Research Report 2 Wireshark

By: Farzaneh Noroozi
Professor: Dr. Murray Jennex

What did you do

Introduction:

In this report, we delve into the process of network and protocol identification and packet capturing using Wireshark, an industry-leading network analysis tool. This section outlines the methodology and approach I followed during the exercise, explaining how Wireshark works and how I utilized it to achieve the objectives set. The report emphasizes a concise and comprehensive understanding of the data manipulations, analysis techniques, and Wireshark's functionality.

How network and protocol identification and packet capturing were done:

Wireshark Overview:

Wireshark is a powerful open-source network protocol analyzer that enables users to capture and inspect network packets in real-time. Its versatile capabilities make it an invaluable tool for network administrators, security experts, and researchers alike. With Wireshark, one can capture, filter, and analyze network traffic, helping to diagnose network issues, investigate security incidents, and gain deep insights into network communication.

Methodology and Approach:

a. Familiarization with Wireshark: Before beginning the exercise, I thoroughly explored the resources provided by the professor, gaining a clear understanding of the objectives. To ensure a comprehensive grasp of Wireshark's functionalities, I referred to additional online resources and watched tutorial videos on platforms like YouTube. This thorough familiarization with the tool laid the foundation for an effective packet-capturing and analysis process.

b. Wireshark Installation: With a solid understanding of Wireshark, I proceeded to install the software on my computer. The installation process involved visiting the official Wireshark website, selecting the appropriate version for my operating system, and following the installation wizard to set up the application successfully. Ensuring proper installation was crucial to ensure smooth functioning during the packet-capturing phase.

c. Network Selection: To conduct the packet capture and analysis, I decided to utilize my home Wi-Fi as the testing environment. This choice allowed for a controlled and familiar setting to explore the network's behavior. Additionally, the use of a home network allowed me to capture a diverse range of network packets, including those from various devices and services.

d. Capturing Packets: Utilizing Wireshark's capture feature, I recorded network packets from my home network for a duration of up to 5 minutes. Throughout this period, I closely monitored the packet capture to ensure comprehensive data collection.

Packet Capturing and Network Identification:

a. Capturing Packets: Utilizing Wireshark's capture feature, I recorded network packets from my home Wi-Fi for a duration of up to 5 minutes. Throughout this period, I closely monitored the packet capture to ensure comprehensive data collection. Capturing packets in real time provided a snapshot of the network's current state, enabling in-depth analysis of its communication patterns.

b. Network and Protocol Identification: Following the packet capture, I diligently analyzed the collected data to identify the various networks and protocols in use. This process provided insights into the network's architecture and the communication patterns among devices and services. The identification of specific protocols allowed for a detailed understanding of the applications and services running on the network.

c. Analysis of Encrypted Content: While examining the captured packets, I paid particular attention to detecting any encrypted data. Understanding the presence of encryption was vital in assessing the network's security posture and potential vulnerabilities. Additionally, deciphering encrypted content provided insights into the types of encryption methods used within the network.

Wireless Network Signal Strength Analysis for our house and our neighbor's house:

a. Network Signal Assessment: I measured the signal strength of my Wi-Fi network at various points outside my house. To determine if unauthorized access was possible from the street, I tried to connect to my Wi-Fi network from different locations beyond the house boundaries.
b. Neighbor's Network Analysis: also investigated the signal strength of neighboring Wi-Fi networks to evaluate their security posture.

Exporting and Filtering Data for Comparison:

To facilitate further analysis and comparison, I utilized Wireshark's data export and filtering functionalities. By exporting the captured packet data, I could save it in various formats for later examination or share it with others for collaborative analysis. Additionally, I applied filters to isolate specific network packets based on criteria such as source IP address, destination port, or protocol type. These filtering capabilities allowed me to focus on relevant subsets of data and identify suspicious or unusual network activity effectively.

How the software works:

Wireshark functions as a network protocol analyzer, and its core functionality revolves around capturing, dissecting, and analyzing network packets. When you run Wireshark on your computer, it listens to the network interface, allowing it to intercept and capture packets that traverse the network. It operates in "promiscuous mode," meaning it captures all packets on the network, even those not specifically addressed to the machine running the software. This mode enables a comprehensive view of network traffic, making it an excellent tool for network analysis and troubleshooting.
Once Wireshark captures packets, it presents the data in a user-friendly graphical interface. It allows you to examine individual packets and understand the information they contain. The software supports various display filters, which allow you to narrow down the packets based on specific criteria, such as source or destination IP addresses, protocols, or port numbers. By using filters, you can focus on relevant packets and ignore the rest, which aids in the analysis process.
Wireshark's packet dissection capabilities are one of its strengths. It can interpret packets from numerous protocols and display their contents in a human-readable format. By analyzing packet contents, you can determine the protocols in use, understand the data exchanged between devices, and detect any abnormalities or security issues.
Additionally, Wireshark provides extensive statistical tools and graphs to help you visualize network trends and performance. These features enable you to identify patterns, track network usage over time, and diagnose issues such as latency, packet loss, or unusual traffic behavior.

How you analyzed the output:

Upon capturing network packets using Wireshark, the next step was to analyze the output to achieve the objectives of network and protocol identification, as well as gain insights into network behavior. The analysis process involved several key steps:
a. Network and Protocol Identification: After capturing packets from the home network, I examined the captured data to identify different networks and protocols in use. Wireshark's ability to dissect packets and interpret their contents allowed me to determine the communication protocols employed by various

devices and services on the network. This provided valuable information about the network's structure and the way devices interacted.

b. Analysis of Encrypted Content: During the examination of captured packets, I focused on detecting any encrypted data. Encryption is a crucial aspect of network security, and identifying encrypted traffic helped assess the network's security posture. While the encrypted content itself is not visible, the presence of encrypted data indicated that security measures were in place for sensitive communications.

c. Exporting and Filtering Data for Comparison: To facilitate further analysis and comparison, I utilized Wireshark's export and filtering functionalities. By exporting specific packet data, I could save it in various formats for later examination or sharing with others. Additionally, applying filters allowed me to isolate specific subsets of data based on criteria such as source IP address, destination port, or protocol type. These filtered subsets were instrumental in identifying and analyzing specific network activities or issues effectively.

d. Identifying Suspicious Ports: One of the crucial aspects of the analysis involved identifying packets associated with suspicious ports. By closely scrutinizing the captured data and cross-referencing with common port numbers used for standard services, I could flag any packets using uncommon or unauthorized ports. This process helped detect potential unauthorized network access or attempts at communication with unauthorized services, aiding in identifying potential security threats.

e. Analysis of Open Networks:

- **Detection of Open Networks:** In addition to analyzing my home network, I actively searched for and identified any open networks in the vicinity during the packet capture. Identifying open networks was important to assess their security implications and understand potential risks associated with unsecured networks.
- **Analysis of Open Networks:** The analysis of open networks involved assessing their security implications, highlighting potential risks associated with unsecured networks, and evaluating their impact on the overall attack surface. Analyzing open networks provided valuable insights into the broader network security landscape and offered opportunities for improving overall network security measures.

What are the results?

What can you see in the networks and protocols identified in the captured packets?

In the captured packets, we can observe various network protocols being used for communication. Some of the protocols are identified below:

a. QUIC Protocol Handshake: There are several instances of the QUIC protocol handshake (e.g., "Handshake, SCID", "0-RTT, DCID"). QUIC is a secure transport protocol designed by Google and has built-in security features. It is commonly used by services like Google, YouTube, and others. While the presence of QUIC packets is normal for web browsing, further inspection is necessary to validate the authenticity of the connections.

b. TCP Keep-Alive: The TCP Keep-Alive packets are a normal part of maintaining connections between hosts. They are used to ensure that the connection remains active, and their presence alone does not indicate any cyber-attack.

c. Application Data Packets: These packets contain data sent over TLS (Transport Layer Security) and potentially over other encrypted channels. Analyzing the content of encrypted packets is challenging without the encryption keys, so their nature cannot be determined without further decryption.

d. Protected Payload (KP0): Packets with "Protected Payload" often indicate encrypted data transferred through secure protocols. It's common for secure connections to be established during web browsing and other internet communications.
e. Discovery Protocols (SSDP, IGMPv2, IGMPv3, TiVoConnect): These are network discovery protocols used to locate devices and services on the local network. They are generally harmless and used for internal device discovery.
f. Dropbox LAN Sync Discovery (DB-LSP-DISC/JSON): Dropbox LAN sync discovery is used for Dropbox clients to discover other devices on the local network that are running Dropbox. It's a normal part of the Dropbox service.

Our house and our neighbor's house Wireless Signal Reach result:

a. Our network unauthorized Access: The wireless signal of my home network extended to approximately 15 feet outside my house/apartment. Despite the signal reaching outside, I am pleased to report that my network's security measures were effective. I was unable to connect to my Wi-Fi network from the street.
b. Neighbor's Network Security: The analysis of neighboring networks indicated that they were adequately secured. I could not access any of the neighboring Wi-Fi networks.

Do any packets reflect a cyber-attack?

As the results show it is not explicitly stated whether any packets reflect a cyber-attack. To determine if there are any cyber-attacks in the captured packets, further analysis and context are needed. Cyber-attacks could include actions like unauthorized access attempts, denial-of-service (DoS) attacks, malware propagation, or other malicious activities. It would be necessary to look for specific patterns or indicators of compromise within the packets to identify potential cyber-attacks.

How can you tell if there is a cyber-attack in the captured packets?

To determine if there is a cyber-attack in the captured packets, a detailed analysis is required. The process involves examining the packets for any signs of suspicious or malicious activities. Some common indicators of cyber-attacks in network traffic include:
a. unusual traffic patterns: A sudden increase in network traffic or unexpected types of traffic could indicate a DoS or DDoS attack.
b. Port scanning: Frequent attempts to connect to various ports may suggest a hacker probing for vulnerabilities.
c. Anomalous behavior: unusual packet sizes, malformed packets, or unexpected protocol usage might indicate an attack.
d. Exploits and payloads: Identifying known attack signatures or payloads in the packets can indicate specific attack attempts.
e. Unauthorized access attempts: Repeated login failures or authentication requests from unknown sources may indicate brute-force attacks.

Analyze the attack surface presented by the network and packets.

The attack surface refers to all the potential points of entry or vulnerabilities that attackers can exploit to compromise a system or network. From the provided packets, it is not immediately evident what the complete attack surface is. To analyze the attack surface, one would need more comprehensive information about the network's architecture, exposed services, and configurations.
The analysis should involve:

a. Identifying open ports and services: Analyzing the packets for open ports and services can reveal potential entry points for attackers.
b. Assessing security configurations: Evaluating security settings and configurations can highlight potential weaknesses.
c. Identifying software versions: Knowing the software versions can help determine if any known vulnerabilities exist.
d. Investigating device and network configurations: Understanding the devices' configurations and network topology can provide insights into potential weak points.

What are the areas subject to a cybersecurity attack based on the captured packets?

It's challenging to identify all the areas subject to a cybersecurity attack. However, in a general network context, potential areas subject to cybersecurity attacks include:
a. Internet-facing services: Services accessible from the internet are often targeted by attackers, such as web servers (ports 80 and 443), mail servers (port 25), or DNS servers (port 53).
b. Vulnerable software: Systems running outdated or unpatched software can be vulnerable to known exploits.
c. Misconfigured services: Services with poor configurations may expose sensitive information or allow unauthorized access.
d. social engineering targets: Attackers may use information from captured packets to craft social engineering attacks against individuals or organizations.
e. Unknown protocols: Protocols that are less common or proprietary could have unexplored vulnerabilities.
A comprehensive cybersecurity assessment requires a more in-depth analysis of the entire network environment, including configurations, security policies, and network architecture.

What are the results:

What I learned about digital networks, packets, and attack surface:

During the analysis using Wireshark, I gained valuable insights into digital networks, packets, and the concept of the attack surface. Some key learnings include:
a. Digital Networks: I learned that digital networks are intricate systems of interconnected devices that enable communication and data exchange. These networks consist of various components such as routers, switches, and access points, all working together to facilitate data transmission. Understanding digital networks is crucial for analyzing network traffic effectively.
b. Packets: In the context of digital networks, data is transmitted in small units called packets. Each packet contains essential information, including the source and destination addresses, protocol details, and the actual data payload. Analyzing packets using tools like Wireshark provides valuable insights into how devices communicate and what information they exchange.
c. Attack Surface: The concept of the attack surface refers to all the potential points of vulnerability in a network or system that an attacker could exploit. It includes open ports, exposed services, misconfigurations, and software vulnerabilities. Analyzing the attack surface helps identify potential weak points that require attention to enhance network security.

How I can use them in the future:

The knowledge gained about digital networks, packets, and the attack surface using Wireshark has practical applications for my future endeavors:

a. Network Troubleshooting: Understanding digital networks and how packets are transmitted allows me to troubleshoot network issues effectively. I can use Wireshark to diagnose network problems, identify bottlenecks, and pinpoint communication errors.

b. Network Security Analysis: Knowledge of the attack surface and how to analyze network packets enables me to assess network security comprehensively. I can identify potential vulnerabilities, monitor for suspicious activities, and implement measures to protect against cyber-attacks.

c. Cybersecurity Career: The insights gained from this analysis can serve as a stepping stone for a career in cybersecurity. By mastering network analysis techniques, I can contribute to securing digital infrastructures, detecting threats, and implementing robust security measures.

How they could be of value to the organization in the future:

The knowledge acquired about digital networks, packets, and the attack surface can be highly valuable for organizations:

a. Enhanced Network Security: By conducting regular network analysis using tools like Wireshark, the organization can strengthen its security posture. Identifying potential attack vectors and mitigating vulnerabilities can significantly reduce the risk of data breaches and unauthorized access.

b. Efficient Troubleshooting: Understanding how to analyze network packets helps IT teams in organizations troubleshoot network issues swiftly and accurately. This leads to reduced downtime and improved network performance, positively impacting productivity.

c. Proactive Cyber Defense: With knowledge of the attack surface, the organization can proactively identify weak points and prioritize security efforts. Implementing robust security measures based on the analysis can prevent potential cyber-attacks before they occur.

d. Compliance and Auditing: In regulated industries, conducting network analysis is essential for compliance and auditing purposes. Analyzing packets can help ensure that data is transmitted securely and in line with industry regulations.

e. Incident Response: During cybersecurity incidents, analyzing network traffic with tools like Wireshark can provide critical insights into the nature and scope of the attack. This information is invaluable for incident response teams to contain and remediate the incident effectively.

In conclusion, the analysis of digital networks, packets, and the attack surface using Wireshark has provided me with valuable knowledge applicable to network troubleshooting, cybersecurity, and organizational security enhancement. The insights gained can be leveraged in the future to contribute to improved network performance, better cybersecurity practices, and a proactive approach to defending against cyber threats within organizations.