

Chapter 3: Labs

Lab Exercises

Activity 3.1: Port Scanning

In this exercise, you will use a Kali Linux virtual machine to

- Perform a port scan of a vulnerable system using nmap
- Identify the remote system's operating system and version
- Capture packets during the port scan

Part 1: Set up virtual machines

Information on downloading and setting up the Kali Linux and Metasploitable virtual machines can be found in the introduction of this book. You can also substitute your own system if you have one already set up to run nmap.

Boot the Kali Linux and Metasploitable virtual machines and log into both. The username/password pair for Kali Linux is root/toor, and Metasploitable uses msfadmin/msfadmin.

Run ifconfig from the console of the Metasploitable virtual machine. Take note of the IP address assigned to the system.

```
biddion@kali:~  
File Actions Edit View Help  
→ ~ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255  
    inet6 fe80::a00:27ff:fe50:4c14 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)  
    RX packets 8 bytes 3694 (3.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 13 bytes 1808 (1.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentat  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr  
    inet addr:192.168.56.102  
    inet6 addr: fe80::a00:27ff
```

Part 2: Perform a port scan

Now we will perform a port scan of the Metasploitable virtual machine. Metasploitable is designed to be vulnerable, so we should anticipate seeing many services that might not otherwise be available on a properly secured Linux system.

Open a Terminal window using the menu bar at the top of the screen.

To run nmap, simply type nmap and the IP address of the target system. Use the IP address of the Metasploitable system: nmap [target IP].

What ports are open, and what services are identified?

nmap 192.168.56.102

```
→ ~ nmap 192.168.56.102  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-19 00:59 EST  
Nmap scan report for 192.168.56.102  
Host is up (0.0010s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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  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  
  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

```
→ ~ █
```

Do you believe that you have identified all the open ports on the system? No!

```
nmap 192.168.56.102 -p-
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
→ ~ nmap 192.168.56.102 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-19 01:01 EST
Nmap scan report for 192.168.56.102
Host is up (0.00072s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34097/tcp open  unknown
40293/tcp open  unknown
42629/tcp open  unknown
57485/tcp open  unknown
```

all ports

```
Nmap done: 1 IP address (1 host up) scanned in 21.78 seconds
→ ~ █
```

Now we will identify the operating system of the Metasploitable virtual machine. This is enabled using the `-O` flag in nmap. Rerun your nmap, but this time type `nmap -O [target IP]` and add `-p 1-65535` to capture all possible ports.

Which operating system and version is the Metasploitable virtual machine running? Which additional ports showed up?

```
→ ~ sudo nmap 192.168.56.102 -p 1-65535 -O
[sudo] password for biddio:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-19 01:04 EST
Nmap scan report for 192.168.56.102
Host is up (0.00065s latency).
Not shown: 65505 closed tcp ports (reset)
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  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34097/tcp open  unknown
40293/tcp open  unknown
42629/tcp open  unknown
57485/tcp open  unknown
```

Linux 2.6.X

```
MAC Address: 08:00:27:DB:16:2C (Oracle VM VirtualBox Virtual NIC)
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 18.41 seconds
→ ~ █
```

Activity 3.2: Write an Intelligence Gathering Plan

For this activity, design a passive intelligence gathering plan for an organization of your choice. You may want to reference a resource like OSSTMM, NIST SP 800-115, or pentest-standard.org before you write the plan.

http://www.pentest-standard.org/index.php/Main_Page

Your intelligence gathering plan should identify the following:

The target

How you would gather passive data, including what data you would look for?

mx servers, cname, a record, ip addresses, domain issuer/date, location

What tools you would use?

- host
- dig
- nslookup


<https://dns.google>


<https://mxtoolbox.com/ReverseLookup.aspx>

For external footprinting, we first need to determine which one of the WHOIS servers contains the information we're after.

<https://www.iana.org> (I actually am unsure how to find whois servers)

Once you are done, use one or more of the references listed earlier to review your plan. Identify what you missed and what additional data you could gather.

 OSSTMM.3.pdf17 MB

 nistspecialpublication800-115.pdf515 kB

Repeat the activity, documenting how you would perform active intelligence gathering, including how you would determine network topology, what operating systems are in use, and what services are accessible. Remember to account for variables like wired and wireless networks, on-site and cloud hosting, and virtual versus physical hosts.

To determine network topology I would first use Zenmap,

Target: Walmart

One of the major goals of intelligence gathering during a penetration test is to determine hosts which will be in scope. There are a number of techniques which can be used to identify systems, including using reverse DNS lookups, DNS bruting, WHOIS searches on the domains and the ranges

```
→ ~ nslookup 23.51.28.149
149.28.51.23.in-addr.arpa      name = a23-51-28-149.deploy.static.akamaitechnologies.com.

Authoritative answers can be found from:
```

```
→ ~ host www.walmart.com
www.walmart.com is an alias for www.walmart.com.edgekey.net.
www.walmart.com.edgekey.net is an alias for e4373.x.akamaiedge.net.
e4373.x.akamaiedge.net has address 23.51.28.149
→ ~ █
```

```
→ ~ dig www.walmart.com

; <<>> DiG 9.17.21-1-Debian <<>> www.walmart.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 18340
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
;www.walmart.com.      IN      A

;; ANSWER SECTION:
www.walmart.com.      62      IN      CNAME   www.walmart.com.edgekey.net.
www.walmart.com.edgekey.net. 7064 IN      CNAME   e4373.x.akamaiedge.net.
e4373.x.akamaiedge.net. 20      IN      A       23.51.28.149
```

```
e4373.x.akamailedge.net. 20      IN      A      23.51.28.149

;; Query time: 8 msec
;; SERVER: 210.220.163.82#53(210.220.163.82) (UDP)
;; WHEN: Wed Jan 19 01:43:11 EST 2022
;; MSG SIZE  rcvd: 137
```

Activity 3.3: Intelligence Gathering Techniques

Match each of the information types in the following chart to the tool that can help gather it.

Route to a system	netstat
Open services via a network	Whois
IP traffic flow and volume	traceroute
Organizational contact information associated with domain registration	Wireshark
Connections listed by protocol	Nmap
Packet capture	Creepy
Zone transfer	dig
Social media geotagging	netflow