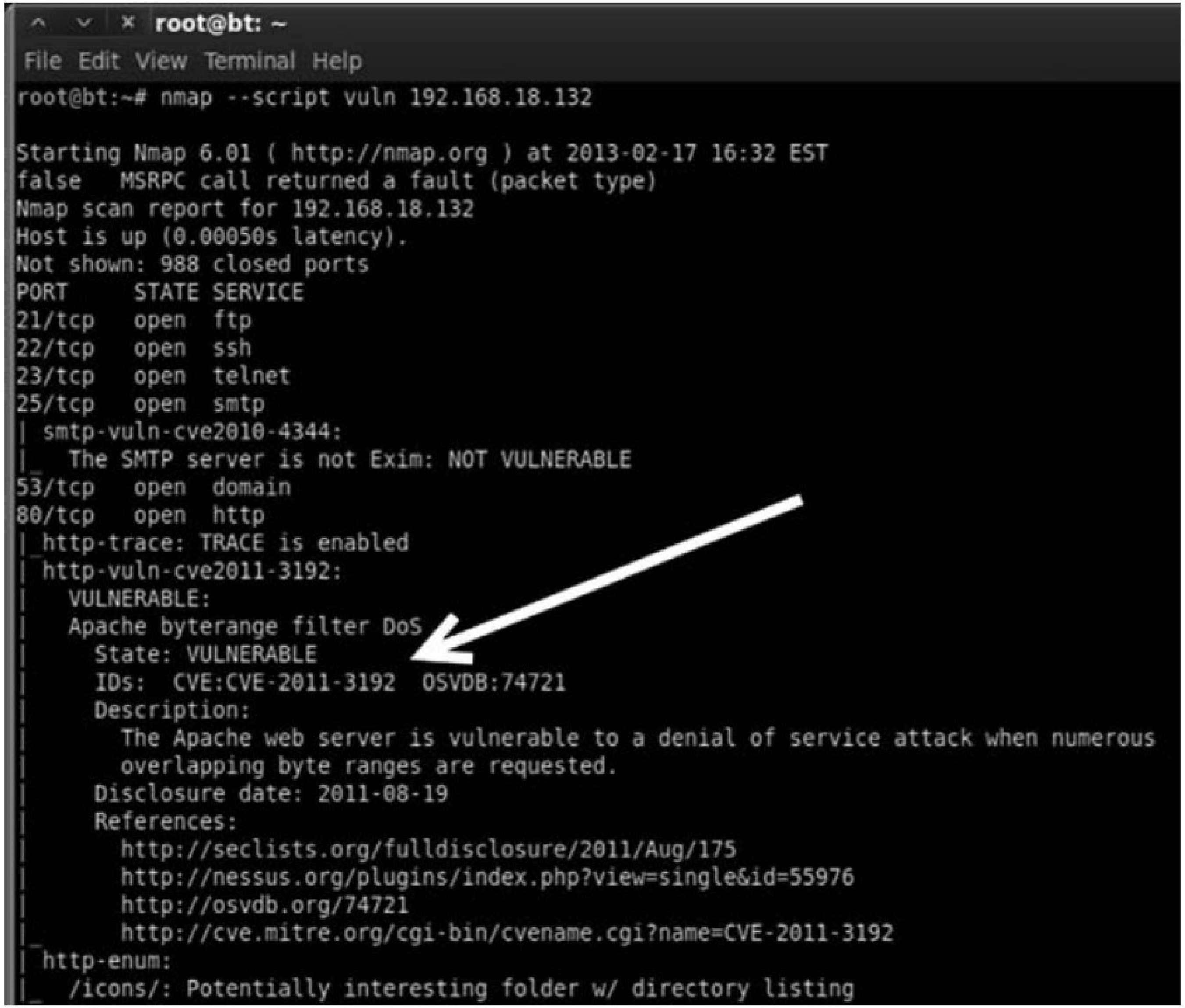
Similarly we could invoke an entire family or category of scripts by using the "--script category_name" format as shown below:

```
nmap --script vuln 192.168.18.132
```

The "vuln" category will run a series of scripts which look for known issues on the target system. This category typically provides output only when a vulnerability is discovered. The "vuln" functionality of the NSE is an excellent precursor to our conversation on vulnerability scanning.

OUTPUT OF RUNNING NSE VULN SCAN

Shashi KS



```
root@bt:~# nmap --script vuln 192.168.18.132

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-17 16:32 EST
false   MSRPC call returned a fault (packet type)
Nmap scan report for 192.168.18.132
Host is up (0.00050s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  OSVDB:74721
|     Description:
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       http://seclists.org/fulldisclosure/2011/Aug/175
|       http://nessus.org/plugins/index.php?view=single&id=55976
|       http://osvdb.org/74721
|_      http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
```

4.Scanning the system for vulnerabilities with Nessus.

Shashi KS

The final step in our scanning method is step 4, vulnerability scanning.
Vulnerability scanning is the process of locating and identifying known weaknesses in the services and software running on a target machine.

The discovery of known vulnerabilities on a target system is definitely a win for the penetration tester. Many systems today can be exploited directly with little or no skill when a machine is discovered to have a known vulnerability

VULNERABILITY SCANNING

Shashi KS

After scanning, We have a list of IPs, open ports, and services on each machine, it is time to scan the targets for vulnerabilities.

Vulnerability is a weakness in the software or system configuration that can often be exploited. Vulnerabilities can come in many forms but most often they are associated with missing patches. Vendors often release patches to fix a known problem or vulnerability.

Unpatched software and systems often lead to quick penetration tests because some vulnerabilities allow remote code execution. Remote code execution is definitely one of the holy grails of hacking.

To scan systems for vulnerabilities, we will use a vulnerability scanner. There are several good scanners available, We will be focusing on Nessus.

NESSUS TOOL FOR VULNERABILITY SCANNING

Shashi KS

Nessus is a great tool and available for free (as long as you are a home user), from their website at http://www.tenable.com/products/nessus.

Tenable, the makers of Nessus, allows you to download a full-fledged version and get a key for free. If you are going to use Nessus in a corporate environment, you will need to sign up for the professional feed rather than the HomeFeed.

Nessus runs on all major operating systems including Linux, Windows, OS X, FreeBSD and more.

Nessus runs using a client/server architecture, which allows you to have multiple clients, connect to the server instance if you want to. Once set up, the server runs quietly in the background, and you interact with the server through a browser. There are many good tutorials on the Internet for installing Nessus on Kali (or any Linux system).

In general, to install Nessus, you need to complete the following steps:

Shashi KS

1. Download the installer from www.nessus.org.

2. Register for a noncommercial HomeFeed key on the Nessus website by submitting your e-mail address. The Nessus crew will e-mail you a unique product key that can be used to register the product. Please be sure to pay special attention to the end-user license agreement that restricts how a HomeFeed can be used.

3. Install the program. 4. Create a Nessus user to access the system.

5. Enter your HomeFeed (or Professional) key.

6. Update the plug-ins.

7. Use a browser to connect to the Nessus server

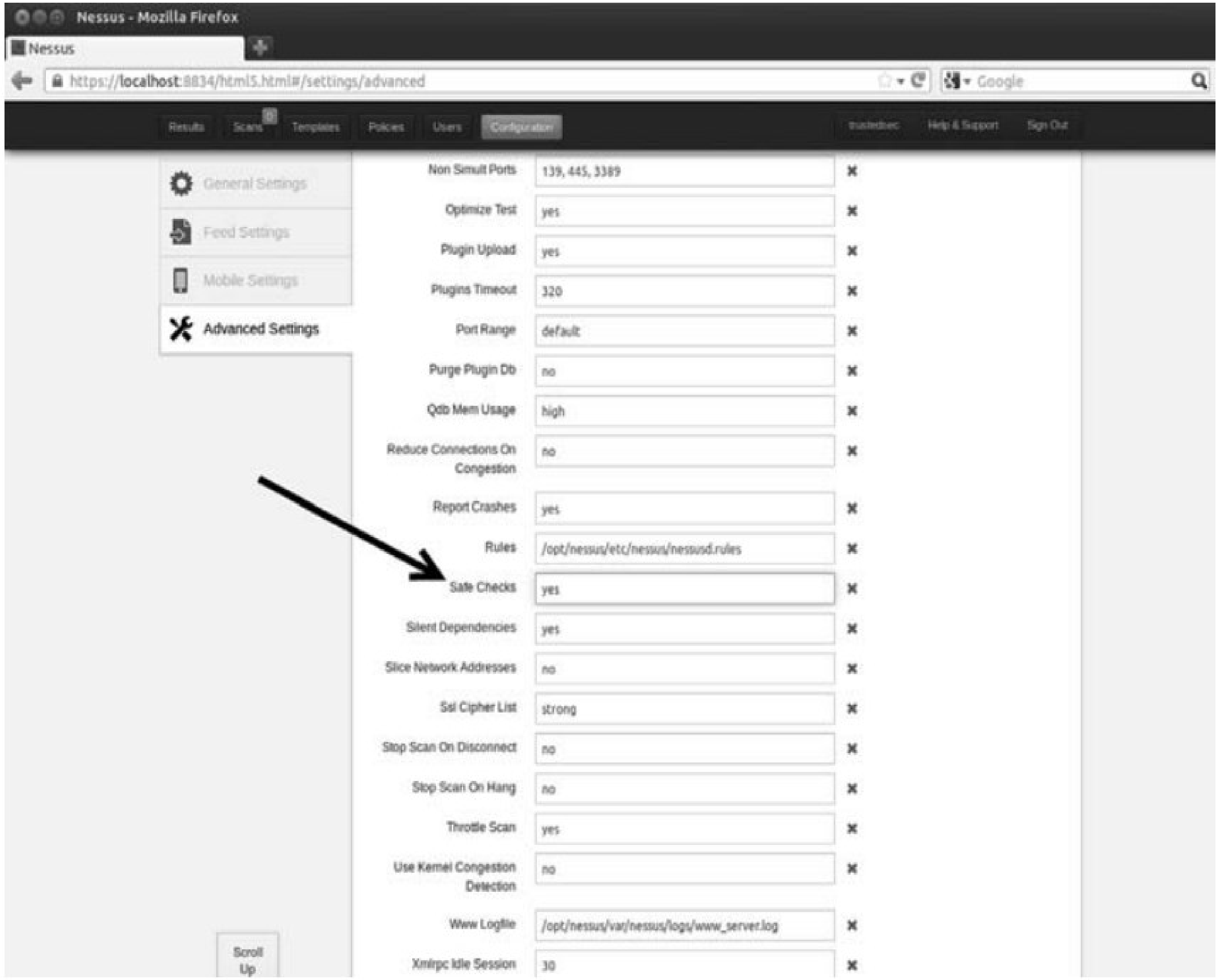
Once you have installed the Nessus server, you can access it by opening a browser and entering https://127.0.0.1:8834 in the uniform resource locator

NAVIGATING NESSUS

You can navigate Nessus by clicking the various headings at the top of the page. Each heading represents a different component of the Nessus tool including: Results, Scans, Templates, Policies, Users, and Configuration. Before we can use Nessus, we need to either create a custom policy or make use of one of the predefined policies that Nessus creates for us.

You can create a custom policy by clicking the “Policies” tab at the top of the web page. To set up a scan policy, you need to provide a name. If you are going to set up multiple policies, you should also enter a description.

Next, we move into the scan policies, which allow you to customize what type of policies you can use within the Nessus interface. There are many options that you can use to customize your scan policy. For the purpose of this book, we will use the defaults.



Non Simult Ports	139, 445, 3389
Optimize Test	yes
Plugin Upload	yes
Plugins Timeout	320
Port Range	default
Purge Plugin Db	no
Qdb Mem Usage	high
Reduce Connections On Congestion	no
Report Crashes	yes
Rules	/opt/nessus/etc/nessus/nessusd.rules
Safe Checks	yes
Silent Dependencies	yes
Slice Network Addresses	no
Ssl Cipher List	strong
Stop Scan On Disconnect	no
Stop Scan On Hang	no
Throttle Scan	yes
Use Kernel Congestion Detection	no
Www Logfile	/opt/nessus/var/nessus/logs/www_server.log
Xmlrpc Idle Session	30

FIGURE 3.7
Setting up a “safe” scan option in configurations.

SETTING UP NESSUS SCAN

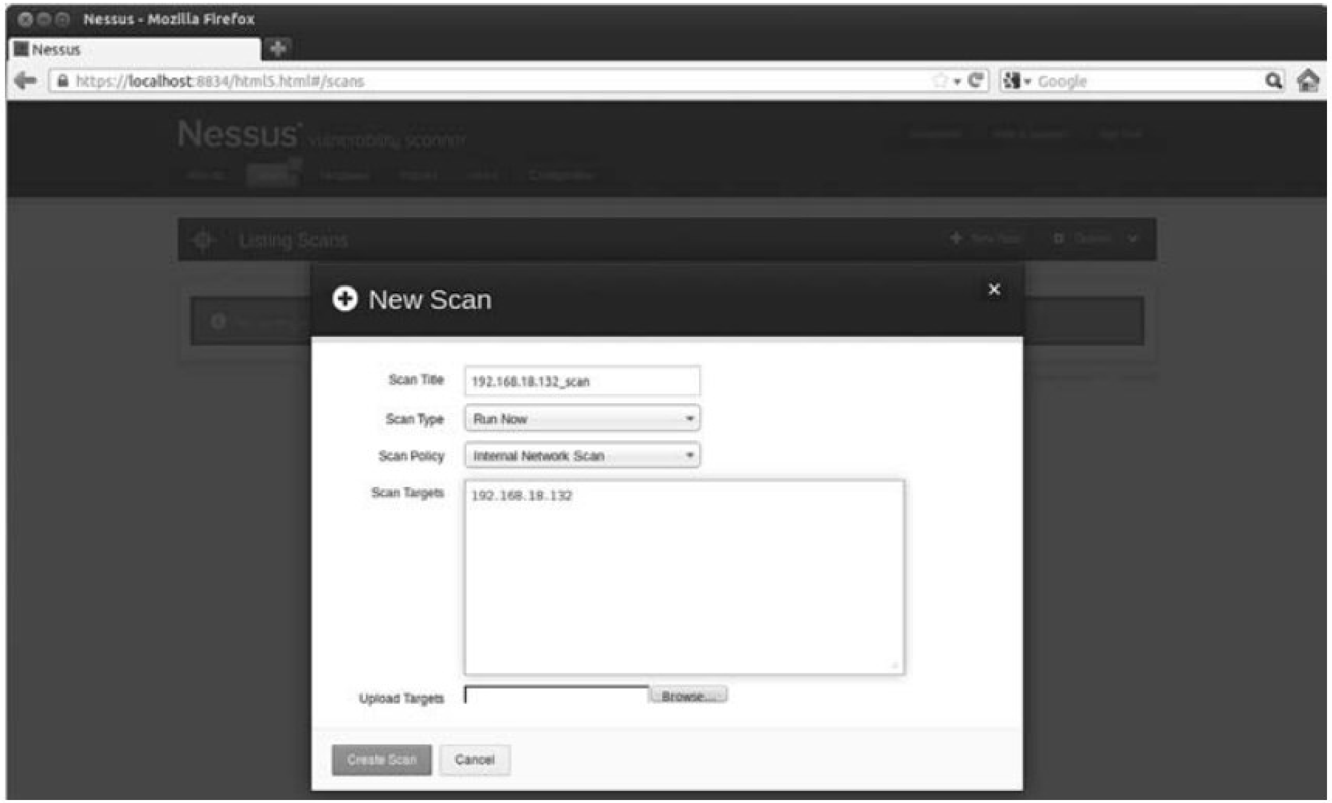
Shashi KS

Once you have a policy setup, you can run a scan against your target.

To set up a scan, you need to click the “Scans” link located in the top menu followed by the “New Scan” button located on the right-hand side of the page.

Nessus will bring up a new window that can be used to configure and customize your scan. You can enter individual addresses to scan a single target or a list of IPs to scan multiple hosts.

New scan screen



Scan Title: 192.168.18.132_scan

Scan Type: Run Now

Scan Policy: Internal Network Scan

Scan Targets: 192.168.18.132

Upload Targets:

FIGURE 3.8

Setting up the Nessus scan.

Vulnerability scanning with Nessus

Before launching the scan, you need to provide a name, select a policy, and enter the IP address of your targets.

Shashi KS

Provide a descriptive name to your scan, to quickly locate and sort your scan results at a later date.

You can enter your target IP addresses individually in the “**Scan Targets**” box or if you have your target IP addresses saved to a text file, you can use the “Browse.” button to locate and load it.

The latest versions of Nessus provide you with the ability to either run your scan immediately or create a Template and schedule the scan to kick off at a later date and time.

This can be extremely handy if you need to kick your scan off at a particular time. Once your options are set, you can click the “Create Scan” button in the lower right.

Nessus will provide you with information about the progress of your scan while it is running.

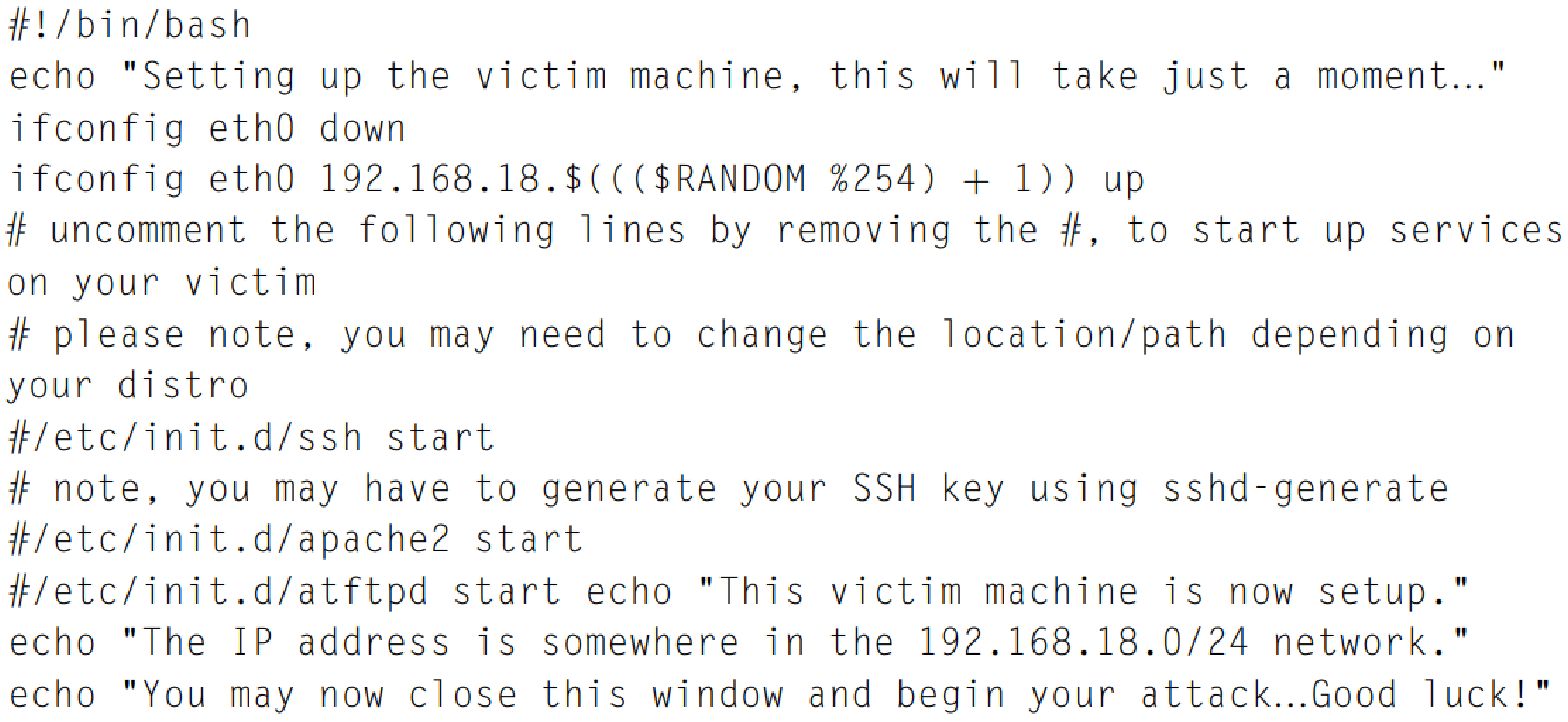
When Nessus finishes the scan, you will be able to review the results by clicking the “Results” link in the menu bar. The report will provide you with a detailed listing of all the vulnerabilities that Nessus discovered. We are especially interested in vulnerabilities labeled high or critical.
You should take time to closely review the report and make detailed notes about the system. We will use these results in the next step to gain access to the system. Once we have completed port scanning and vulnerability scanning for each of our targets, we should have enough information to begin attacking the system.

Script to hide your system in a given subnet

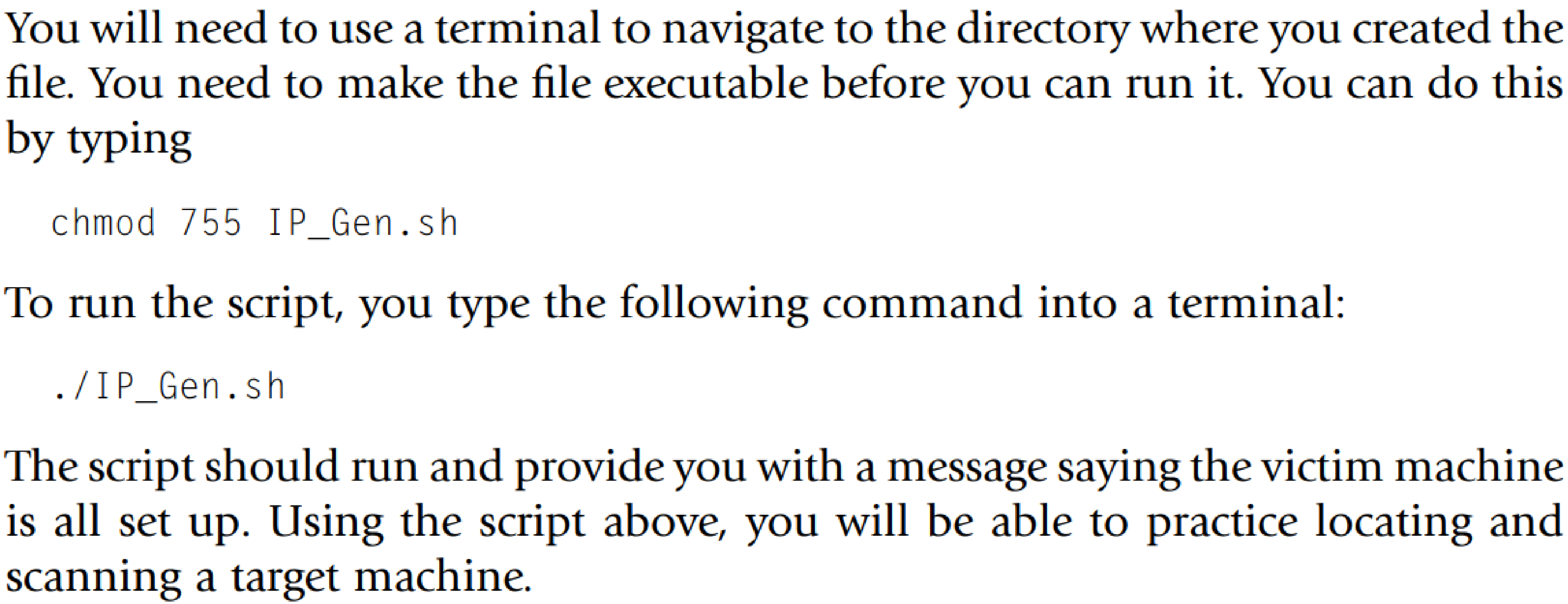
A simple script has been created, which can be used to “hide” your system in a given subnet.

Shashi KS

The code is designed to run purely on a Linux operating system. We can modify it by changing the first three octets of the IP address so that it will work on your network and system.
Modify the “eth” number to match your system.
The script generates a random number between 1 and 254. This number is to be used as the final octet in the IP address.
Once the random IP address is created, the script applies the address to the machine



```
#!/bin/bash
echo "Setting up the victim machine, this will take just a moment..."
ifconfig eth0 down
ifconfig eth0 192.168.18.$((($RANDOM %254) + 1)) up
# uncomment the following lines by removing the #, to start up services
on your victim
# please note, you may need to change the location/path depending on
your distro
#/etc/init.d/ssh start
# note, you may have to generate your SSH key using sshd-generate
#/etc/init.d/apache2 start
#/etc/init.d/atftpd start echo "This victim machine is now setup."
echo "The IP address is somewhere in the 192.168.18.0/24 network."
echo "You may now close this window and begin your attack...Good luck!"
```



You will need to use a terminal to navigate to the directory where you created the file. You need to make the file executable before you can run it. You can do this by typing

```
chmod 755 IP_Gen.sh
```

To run the script, you type the following command into a terminal:

```
./IP_Gen.sh
```

The script should run and provide you with a message saying the victim machine is all set up. Using the script above, you will be able to practice locating and scanning a target machine.

Nmap command switches

Shashi KS

Nmap switches provide extended functionality that may be useful to you as you progress in your penetration testing career.

The “-sV” switch is used for version scanning. When conducting version scanning, Nmap sends probes to the open port in an attempt to determine specific information about the service that is listening.

When possible, Nmap will provide details about the service including version numbers and other banner information. This information should be recorded in your notes.

It is recommended that you use the “-sV” switch whenever possible, especially on unusual or unexpected ports, because a wily administrator may have moved his web server to port 34567 in an attempt to obscure the service.

Changing the speed of your port scan is done with the “-T” switch. The timing switch ranges on a numeric scale from 0 to 5, with 0 being the slowest scan and 5, the fastest.

Timing options can be extremely useful depending on the situation. Slow scans are great for avoiding detection while fast scans can be helpful when you have a limited amount of time or large number of hosts to scan.

The “-O” switch can be useful for fingerprinting the operating system. This is handy for determining if the target you are attacking is a Windows, Linux, or other type of machine.

Knowing the operating system of your target will save you time by allowing you to focus your attacks to known weaknesses of that system.

There is no use in exploring exploits for a Linux machine if your target is running Windows.

Shashi KS

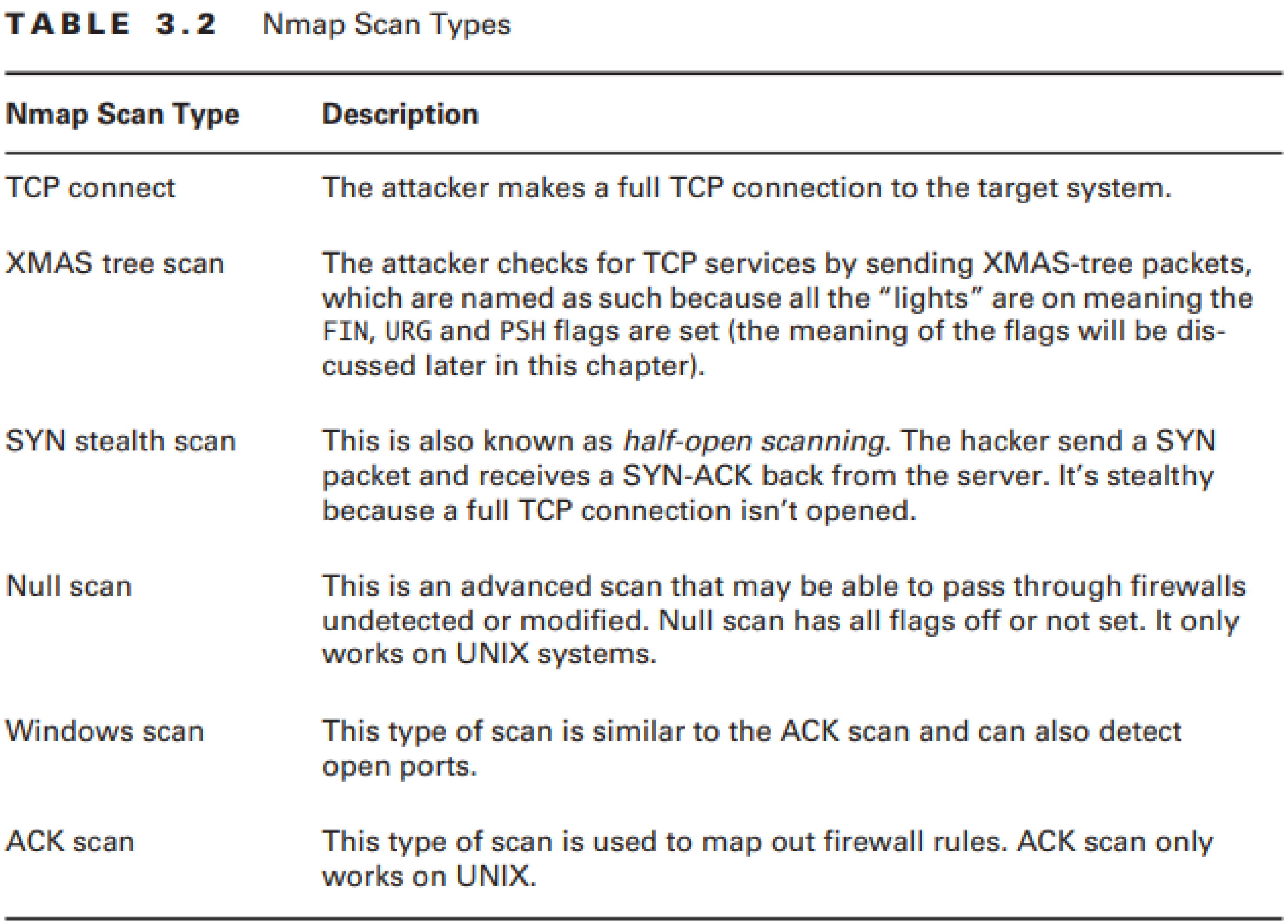
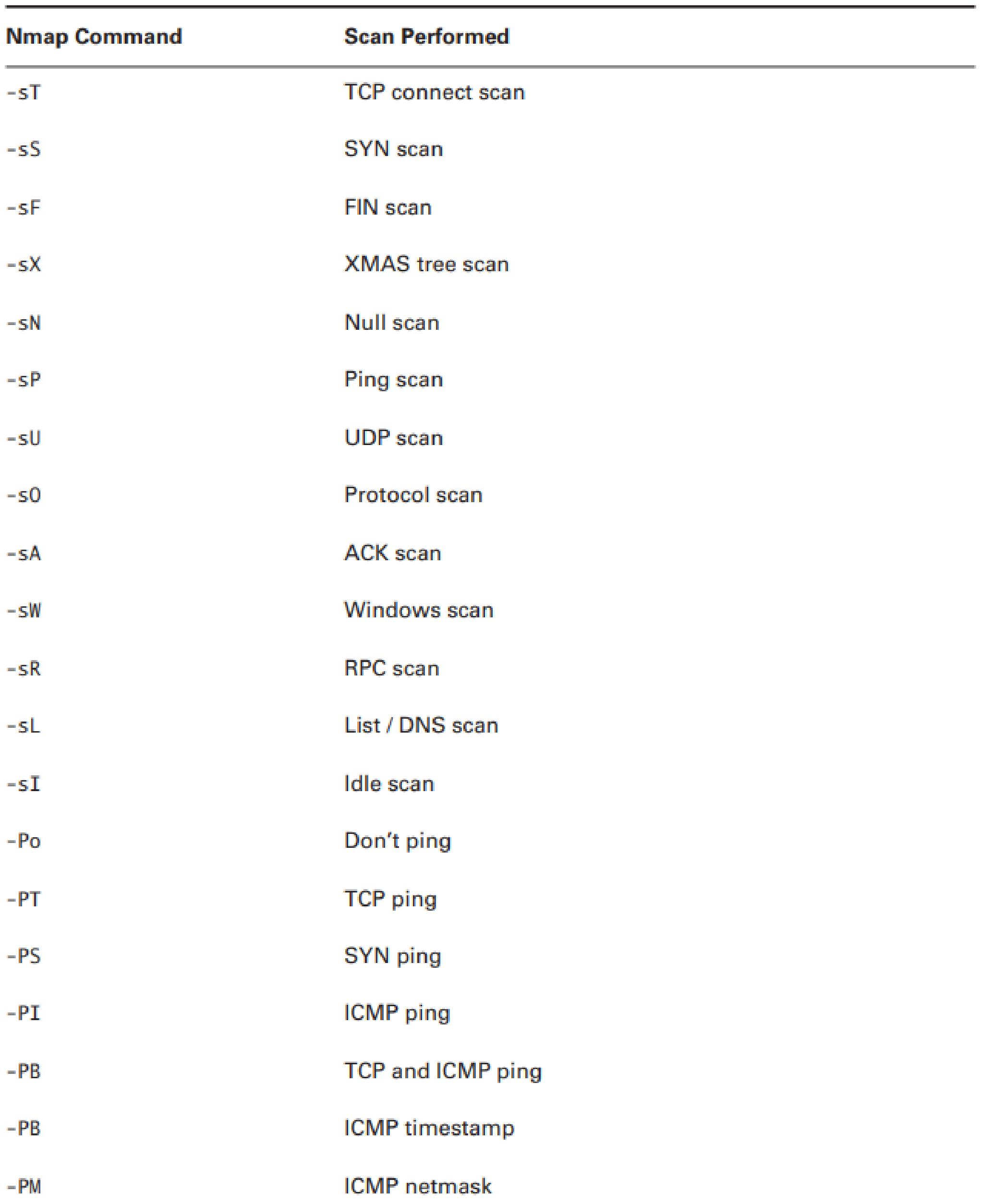


TABLE 3.2 Nmap Scan Types

Nmap Scan Type	Description
TCP connect	The attacker makes a full TCP connection to the target system.
XMAS tree scan	The attacker checks for TCP services by sending XMAS-tree packets, which are named as such because all the "lights" are on meaning the FIN, URG and PSH flags are set (the meaning of the flags will be discussed later in this chapter).
SYN stealth scan	This is also known as *half-open scanning*. The hacker send a SYN packet and receives a SYN-ACK back from the server. It's stealthy because a full TCP connection isn't opened.
Null scan	This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on UNIX systems.
Windows scan	This type of scan is similar to the ACK scan and can also detect open ports.
ACK scan	This type of scan is used to map out firewall rules. ACK scan only works on UNIX.



Nmap Command	Scan Performed
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List / DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask

Shashi KS

Nmap command switches to perform different types of scans

SYN, Stealth, XMAS, NULL, IDLE, and FIN Scans

Shashi KS

1. SYN

A **SYN or stealth scan** is also called a half-open scan because it doesn’t complete the TCP three-way handshake. The TCP/IP three-way handshake will be covered in the next section. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it’s assumed the target would complete the connect and the port is listening. If a RST is received back from the target, then it’s assumed the port isn’t active or is closed. The advantage of the SYN stealth scan is that fewer IDS systems log this as an attack or connection attempt.

2.XMAS

XMAS scans send a packet with the FIN, URG, and PSH flags set. If the port is open, there is no response; but if the post is closed, the target responds with a RST/ACK packet. XMAS scans work only on target systems that follow the RFC 793 implementation of TCP/IP and don’t work against any version of Windows.

3.FIN

A FIN scan is similar to an XMAS scan but sends a packet with just the FIN flag set. FIN scans receive the same response and have the same limitations as XMAS scans.

NULL

A NULL scan is also similar to XMAS and FIN in its limitations and response, but it just sends a packet with no flags set.

IDLE

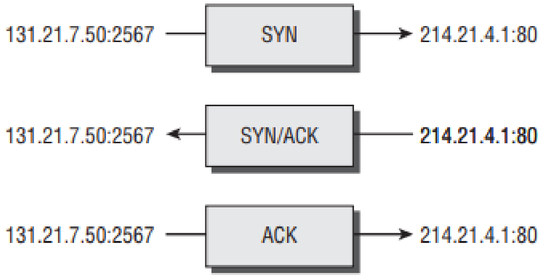
An IDLE scan uses a spoofed IP address to send a SYN packet to a target. Depending on the response, the port can be determined to be open or closed. IDLE scans determine port scan response by monitoring IP header sequence numbers.

TCP Communication Flag Types

TCP scan types are built on the TCP three-way handshake. TCP connections require a threeway handshake before a connection can be made and data transferred between the sender and receiver.

Figure 3.2 details the steps of the TCP three-way handshake.

FIGURE 3.2 TCP three-way handshake



Because TCP is a connection-oriented protocol, a process for establishing a connection (three-way handshake), restarting a failed connection, and finishing a connection is part of the protocol. These protocol notifications are called flags.

TCP contains ACK, RST, SYN, URG, PSH, and FIN flags.

The following list identifies the function of the TCP flags:

SYN—Synchronize. Initiates a connection between hosts.
ACK—Acknowledge. Established connection between hosts.
PSH—Push. System is forwarding buffered data.
URG—Urgent. Data in packets must be processed quickly.
FIN—Finish. No more transmissions.
RST—Reset. Resets the connection.

TCP scan types

Shashi KS

A hacker can attempt to bypass detection by using flags instead of completing a normal TCP connection.

The TCP scan types in Table 3.4 are used by some scanning tools to elicit a response from a system by setting one or more flags.

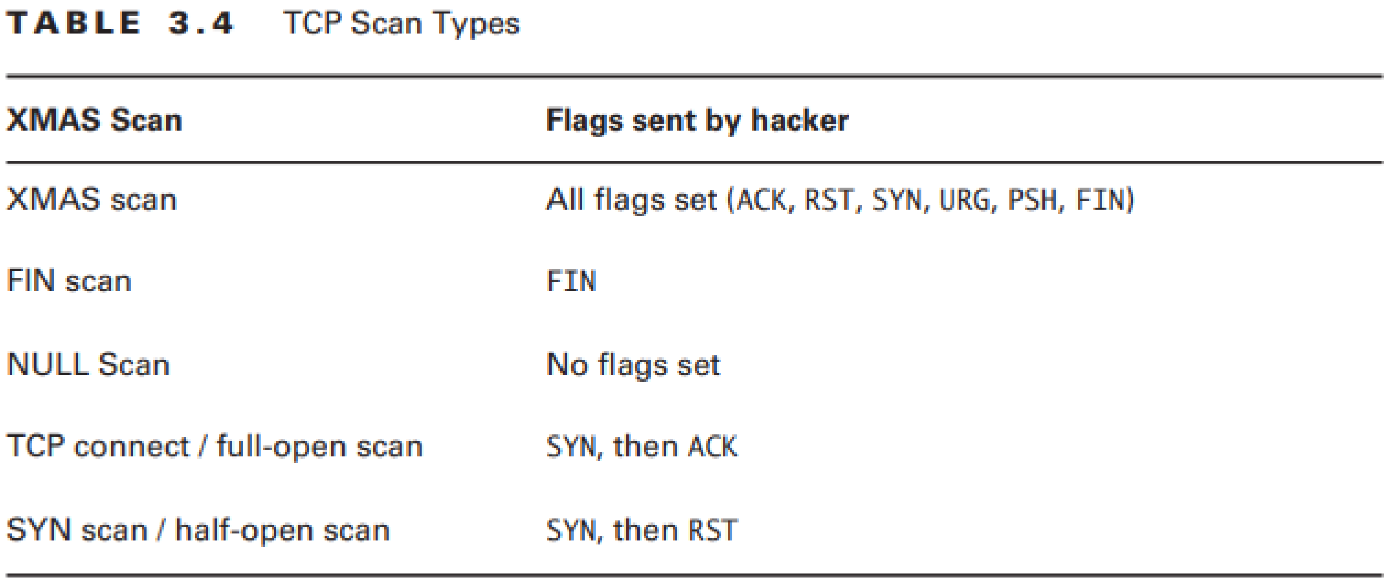


TABLE 3.4 TCP Scan Types

XMAS Scan	Flags sent by hacker
XMAS scan	All flags set (ACK, RST, SYN, URG, PSH, FIN)
FIN scan	FIN
NULL Scan	No flags set
TCP connect / full-open scan	SYN, then ACK
SYN scan / half-open scan	SYN, then RST

Hacking Tools for port scanning

Shashi KS

IPEye is a TCP port scanner that can do SYN, FIN, Null, and XMAS scans. It's a command-line tool.

IPEye probes the ports on a target system and responds with either closed, reject, drop, or open.

Closed means there is a computer on the other end, but it doesn't listen at the port. Reject means a firewall is rejecting (sending a reset back) the connection to the port.

Drop means a firewall is dropping everything to the port, or there is no computer on the other end.

Open means some kind of service is listening at the port. These responses help a hacker identify what type of system is responding.

IPSecScan is a tool that can scan either a single IP address or a range of addresses looking for systems that are IPSec enabled

Ping sweeping techniques

Shashi KS

A scan of a range of IP addresses that shows which IP addresses are in use and which aren’t are called **ping sweep** techniques. Ping sweeps may include retrieving the DNS name for each live IP address.

- ❑ The CEH scanning methodology starts with checking for systems that are live on the network, meaning that they respond to probes or connection requests.
- ❑ The simplest way to determine whether systems are live is to perform a ping sweep of the IP address range. All systems that respond with a ping reply are considered live on the network.
- ❑ Internet Control Message Protocol (ICMP) scanning is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings.
- ❑ A benefit of ICMP scanning is that it can be run in parallel, meaning all system are scanned at the same time; thus it can run quickly on an entire network. Most hacking tools include a ping-sweep option, which essentially means performing an ICMP request to every host on the network.
- ❑ One considerable problem with this method is that personal firewall software and network based firewalls can block a system from responding to ping sweeps. Another problem is that the computer must be on to be scanned.

Hacker tools:

Pinger, Friendly Pinger, and WS_Ping_Pro are all tools that perform ICMP queries.

Detecting Ping Sweeps

Shashi KS

✓ Almost any IDS or intrusion prevention system (IPS) system will detect and alert the security administrator to a ping sweep occurring on the network.

✓ Most firewall and proxy servers block ping responses so a hacker can't accurately determine whether systems are available using a ping sweep alone.

✓ More intense port scanning must be used if systems don't respond to a ping sweep.

✓ Just because a ping sweep doesn't return any active hosts on the network doesn't mean they aren't available—you need to try an alternate method of identification. Hacking takes time, patience, and persistence

Banner Grabbing and OS Fingerprinting Techniques

Shashi KS

Banner grabbing and operating system identification, which can also be defined **as fingerprinting the TCP/IP stack,** is the fourth step in the CEH scanning methodology.

The process of **fingerprinting** allows the hacker to identify particularly vulnerable or high value targets on the network. Hackers are looking for the easiest way to gain access to a system or network.

Banner grabbing is the process of opening a connection and reading the banner or response sent by the application. Many e-mail, FTP, and web servers will respond to a telnet connection with the name and version of the software.

The aids a hacker in **fingerprinting the OS and application software**. For example, a Microsoft Exchange e-mail server would only be installed on Windows OS.

Types of fingerprinting

Shashi KS

Active stack fingerprinting is the most common form of fingerprinting. It involves sending data to a system to see how the system responds. It’s based on the fact that various operating system vendors implement the TCP stack differently, and responses will differ based on the operating system.

The responses are then compared to a database to determine the operating system. Active stack fingerprinting is detectable because it repeatedly attempts to connect with the same target system.

Passive stack fingerprinting is stealthier and involves examining traffic on the network to determine the operating system. It uses sniffing techniques instead of scanning techniques.

Passive stack fingerprinting usually goes undetected by an IDS or other security system but is less accurate than active fingerprinting.

Netcraft and HTTrack

Shashi KS

Netcraft and HTTrack are tools that fingerprint an operating system. Both are used to determine the OS and web-server software version numbers.

Netcraft is a website that periodically polls web servers to determine the operating system version and the web-server software version.

Netcraft can provide useful information the hacker can use in identifying vulnerabilities in the web server software.

Netcraft has an anti-phishing toolbar and web-server verification tool you can use to make sure you're using the actual web server rather than a spoofed web server.

HTTrack arranges the original site's relative link structure. You open a page of the mirrored website in your browser, and then you can browse the site from link to link as if you were viewing it online. HTTrack can also update an existing mirrored site and resume interrupted downloads.