**Name:** Amarachi Anthony

**Buff Id:** 1130441

**Course:** CIDM 6341(Cybersecurity)

**Assignment:** Wireless Survey/Phishing

**What did you do?**

I started by installing and opening Wireshark, a widely used tool for analyzing packets that capture, and log data transmitted through a device's network interface cards (NICs). Wireshark utilizes the npcap library from Nmap, a packet capture engine that intercepts network traffic. When set to promiscuous mode, Wireshark extends its capabilities beyond capturing traffic from just the host device to traffic from any local area network (LAN) device.

Wireshark's packet capture is comprehensive, as it monitors and records all network packets in real-time. These packets encompass all data exchanges between devices, whether browsing the Internet, streaming, or accessing local network services. The software tracks each packet moving through the network, enabling a thorough inspection of the packet headers, payloads, and other metadata. Wireshark also offers robust filtering capabilities, which allow users to focus on specific types of traffic, protocols, or devices to reduce unnecessary data clutter.

For my analysis, I utilized my home network, selected the appropriate network interface, and commenced capturing traffic. As soon as I began, Wireshark immediately started logging packets as they traversed the network. I employed filters to center the capture on specific criteria, such as IP addresses, protocols (such as TCP and UDP), and ports, to emphasize pertinent data while disregarding irrelevant traffic.

During the capture process, Wireshark documented Ethernet, ARP (Address Resolution Protocol), UDP (User Datagram Protocol), and TCP (Transmission Control Protocol) packets. These protocols are fundamental for network communication. Wireshark furnishes detailed information on the source and destination of each packet, the protocol used, the data's length, and the transmission time.

After about five minutes of data capture, I saved the log for additional analysis. The captured packets provided insight into which devices were communicating, the types of services being accessed, and the state of data transmission, like whether secure encryption methods like TLS were in use. By scrutinizing these packets, I could identify potential vulnerabilities, such as open services that expose the network to external attacks or unencrypted traffic that could be intercepted.

**What was the result?**

After installing and launching Wireshark, the capture interface showed real-time network activities. Upon starting the packet capture, the log displayed various network interactions, showing the number of packets, the timestamp for each packet, the source and destination IP addresses, the protocols used, the length of each packet, and additional information about the communication.A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The packets that were captured revealed the following:

**Packets 1 and 4: These** two packets are Ethernet broadcast messages used by devices within the local network. They are Address Resolution Protocol (ARP) requests used by devices to determine the MAC address associated with specific IP addresses.

**Packet 2: This** packet utilizes the User Datagram Protocol (UDP) to discover a service. This suggests that a service or application is broadcasting information across the network.

**Packets 3 and 5: These** packets indicate an ongoing Transmission Control Protocol (TCP) communication between the IP addresses. They acknowledge previously transmitted data, with sequence and acknowledgment numbers reflecting the current state of the communication. This indicates reliable data exchange between the two devices.

**Packets 6 to 9 These** packets are part of a Transport Layer Security (TLS) v1.2 communication, indicating establishing a secure session. This is likely related to HTTPS or another encrypted protocol. The packets involve the same devices as the preceding TCP packets, suggesting the continuation of the secure communication session.

The data obtained from Wireshark emphasizes the importance of implementing network monitoring to gain insight into the network's susceptibility to potential security breaches. Specifically, ARP requests, open TCP ports, and UDP broadcasts significantly amplify the network's exposure to potential attacks by revealing active devices and services. Moreover, the existence of TLS communications signifies the presence of encrypted traffic; however, it's imperative to note that encryption alone is inadequate without implementing robust encryption practices. In the absence of adequately configured or robust encryption, the risk of sensitive data being intercepted exists.

Frequent and consistent use of Wireshark is crucial for ongoing network monitoring. It enables the detection of any deviations in traffic patterns, appearance of new devices, or exposure of services that may pose security risks. Regular use of Wireshark is instrumental in identifying any unusual or unexpected network activities that could signify unauthorized access or a potential breach in the system. Incorporating Wireshark into regular monitoring practices empowers organizations to proactively identify vulnerabilities, allowing them to address and mitigate risks before they lead to an actual attack.

Intermittent use of tools such as Wireshark is essential for effective security planning. It facilitates the discovery of new attack pathways, adjustment of firewall rules, and updates to encryption methods to ensure long-term protection. Wireshark provides comprehensive insights into the flow of data across the network, enabling the identification of potential weaknesses and gradually reducing the network's overall vulnerability to attacks over time.

**What did you learn?**

Using Wireshark has significantly improved my understanding of network traffic capture and analysis. This tool provides a comprehensive overview of all network activities, making it crucial for identifying vulnerabilities and potential threats. With Wireshark, I have gained insight into how it dissects and presents individual data packets, revealing critical details such as source and destination IP addresses, protocols (e.g., ARP, TCP, and UDP), and even the security layers in encrypted traffic (e.g., TLS). This meticulous packet analysis is valuable for determining whether network issues are performance-related or security-related.

I have observed that ARP requests (as seen in packets 1 and 4 of my capture) risk exposing devices to ARP spoofing attacks, potentially enabling malicious actors to redirect traffic. Similarly, broadcasting UDP packets (as evidenced in packet 2) may expose network services or applications, expanding the attack surface and leaving these services vulnerable to potential attackers. Even with the implementation of secure protocols such as TLS for data encryption (seen in packets 6 to 9), Wireshark has highlighted the potential compromise of data due to misconfigurations within these encrypted sessions.

A vital observation is the proactive nature of regular network monitoring. Wireshark is not just a one-time tool; it should be integrated into routine network assessments to detect new vulnerabilities and suspicious activity effectively. Unforeseen network traffic or unfamiliar devices may indicate unauthorized access or misconfigured services. Through consistent packet data analysis, proactive identification of risks, such as unencrypted data transmission, unsecured protocols, or unauthorized device communications, can be achieved. This proactive stance can help bolster security controls, including firewall adjustments or encryption method upgrades, offering greater control over network security.

Another critical consideration is the ethical responsibility associated with the use of Wireshark. Examining network traffic has the potential to expose sensitive information and, in the absence of proper authorization, could violate privacy laws and organizational policies. Whether in an enterprise context or a home network environment, Wireshark's thoughtful and guideline-adherent use is essential to avoid legal consequences. A comprehensive understanding and adherence to these ethical considerations are crucial for maintaining a secure and trustworthy network environment.

In conclusion, Wireshark provides valuable insights into network traffic and security. However, it is essential to use it consistently to maintain a secure network posture. Its ability to proactively identify vulnerabilities is crucial for significantly reducing the attack surface and informing comprehensive security strategies, making it an indispensable tool for network troubleshooting and security planning.