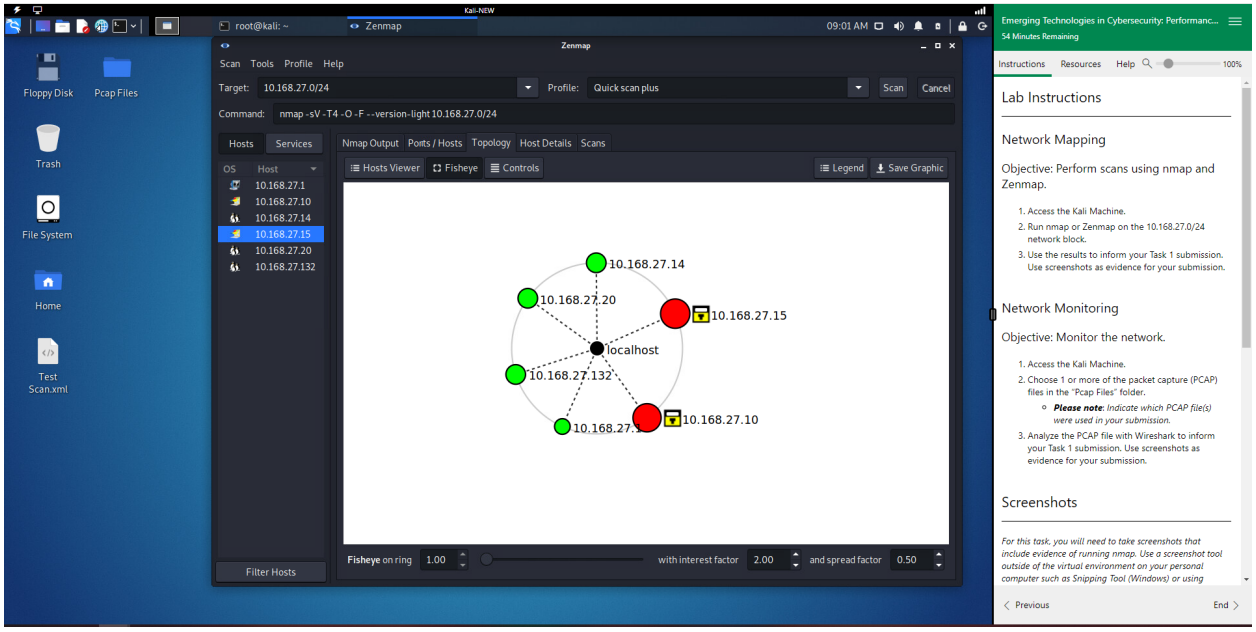
C844 Task 1: NMAP and Wireshark.

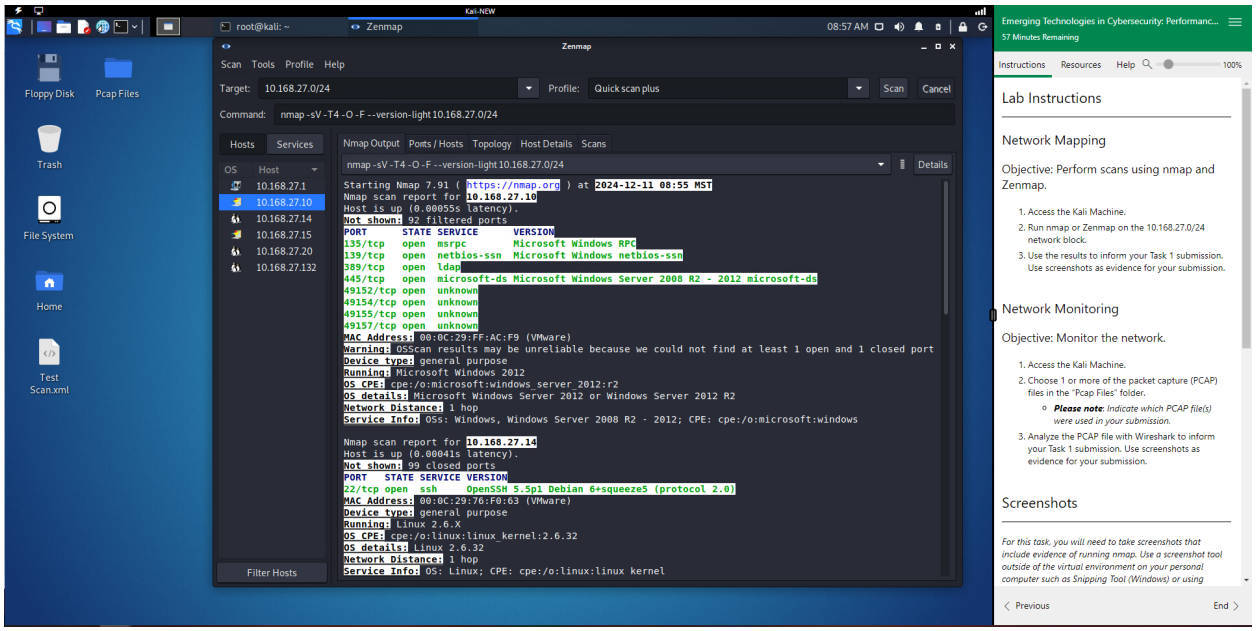
By Griffin Haas

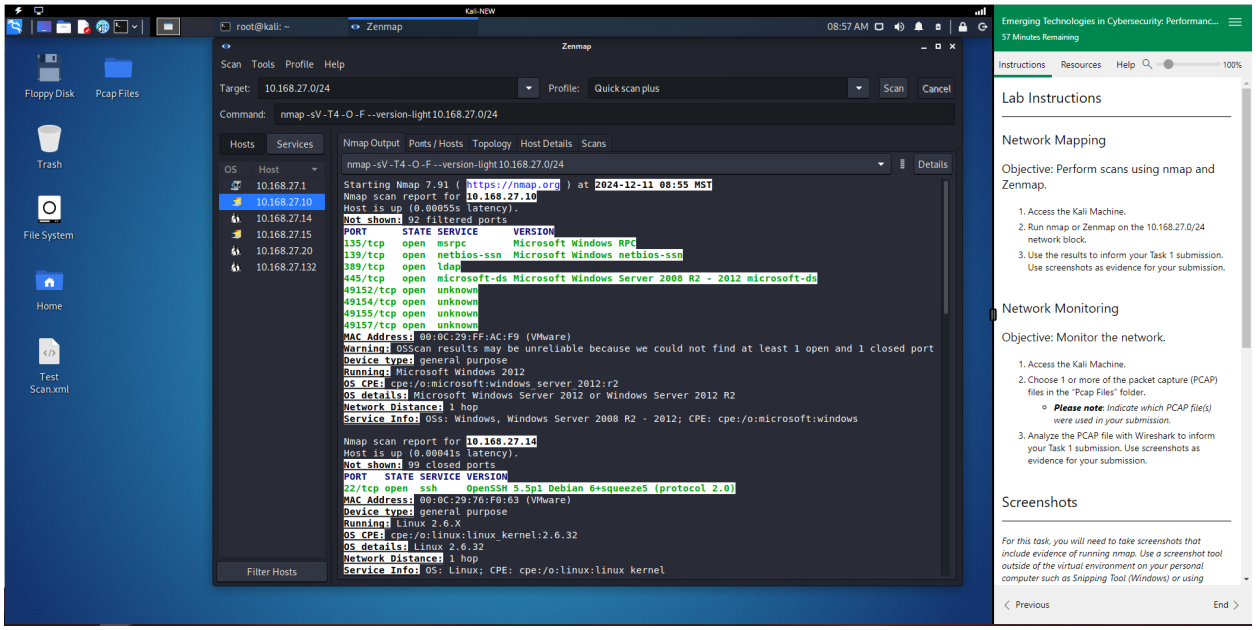
Network Scanning and Topology

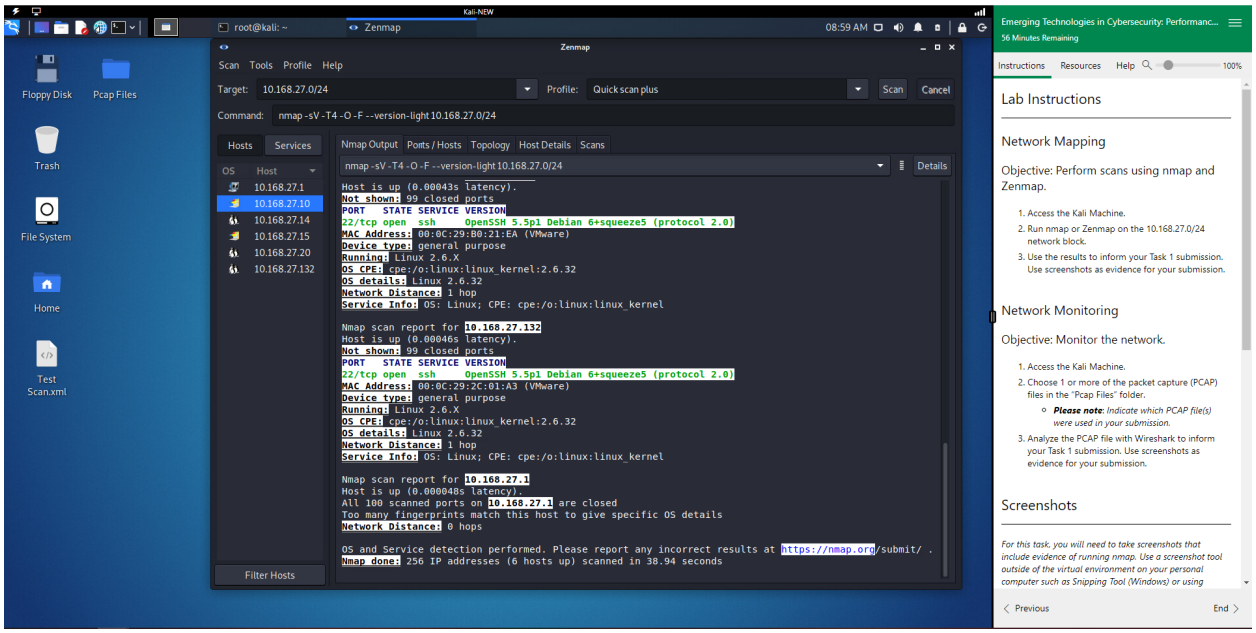
In this lab, we started by scanning the subnet 10.168.27.0/24. When the scan was completed, it gave us six machines: two Microsoft Windows server machines, three Linux Machines, and a router.



This scan shows us that the network is a star. Here is the list of open ports and running services on each machine.


Kali-NEW
root@kali: ~
Zenmap
08:57 AM
Zenmap
Scan Tools Profile Help
Target: 10.168.27.0/24
Profile: Quick scan plus
Scan Cancel
Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24
Hosts Services
OS Host
10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.132
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sV -T4 -O -F --version-light 10.168.27.0/24
Details
Starting Nmap 7.91 (https://nmap.org) at 2024-12-11 08:55 MST
Nmap scan report for 10.168.27.10
Host is up (0.00055s latency).
Not shown: 92 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49157/tcp open unknown
MAC Address: 00:0C:29:FF:AC:F9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.168.27.14
Host is up (0.00041s latency).
Not shown: 99 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:76:F0:63 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
Floppy Disk
Pcap Files
Trash
File System
Home
Test Scan.xml
Emerging Technologies in Cybersecurity: Performanc...
57 Minutes Remaining
Instructions Resources Help 100%
Lab Instructions
Network Mapping
Objective: Perform scans using nmap and Zenmap.
1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.
Network Monitoring
Objective: Monitor the network.
1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the "Pcap Files" folder.
Please note: Indicate which PCAP file(s) were used in your submission.
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.
Screenshots
For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using
Previous
End


Kali-NEW
root@kali: ~
Zenmap
08:57 AM
Zenmap
Scan Tools Profile Help
Target: 10.168.27.0/24
Profile: Quick scan plus
Scan Cancel
Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24
Hosts Services
OS Host
10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.132
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sV -T4 -O -F --version-light 10.168.27.0/24
Details
Starting Nmap 7.91 (https://nmap.org) at 2024-12-11 08:55 MST
Nmap scan report for 10.168.27.10
Host is up (0.00055s latency).
Not shown: 92 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49157/tcp open unknown
MAC Address: 00:0C:29:FF:AC:F9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.168.27.14
Host is up (0.00041s latency).
Not shown: 99 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:76:F0:63 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
Floppy Disk
Pcap Files
Trash
File System
Home
Test Scan.xml
Emerging Technologies in Cybersecurity: Performanc...
57 Minutes Remaining
Instructions Resources Help 100%
Lab Instructions
Network Mapping
Objective: Perform scans using nmap and Zenmap.
1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.
Network Monitoring
Objective: Monitor the network.
1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the "Pcap Files" folder.
Please note: Indicate which PCAP file(s) were used in your submission.
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.
Screenshots
For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using
Previous
End



Vulnerabilities, The Implications and Solution.

The first vulnerability we will be looking at will be **CVE-2023-38408**. This vulnerability is shown to be on 10.168.27.15, 10.168.27.14, and 10.168.27.132. This vulnerability occurs in OpenSSH before 9.3p2. In which the service has an untrustworthy search path, allowing attackers to perform remote code execution. Which means an attacker could execute malicious code through this vulnerability.

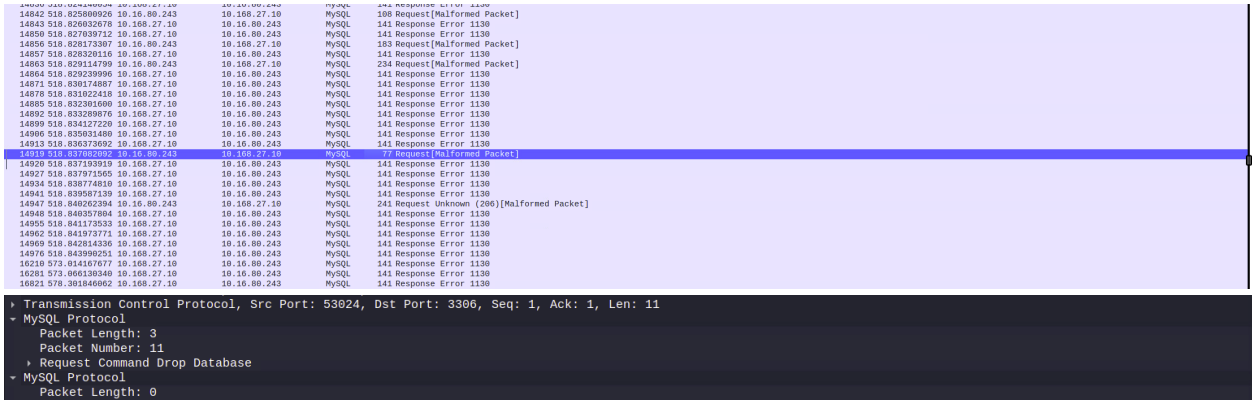
The next vulnerability will be **CVE-2016-1908** which is found on all machines listed on the previous vulnerability. This vulnerability occurs in versions of OpenSSH before 7.2. This vulnerability mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access control decisions. Which allows remote X11 clients to obtain trusted X11 forwarding privileges by leveraging configuration issues. X11 forwarding is an SSH protocol that enables users to run graphical applications on a remote server and interact with the system. If attackers are allowed to obtain trusted X11 forwarding privileges, it would allow them to perform actions the machine with no authentication.

The final vulnerability we will be looking at is **CVE-2015-5600** which is found on all machines listed in the first vulnerability. This vulnerability affects OpenSSH versions through 6.9. The kbdint_next_device function in the file auth2-chall.c in sshd does not properly restrict the processing of keyboard-interactive within a single connection, allowing the execution of brute force attacks from remote attackers or causing a DOS (Denial-of-service) attack.

All these vulnerabilities are caused by using a legacy version of OpenSSH. The recommended solution to these vulnerabilities would be to upgrade OpenSSH to a version that is greater than 9.3p2. Preferably the most current version, which is 9.9p2. This allows all listed vulnerabilities to be patched, as well as many others I did not list.

Wireshark Anomalies, Implications, and Solutions.

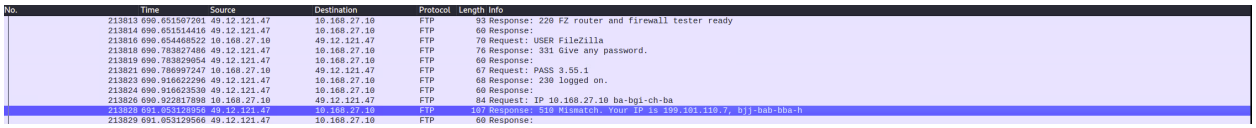
While looking through the first .pcap file, there are many anomalies we can see throughout the recorded packets. The first anomaly we see is between 14927 and 16821. These packets are shown to be from the MySQL service. In these next screenshots you can see some malformed packets that seem to try execute code through these packets.



You can see that the drop database command was used which tries to delete the database. This implies that an attacker is attempting to connect to the database and try to execute commands.

To fix this anomaly, a solution is to use a version of MySql that uses TLS. Setting up MySql with TLS will encrypt the commands using certificates to verify the user executing commands.

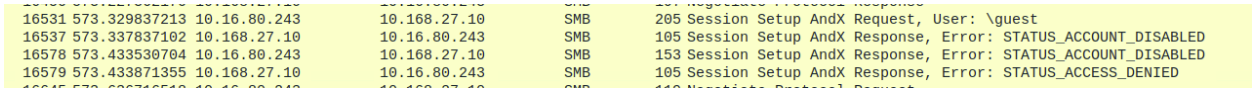
FTP packets between 213816-213828 show a user successfully logging into an FTP server and attempting to download data. Fortunately, it seems that the IP was rejected as it was an IP out of network.



No.	Time	Source	Destination	Protocol	Length	Info
213813	690.651507201	49.12.121.47	10.168.27.10	FTP	93	Response: 220 FZ router and firewall tester ready
213814	690.651514416	49.12.121.47	10.168.27.10	FTP	60	Response:
213816	690.654468522	10.168.27.10	49.12.121.47	FTP	70	Request: USER FileZilla
213818	690.783827486	49.12.121.47	10.168.27.10	FTP	76	Response: 331 Give any password.
213819	690.783829054	49.12.121.47	10.168.27.10	FTP	60	Response:
213821	690.786997247	10.168.27.10	49.12.121.47	FTP	67	Request: PASS 3.55.1
213823	690.916622296	49.12.121.47	10.168.27.10	FTP	68	Response: 230 logged on.
213824	690.916623530	49.12.121.47	10.168.27.10	FTP	60	Response:
213826	690.922817898	10.168.27.10	49.12.121.47	FTP	84	Request: IP 10.168.27.10 ba-bgi-ch-ba
213828	691.053128956	49.12.121.47	10.168.27.10	FTP	107	Response: 510 Mismatch, Your IP is 199.101.110.7, bjj-bab-bba-h
213829	691.053129566	49.12.121.47	10.168.27.10	FTP	60	Response:

A solution to this kind of anonmaly would be to stop any FTP traffic through the firewall.

The final anomaly occurs in SMB packets between 16537-16645 shows a user attempt to login to an account named guest. However the account get's disabled then denied. This implies an attacker brute forcing accounts on servers with an SMB server.



16531	573.329837213	10.16.80.243	10.168.27.10	SMB	205	Session Setup AndX Request, User: \guest
16537	573.337837102	10.168.27.10	10.16.80.243	SMB	105	Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
16578	573.433530704	10.16.80.243	10.168.27.10	SMB	153	Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
16579	573.433871355	10.168.27.10	10.16.80.243	SMB	105	Session Setup AndX Response, Error: STATUS_ACCESS_DENIED

A good solution to this problem would be to disable the guest account and block remote SMB traffic.

Works Cited

Divinsky, Yair. “How to Fix CVE-2023-38408 in OpenSSH.” *Vulcan Cyber*, 20 July 2023, vulcan.io/blog/how-to-fix-cve-2023-38408-in-openssh/.

“MySQL :: MySQL 8.4 Reference Manual :: 8.3 Using Encrypted Connections.” *Mysql.com*, 2024, dev.mysql.com/doc/refman/8.4/en/encrypted-connections.html.

NIST. “NVD - CVE-2023-38408.” *Nvd.nist.gov*, 2023, nvd.nist.gov/vuln/detail/CVE-2023-38408.

“NVD - Cve-2015-5600.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/cve-2015-5600.

“NVD - Cve-2016-1908.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/cve-2016-1908.

PatAltimore. “Secure SMB Traffic in Windows Server.” *Learn.microsoft.com*, learn.microsoft.com/en-us/windows-server/storage/file-server/smb-secure-traffic.