November 1, 2024

EMERGING TECHNOLOGIES IN CYBERSECURITY

Task 1 - Nmap and Wireshark

Kershia Mukoro Shin

NETWORK TOPOLOGY

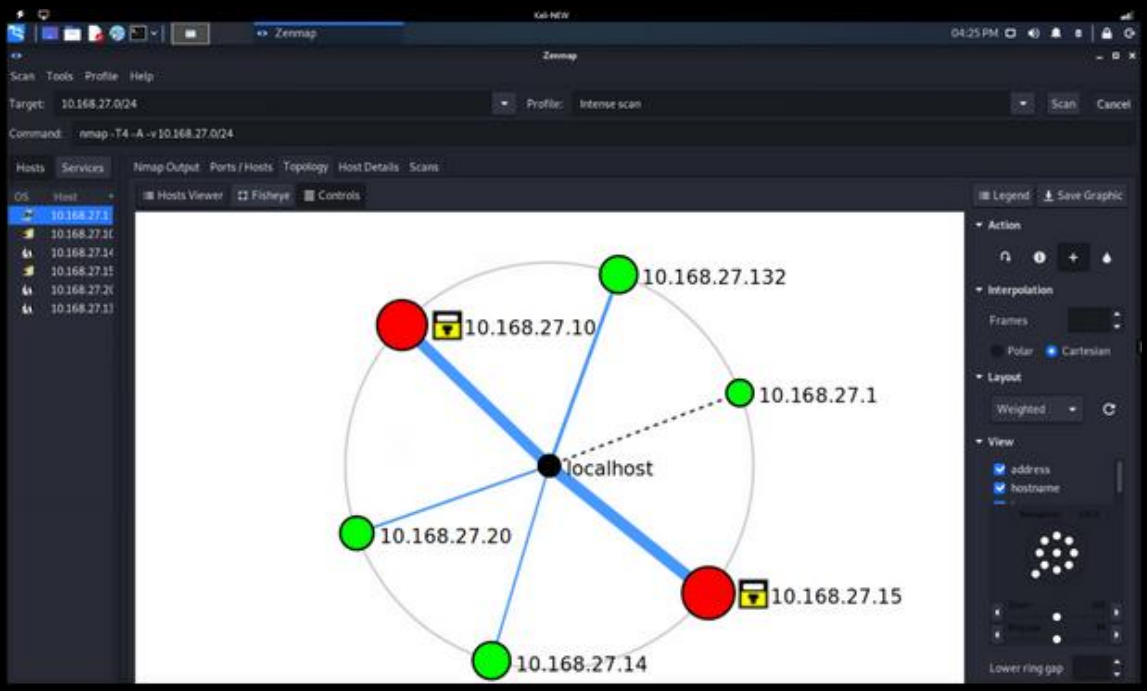

FIGURE 1. THE ZENMAP GUI REVEALS THE 10.168.27.0/24 SUBNET USES A STAR TOPOLOGY

The Nmap scan shows multiple active hosts arranged in a star topology. In Figure 1, each of the five active hosts on the 10.168.27.0/24 subnet connects to a central node labeled localhost. Additionally, the visualization highlights the central roles and connectivity of Hosts 10.168.27.10 and 10.168.27.15. Both hosts are significant points within the network, hosting multiple open ports and critical services (see Figure 2).

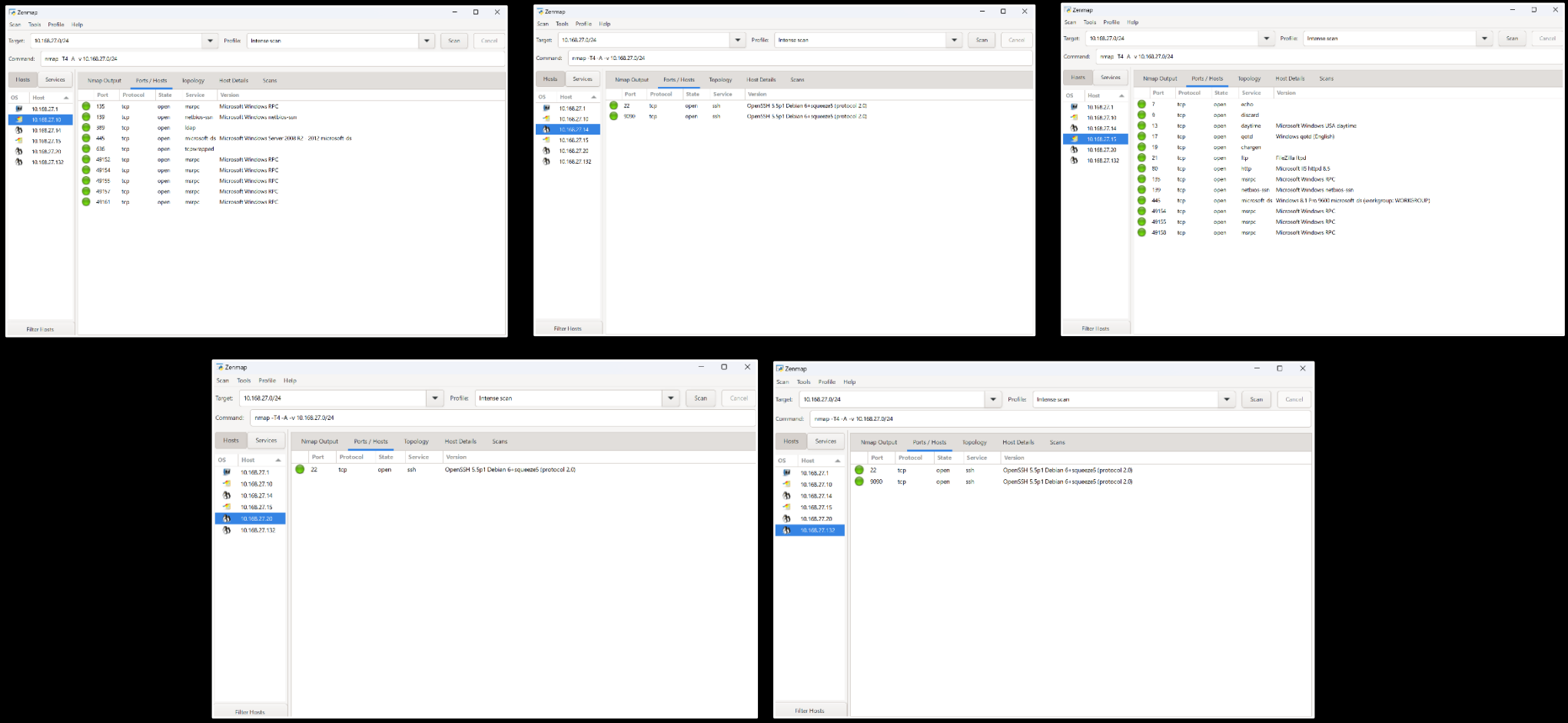

FIGURE 2. PORTS/HOSTS IDENTIFIED DURING AN INTENSE SCAN

An intense scan of the 10.168.27.0/24 subnet identified the following hosts, Operating Systems, and services (see Figure 2):

10.168.27.1

Appears as a standard, lower-risk asset in green on the topology map. This host likely has limited services or vulnerabilities, exhibiting no high-alert services.

10.168.27.10: Windows Server 2012 or Server 2008 R2

Shown in red with a server icon, running Microsoft Windows Server 2012 or Server 2008 R2 appears to be a critical asset. This host provides essential services, including SMB (445/tcp), NetBIOS (139/tcp), LDAP (389/tcp), and various high-numbered dynamic RPC ports.

10.168.27.14: Linux (Kernel 2.6.x)

It appears in green, suggesting it holds a standard role within the network. This host provides SSH access on ports 22 and 9090.

10.168.27.15: Windows 8.1 Pro or Windows Server 2008 R2

A high-value target in red on the topology map. This host supports multiple services, including HTTP (port 80), FTP with anonymous access, SMB, and legacy diagnostic services (e.g., Echo, Discard).

10.168.27.20: Linux (Kernel 2.6.x)

Another Linux-based server running on Kernel 2.6.x appears in green, indicating a standard role like Host 10.168.27.14. This host provides SSH access on port 22 and runs an outdated version of OpenSSH (5.5p1).

10.168.27.132: Linux (Kernel 2.6.x)

Another Linux server is shown in green on the map, indicating standard access. Like Host 10.168.27.14, it provides SSH services on both standard and non-standard ports (22 and 9090).

NMAP VULNERABILITIES, IMPLICATIONS, & RECOMMENDATIONS

Summary of Network Vulnerabilities

A network scan revealed vulnerabilities across multiple hosts, areas of concern include:

SMB (Server Message Block) and NetBIOS Services - Hosts 10.168.27.10 and 10.168.27.15

Ports: 445/tcp (SMB), 139/tcp (NetBIOS-ssn)

Risk: SMB and NetBIOS are widely exploited protocols, especially in Windows environments. They are often targeted for remote code execution attacks, lateral movement, and ransomware propagation. Attackers use these services to exploit vulnerabilities like EternalBlue, which was infamously used in the WannaCry ransomware attack (Islam et al., n.d., para. 1).

Implications: Leaving these ports exposed, especially without network segmentation or restrictions, increases the risk of unauthorized access and malware spread within the network. Barracuda researchers found that 91.88% of the attacks on port 445 attempted to use the EternalBlue exploit

Recommendation: Restrict SMB and NetBIOS access to local or VPN-only traffic and consider disabling them if they are not essential.

Anonymous FTP Access - Host 10.168.27.15

Port: 21/tcp (FTP)

Risk: Anonymous FTP access allows anyone to connect to the server without credentials, potentially exposing sensitive files. Attackers could also use this access to upload malicious files, which could be used to compromise other systems in the network (FasterCapital, 2024).

Implications: This open access poses a significant risk for data exfiltration, malware distribution, and unauthorized modifications, potentially compromising data integrity and confidentiality (Specops Software, 2022).

Recommendation: Disable anonymous FTP or restrict access to authenticated users only. Implement encryption protocols and consider using more secure alternatives like FTPS, HTTPS, or SFTP as a secure alternative (Cerberus FTP, 2023).

Outdated SSH Services - Hosts 10.168.27.14, 10.168.27.20, and 10.168.27.132

Ports: 22/tcp (standard SSH), 9090/tcp (non-standard SSH)

Risk: The outdated version of OpenSSH (5.5p1) used on these hosts may lack recent security patches, making it vulnerable to known exploits, including potential memory leaks and unauthorized access (MITRE, n.d.). Multiple SSH ports on some hosts increase the attack surface (SSH Communications Security, n.d.).

Implications: Vulnerabilities in SSH can lead to unauthorized access, allowing attackers to control the host and potentially use it to pivot to other systems within the network (Vulcan, 2023).

Recommendation: Upgrade OpenSSH to the latest stable version, consolidate SSH access to a single port, and implement strong authentication, such as key-based authentication, to reduce brute-force and unauthorized access risks (SSH Communications Security, n.d.).

WIRESHARK VULNERABILITIES, IMPLICATIONS, & RECOMMENDATIONS

Summary of Network Vulnerabilities

An analysis of packet capture file 1 via Wireshark revealed the following areas of concern:

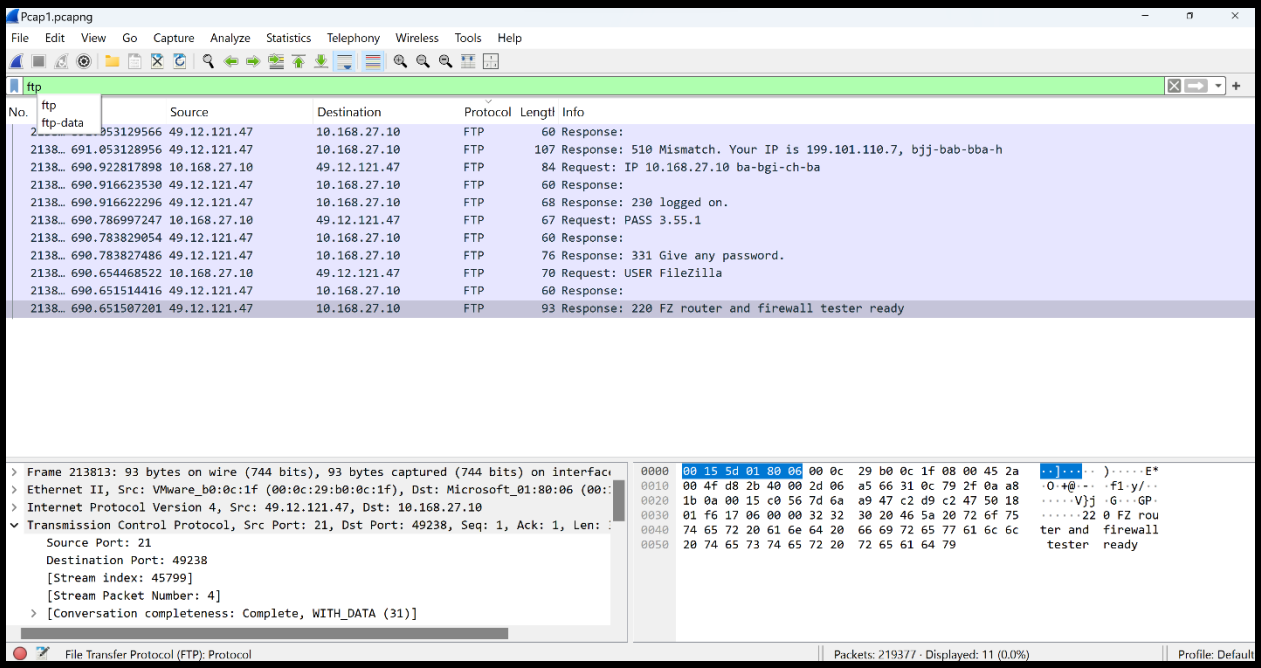

FIGURE 3. WIRESHARK ANALYSIS REVEALS AN FTP ANOMALY

Anomaly 1: FTP Protocol

Description: In the FTP traffic screenshot (Figure 3), a response indicates an IP address mismatch ("`510 Mismatch. Your IP is 199.101.110.7`"). This suggests the FTP server detected an unexpected IP, possibly due to a proxy, NAT issue, or spoofing attempt (Cerberus FTP, 2023). Additionally, the server responds with "`331 Give any password`," implying it may accept any password, a weak security setting that could allow unauthorized access (JSCAPE, 2022).

Packet Range: Packets around 213818, as shown in the screenshot, display FTP responses, including the IP mismatch error and insecure password requirements.

Implications: This configuration might allow unauthorized access to the FTP server if users can bypass authentication by providing any input (Stream Security, n.d.). The IP mismatch may also indicate potential spoofing or misconfiguration, raising security concerns if attackers attempt to bypass restrictions (Specops Software, 2022).

Recommendations:

Enforce Strong Authentication Settings: Reconfigure the FTP server to require valid credentials and disable the "`331 Give any password`" response. Implement stricter password requirements and authentication protocols to prevent unauthorized access (JSCAPE, 2022).

Inspect and Adjust IP Verification Settings: Review the FTP server's IP verification settings to ensure it properly recognizes and verifies client IPs (Cerberus FTP, 2023). Adjust NAT or proxy configurations to align expected and actual Ips.

Enable IP Allowlisting (if applicable): Limit FTP access to trusted IP addresses through IP allowlisting, reducing exposure to potential spoofed or unauthorized connections (Cerberus FTP, 2023).

Monitor FTP Traffic for Anomalies: Monitor and alert for unusual FTP connection patterns or frequent IP mismatches, which may indicate potential attacks or misconfigurations (JSCAPE, 2022).

Update and Patch FTP Server Software: Ensure the FTP server is up to date with the latest security patches, reducing vulnerabilities that could be exploited in bypassing authentication (Specops Software, 2022).

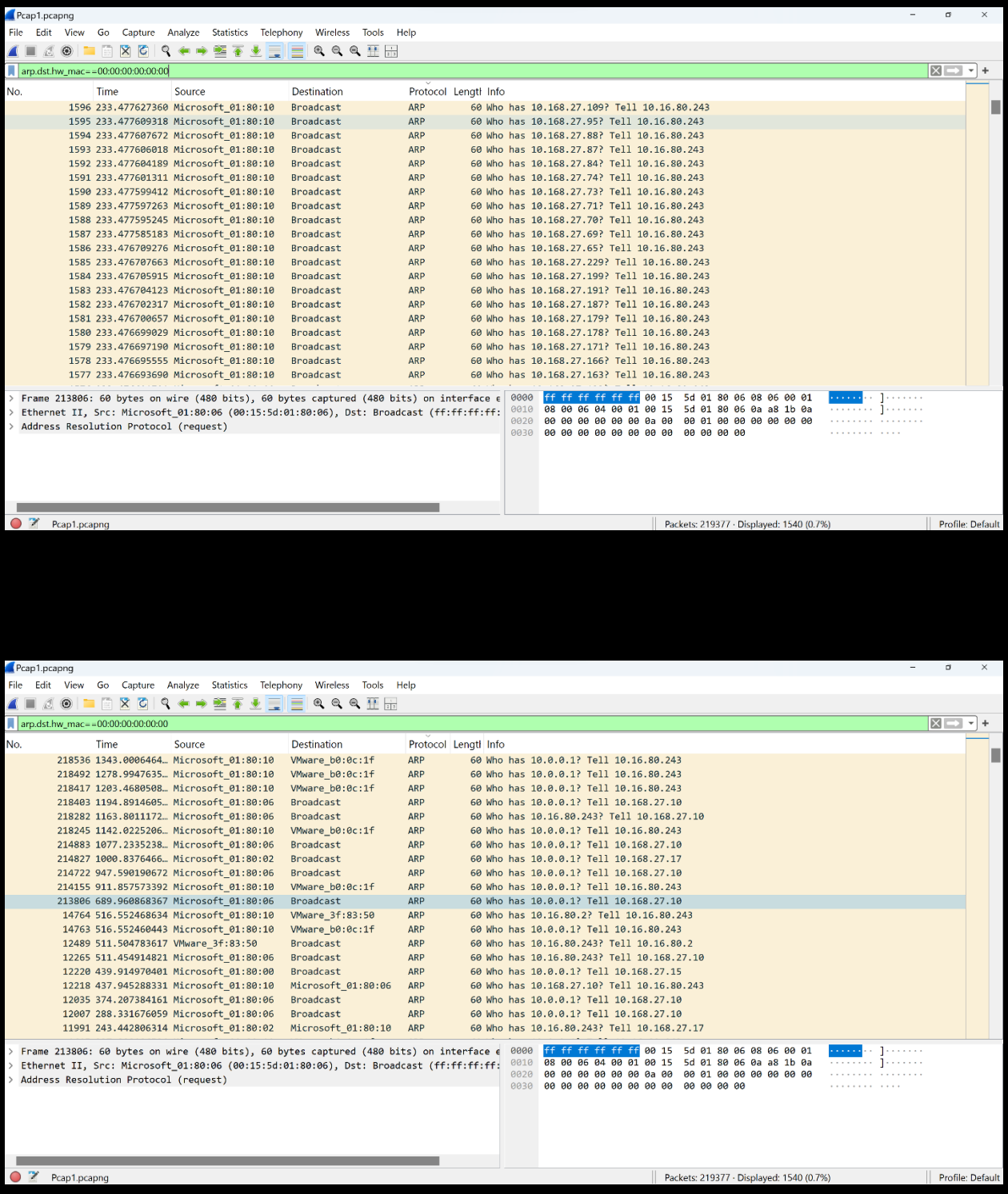

FIGURE 4. WIRESHARK ANALYSIS REVEALS AN ARP STORM

Anomaly 2: ARP Broadcast Storm

Description: The screenshots (Figure 4) show excessive Address Resolution Protocol (ARP) requests, specifically broadcasts asking "Who has" various IP addresses within a short period. This behavior, known as an ARP broadcast storm, typically indicates that a device is continually broadcasting ARP requests to locate other devices on the network.

Packet Range: Packets around 213806 and in the 233. xxx. xxx range, as shown in the screenshots, with a high frequency of ARP requests from the same MAC address, Microsoft_01:80:10, directed to multiple IP addresses.

Implications: An ARP broadcast storm can lead to network congestion, degrading network performance for all devices on the subnet. It could be symptomatic of a misconfigured device, a network loop, or even a malicious attack attempting to gather information about the network (NetApp, 2024; Varonis, 2024).

Recommendations:

Identify the Source Device: Locate the device with the MAC address Microsoft_01:80:10 and inspect it for configuration issues or malware (Auvik Networks, 2024).

Update ARP Tables: Ensure ARP tables on network devices are current to prevent repeated requests (NetApp, 2024).

Network Segmentation: If possible, segment the network to isolate the source of the broadcasts to prevent network-wide impact. VLANs reduce the scope of broadcast domains and limit the impact of storms (The Final Hop, 2024).

Implement ARP Rate Limiting: Configure network equipment to limit the rate of ARP requests, reducing the potential for a broadcast storm (PingPlotter, n.d.; The Final Hop, 2024).

Inspect for Network Loops: Ensure there are no physical or logical network loops, as they can amplify broadcast storms. Implement protocols like Spanning Tree Protocol (STP) or its enhanced versions, such as RSTP, to help mitigate such issues (Auvik Networks, 2024; The Final Hop, 2024).

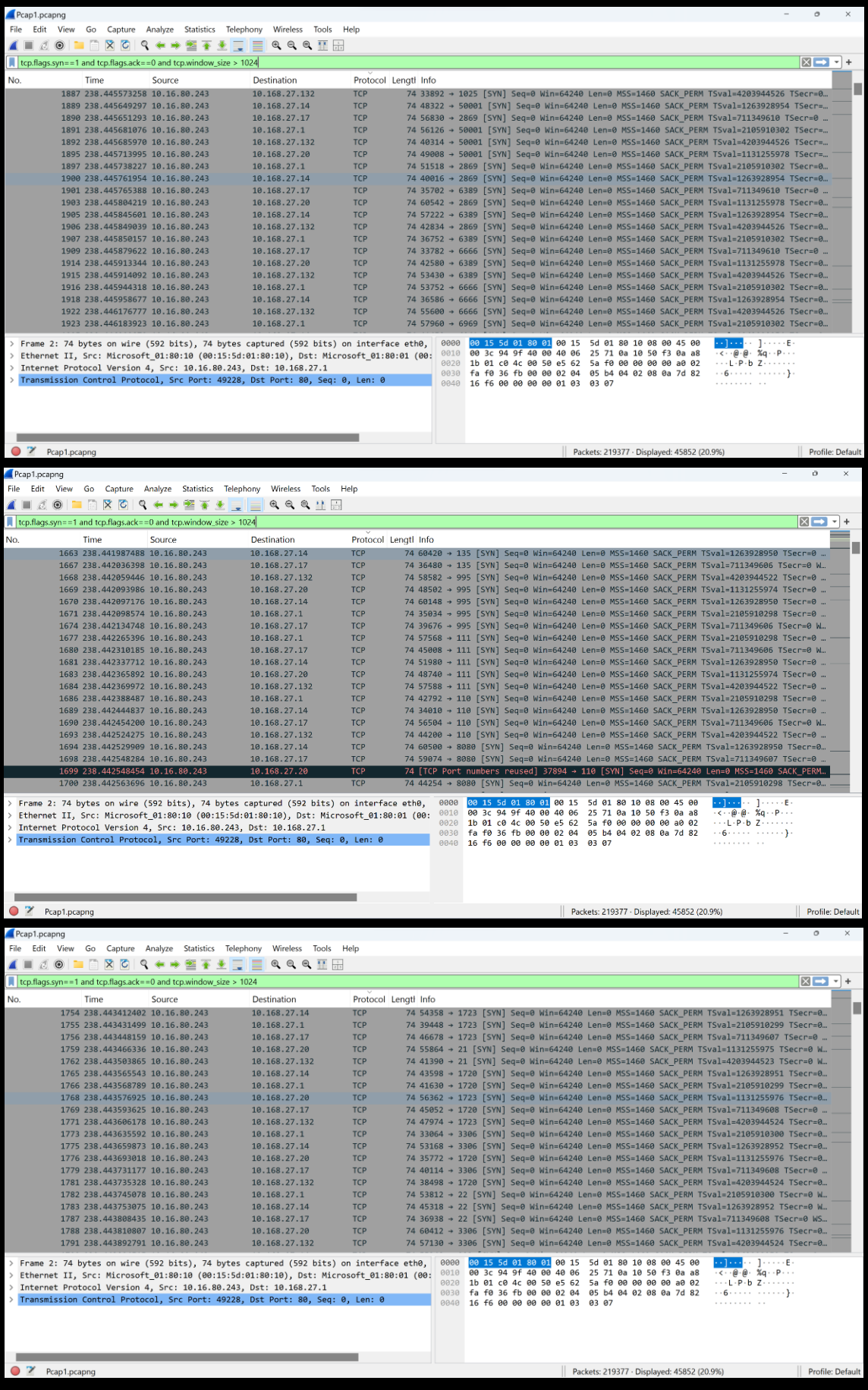

FIGURE 5. WIRESHARK ANALYSIS REVEALS A POSSIBLE SYN FLOOD

Anomaly 3: SYN Flood

Description: The screenshots (Figure 5) show a large number of SYN packets with no corresponding ACK or RST responses. Each packet originates from IP 10.16.80.243 and is directed at various IP addresses within the 10.168.27.x network. The high TCP window size (Win=64240) and repetitive SYN packets with ACK=0 indicate an attempt to initiate numerous connections without completing any handshakes. This traffic pattern is consistent with either a SYN flood, where an attacker tries to exhaust resources by initiating connections, or a port scan, where an attacker probes for open ports.

Packet Range: Packets 1663 to 1923, as shown in the screenshots, exhibit this unusual SYN traffic pattern.

Implications:
Resource Exhaustion: A SYN flood attack could overload the target system's resources, causing slowdowns or denial of service for legitimate users. (Akamai, n.d.; ClouDNS, 2024).

Reconnaissance: If these packets are part of a port scan, it may indicate an attacker's attempt to map active services on the network, potentially identifying vulnerabilities (Blue Goat Cyber, 2024).

Network Disruption: SYN floods and aggressive port scans can disrupt normal network operations and create latency (Heimdal Security, 2023).

Recommendations:

Enable SYN Cookies: Activate SYN cookies on the target system to mitigate SYN flood attacks by limiting resource allocation for uncompleted handshakes (Akamai, n.d.).

Implement TCP Connection Limits: Use firewall or router settings to limit the rate of incoming SYN packets, helping to filter out excessive attempts from the same source IP (Blue Goat Cyber, 2024).

Deploy Intrusion Detection Systems (IDS): Use an IDS, such as Snort or Suricata, to monitor for and alert on abnormal SYN traffic patterns. Set rules to detect SYN floods or port scanning activities (PurpleSec, 2024).

Use Access Control Lists (ACLs): Set up ACLs on firewalls to block or limit access to sensitive IP ranges or to allow only trusted IP ranges where possible (Heimdal Security, 2023).

Log and Monitor Network Traffic: Regularly log and monitor network traffic with tools like Wireshark. Use filters to catch repeated SYN packets from the same source, which may indicate potential attacks (Mailgun Blog, 2023).

REFERENCES

1. Akamai. (n.d.). What Are SYN Flood DDoS Attacks? Retrieved November 4, 2024, from https://www.akamai.com/glossary/what-are-syn-flood-ddos-attacks
2. Barracuda. (2022, May 11). The majority of attacks against SMB protocol attempt to exploit EternalBlue. Barracuda Blog. Retrieved November 3, 2024, from https://blog.barracuda.com/2022/05/11/attacks-smb-protocol-eternalblue
3. Blue Goat Cyber. (2024). Mitigating SYN Flood Attacks Effectively. Retrieved November 4, 2024, from https://bluegoatcyber.com/blog/mitigating-syn-flood-attacks-effectively
4. Cerberus FTP. (2023). IP Allow/Deny Lists - Cerberus FTP Server. Retrieved November 3, 2024, from https://www.cerberusftp.com/features/access-protection/ip-allow-deny-lists/
5. Cerberus FTP. (2023, June 26). Is FTP Secure? How you can mitigate the risks of using File Transfer Protocol. Retrieved from https://www.cerberusftp.com/blog/how-secure-is-ftp-how-you-can-mitigate-the-risks-of-using-file-transfer-protocol/
6. CIS. (2024, February 16). CIS OpenSSH Server Benchmark v2.1.0 Released. Center for Internet Security. Retrieved November 3, 2024, from https://www.cisecurity.org/insights/blog/cis-openssh-server-benchmark-v2-1-0-released
7. ClouDNS. (2024). Understanding SYN Flood Attack. Retrieved November 4, 2024, from https://www.cloudns.net/blog/understanding-syn-flood-attack/
8. Developer Tech. (2024, March 15). Critical OpenSSH vulnerability affects millions of Linux systems. Retrieved November 3, 2024, from https://developer-tech.com/news/2024/mar/15/critical-openssh-vulnerability-affects-millions-linux-systems/
9. FasterCapital. (n.d.). Anonymous FTP: Unveiling the Pros and Cons of Anonymous File Transfers. Retrieved November 3, 2024, from https://fastercapital.com/content/Anonymous-FTP--Unveiling-the-Pros-and-Cons-of-Anonymous-File-Transfers.html
10. Heimdal Security. (2023). SYN Flood Explained: How to Prevent This Attack from Taking Over Your Network. Retrieved November 4, 2024, from https://heimdalsecurity.com/blog/syn-flood/
11. Islam, A., Oppenheim, N., & Thomas, W. (n.d.). SMB Exploited: WannaCry Use of "EternalBlue." Google Cloud Blog. Retrieved November 3, 2024, from

https://cloud.google.com/blog/topics/threat-intelligence/smb-exploited-wannacry-use-of-eternalblue/

12. JSCAPE. (2022, December 6). How to Secure FTP Servers in 5 Steps. Retrieved November 3, 2024, from https://www.jscape.com/blog/5-steps-to-a-secure-ftp-server
13. Mailgun Blog. (2023). What Are SYN Flood Attacks, and How Can You Defend Against Them? Retrieved November 4, 2024, from https://www.mailgun.com/blog/it-and-engineering/syn-flood-defense/
14. Microsoft. (2022, March 21). FTP IP Security <ipSecurity>. Microsoft Learn. Retrieved November 3, 2024, from https://learn.microsoft.com/en-us/iis/configuration/system.ftpserver/security/ipsecurity/
15. Microsoft. (n.d.). Preventing SMB traffic from lateral connections and entering or leaving the network. Microsoft Support. Retrieved November 3, 2024, from https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a
16. MITRE. (n.d.). CVE - Search Results. Common Vulnerabilities and Exposures. Retrieved November 3, 2024, from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=OpenSSH+%285.5p1%29
17. PurpleSec. (2024). How To Prevent A SYN Flood Attack. Retrieved November 4, 2024, from https://purplesec.us/learn/prevent-syn-flood-attack/
18. Specops Software. (2024, September 30). TCP port 21 FTP vulnerabilities. Retrieved November 3, 2024, from https://specopssoft.com/blog/tcp-port-21-ftp-vulnerabilities/
19. SSH Communications Security. (n.d.). FTP Server – Beware of Security Risks. SSH Academy. Retrieved November 3, 2024, from https://www.ssh.com/academy/ssh/ftp/server
20. SSH Communications Security. (n.d.). SSH (Secure Shell). SSH Academy. Retrieved November 3, 2024, from https://www.ssh.com/academy/ssh
21. Stream Security. (n.d.). Ensure no unrestricted inbound access to TCP port 21 (FTP) exists. Retrieved November 3, 2024, from https://www.stream.security/rules/ensure-there-is-no-unrestricted-inbound-access-to-tcp-port-21-ftp
22. Vulcan. (2023, August 14). OpenSSH Vulnerabilities: A Comprehensive Guide. Retrieved November 3, 2024, from https://vulcan.io/blog/openssh-vulnerabilities-guide