Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

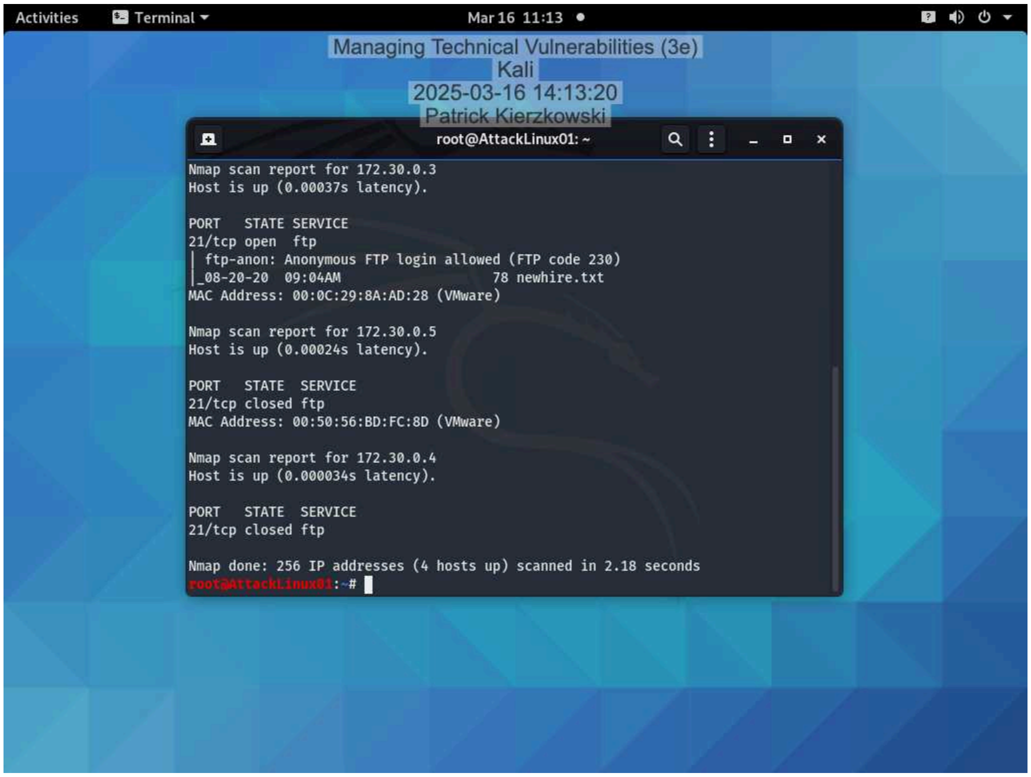
Time on Task:	Progress:
3 hours, 39 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:39 PM

Guided Exercises

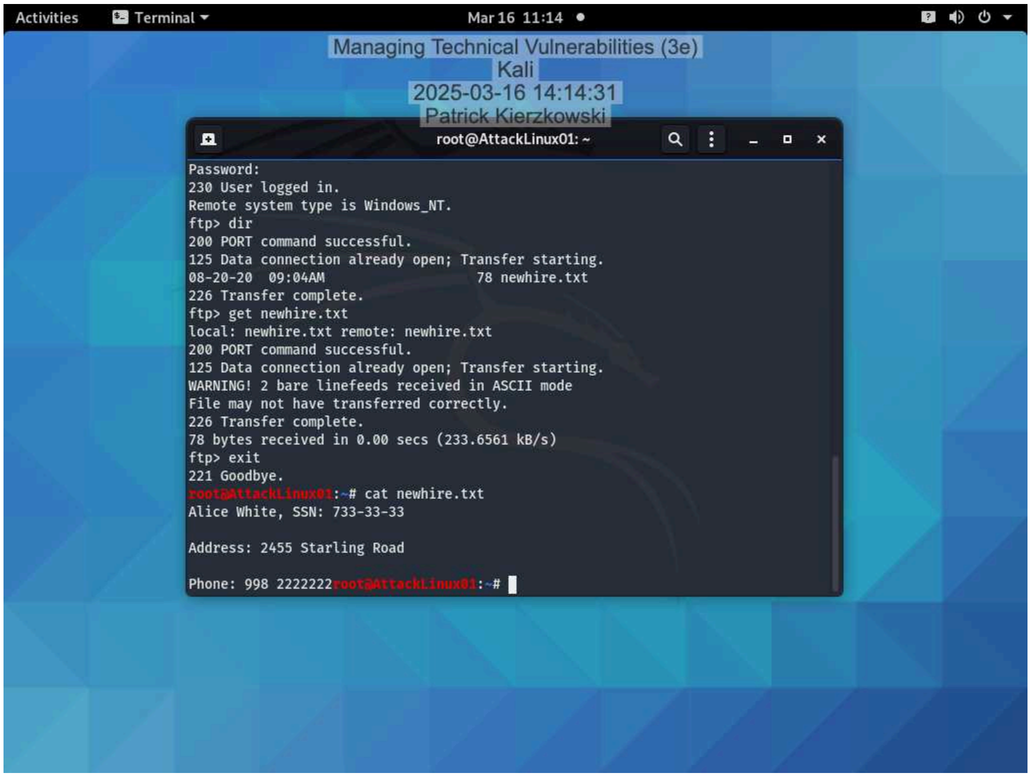
Part 1: Perform a Vulnerability Scan with Nmap

6. **Make a screen capture** showing **nmap results indicating that anonymous FTP is enabled for one of the hosts in the network**.



```
Nmap scan report for 172.30.0.3
Host is up (0.00037s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_08-20-20  09:04AM                   78 newhire.txt
MAC Address: 00:0C:29:8A:AD:28 (VMware)

Nmap scan report for 172.30.0.5
Host is up (0.00024s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 00:50:56:BD:FC:8D (VMware)

Nmap scan report for 172.30.0.4
Host is up (0.000034s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.18 seconds
root@AttackLinux01:~# 
```

14. **Make a screen capture** showing the **contents of the newhire.txt file**.



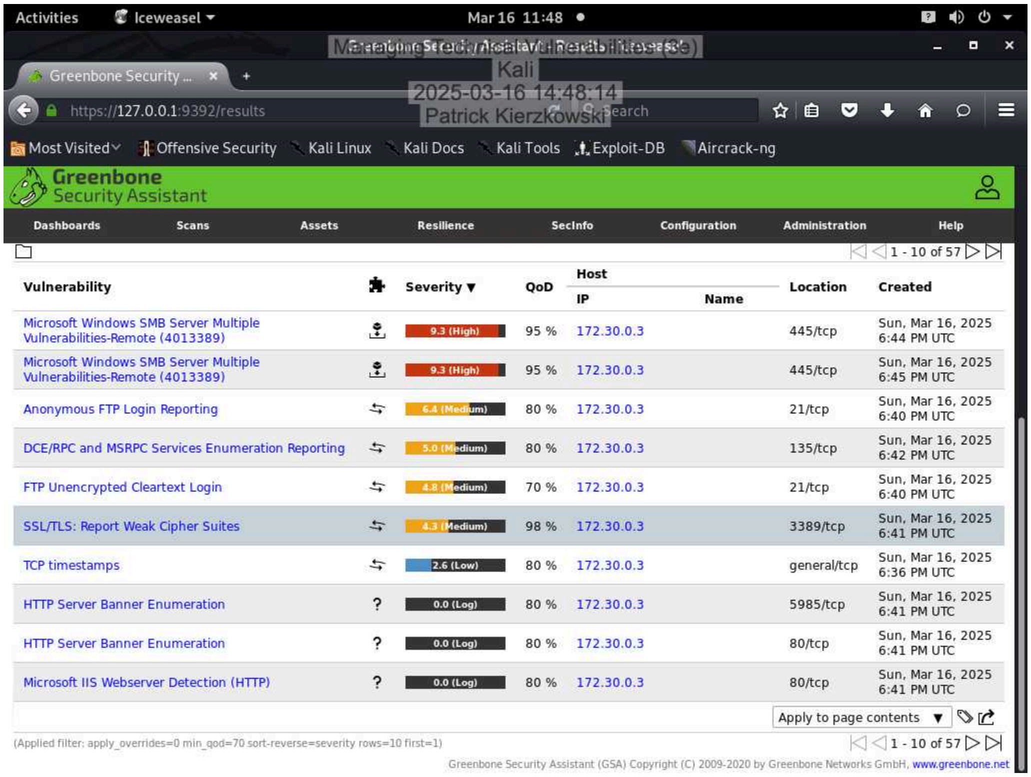
```
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-20-20  09:04AM                   78 newhire.txt
226 Transfer complete.
ftp> get newhire.txt
local: newhire.txt remote: newhire.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 2 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
78 bytes received in 0.00 secs (233.6561 kB/s)
ftp> exit
221 Goodbye.
root@AttackLinux01:~# cat newhire.txt
Alice White, SSN: 733-33-33

Address: 2455 Starling Road

Phone: 998 2222222root@AttackLinux01:~# 
```

17. **Record** whether each IP address has port 445 open or closed and whether it is also vulnerable to an SMB vulnerability.

172.30.0.2 Port 445 open not vulnerable. 172.30.0.3 Port 445 open and vulnerable. 172.30.0.4 Port 445 open not vulnerable. 172.30.0.5 Port 445 not vulnerable

Part 2: Perform a Vulnerability Scan with the GVM Framework

15. **Make a screen capture** showing the **first page of detected vulnerabilities in the Greenbone Security Assistant.**



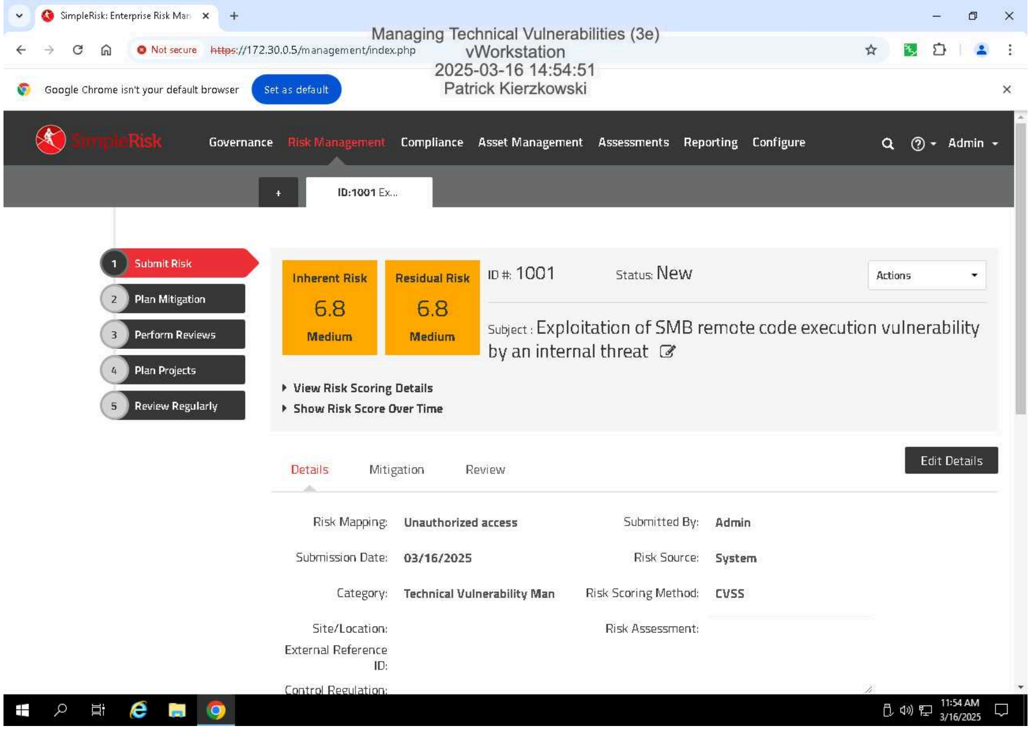
Vulnerability	🧩	Severity ▼	QoD	Host		Location	Created
				IP	Name		
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	⭳	9.3 (High)	95 %	172.30.0.3		445/tcp	Sun, Mar 16, 2025 6:44 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	⭳	9.3 (High)	95 %	172.30.0.3		445/tcp	Sun, Mar 16, 2025 6:45 PM UTC
Anonymous FTP Login Reporting	⇆	6.4 (Medium)	80 %	172.30.0.3		21/tcp	Sun, Mar 16, 2025 6:40 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	172.30.0.3		135/tcp	Sun, Mar 16, 2025 6:42 PM UTC
FTP Unencrypted Cleartext Login	⇆	4.8 (Medium)	70 %	172.30.0.3		21/tcp	Sun, Mar 16, 2025 6:40 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	4.3 (Medium)	98 %	172.30.0.3		3389/tcp	Sun, Mar 16, 2025 6:41 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	172.30.0.3		general/tcp	Sun, Mar 16, 2025 6:36 PM UTC
HTTP Server Banner Enumeration	?	0.0 (Log)	80 %	172.30.0.3		5985/tcp	Sun, Mar 16, 2025 6:41 PM UTC
HTTP Server Banner Enumeration	?	0.0 (Log)	80 %	172.30.0.3		80/tcp	Sun, Mar 16, 2025 6:41 PM UTC
Microsoft IIS Webserver Detection (HTTP)	?	0.0 (Log)	80 %	172.30.0.3		80/tcp	Sun, Mar 16, 2025 6:41 PM UTC

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=severity rows=10 first=1)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

Part 3: Document Vulnerabilities with SimpleRisk

24. **Make a screen capture** showing the **submitted SMB remote code execution risk, including the Inherent and Residual Risk values**.



Managing Technical Vulnerabilities (3e)
vWorkstation
2025-03-16 14:54:51
Patrick Kierzkowski

Inherent Risk 6.8 Medium

Residual Risk 6.8 Medium

ID #: 1001

Status: New

Subject : Exploitation of SMB remote code execution vulnerability by an internal threat

Risk Mapping:	Unauthorized access	Submitted By:	Admin
Submission Date:	03/16/2025	Risk Source:	System
Category:	Technical Vulnerability Man	Risk Scoring Method:	CVSS
Site/Location:		Risk Assessment:	
External Reference ID:			
Control Regulation:			

Challenge Exercise

Host 1 - IP address, operating system, and open ports

172.30.0.2, Ports 135, 139, 445, 3389, 5901. Microsoft Windows Server 2012

Host 2 - IP address, operating system, and open ports

172.30.0.3, Microsoft Windows Server 2016 build 10586 -14393. Ports 21, 22, 53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389

Host 3 - IP address, operating system, and open ports

172.30.0.4 , Linux 2.6.32. Ports 22 and 111

Host 4 - IP address, operating system, and open ports

172.30.0.5 , Linux 2.6.32. Ports 80 and 443