

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

3 hours, 39 minutes

Progress:

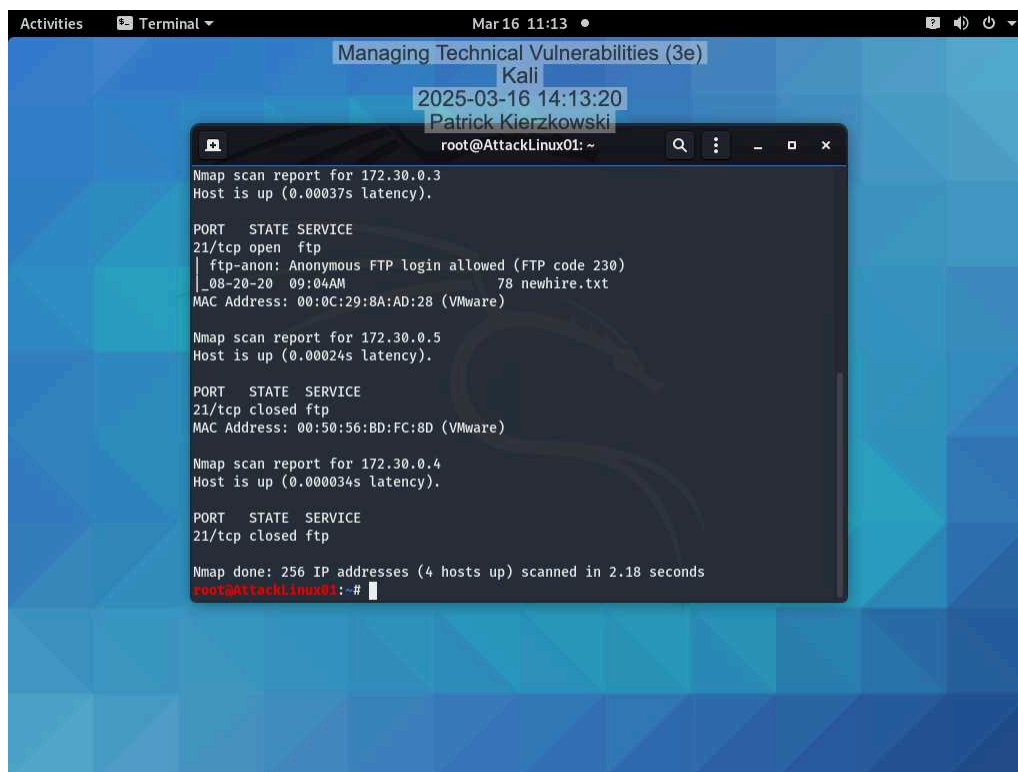
100%

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

Guided Exercises

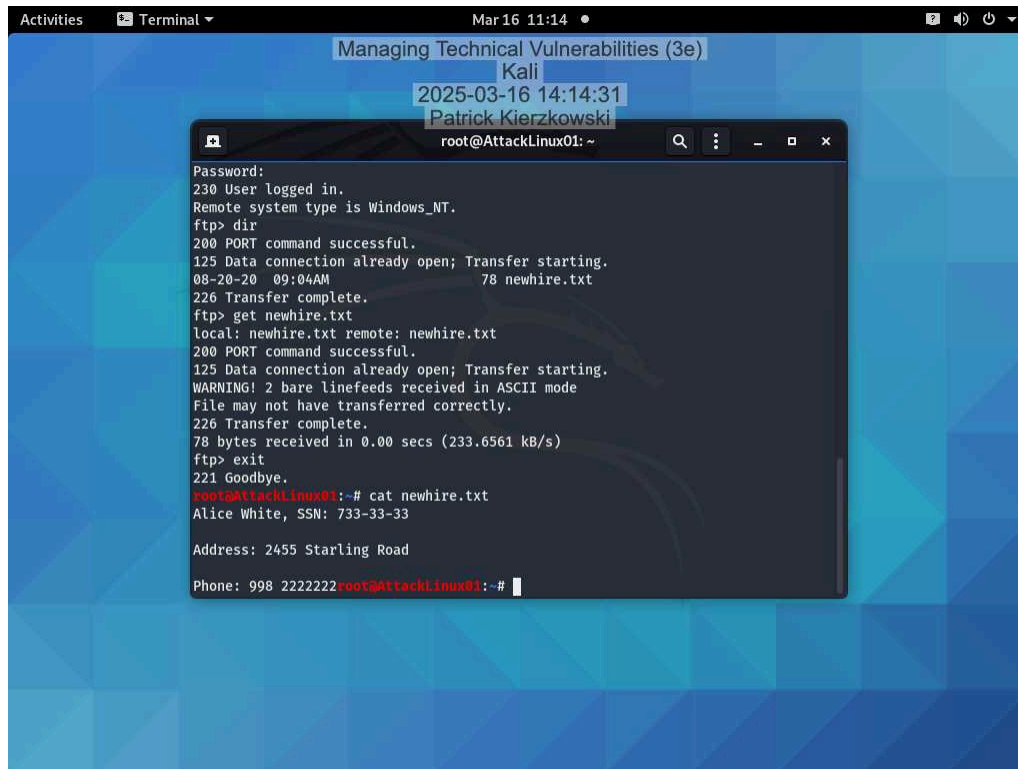
Part 1: Perform a Vulnerability Scan with Nmap

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



```
Activities Terminal Mar 16 11:13 Managing Technical Vulnerabilities (3e) Kali 2025-03-16 14:13:20 Patrick Kierzkowski root@AttackLinux01: ~ 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 (0.00034s 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**.



```
Activities Terminal Mar 16 11:14
Managing Technical Vulnerabilities (3e)
Kali
2025-03-16 14:14:31
Patrick Kierzkowski
root@AttackLinux01: ~
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

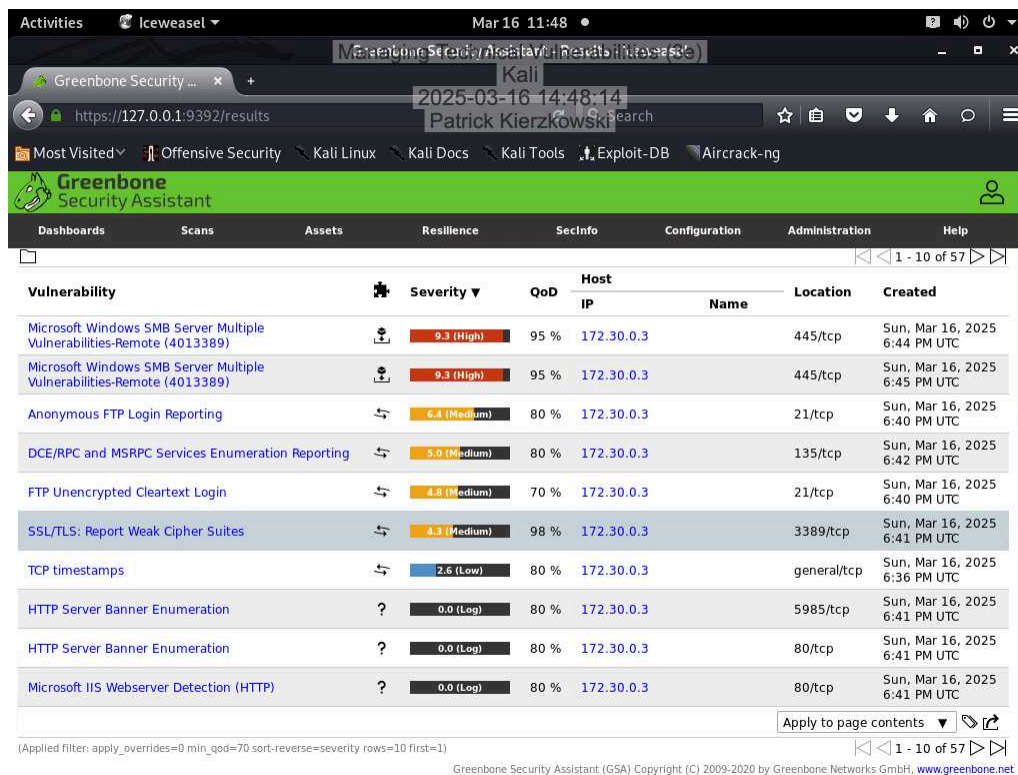
Phone: 998 2222222 root@AttackLinux01:~#
```

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.



The screenshot shows the Greenbone Security Assistant (GSA) web interface. The browser address bar displays the URL `https://127.0.0.1:9392/results`. The interface features a navigation bar with tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main content area displays a table of detected vulnerabilities. The table has columns for Vulnerability, Severity, QoD, Host (IP), Name, Location, and Created. The vulnerabilities listed include Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389), Anonymous FTP Login Reporting, DCE/RPC and MSRPC Services Enumeration Reporting, FTP Unencrypted Cleartext Login, SSL/TLS: Report Weak Cipher Suites, TCP timestamps, HTTP Server Banner Enumeration, and Microsoft IIS Webserver Detection (HTTP). The table is sorted by severity in descending order, with the highest severity being 9.3 (High).

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
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.

The screenshot displays the SimpleRisk Enterprise Risk Management web application. The browser window title is "Managing Technical Vulnerabilities (3e)". The address bar shows a "Not secure" connection to "https://172.30.0.5/management/index.php". The page header includes the SimpleRisk logo and navigation tabs: Governance, Risk Management (active), Compliance, Asset Management, Assessments, Reporting, and Configure. A search icon and an "Admin" link are also present. Below the header, a sidebar on the left contains a vertical list of steps: 1. Submit Risk (highlighted in red), 2. Plan Mitigation, 3. Perform Reviews, 4. Plan Projects, and 5. Review Regularly. The main content area shows a risk entry for "ID: 1001 Ex...". The risk details include: Inherent Risk of 6.8 (Medium), Residual Risk of 6.8 (Medium), ID #: 1001, Status: New, and Subject: "Exploitation of SMB remote code execution vulnerability by an internal threat". Below the risk summary, there are links for "View Risk Scoring Details" and "Show Risk Score Over Time". A tabbed interface at the bottom shows "Details" (selected), "Mitigation", and "Review". The "Details" tab contains fields for Risk Mapping (Unauthorized access), Submission Date (03/16/2025), Category (Technical Vulnerability Man), Site/Location, External Reference ID, Control/Regulation, Submitted By (Admin), Risk Source (System), Risk Scoring Method (CVSS), and Risk Assessment. The Windows taskbar at the bottom shows the time as 11:54 AM on 3/16/2023.

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