Project 5: Enumerating Metasploitable 2 (15 points)

What You Need

1. A Kali Linux machine, real or virtual
2. The "Metasploitable 2" vulnerable Linux Server you prepared in a previous project

---

Setup

Start your Kali VM and log in as **root** with the password **toor**

Start your Metasploitable 2 VM and log in as **msfadmin** with the password **msfadmin**

Execute the **ifconfig** command on both machines and ping from one to the other. Make sure you get replies, as shown below.

```
root@kali:~# ifconfig eth0
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 172.16.1.188  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::20c:29ff:fe52:bb35  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:52:bb:35  txqueuelen 1000  (Ethernet)
        RX packets 7084  bytes 6116605 (5.8 MiB)
        RX errors 5857  dropped 0  overruns 0  frame 0
        TX packets 3689  bytes 3160313 (3.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2024

root@kali:~# ping 172.16.1.190
PING 172.16.1.190 (172.16.1.190) 56(84) bytes of data.
64 bytes from 172.16.1.190: icmp_seq=1 ttl=64 time=0.274 ms
64 bytes from 172.16.1.190: icmp_seq=2 ttl=64 time=0.453 ms
^C
```

Task 1: Finding Hosts & Open Ports

In Kali, execute this command to locate all hosts on your network.

Replace the subnet address below with the correct subnet for your machine. Usually all you need is the first 3 bytes of the IP address, as highlighted in the image above.

```
netdiscover -r 172.16.1.0/24
```

As shown below, the scanner finds all the machines on your network. One of them should be your Metasploitable 2 machine.

Press **Ctrl+C** to exit netdiscover.

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

 ___________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------------
 172.16.1.1      00:50:56:c0:00:08      1      60  Unknown vendor
 172.16.1.2      00:50:56:f0:8a:91      1      60  Unknown vendor
 172.16.1.190    00:0c:29:8b:bb:aa      1      60  Unknown vendor
 172.16.1.254    00:50:56:f4:d5:ce      1      60  Unknown vendor
```

Execute this command to scan all 65,536 TCP ports on the target, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
nmap -sS -p- 172.16.1.190
```

This scan quickly finds all open ports, as shown below, but it doesn't find versions of the services.

```
root@kali:~# nmap -sS -p- 172.16.1.190

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-17 15:27 EDT
Nmap scan report for 172.16.1.190
Host is up (0.00023s latency).
Not shown: 65505 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  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
39551/tcp open  unknown
50081/tcp open  unknown
53402/tcp open  unknown
56812/tcp open  unknown
MAC Address: 00:0C:29:8B:BB:AA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

Execute this command to scan 1000 common ports on the target, with version detection and OS detection. Replace the IP

address with the IP address of your Metasploitable 2 VM.

```
nmap -sS -sV -O 172.16.1.190
```

This scan finds many version numbers, as shown below.

```
root@kali:~# nmap -sS -sV -O 172.16.1.190

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-17 15:33 EDT
Nmap scan report for 172.16.1.190
Host is up (0.00032s 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 8ubuntu1 (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)
111/tcp  open  rpcbind     2 (RPC #100000)
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?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
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 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:8B:BB:AA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

Capturing a Screen Image

Make sure the "**vsftpd 2.3.4**" message is visible, as shown above.

Capture a whole-desktop image and save it as "**Proj 5a**".

YOU MUST SEND IN A WHOLE-DESKTOP IMAGE FOR FULL CREDIT

> ***Replace all the IP addresses in commands below with the IP address of your Metasploitable 2 target machine.***

Execute this command to scan UDP ports on the target.

```
nmap -sU 172.16.1.190
```

This scan will take about 15 minutes to run, so leave it going and open a new Terminal window to continue with the rest of the project while it runs.

When it finishes, it finds several UDP-based services, as shown below.

```
root@kali:~# nmap -sU 172.16.1.190

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-17 15:41 EDT
Nmap scan report for 172.16.1.190
Host is up (0.00031s latency).
Not shown: 991 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
1007/udp  open|filtered unknown
2049/udp  open          nfs
44185/udp open|filtered unknown
MAC Address: 00:0C:29:8B:BB:AA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1078.49 seconds
```

Task 2: Enumerating Users

Enumerating with Nmap

Execute this command to run the Nmap script "smb-enum-users" on the target. This will find a list of user accounts from the SMB service, which is available if a host is sharing files with Windows systems.

```
nmap --script smb-enum-users.nse -p 445 172.16.1.190
```

This produces a long list of user accounts, as shown below.

```
root@kali:~# nmap --script smb-enum-users.nse -p 445 172.16.1.190

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-17 15:45 EDT
Nmap scan report for 172.16.1.190
Host is up (0.00027s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:8B:BB:AA (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
```

Enumerating with rpcclient

You can also enumerate users via Null sessions with the "rpcclient" command. Execute this command:

```
rpcclient -U "" 172.16.1.190
```

When it asks for a password, press **Enter**.

This displays an "rpcclient $>" prompt. Execute this command:

```
querydominfo
```

This shows that there are 35 users on the system, as shown below.

```
root@kali:~# rpcclient -U "" 172.16.1.190
Enter 's password:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1502999513
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $>
```

Execute this command to list all 35 user accounts.

```
enumdomusers
```

This lists all the user accounts, with their "Relative ID" numbers (rid), as shown below.

```
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
```

Execute this command to get more information about the "msfadmin" account.

```
queryuser msfadmin
```

This shows that user's profile path, and other information, as shown below.

```
rpcclient $> queryuser msfadmin
        User Name   :   msfadmin
        Full Name   :   msfadmin,,,
        Home Drive  :   \\metasploitable\msfadmin
        Dir Drive   :
        Profile Path:   \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time              :      never
        Kickoff Time             :      never
        Password last set Time   :      Wed, 28 Apr 2010 02:56:18 EDT
        Password can change Time :      Wed, 28 Apr 2010 02:56:18 EDT
        Password must change Time:      never
        unknown_2[0..31]...
        user_rid :      0xbb8
        group_rid:      0xbb9
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

Execute the **exit** command to leave "rpcclient".

Enumerating with enum4linux

enum4linux is a Perl script that uses smbclient, rpcclient, net, and nmblookup to automatically enumerate a target.

Execute this command to see the options for the enum4linux command.

```
enum4linux --help
```

Not specifying any options runs them all. Execute this command to enumerate the target:

```
enum4linux 172.16.1.190
```

A lot of output scrolls by. First there are a couple lists of all the usernames, as we found previously with other tools.

Then a "Share Enumeration" appears, showing that the **/tmp** folder is shared, as shown below. This has a note of "oh noes!" because **/tmp** is world-writeable. This means we can probably upload scripts into that folder and execute them :).

```
 =========================================
|    Share Enumeration on 172.16.1.190    |
 =========================================
WARNING: The "syslog" option is deprecated
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))

        Server               Comment
        ---------            -------
        METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

Capturing a Screen Image

Make sure the "**oh noes!**" message is visible, as shown above.

Capture a whole-desktop image and save it as "**Proj 5b**".

YOU MUST SEND IN A WHOLE-DESKTOP IMAGE FOR FULL CREDIT

Turning in Your Project

Email the images to **cnit.124@gmail.com** with a subject line of "**Proj 5 From YOUR NAME**", replacing "YOUR NAME" with your real name.

Send a Cc to yourself.

Credits

I followed this guide:
[Metasploitable 2 enumeration]

Last Modified: 8-17-17 1:19 pm