A. Describe the network topology you found when running Nmap. Include screenshots as evidence of running Nmap.

Nmap discovered six hosts on the 10.168.27.0/24 subnet, displaying a star topology. This network topology is described as endpoint devices all connecting to a central host such as a switch or hub. Nmap is an open-source software that can be downloaded and used from the command line or using Zenmap, a graphical user interface for Nmap. Nmap uses scanning techniques in various ways to discover network hosts for open ports and vulnerabilities. This tool is used for security testing, port scanning, vulnerability detection, network inventory, and rogue system detection.

Figure A1. Zenmap Network Topology Evidence (Screenshot).

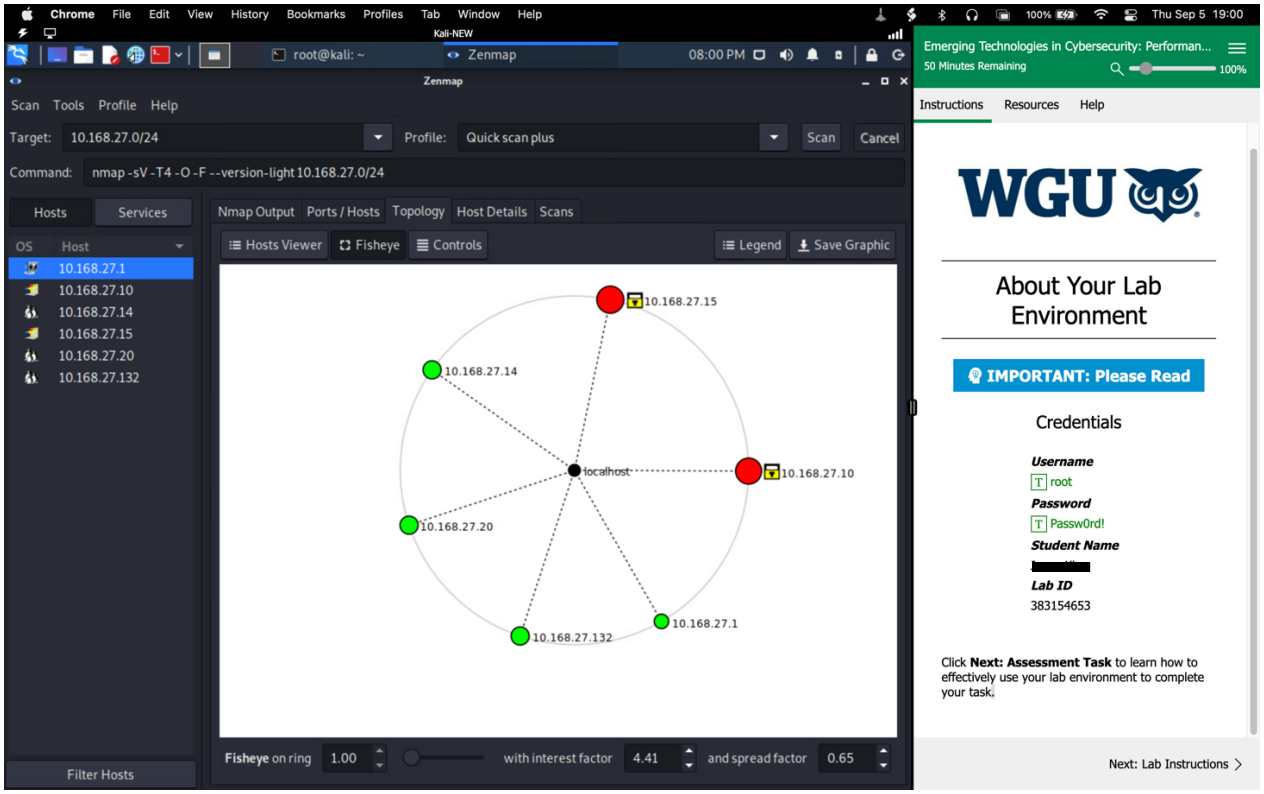


Figure A2. Network Topology, 6 hosts discovered on subnet 10.168.27.0/24

Host	OS	# Open Ports	Notable Ports Used	IPv4	IPv6	MAC
10.168.27.1	N/A	0	0	IPv4	N/A	N/A
10.168.27.10	Microsoft Server 2012 or Windows Server 2012 R2	8	TCP 389 (LDAP)	IPv4	N/A	00:0C:29:08:A1:4F
10.168.27.14	Linux 2.6.X (32)	1	TCP 22 (SSH)	IPv4	N/A	00:0C:29:AB:DD:C9
10.168.27.15	Microsoft Server 2008 RD or Windows 8.1	10	TCP 21 (FTP)	IPv4	N/A	00:15:5D:01:80:07
10.168.27.20	Linux 2.6.X(32)	1	TCP 22 (SSH)	IPv4	N/A	00:0C:29:40:D9:59
10.168.27.132	Linux 2.6.x	1	TCP 22 (SSH)	IPv4	N/A	00:0c:29:75:95:be

Figure A3. Nmap screenshot evidence 1

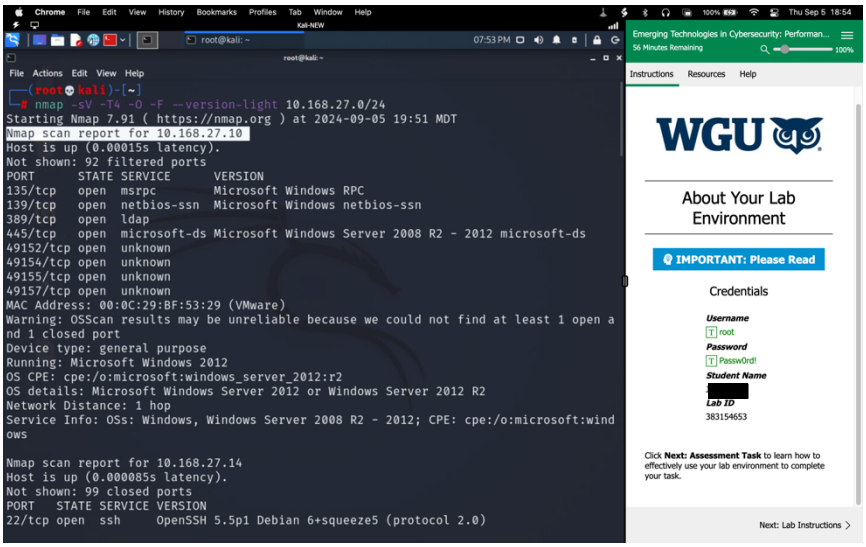


Figure A4. Nmap evidence screenshot 2

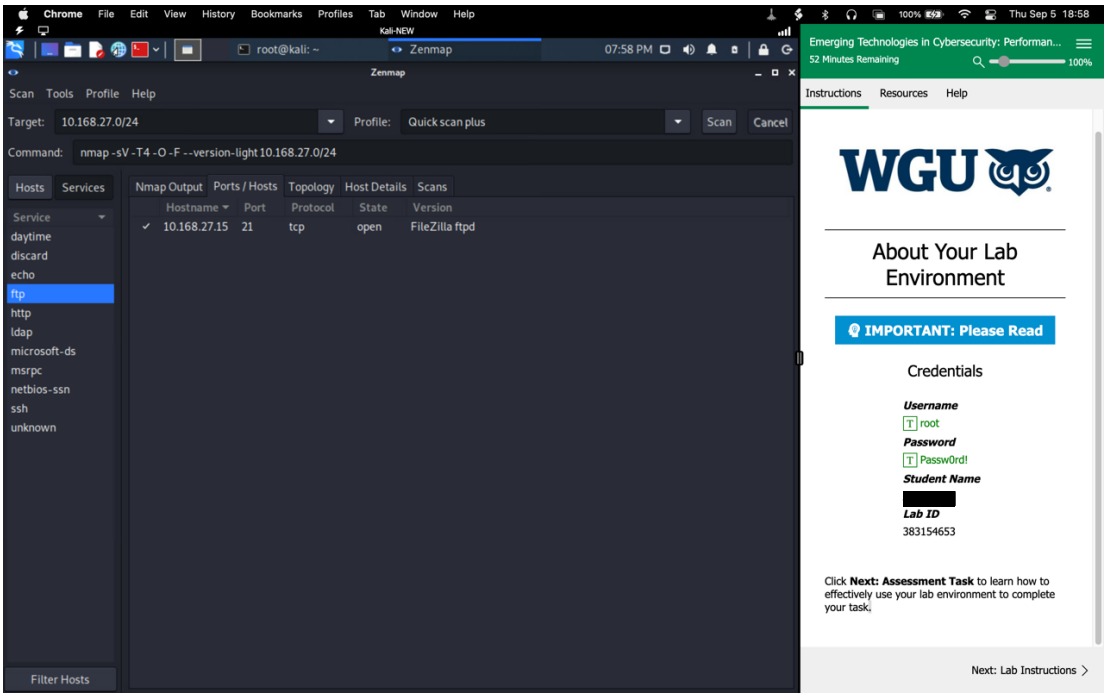
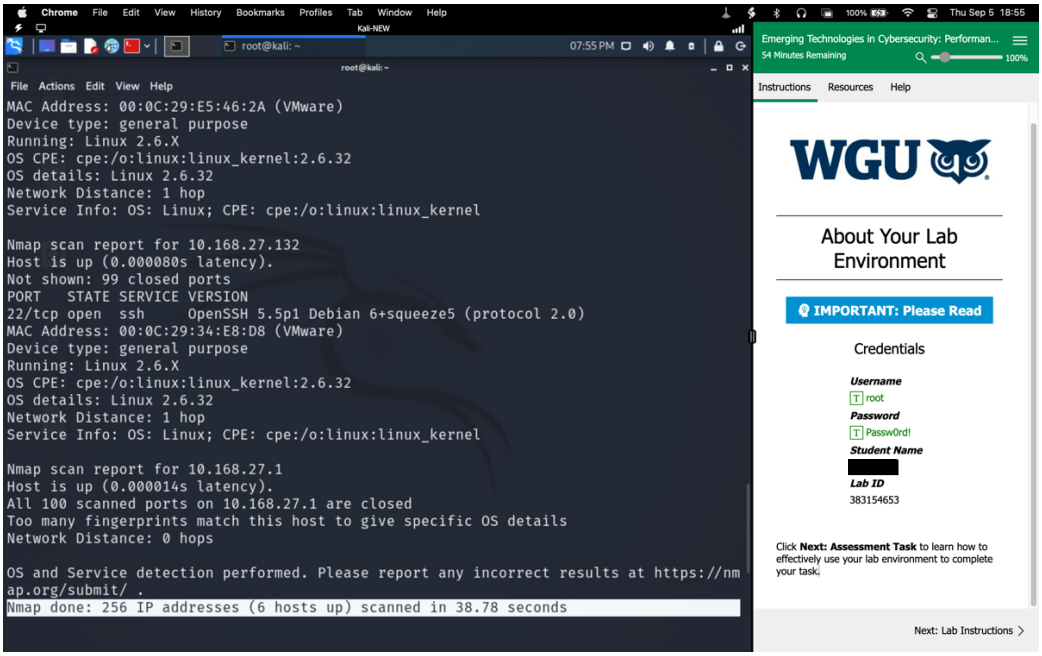


Figure A5. Nmap evidence screenshot 3



B. Summarize the vulnerabilities on the network and their potential implications based on your Nmap results.

1. **Host 10.168.27.10:**
    - **Vulnerability:** The host is running an insecure operating system on Windows Server 2012 R2, which is affected by the “Windows Runtime Elevation of Privilege Vulnerability" (CVE-2019-0570).

    - **Implications:** This vulnerability allows an elevation of privilege when Windows Runtime mishandles objects in memory. This allows the attacker unauthorized access to sensitive to data or execute arbitrary commands through the affected system.

2. **Host 10.168.27.15:**

    - **Vulnerability**: The host is running FTP on port 21, which uses clear-text passwords and usernames for authentication without encrypting communications. WS_FTP server versions before 2022.0.7 (8.8.7) allow users to bypass the second-factor verification and log in with just their username and password (CVE-2024-7745).

    - **Implications**: This vulnerability allows attackers to bypass the multi-factor authentication implementation, providing attackers with unauthorized access and interception of user credentials.

3. **Host 10.168.27.132:**

    - **Vulnerability**: The host is running an insecure Linux version kernel 2.6.32. This vulnerability is affected by the stack-based overflow in the Marvell WIFI chip driver (CVE-2019-14897).

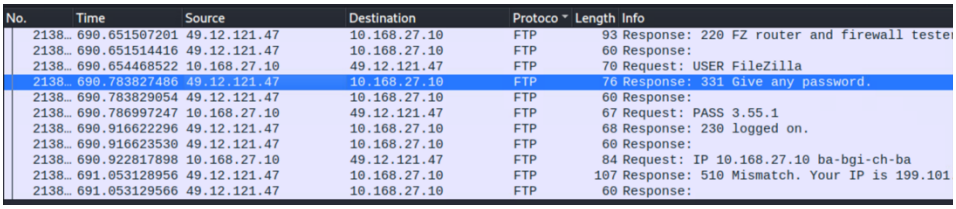
    - **Implications**: The stack-based overflow vulnerability allows an attacker to execute arbitrary code or lead to a system crash (DoS). This can grant an attacker kernel-level privileges to run malicious code to compromise a system.

C. Describe the anomalies you found when running Wireshark, on the network capture file, and include evidence of the range of packets associated with *each anomaly*.

The Wireshark packet capture used to identify anomalies on the network capture file was Pcap pcap1.pcapng.

1. **Anomaly 1: Cleartext username and password authentication using FTP.**

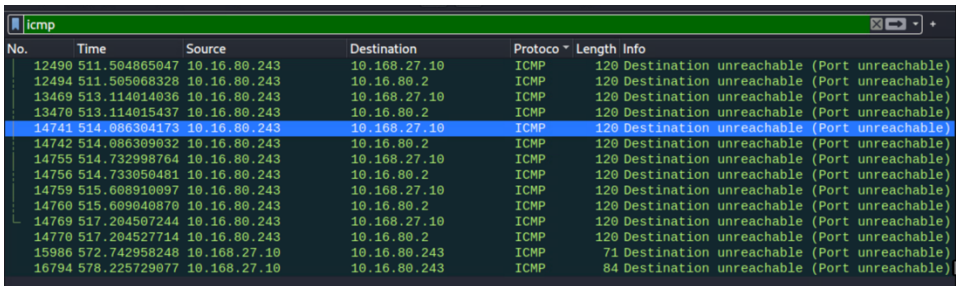
    - The first anomaly discovered was the clear text username and password communication between client and server using FTP port 21. The FTP commands USER and PASS were found in the packet details. An attacker can perform packet sniffing on the network and spoof a user's credentials to gain unauthorized access to a Company's network.



No.	Time	Source	Destination	Protoco	Length	Info
2138…	690.651507201	49.12.121.47	10.168.27.10	FTP	93	Response: 220 FZ router and firewall teste
2138…	690.651514416	49.12.121.47	10.168.27.10	FTP	60	Response:
2138…	690.654468522	10.168.27.10	49.12.121.47	FTP	70	Request: USER FileZilla
2138…	690.783827486	49.12.121.47	10.168.27.10	FTP	76	Response: 331 Give any password.
2138…	690.783829054	49.12.121.47	10.168.27.10	FTP	60	Response:
2138…	690.786997247	10.168.27.10	49.12.121.47	FTP	67	Request: PASS 3.55.1
2138…	690.916622296	49.12.121.47	10.168.27.10	FTP	68	Response: 230 logged on.
2138…	690.916623530	49.12.121.47	10.168.27.10	FTP	60	Response:
2138…	690.922817898	10.168.27.10	49.12.121.47	FTP	84	Request: IP 10.168.27.10 ba-bgi-ch-ba
2138…	691.053128956	49.12.121.47	10.168.27.10	FTP	107	Response: 510 Mismatch. Your IP is 199.101
2138…	691.053129566	49.12.121.47	10.168.27.10	FTP	60	Response:

2. **Anomaly 2: IP protocol Scan by unidentified IP address**

    - It was discovered that an IP protocol scan was being conducted from an unidentified IP address, 10.16.80.243. This technique is performed with Nmap using ICMP or TCP/UDP packets to identify open ports and network protocols supported by the target operating system at 10.168.27.10. This allows attackers to gain more information on a target system's network.

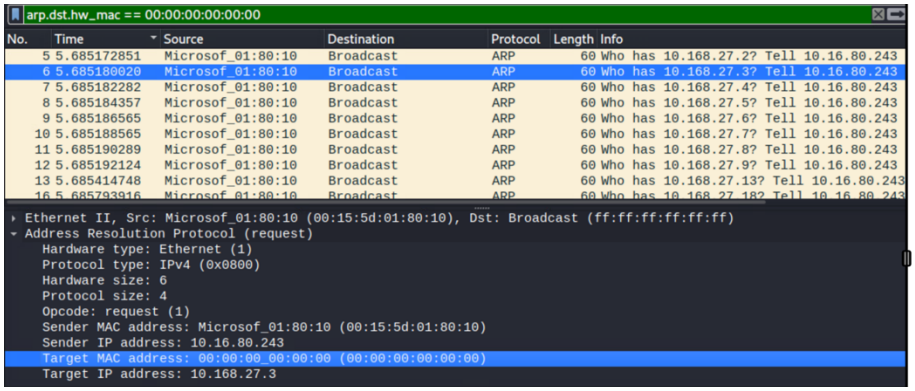


icmp

No.	Time	Source	Destination	Protoco	Length	Info
12490	511.504865047	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
12494	511.505068328	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
13469	513.114014036	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
13470	513.114015437	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
14741	514.086304173	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
14742	514.086309032	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
14755	514.732998764	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
14756	514.733050481	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
14759	515.608910097	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
14760	515.609040870	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
14769	517.204507244	10.16.80.243	10.168.27.10	ICMP	120	Destination unreachable (Port unreachable)
14770	517.204527714	10.16.80.243	10.16.80.2	ICMP	120	Destination unreachable (Port unreachable)
15986	572.742958248	10.168.27.10	10.16.80.243	ICMP	71	Destination unreachable (Port unreachable)
16794	578.225729077	10.168.27.10	10.16.80.243	ICMP	84	Destination unreachable (Port unreachable)

3. Anomaly 3: ARP spoofing attack

- This capture filter identifies an ARP spoofing attack. The attacker performs this attack by sending broadcast packets (ff:ff:ff:ff:ff:ff) with a target MAC address of 00:00:00:00:00:00. This allows an attacker to discover live IP addresses on the local network.



D. Summarize the potential implications of not addressing *each* of the anomalies found when running Wireshark.

The potential implications of not addressing each of the anomalies discovered on Wireshark can lead to spoofing, man-in-the-middle attacks, and unauthorized access/discovery to confidential information held by the Company.

1. **FTP Cleartext credentials:**
    - **Implications:** Not addressing the first FTP anomaly allows an attacker to gain unauthorized access to the Company's systems and information. Once an attacker gains unauthorized access, the attacker can perform lateral movement to gain further access into a company's network and access different folders through directory traversal or privilege escalation. Unauthorized access can lead to system compromise, data theft, and disruption of business operations.
2. **IP protocol scan:**
    - **Implications**: Not addressing the second IP protocol scan anomaly significantly increases the Company's attack surface. The Nmap tool is being used to discover a Company's network configuration through port scanning, using a command syntax such as nmap -sO <target> to discover potential vulnerabilities in the Company's network and systems. This can allow the attacker to plan network attacks and exploit vulnerabilities on the network.
3. **ARP Spoofing attack:**
    - **Implications**: Not addressing the 3rd ARP spoofing anomaly allows an attacker to intercept and manipulate communications through forged ARP packets between devices on a local network. This allows an attacker to eavesdrop on sensitive communications between devices or insert malicious commands into devices. ARP spoofing can

compromise data, exfiltration, or disrupt communication between devices.

E. Recommend solutions for eliminating or minimizing *all* identified vulnerabilities or anomalies from Wireshark and Nmap. Use current, industry-respected, reliable research and sources to support your recommendations for *each* vulnerability or anomaly.

1. **Recommended solutions for eliminating and minimizing vulnerabilities found from Nmap.**

   Host 10.168.27.10 (CVE-2019-0570):

   - The first recommendation for host 10.168.27.10, with the CVE-2019-0570 vulnerability, would be to update their Microsoft operating system to the current version. This will mitigate the CVE-2019-0570 vulnerability.

   Host 10.168.27.15 (CVE-2024-7745)

   - **Recommendation**: Upgrade the WS_FTP server versions to the current version 2022.0.8 (8.8.8). This version fixed the vulnerabilities found from the previous versions with this update.

   Host 10.168.27.132 (CVE-2019-14897):

   - **Recommendation**: Implement detection methods such as fuzzing and static application security testing (SAST) to identify vulnerabilities found in software, as recommended by MITRE.

2. **Recommendations solutions for eliminating and minimizing vulnerabilities discovered from Wireshark.**

FTP Cleartext Credentials:

- **Recommendation**: “The FTP protocol has been largely replaced by **SFTP** and **SSH** (SSH Communications Security, n.d).” Using SFTP (Secure File Transfer Protocol) or FTPS (FTP Secure) provides encryption to communication and protects data from interception.

IP Protocol Scan:

- **Recommendation**: Implement a strong firewall to protect against unauthorized scanning activity, including using TCP wrappers to uncover network gaps.

ARP Spoofing Attack:

- **Recommendation**: “Rate Limiting Incoming ARP Packets (Sans Institute, 2009).” Configure network switches to rate limit ARP packet requests and responses. Enable ARP monitoring and ARP inspection to protect against ARP spoofing attacks.

References:

CVE-2019-14897. (2018, November 29). *Common Vulnerability Exposures*. Retrieved from **https://www.cve.org/CVERecord?id=CVE-2019-14897.**

CVE-2024-7745. (2024, August 28). *Common Vulnerability Exposures*. Retrieved from **https://www.cve.org/CVERecord?id=CVE-2024-7745.**

CVE-2019-0570. (2019, January 8). *Common Vulnerability Exposures*. Retrieved from https://www.cve.org/CVERecord?id=CVE-2019-0570.

MITRE. (n.d.). *CWE-121: Stack-based Buffer Overflow*. Retrieved from https://cwe.mitre.org/data/definitions/121.html.

Progress Software Corporation. (2024, August 27). *WS_FTP Server Service Pack - August 2024*. Retrieved from **https://community.progress.com/s/article/WS-FTP-Server-Service-Pack-August-2024.**

SANS Institute. (2009, November 11). *Layer 2 Protections Against Man-in-the-Middle Attacks*. Retrieved from **https://isc.sans.edu/diary/Layer+2+Network+Protections+against+Man+in+the+Middle+Attacks/7567.**

SSH Communications Security. (n.d.). *FTP Server – Beware of Security Risks*. Retrieved from **https://www.ssh.com/academy/ssh/ftp/server.**