Kiarah Pettaway
[redacted]
C844: Emerging Technologies in Cybersecurity

C844 - Task 1: Network Mapping & Monitoring

A. Network Topology

Upon conducting an Nmap scan of the **10.168.27.0/24** target, I identified that the network topology is consistent with a Star topology. This configuration includes a central device, typically a hub or switch, referred to as the localhost, which serves as the focal point for communication among devices such as PCs and printers. As shown in Figure 1 below, all network devices are connected to the localhost, resembling a star configuration.

The Star topology is a favored design in the industry for its ease of adding or removing devices, as well as its ability to isolate device failures, preventing them from affecting the rest of the network. However, it has a drawback of being vulnerable to a single point of failure - if the central localhost fails, all devices connected to it will also lose connectivity. But there are ways to mitigate this risk, such as adding redundant devices and connections to the network.

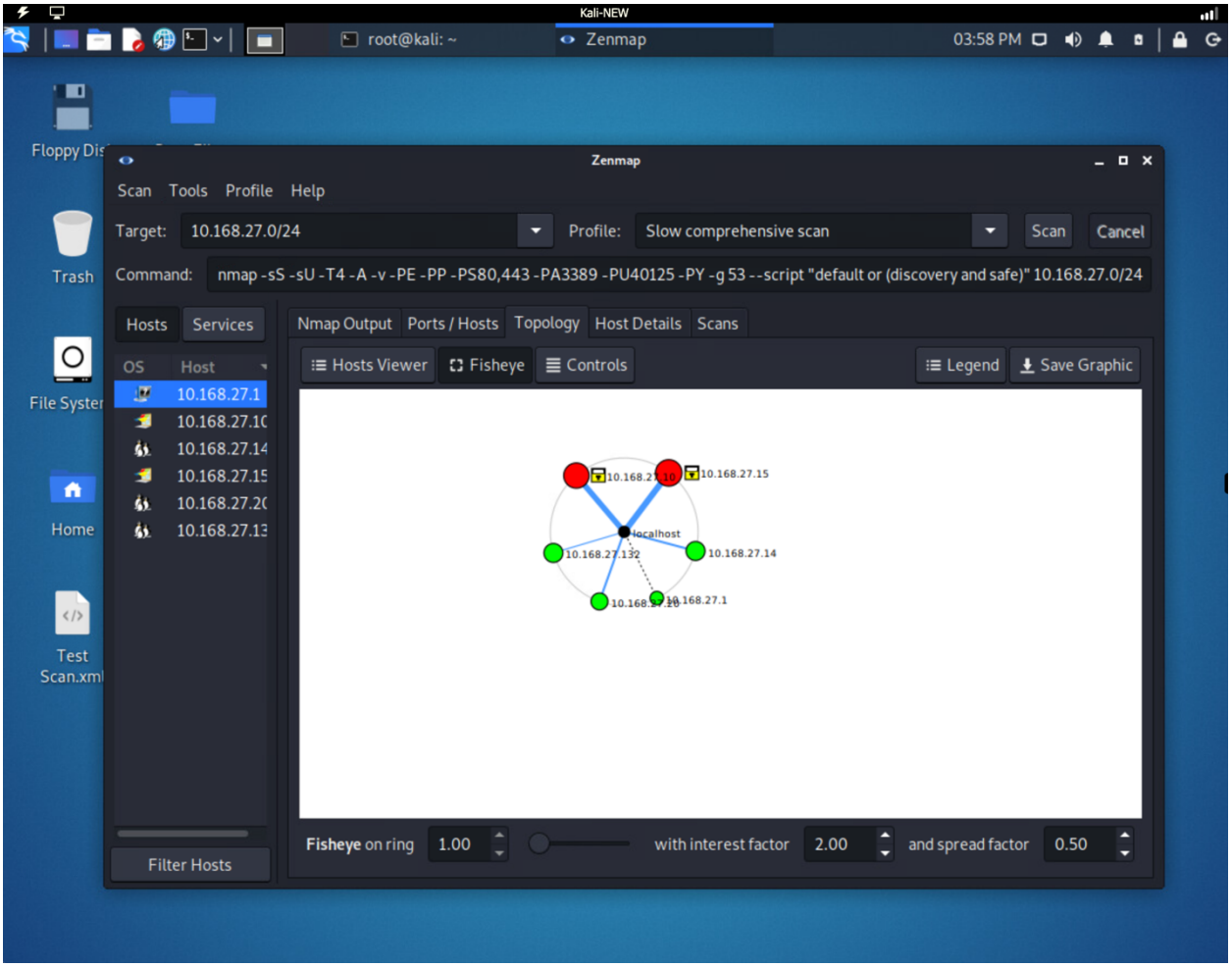

Figure 1

B. Vulnerabilities

1B. FTP

As displayed in Figure 2; For host **10.168.27.15**, I noticed that port 21 is being used, which is the insecure variation of FTP, and is considered bad practice due to several security vulnerabilities inherent in the protocol. FTP sends data, including usernames, passwords, and file contents, in plain text, making it vulnerable to eavesdropping attacks. Additionally, FTP does not provide any built-in encryption, authentication, or integrity checking mechanisms, further exposing the data to interception and tampering.

A better alternative providing security is FTPS, which operates on port 990 for implicit, and 21 for explicit; with the utilization of TLS/SSL OR SFTP, which uses SSH and operates on port 22.

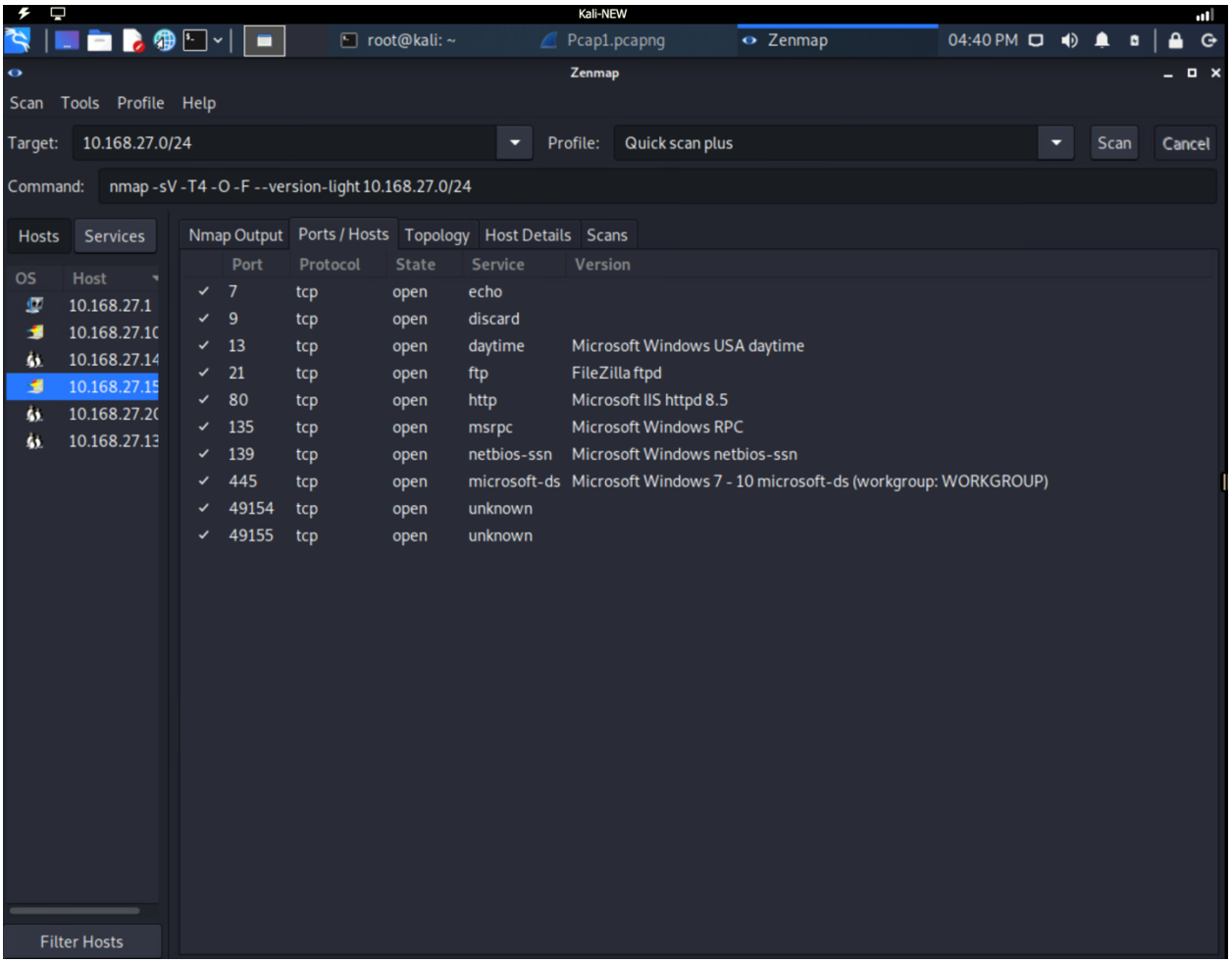

Figure 2

2B. LDAP

In Figure 3, I noticed host **10.168.27.10** is using port 389 for LDAP communication, which is an insecure port/version of LDAP. Port 389 can pose significant security risks. LDAP traffic transmitted over this port is vulnerable to eavesdropping and interception by malicious actors, due to it being in plaintext, which can lead to the exposure of sensitive information, including user credentials and directory data. Therefore, using LDAPS (over SSL/TLS), which runs on Port 636, is a better alternative to secure LDAP communication. LDAPS encrypts the LDAP traffic, providing confidentiality and integrity protection.

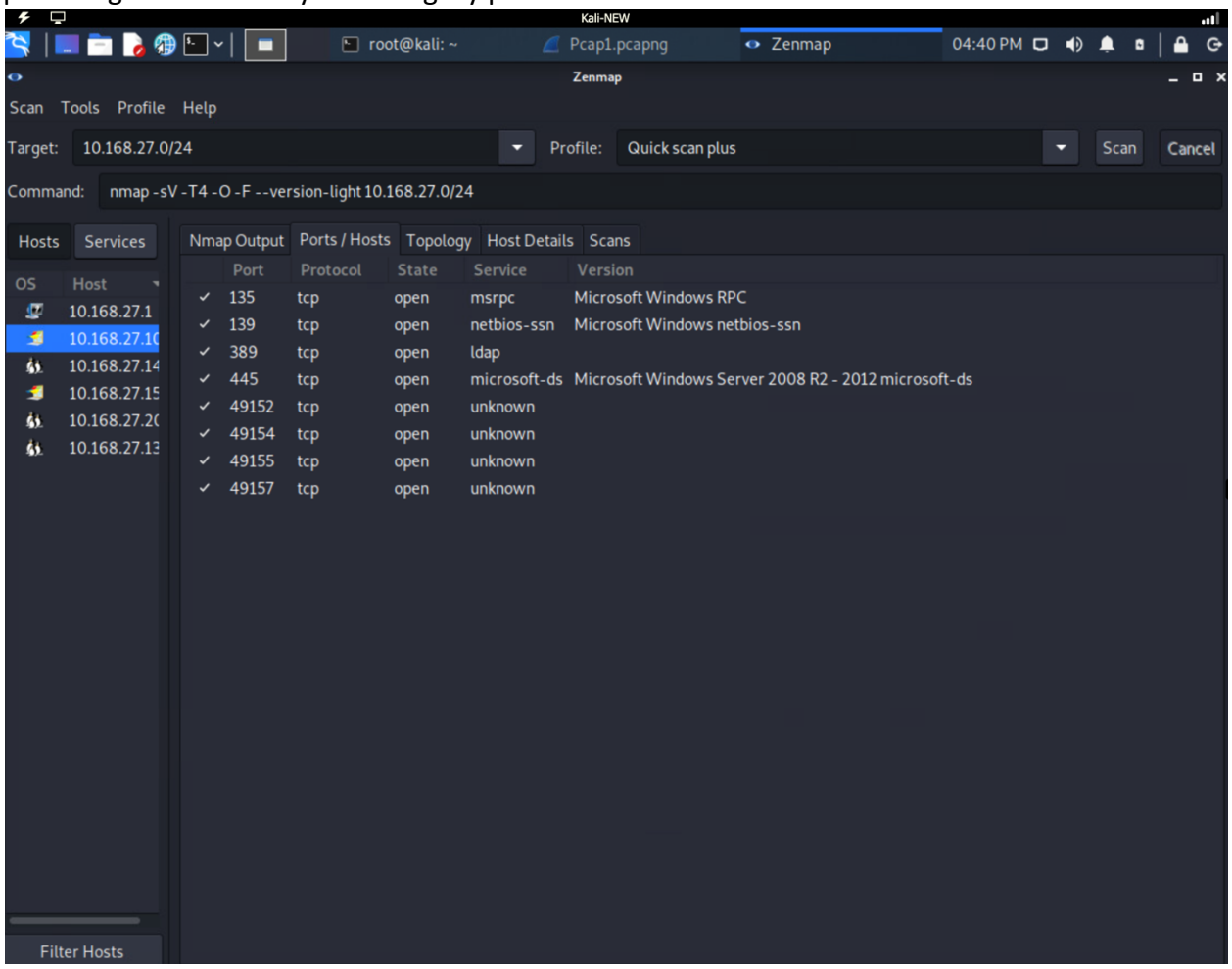

Figure 3

3B. Windows Server 2012 R2

In Figure 4, it shows the current OS in **10.168.27.10** is Windows Server 2012 R2. This OS is outdated and lacks security updates, making it vulnerable to attacks. A remote code execution vulnerability exists in the Windows Jet Database Engine, which allows attackers to execute arbitrary code on a target system. Windows Server 2012 R2 reached its end of support on October 10, 2023, and Microsoft no longer provides security updates or patches for this version. This means that any vulnerabilities, such as the Jet Database Engine vulnerability, remain unpatched and leave systems running Windows Server 2012 R2 exposed to potential attacks.

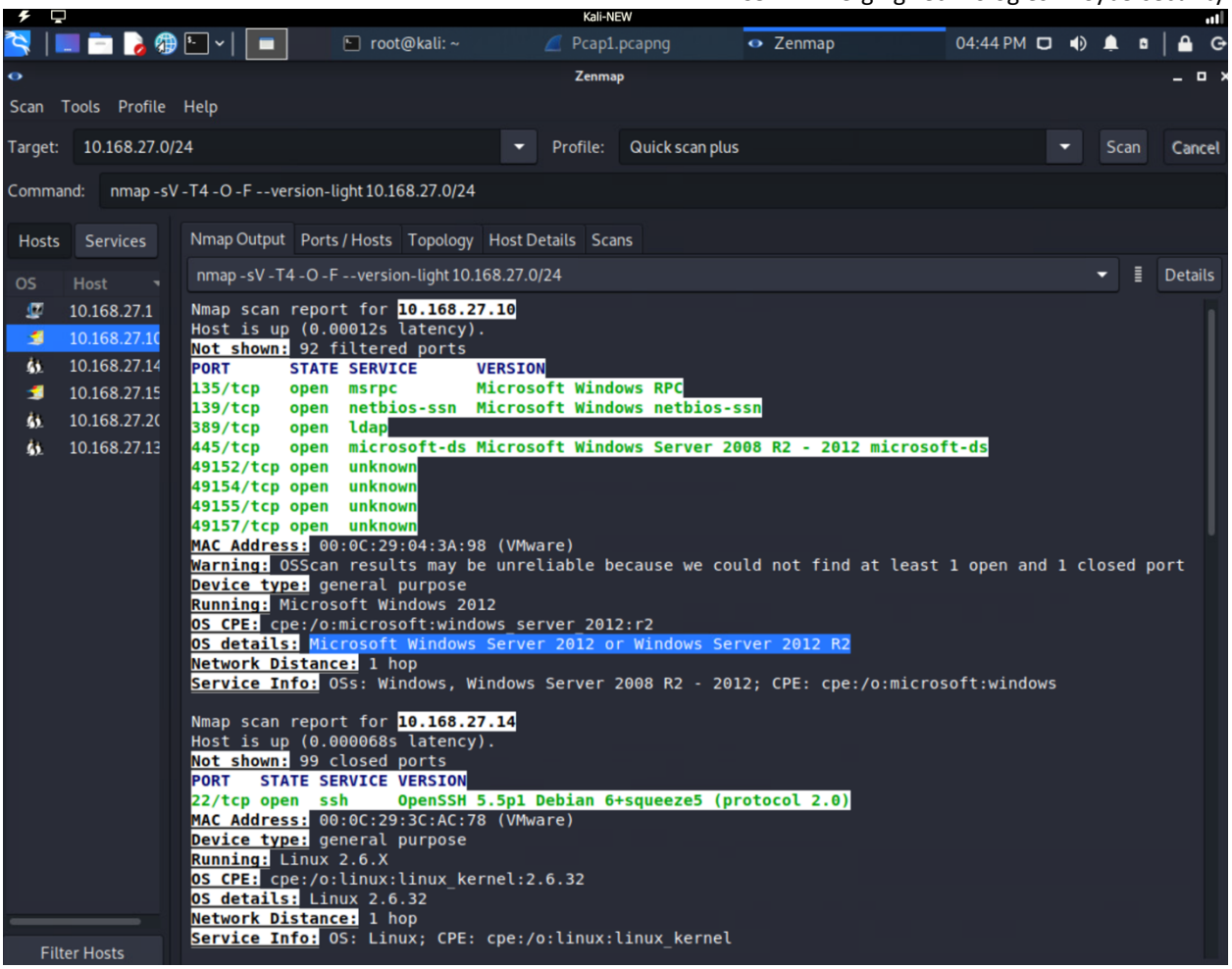

Figure 4

C. Finding Vulnerabilities

1C. ICMP

In Figure 5, Frame 199 clearly shows that the host at **10.168.27.10** attempted to ping 8.8.4.4 but received an ICMP packet stating "destination unreachable (port unreachable)." Based on this, it is highly likely that the port for ICMP packets is blocked, which is preventing 10.168.27.10 from reaching 8.8.4.4.

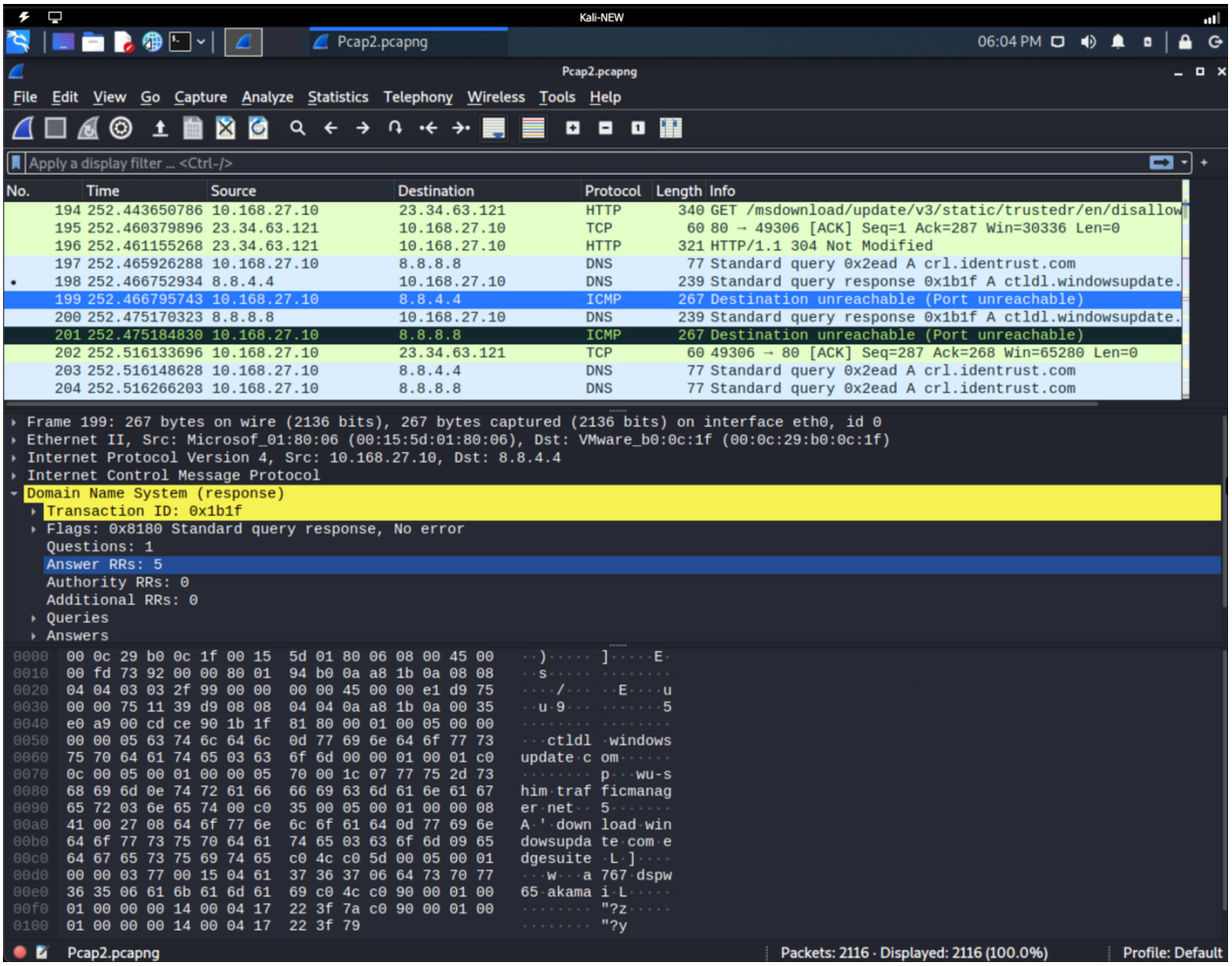

Figure 5

2C. HTTP

In Figure 6, Frame 194 provides cleartext of what **10.168.27.10** is downloading via HTTP from 23.34.63.121, which seems to be some sort of Microsoft update. This poses significant security risks and is considered bad practice because HTTP traffic is transmitted in cleartext, meaning that anyone monitoring the network can intercept and view the contents of the communication, including sensitive information such as URLs, file contents, and potentially credentials.

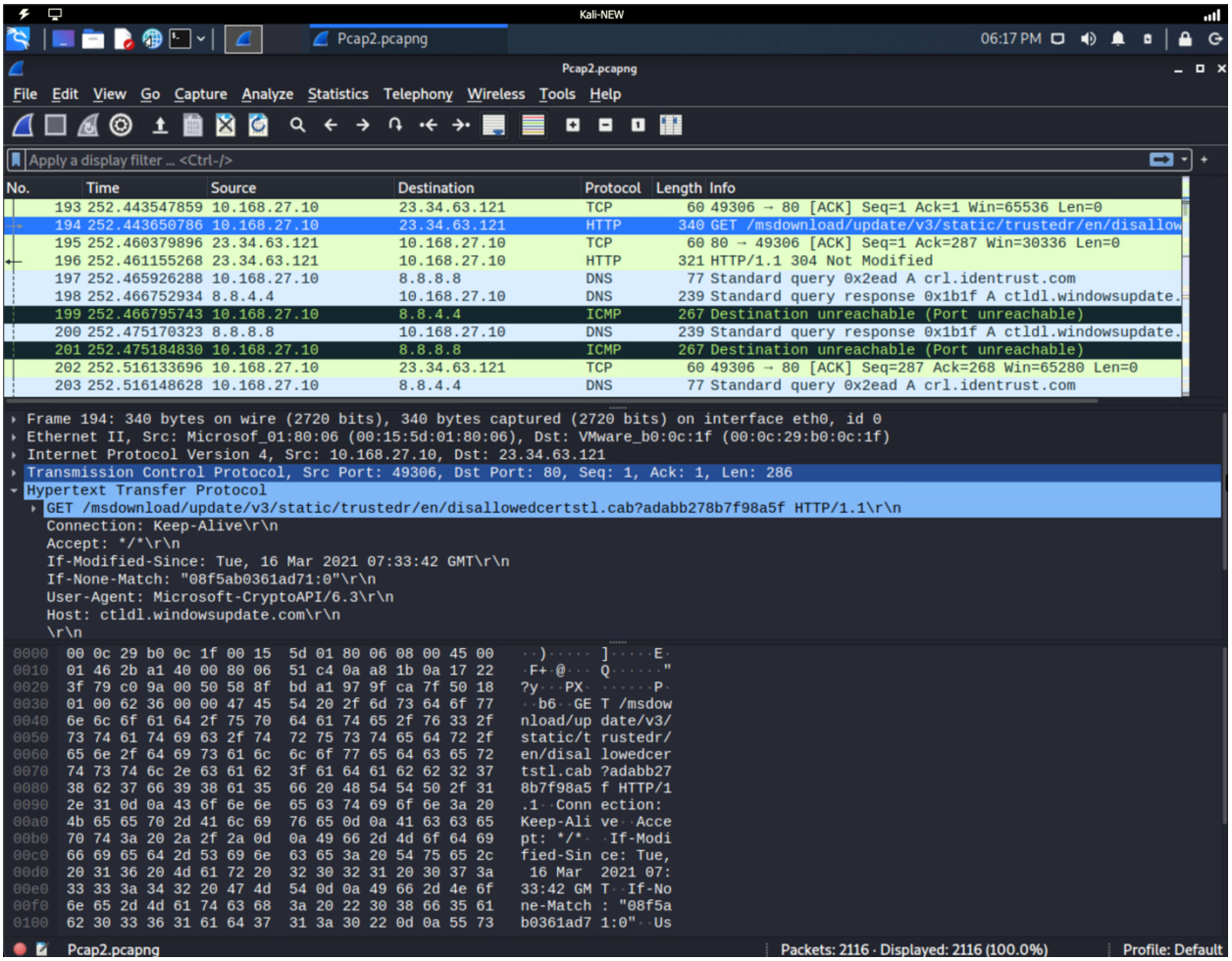

Figure 6

3C. TCP

In Figure 7, as mentioned in Frame 1300, it appears that 10.16.80.243 is unable to receive a TCP ACK from **10.168.27.10,** resulting in the error code "TCP ACKed unseen segment". This error indicates a potential vulnerability known as a TCP sequence number attack or TCP sequence prediction attack.

In a standard TCP communication, every segment has a sequence number that helps the receiver to reconstruct the data stream in the correct order. The ACK flag is used to confirm that a segment has been received successfully.

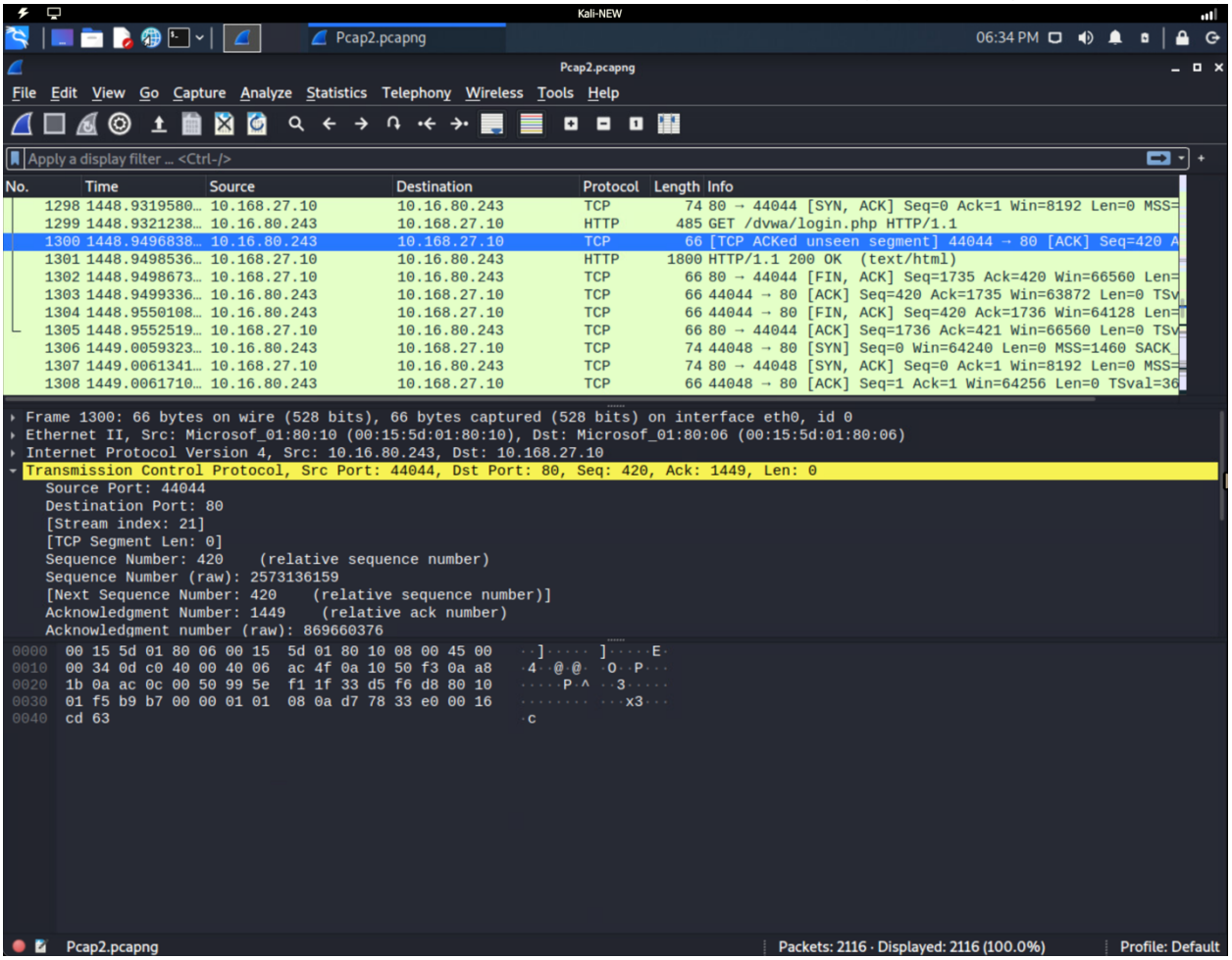

Figure 7

D. Vulnerability Insight

a. **ICMP Protocol** (1C): Detecting ICMP packets with the message "destination unreachable (port unreachable)" is a clear indication that certain ports are blocked, which can cause communication problems and severely impact network performance. Ignoring this issue could lead to increased network latency, failed connections, and make it difficult to troubleshoot network issues. Therefore, it is crucial to address this anomaly as soon as possible to ensure optimal network performance.

b. **HTTP Protocol** (2C): Viewing HTTP traffic in cleartext exposes sensitive information, such as URLs, file contents, and potentially credentials, to interception by unauthorized parties. Not addressing this problem could lead to data breaches, unauthorized access to sensitive information, and potential loss of confidentiality.

c. **TCP Protocol** (3C): The message "TCP ACKed unseen segment" suggests a potential TCP sequence number attack, which could lead to data injection, disruption of TCP connections, and potential session hijacking. Refusing to address this anomaly could

result in compromised network integrity, data manipulation, and unauthorized access to network resources.

E. Vulnerability Mitigation

NMAP

1. FTP Protocol:

Solution: Replace FTP with a more secure file transfer protocol, such as SFTP or FTPS, which encrypts data during transmission. Disable anonymous FTP access and implement strong authentication mechanisms(CSRC, 2024).

2. LDAP Protocol:

Solution: Ensure that LDAP traffic is encrypted using LDAPS (LDAP over SSL/TLS) to protect sensitive information, such as user credentials, from eavesdropping(Deland-Han, 2023). Use strong authentication mechanisms, such as LDAP simple bind with SSL/TLS.

3. Windows Server 2012 R2:

Solution: Upgrade to a supported version of Windows Server, such as Windows Server 2019 or Windows Server 2022, to receive security updates and patches(Nakarnam, 2023). Implement security best practices, such as regular patching and configuration hardening, to protect against known vulnerabilities.

WIRESHARK

1. ICMP Protocol:

Solution: Implement strict firewall rules to control ICMP traffic and prevent unauthorized access (Naidu, Krishni, 2024). Use network IDS (NIDS)bto detect and block ICMP-based attacks. Regularly update firewall rules and IDS signatures to protect against emerging threats.

2. HTTP Protocol:

Solution: Encrypt HTTP traffic using HTTPS to protect sensitive information from interception. Ensure that web servers and clients are configured to use HTTPS by default(Iramar, Ricardo, et al , 2024). Use secure coding practices to prevent HTTP-based attacks, such as cross-site scripting (XSS) and SQL injection.

3. TCP Protocol:

Solution: Enable TCP sequence number randomization to prevent sequence number prediction attacks. Regularly update network equipment and software to mitigate known TCP vulnerabilities(CISA, 2024). Use intrusion detection and prevention systems to detect and block malicious TCP traffic.

Resource(s) and Citations:

"Search CVE List." *CVE*, cve.mitre.org/cve/search_cve_list.html. Accessed 30 Mar. 2024.

Editor, CSRC Content. "SFTP - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/sftp. Accessed 30 Mar. 2024.

Deland-Han. "Enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) - Windows Server." *Enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) - Windows Server | Microsoft Learn*, learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/enable-ldap-over-ssl-3rd-certification-authority. Accessed 30 Mar. 2024.

Nakarnam. "Windows Server 2012 and 2012 R2 Reaching End of Support - Microsoft Lifecycle." *Microsoft Lifecycle | Microsoft Learn*, learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support. Accessed 30 Mar. 2024.

Naidu, Krishni. *Firewall Checklist*, www.sans.org/media/score/checklists/FirewallChecklist.pdf. Accessed 31 Mar. 2024.

Iramar, Ricardo, et al. "Owasp Secure Headers Project." *OWASP Secure Headers Project | OWASP Foundation*, owasp.org/www-project-secure-headers/. Accessed 30 Mar. 2024.

Vulnerabilities in TCP: CISA, Cybersecurity and Infrastructure Security Agency CISA, 29 Mar. 2024, www.cisa.gov/news-events/alerts/2004/04/20/vulnerabilities-tcp.