Vernice Tanquerido

CIDM 6340 Network Management and Information Security

 Research report 2 – Wireshark

**What did you do**

Wireshark is an open-source network protocol and packet analyzer. Wireshark captures packets that are transmitted over a network or interface. It then returns information about each packet such as source and destination address, protocol used, length of the packet, and other information. A machine can have several interfaces and Wireshark will list each of these on the homepage.

In the guided project, Wireshark was accessed through the cloud workspace in Coursera. The exercise was divided into seven tasks

1. Getting to know Wireshark and its basic functionalities

In the first task, a pre-saved packet capture file was available to analyze. When you open the capture file, you will be able to see the time, source and destination Ip addresses, protocol used, length of the packet, and other information.

A screenshot of a computer

Description automatically generated

There are two ways to filter packets on the interface: display and capture filters. Both of these are used to manage the list of packets returned by Wireshark but have different purposes and applied at different stages in your analysis. The capture filter is used before you open the interface and Wireshark will only return those that meet the criteria set. While the display filter is used post-capture to only display the specific packets.

A screenshot of a computer

Description automatically generated

1. Generate and capture RADIUS Traffic

For the second task, we analyzed RADIUS – a simple clear text protocol. RADIUS provides centralized authentication and accounting management for users who connect to a network service. Filter port 1812 was used in the capture filter on Wireshark to capture traffic with RADIUS protocols. A server and Ip address was provided for the purpose of the exercise.

1. Analyze a HTTP Basic Authentication

HTTP is an application layer protocol that is designed for communication between web browsers and servers. Basic authentication is a simple challenge and response system where a server can request a username and password from a user.

HTTP works on port 80 which was applied to the capture filter on Wireshark. The project used a bookmarked webpage that captures username and password for analysis. Wireshark is set to run while information is sent over the server. The packet containing this information is then analyzed.

1. HTTP form-based authentication and DNS

Form based authentications use the standard HTML form fields to capture data. It also works on port 80 but send a POST request rather than a GET request. The project used a form-based webpage that captures username and password for analysis.

1. Initiate, capture, and analyze Telnet sessions

Telnet is a computer protocol for interacting with remove devices. It operates on TCP port 23. Traffic from tty.sdf.org was used for analysis in this project.

1. Capturing and analyzing SSH sessions

Like telnet, SSH is also used to communicate with remote devices. The main difference is that SSH uses encryption. SSH uses port 22.

A slightly different approach was used for this task. The same host was used for telnet was also used for SSH. All traffic happening in the interface was captured on wireshark to capture both telnet and SSH so we can compare. Wireshark can tell how many conversations are in a packet. This can be accessed when you go to statistics then conversations. The host, tty.sdf.org was analyzed, and in our case, we had two conversations – telnet and SSH.

1. Generate, capture, analyze then decrypt https traffic

In this task, we decrypted traffic by using a premaster secret key browser. This key is generated by the browser and logged into an SSL key log file. This key is used by the server to generate a master secret key that secures the data. The premaster key logged in the file is fed to Wireshark to decrypt the data in the packet.

**What are the results**

Results will be discussed by task:

1. Getting to know Wireshark and its basic functionalities

The pre-saved capture file uses a RADIUS protocol and all information are available for analysis. There was no encryption in all of the packets therefore data is vulnerable to cyber attacks.

1. Generate and capture RADIUS Traffic

RADIUS is a clear text protocol. It is unencrypted. All information about the packets is available without further effort. Using the credentials entered in the host server, we can see that the username is visible but the password is encyrpted. However this is a weak protection of the user’s credentials.

A screenshot of a computer

Description automatically generated

Wireshark can decrypt this password by providing the Shared Secret on the RADIUS protocol under preferences. Making it prone to cyber attacks.

A screenshot of a computer

Description automatically generated

1. Analyze a HTTP Basic Authentication

An HTTP basic authentication requires a simple username and password request from the user. When we entered port 80 on the capture filter, we are met with unencrypted data on all of the packets. We can see everything that is communicated within the network.

A screenshot of a computer

Description automatically generated

Looking at the server where we entered a username and password, wireshark was able to decrypt the base 64 encryption of the password, revealing the user’s credentials. This is an attack surface on the HTTP protocol and therefore must not be used when dealing with sensitive information.

A screenshot of a computer

Description automatically generated

1. HTTP form-based authentication and DNS

In this task form-based authentication was used instead of the basic authentication. However, the exercise has shown that this method is even less secure than the former when done on an HTTP protocol. The credentials are in the form of an html form field and is not even base 64 encoded. Therefore, all information is in clear text.

This opens areas for attackers to take advantage of user information. Thus, it is important to take note whether a form or website is running on HTTP or HTTPS.

A screenshot of a computer

Description automatically generated

DNS traffic is also not secure therefore precautionary measures should be taken when transferring data over these networks.



1. Initiate, capture, and analyze Telnet sessions

Telnet communicates with remote devices. Like the previous protocols, telnet is not a safe route when transferring data. All packets returned on wireshark are unencrypted meaning all information are available in clear text making it also susceptible to attacks.

A screenshot of a computer

Description automatically generated

1. Capturing and analyzing SSH sessions

Like telnet, SSH also interacts with remote devices. However, data is encrypted with an algorithm and uses an encryption key. It even has secondary security like asking users for authentication if they want to connect to a new host.

A screenshot of a computer

Description automatically generated

1. Generate, capture, analyze then decrypt HTTPS traffic

In this task, we decrypted traffic by using a premaster secret key browser. This is another security risk as confidential information may be revealed with this function.

A screenshot of a computer

Description automatically generated

**What did you learn**

In this assignment, I learned how to analyze network traffic using Wireshark. The exercise helped me identify the vulnerabilities and potential security risks posed by different protocols such as RADIUS, HTTP, HTTPS, DNS, Telnet, and SSH Traffic. The exercise identified the limitations and attack surfaces on traffic if not properly encrypted. Even in encrypted packets, we also need to recognize that these also have weaknesses and the potential to be decoded. I learned the importance of looking into the services where we provide sensitive information such as SSN, bank information, and other personal details and make sure that our data is secure before sending it to the server. By learning to analyze network traffic and understand the risks associated with transferring data over different networks, I can say that I’m better equipped to handle sensitive information and improve network security.