Student: Bradley Adams	Email: badams10@my.athens.edu

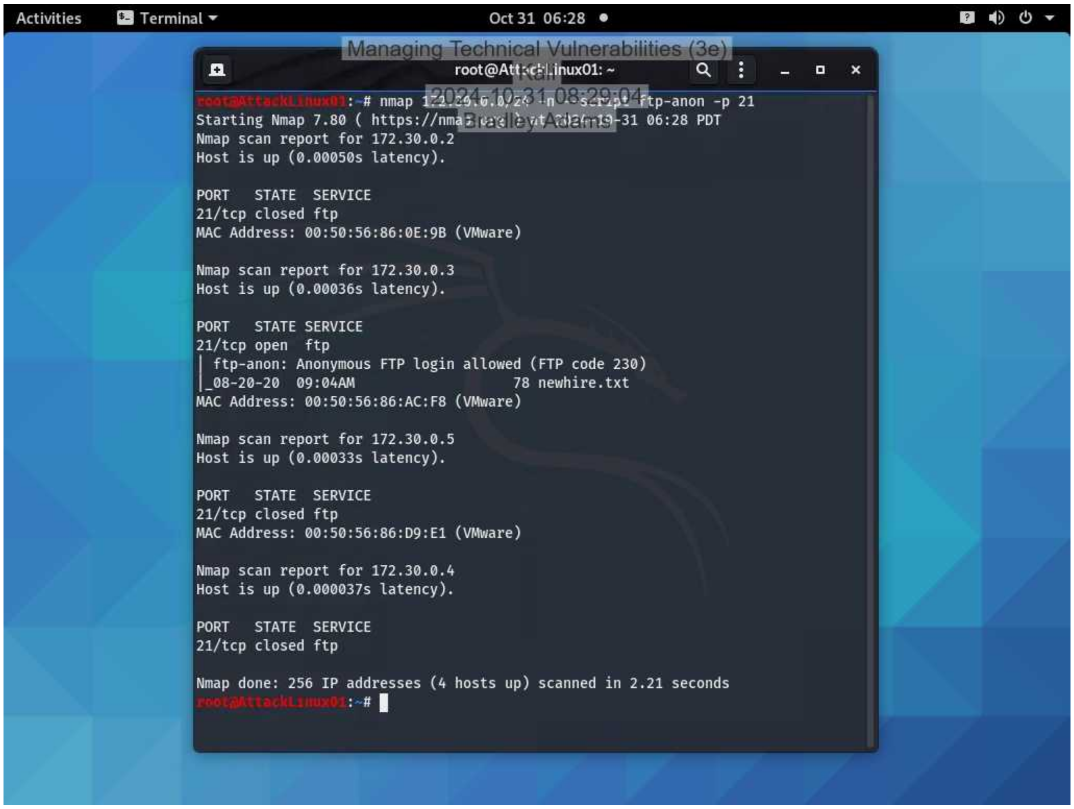
Time on Task: 2 hours, 41 minutes	Progress: 100%

Report Generated: Thursday, October 31, 2024 at 1:04 PM

Guided Exercises

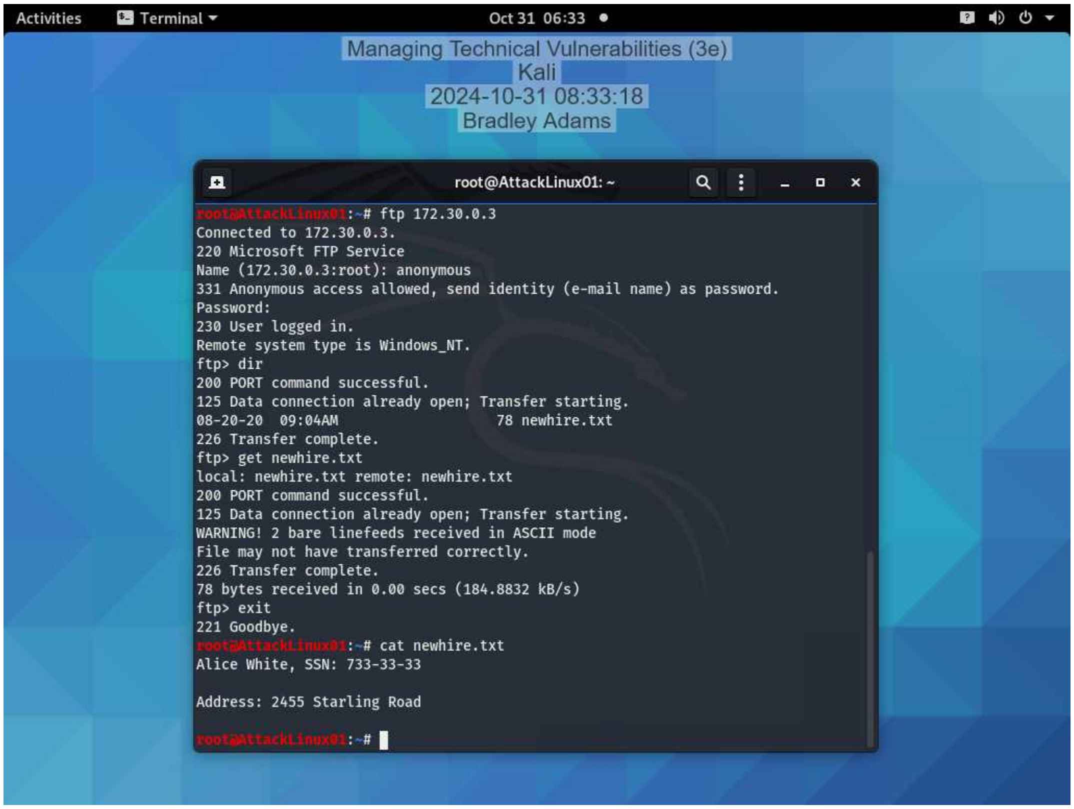
Part 1: Perform a Vulnerability Scan with Nmap

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



```
root@AttackLinux01:~# nmap 172.30.0.0/24 -n --script ftp-anon -p 21
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-31 06:28 PDT
Nmap scan report for 172.30.0.2
Host is up (0.00050s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 00:50:56:86:0E:9B (VMware)

Nmap scan report for 172.30.0.3
Host is up (0.00036s 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: 00:50:56:86:AC:F8 (VMware)

Nmap scan report for 172.30.0.5
Host is up (0.00033s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 00:50:56:86:D9:E1 (VMware)

Nmap scan report for 172.30.0.4
Host is up (0.000037s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.21 seconds
root@AttackLinux01:~#
```

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



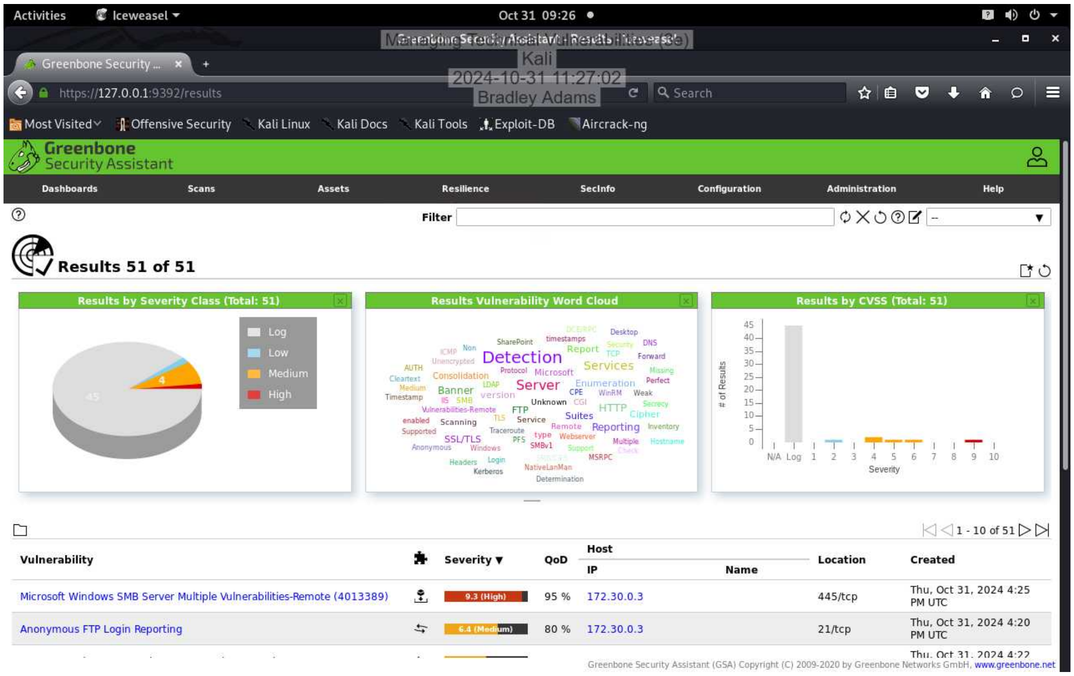
```
root@AttackLinux01:~# ftp 172.30.0.3
Connected to 172.30.0.3.
220 Microsoft FTP Service
Name (172.30.0.3:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 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 (184.8832 kB/s)
ftp> exit
221 Goodbye.
root@AttackLinux01:~# cat newhire.txt
Alice White, SSN: 733-33-33

Address: 2455 Starling Road

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 vulnerable, 172.30.0.4 = port 445 closed not vulnerable, 172.30.0.5 = port 445 closed 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.**



Results 51 of 51

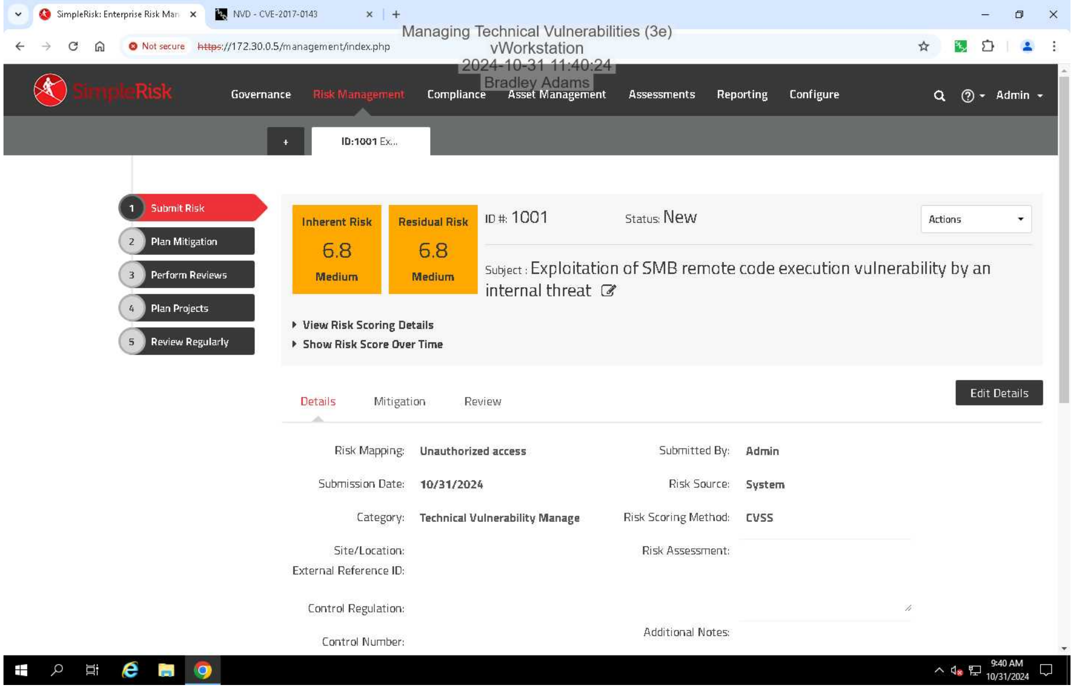
1 - 10 of 51

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95 %	172.30.0.3		445/tcp	Thu, Oct 31, 2024 4:25 PM UTC
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	172.30.0.3		21/tcp	Thu, Oct 31, 2024 4:20 PM UTC
							Thu, Oct 31, 2024 4:22

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**.



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

Submission Date: 10/31/2024

Category: Technical Vulnerability Manage

Site/Location:

External Reference ID:

Control Regulation:

Control Number:

Submitted By: Admin

Risk Source: System

Risk Scoring Method: CVSS

Risk Assessment:

Additional Notes:

Challenge Exercise

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

172.30.0.2, MS Windows Longhorn, ports open(135/tcp, 139/tcp/ 445/tcp, 3389/tcp, 5901/tcp)

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

172.30.0.3, Microsoft Windows Server 2016 build 10586-14393, open ports(21, 22, 53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389 all tcp)

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

172.30.0.4, Linux 2.6.32, open ports (22/tcp, 111/tcp)

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

172.30.0.5, Linux 2.6.32, open ports (80/tcp, 443/tcp)