

# Managing Technical Vulnerabilities (3e)

Managing Risk in Information Systems, Third Edition - Lab 06

Student:

Courtney Watson

Email:

courtney.watson55@gmail.com

Time on Task:

17 hours, 12 minutes

Progress:

100%

Report Generated: Wednesday, April 2, 2025 at 9:43 PM

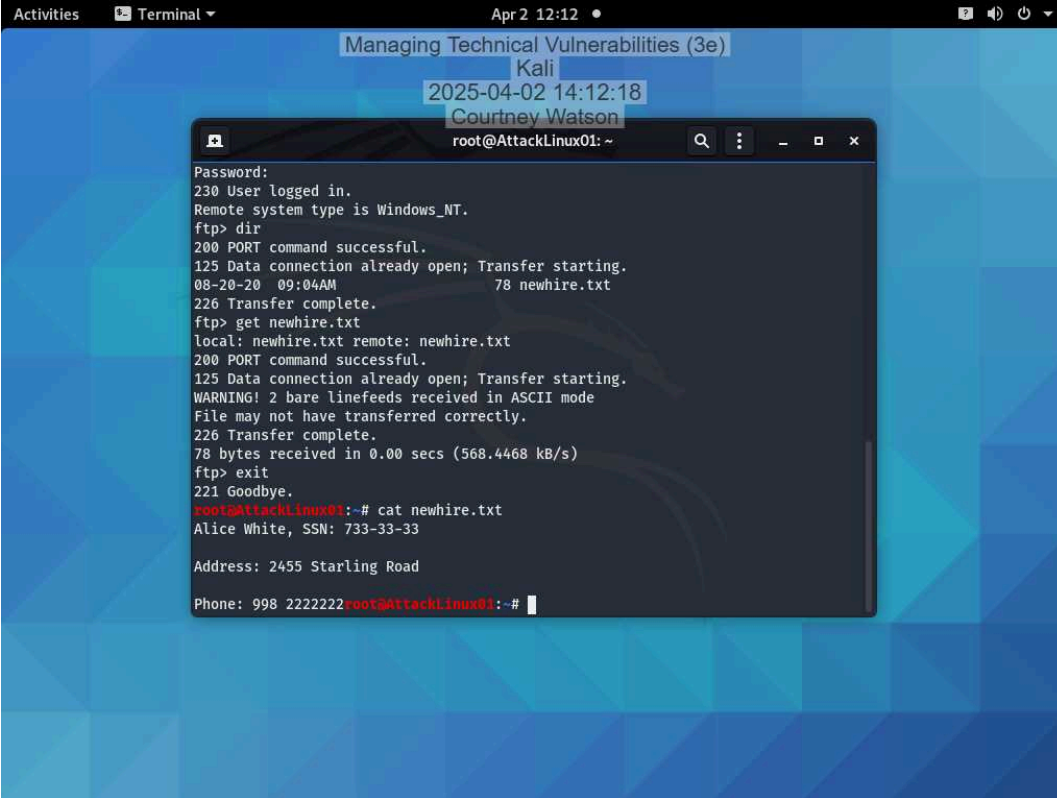
## Guided Exercises

### 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 Apr 2 12:00 • Managing Technical Vulnerabilities (3e) Kali 2025-04-02 14:00:04 Courtney Watson root@AttackLinux01: ~  
Nmap scan report for 172.30.0.3  
Host is up (0.00034s 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: 00:50:56:BD:F8:BC (VMware)  
  
Nmap scan report for 172.30.0.5  
Host is up (0.00030s latency).  
  
PORT      STATE SERVICE  
21/tcp    closed ftp  
MAC Address: 00:50:56:BD:C2:E4 (VMware)  
  
Nmap scan report for 172.30.0.4  
Host is up (0.00033s latency).  
  
PORT      STATE SERVICE  
21/tcp    closed ftp  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.19 seconds  
root@AttackLinux01: ~#
```

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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following text:

```
Activities Terminal Apr 2 12:12 •
Managing Technical Vulnerabilities (3e)
Kali
2025-04-02 14:12:18
Courtney Watson
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 (568.4468 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.

Mac Address 00:50:56:BD:CE:A6 port is open and not vulnerable MAC address 00:50:56:BD:F8:BC port is open and vulnerable MAC address 00:50:56:BD:C2:E4 port is closed 172.30.0.4 port is closed

## 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) interface in a web browser. The browser's address bar shows the URL `https://127.0.0.1:9392/results`. The GSA interface has a green header with the logo and a navigation bar with tabs: 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 first vulnerability listed is 'Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)' with a severity of 9.3 (High) and a QoD of 95%. Other vulnerabilities include 'Anonymous FTP Login Reporting', 'DCE/RPC and MSRPC Services Enumeration Reporting', 'FTP Unencrypted Cleartext Login', 'SSL/TLS: Report Weak Cipher Suites', 'TCP timestamps', 'Services', 'HTTP Server Banner Enumeration', and 'Traceroute'. At the bottom of the interface, there is a message: 'It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!' with a 'Refresh Iceweasel...' button.

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	Wed, Apr 2, 2025 7:49 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.30.0.3		21/tcp	Wed, Apr 2, 2025 7:45 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.9 (Medium)	80 %	172.30.0.3		135/tcp	Wed, Apr 2, 2025 7:47 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	172.30.0.3		21/tcp	Wed, Apr 2, 2025 7:45 PM UTC
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98 %	172.30.0.3		3389/tcp	Wed, Apr 2, 2025 7:46 PM UTC
TCP timestamps	2.6 (Low)	80 %	172.30.0.3		general/tcp	Wed, Apr 2, 2025 7:41 PM UTC
Services	0.0 (Log)	80 %	172.30.0.3		80/tcp	Wed, Apr 2, 2025 7:41 PM UTC
Services	0.0 (Log)	80 %	172.30.0.3		22/tcp	Wed, Apr 2, 2025 7:41 PM UTC
HTTP Server Banner Enumeration	0.0 (Log)	80 %	172.30.0.3		5985/tcp	Wed, Apr 2, 2025 7:46 PM UTC
Traceroute	0.0 (Log)	80 %	172.30.0.3		general/tcp	Wed, Apr 2, 2025 7:42 PM UTC

## 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 address bar shows the URL <https://172.30.0.5/management/index.php>. The application header includes navigation tabs: Governance, Risk Management (active), Compliance, Asset Management, Assessments, Reporting, and Configure. A search bar and an 'Admin' dropdown are also present.

The main content area shows a risk entry for ID: 1001. On the left, a vertical sidebar contains five steps: 1. Submit Risk (highlighted in red), 2. Plan Mitigation, 3. Perform Reviews, 4. Plan Projects, and 5. Review Regularly. The risk details are displayed in a card format:

- 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

Below the risk card, there are links for 'View Risk Scoring Details' and 'Show Risk Score Over Time'. A tabbed interface at the bottom shows 'Details' (active), 'Mitigation', and 'Review'. The 'Details' tab contains the following information:

Risk Mapping:	Unauthorized access	Submitted By:	Admin
Submission Date:	04/02/2025	Risk Source:	System
Category:	Technical Vulnerability Man	Risk Scoring Method:	CVSS
Site/Location:	Risk Assessment:		

The Windows taskbar at the bottom shows the system clock as 1:24 PM on 4/2/2025.

### Challenge Exercise

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

IP address: 172.30.0.2 Operating system: Microsoft Windows Server 2012 Open ports:  
135-139-445-3389-5901-5985 and listed below

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

172.30.0.3 operating system windows server 2016 open ports 445, 636, 593, 3269, 88, 464, 389, 53,  
139, 22, 3389, 21

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

IP address 172.30.0.4 operating system linux all ports closed

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

IP address 172.30.0.5 operating system VMWARE open ports 443, 80