

Student:

Kaleb Alstott

Email:

alstottk1@mymail.nku.edu

Time on Task:

1 hour, 20 minutes

Progress:

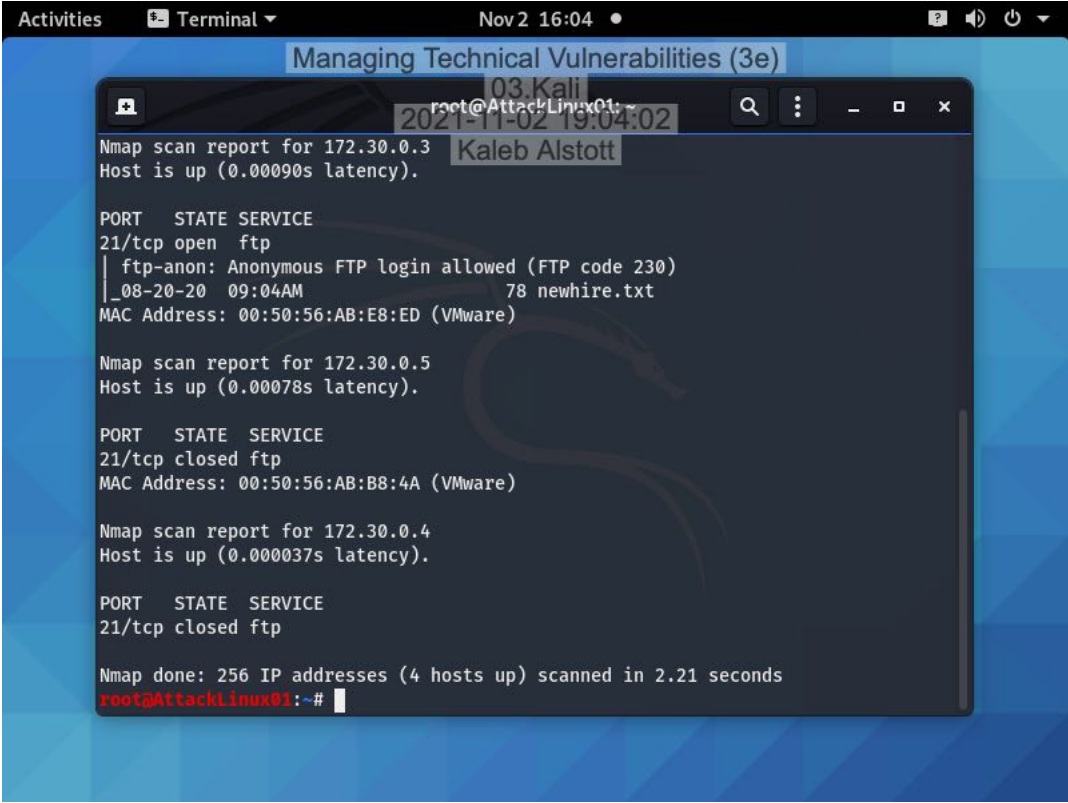
100%

Report Generated: Tuesday, November 2, 2021 at 8:13 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 Nov 2 16:04
Managing Technical Vulnerabilities (3e)
root@AttackLinux01:~#
2021-11-02 19:04:02 Kaleb Alstott

Nmap scan report for 172.30.0.3
Host is up (0.00090s 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:AB:E8:ED (VMware)

Nmap scan report for 172.30.0.5
Host is up (0.00078s latency).

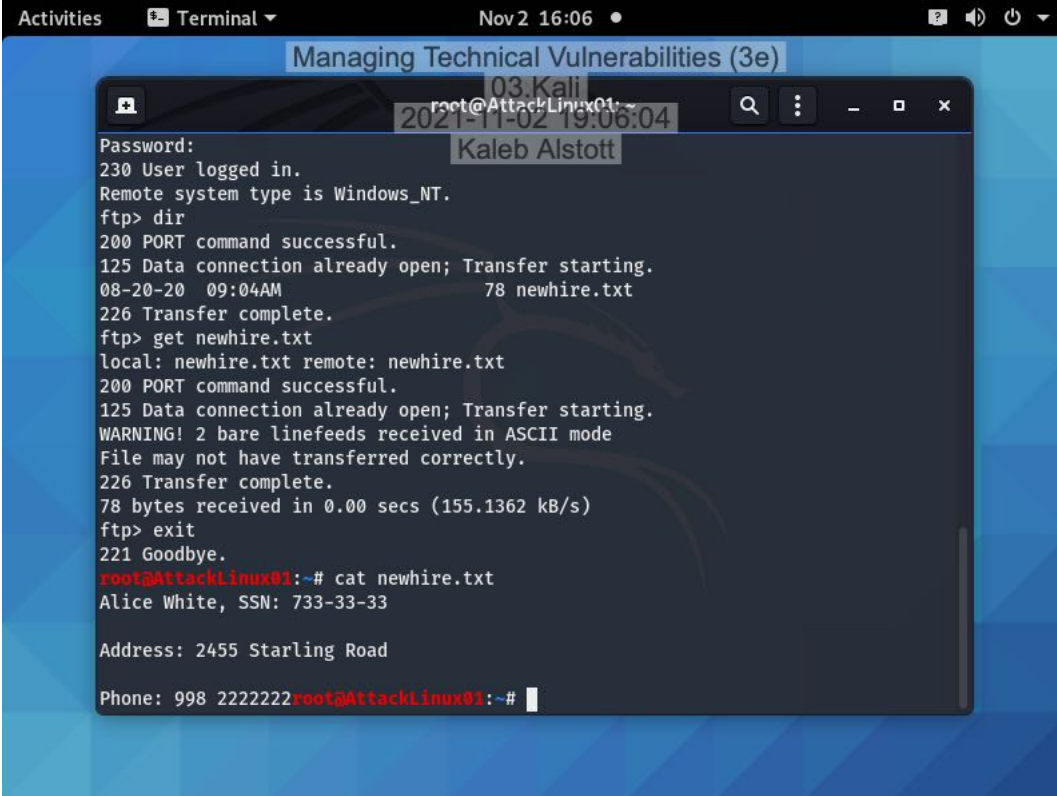
PORT      STATE SERVICE
21/tcp    closed ftp
MAC Address: 00:50:56:AB:B8:4A (VMware)

Nmap scan report for 172.30.0.4
Host is up (0.00037s 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**.



The screenshot shows a terminal window titled "Terminal" with a date and time of "Nov 2 16:06". The terminal output is as follows:

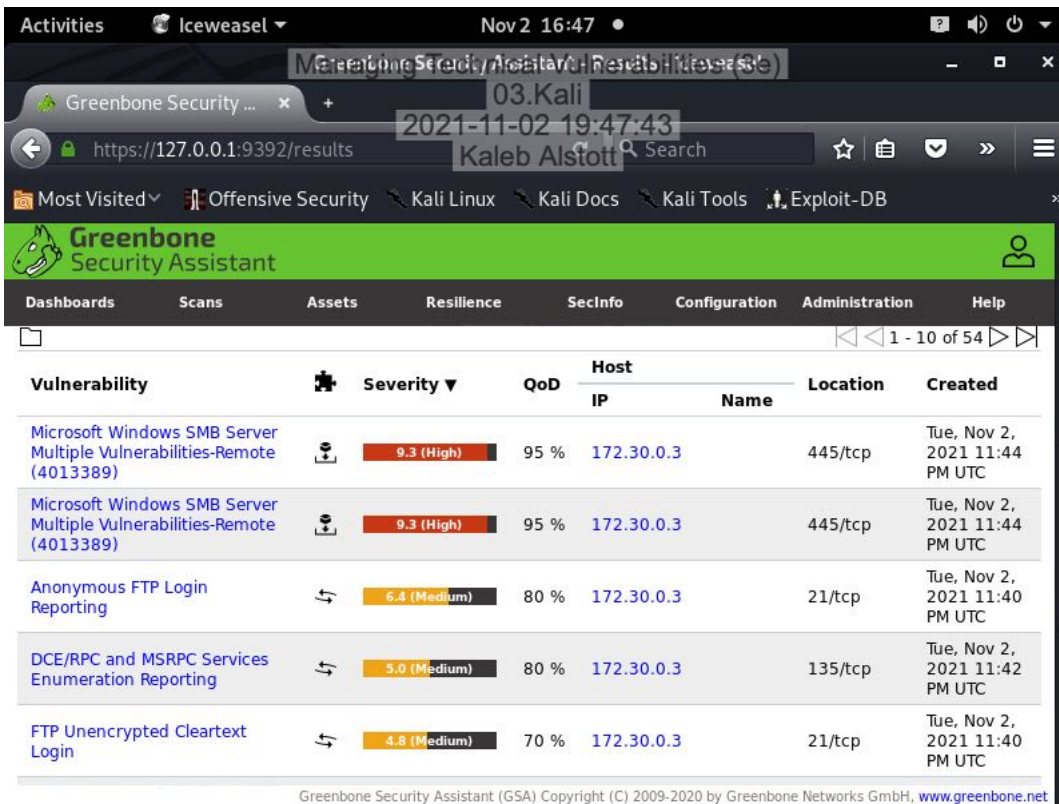
```
root@AttackLinux01:~#  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> dir  
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
08-20-20 09:04AM 78 newhire.txt  
226 Transfer complete.  
ftp> get newhire.txt  
local: newhire.txt remote: 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 (155.1362 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 - 445 is open and is not vulnerable 173.30.0.3 - 445 is open and is vulnerable 172.30.0.4 - 445 is closed 172.30.0.5 - 445 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 displays the URL `https://127.0.0.1:9392/results`. The GSA interface has a green header with the logo and a navigation menu with tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the header, there is a table of detected vulnerabilities. The table has columns for Vulnerability, Severity, QoD, Host IP, Name, Location, and Created. The first two rows show 'Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)' with a severity of 9.3 (High) and a QoD of 95%. The other rows show 'Anonymous FTP Login Reporting' (6.4 Medium), 'DCE/RPC and MSRPC Services Enumeration Reporting' (5.0 Medium), and 'FTP Unencrypted Cleartext Login' (4.8 Medium).

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	Tue, Nov 2, 2021 11:44 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95 %	172.30.0.3		445/tcp	Tue, Nov 2, 2021 11:44 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.30.0.3		21/tcp	Tue, Nov 2, 2021 11:40 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.30.0.3		135/tcp	Tue, Nov 2, 2021 11:42 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	172.30.0.3		21/tcp	Tue, Nov 2, 2021 11:40 PM UTC

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 shows the URL <https://172.30.0.3/management/vulnerabilities>. The page title is "Managing Technical Vulnerabilities (3e)". The user is logged in as "Kaleb Alstott" on "2021-11-02 19:56:54".

The interface features a sidebar with a navigation menu containing five items: "1 Submit Risk", "2 Plan Mitigation", "3 Perform Reviews", "4 Plan Projects", and "5 Review Regularly". The "Submit Risk" item is highlighted in red.

The main content area displays a risk entry for ID # 1001, Status: New. The risk is titled "Subject: Exploitation of SMB remote code execution vulnerability by an internal threat". The risk is categorized as "Inherent Risk 6.8 Medium" and "Residual Risk 6.8 Medium". Below the risk details, there are two expandable sections: "View Risk Scoring Details" and "Show Risk Score Over Time".

The "Details" tab is selected, showing the following information:

- Risk Mapping: Unauthorized access
- Submitted By: Admin
- Submission Date: 11/02/2021
- Risk Source: System
- Category: Technical Vulnerability M
- Risk Scoring: CVSS
- Method:
- Site/Location:
- External Reference ID:
- Risk Assessment:

The Windows taskbar at the bottom shows the time as 4:56 PM on 11/2/2021.

Challenge Exercise

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

IP address- 172.30.0.2 OS- Windows Open Ports- 139, 445, and 3389

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

IP address - 172.30.0.30 OS- Windows Open Ports - 21, 22, 53, 80, 88, 135, 139, 389, 445, and 3389

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

IP address- 172.30.0.4 OS- Linux Open Ports- 22 and 111

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

IP address - 172.30.0.5 OS- Windows Open Ports- 80 and 443