Question 1

Unencrypted Protocols

To begin with the project, I updated and launched Wireshark in the cloud workspace. By following along with the instructional videos, I started off analyzing the general traffic in Wireshark from Ethernet 3. After that, I filtered by DNS on the same network and got a few results back. Next, I entered credentials on the Public RADIUS server, filtered for port 1812 on Wireshark, and opened up NTRadPing. From there, I entered the IP of the server, along with the port again, and sent one successful and one failed request. I went back into Wireshark to analyze the requests on port 1812.

After finishing the RADIUS traffic analysis, it was time for the HTTP Basic analysis. I entered a set of correct credentials and incorrect credentials on httpbin. Back on Wireshark, I filtered by port 80 and analyzed the traffic for both passwords I entered. Now going onto the HTTP Web Scraper Testing Ground, I entered the correct credentials to log in. On Wireshark, I filtered by port 80 again and analyzed traffic on Ethernet 3. Next, I needed to filter by DNS traffic, so I replaced the port 80 filter with port 53. Here, I simply analyzed the query and the response. Moving on to the Telnet section, I created a UNIX Shell Account on sdf.org, and went back onto Wireshark. This time I filtered by port 23 and opened Windows PowerShell to enter the Telnet command and login information. Next, I analyzed the first Telnet packet as well as the TCP Stream on Wireshark.

Encrypted Protocols

Now that the unencrypted protocols RADIUS, HTTP, DNS, and Telnet have been analyzed, and it was time for the encrypted ones, beginning with SSH. Unfortunately, at this point, my cloud workspace session timed out, so I just downloaded Wireshark on my own PC to continue following along. I filtered port 22 on Wireshark for my network and started capturing traffic. I went back onto Windows PowerShell and entered the sdf.org information and exited. From there, I analyzed the TCP conversations on Wireshark, there were 3 because I had entered an incorrect password a couple times. I clicked on the third one and followed the stream to see the encrypted data.

For the last encrypted protocol, HTTPS, I filtered port 443 on my network and captured traffic for a few seconds. I clicked on one of the application data results and looked at the encrypted application data. I made the ssl-keys.log file and made sure it was working by closing my browser and opening a website on it again. Back on Wireshark, I went into preferences and found the TLS protocol and entered the file path for ssl-keys.log in the log filename search box. I filtered port 443 on Wireshark and started to capture traffic. While doing so, I went onto the simple site and stopped capturing traffic. I analyzed the TCP conversations matching Address B

of the website, there were two. I followed the stream of the first one and went back to the packets to be able to analyze detailed information about the website, up to its source code.

How it Works

Capturing Traffic

- **Action:** Wireshark captures all packets transmitted over the network interface.
- **Purpose:** To record the data for later analysis.

Wireshark Filters

- **Purpose:** Filters help focus on specific types of traffic, such as DNS (port 53), HTTP (port 80), RADIUS (port 1812), Telnet (port 23), SSH (port 22), and HTTPS (port 443).
- **Usage:** Filters reduce the noise by showing only relevant packets for the protocol you are analyzing.

Protocol Analysis

- **Unencrypted Protocols:** Analyzing unencrypted traffic shows the data in plaintext, making it easy to see credentials and other information.
- **Encrypted Protocols:** Encrypted traffic is protected, so the data isn't immediately visible. Tools like ssl-keys.log enable decryption for HTTPS, while SSH traffic remains encrypted and shows how secure communication looks.

Authentication Traffic (RADIUS)

- **Process:** RADIUS sends authentication requests (Access-Request) and receives responses (Access-Accept or Access-Reject).
- **Purpose:** To verify network access.

Web Traffic (HTTP/HTTPS)

- **HTTP:** Sends data in plaintext, allowing you to see all details of web requests and responses.
- **HTTPS:** Encrypts data, requiring decryption for analysis.

DNS Traffic

- **Process:** Resolves domain names to IP addresses through DNS queries and responses.

- **Purpose:** Essential for understanding how domain names are translated to machine-readable IP addresses.

Telnet and SSH

- **Telnet:** Transmits data in plaintext, including login credentials.
- **SSH:** Encrypts all traffic, providing secure communication over the network.

Question 2

Results

General Traffic Analysis

- **Observation:** Captured general network traffic on Ethernet 3.
- **Details:** This initial capture included various types of traffic, mainly TCP, TLS, DNS, and others. It provides a broad overview of all communication happening over the network interface.

DNS Traffic Analysis

- **Observation:** DNS traffic was captured and analyzed.
- **Details:** Typical DNS packets that included queries and responses. Saw DNS queries sent from my PC to a DNS server, requesting the IP address for domain names, and the corresponding responses.
- **Security:** DNS traffic can be vulnerable to spoofing and cache poisoning attacks. Unexpected or malformed DNS responses could indicate such attacks.

RADIUS Traffic Analysis

- **Observation:** RADIUS authentication requests and responses were captured.
- **Details:** Saw Access-Request packets sent to the RADIUS server and Access-Accept and Access-Reject responses. Successful authentication includes the user credentials being sent and validated.
- **Security:** Anomalies in RADIUS traffic, such as repeated failed authentication attempts, could indicate a brute-force attack. Unexpected or unauthorized Access-Request packets might indicate an unauthorized access attempt.

HTTP Basic Analysis

- **Observation:** HTTP traffic was captured with both correct and incorrect credentials.

- **Details:** HTTP Basic Authentication sends credentials in Base64 encoded format, which is easily decodable. Saw both usernames and passwords in plaintext within the Authorization tab.
- **Security:** HTTP traffic is vulnerable to interception like a man-in-the-middle attack for example. Capturing credentials in plaintext is a significant security risk. Any unexpected or unauthorized HTTP requests could indicate an attempt to capture credentials or perform other malicious actions.

HTTP Form-Based Analysis

- **Observation:** Logged in with correct credentials and captured the traffic.
- **Details:** Like the basic analysis, I saw the HTTP protocols, and found my username and password information within the HTML Form URL Encoded tab.
- **Security:** Look for any unexpected HTTP requests or anomalies in the data, which could indicate malicious activity such as session hijacking or unauthorized data access.

Additional DNS Analysis

- **Observation:** DNS query and response traffic was captured.
- **Details:** Like the initial DNS analysis, showing the resolution of domain names to IP addresses.
- **Security:** Consistent with previous DNS observations. Watch for suspicious or anomalous DNS responses.

Telnet Traffic Analysis

- **Observation:** Telnet traffic was captured, showing login attempts.
- **Details:** Telnet transmits data in plaintext, I saw my username and password in the packets. The data transmitted during the session is also visible in plaintext.
- **Security:** Telnet is highly insecure due to the lack of encryption. Any unexpected Telnet sessions could indicate unauthorized access attempts or reconnaissance by an attacker.

SSH Traffic Analysis

- **Observation:** SSH traffic was captured, showing encrypted communication.

- **Details:** SSH packets are encrypted, so the actual data (including the username and password) is not visible. I saw the encrypted data in the packets.
- **Security:** SSH provides secure communication, but repeated failed login attempts could indicate a brute-force attack. Patterns or anomalies in the SSH traffic could indicate unauthorized access attempts.

HTTPS Traffic Analysis

- **Observation:** HTTPS traffic was captured and decrypted using the ssl-keys.log file.
- **Details:** Showed the actual data exchanged between my browser and the web server, including potentially sensitive information.
- **Security:** HTTPS ensures data integrity and confidentiality. However, if the ssl-keys.log file is compromised, the encrypted traffic can be decrypted and inspected by an attacker. Unexpected HTTPS sessions or anomalies could indicate a security issue.

Potential Cyber Attacks and Attack Surface Analysis

- **DNS:** Vulnerable to DNS spoofing and cache poisoning. Monitor for unexpected or malformed DNS responses.
- **RADIUS:** Brute-force attacks can be identified by repeated failed authentication attempts. Monitor for unauthorized Access-Request packets.
- **HTTP:** Vulnerable to interception and credential theft. Monitor unauthorized HTTP requests and unexpected data transmissions.
- **Telnet:** Highly insecure due to plaintext transmission. Monitor unauthorized Telnet sessions.
- **SSH:** Provides secure communication, but brute-force attacks can be identified by repeated failed login attempts. Monitor for patterns indicating unauthorized access attempts.
- **HTTPS:** Ensures data security, but compromised ssl-keys.log files can expose encrypted data. Monitor for unexpected HTTPS sessions and anomalies.

Attack Surface Analysis

- **Unencrypted Protocols:** Present a significant attack surface due to plaintext transmission. An attacker can intercept and read the data easily.

- **Encrypted Protocols:** Reduced attack surface due to encryption, but still vulnerable to certain attacks (e.g., brute-force attacks on SSH, and decryption if the ssl-keys.log file is compromised).

Practical Uses of Analysis Results

Network Security Monitoring

- **Detection of Unauthorized Access:** Regularly capturing and analyzing network traffic can help detect unauthorized access attempts. For instance, repeated failed login attempts in RADIUS, SSH, or Telnet traffic can indicate a brute-force attack.
- **Identifying Anomalies:** By understanding normal traffic patterns, anomalies that may suggest a security breach can be identified. For example, unexpected DNS responses or unauthorized HTTP requests can indicate a potential attack.

Vulnerability Assessment

- **Protocol Vulnerabilities:** The analysis highlights the vulnerabilities of various protocols. Unencrypted protocols like HTTP and Telnet are susceptible to interception and should be replaced with secure alternatives like HTTPS and SSH.
- **Security Improvements:** Identifying the use of insecure protocols can prompt network administrators to implement more secure configurations and protocols, thereby reducing the attack surface.

Incident Response

- **Forensic Analysis:** In the event of a security incident, captured traffic can be used for forensic analysis to determine the scope and impact of the breach. Detailed packet analysis can help trace the source of the attack and the method used.
- **Evidence Collection:** Captured packets can serve as evidence in investigating and responding to security incidents. They provide a detailed record of network activity that can be analyzed to understand the attacker's actions.

Compliance and Auditing

- **Regulatory Compliance:** Regular traffic analysis can help ensure compliance with security standards and regulations, such as PCI-DSS, GDPR, or HIPAA. It demonstrates that proactive measures are being taken to protect sensitive data.
- **Security Audits:** The results can be used in security audits to verify that appropriate security measures are in place and effective in protecting the network.

Network Optimization

- **Traffic Management:** Analyzing network traffic helps in understanding usage patterns and can lead to better traffic management. For instance, identifying bandwidth-intensive applications can help in optimizing network performance.
- **Identifying Misconfigurations:** The analysis can reveal network misconfigurations that might not be immediately apparent. For example, incorrect DNS configurations or unnecessary open ports can be identified and corrected.

Training and Education

- **Security Training:** The analysis process and results can be used for training purposes, helping IT staff and security professionals understand network protocols, how to capture and analyze traffic, and how to identify potential security issues.
- **Raising Awareness:** Sharing findings with the broader organization can raise awareness about network security, highlighting the importance of secure protocols and vigilant monitoring.

Question 3

Key Takeaways from the Assignment

1. **Understanding Network Traffic and Protocols**
    - **Variety of Protocols:** Gained hands-on experience with both unencrypted (RADIUS, HTTP, DNS, Telnet) and encrypted protocols (SSH, HTTPS).
    - **Traffic Patterns:** Learned to identify normal traffic patterns for various protocols and recognize deviations that might indicate security issues.
2. **Importance of Secure Protocols**
    - **Encryption:** Realized the critical role of encryption in protecting sensitive information, as evidenced by the difference between HTTP/Telnet and HTTPS/SSH traffic.
    - **Vulnerabilities:** Saw firsthand how unencrypted protocols expose data to potential interception and how encrypted protocols mitigate this risk.
3. **Packet Analysis Skills**
    - **Filtering and Capturing:** Developed skills in filtering specific types of traffic and capturing relevant packets for detailed analysis.
    - **Reading Packets:** Learned to read and interpret packet details, including headers and payloads, to understand the data being transmitted.
4. **Identifying and Analyzing Security Threats**

- **Anomalies:** Recognized how to identify anomalies in network traffic that could indicate security threats, such as repeated failed login attempts or unexpected DNS responses.
- **Attack Surface:** Understood the concept of the attack surface and how different protocols and configurations can either reduce or expand it.

Learning About Digital Networks, Packets, and Attack Surface

1. **Digital Networks**
    - **Complexity:** Networks are complex systems with multiple layers of communication and various protocols interacting simultaneously.
    - **Traffic Flow:** Observed how data flows through a network and how different protocols are used for different types of communication (e.g., DNS for name resolution, HTTP for web traffic).
2. **Packets**
    - **Structure:** Learned about the structure of network packets, including headers and payloads, and how to dissect them using Wireshark.
    - **Data Transmission:** Understood how data is transmitted in packets and the importance of each part of the packet in ensuring correct and secure communication.
3. **Attack Surface**
    - **Definition:** The attack surface is the sum of all the points where an unauthorized user could try to enter or extract data from the environment.
    - **Minimization:** Realized the importance of minimizing the attack surface by using secure protocols, strong authentication, and continuous monitoring.

Future Application and Organizational Value

1. **Personal Application**
    - **Enhanced Skills:** The skills learned will be valuable in any cybersecurity role, particularly in network monitoring, incident response, and vulnerability assessment.
    - **Proactive Security:** Ability to proactively analyze network traffic and identify potential security issues before they become serious threats.
2. **Organizational Value**
    - **Improved Security Posture:** Regular network traffic analysis can help improve the organization's overall security posture by identifying and mitigating vulnerabilities.

- **Incident Response:** Enhanced ability to respond to and investigate security incidents, using packet captures to trace and understand the nature of attacks.
- **Compliance and Auditing:** Assisting the organization in meeting regulatory compliance requirements through regular traffic analysis and secure protocol usage.
- **Training and Awareness:** The insights gained can be used to train other IT staff and raise awareness about network security within the organization.