Project Report By

Name: Nikhil Thakur
Registration Number: 11903558
Section: KE010
Roll Number: B44
Course Code: INT 301
Course: Open-Source Technologies

***Topic**: Suppose you are a network analyst and implemented the sensor inside the firewall, working in the infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieving the Username and password from the given Web URL.*

Under the guidance of

Mr. Manpreet Singh
Department of Computer Science and Engineering
Lovely Professional University, Punjab
April- 2023

Index

1. Introduction

The Network Analyst is part of a team which is responsible for the University campus network infrastructures. The Network Analyst assists in designing, implementing, and maintaining the networks by managing network IP addresses, communicating network information and requirements to connect hosts onto the network, and installing, upgrading, and maintaining network routers, switches, firewalls, wireless access points, wireless controllers, other network devices and servers. The Network Analyst works with vendors to research emerging technologies and diagnose and resolve network problems. The Network Analyst utilizes multiple tools to monitor the network to ensure optimum performance and to assist in troubleshooting issues. The Network Analyst maintains internet links, works with other Information Services units, faculty, staff, and students in the integration, maintenance, and problem resolution of network services, maintains documentation and database information, and works with Procurement Services in the preparation and evaluation of bid specifications for network hardware and software.

The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

A port scanner is an application which is made to probe a host or server to identify open ports. Bad actors can use port scanners to exploit vulnerabilities by finding network services running on a host. They can also be used by security analysts to confirm network security policies.

1.1. Objective of the project

Suppose you are a network analyst and implemented the sensor inside the firewall, working in the infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieving the Username and Password from http://testphp.vulnweb.com/ website. Write the steps involved in scanning the port.

1.2. Description of the project

As a network analyst, the responsibility is to scan the HTTP request protocol by using the open-source port scanning tool Wireshark and retrieving the username and password from the website post scanning the protocol and gathering the user's login credentials.

A port scanner is an application which is made to probe a host or server to identify open ports. Bad actors can use port scanners to exploit vulnerabilities by finding network services running on a host. They can also be used by security analysts to confirm network security policies.

1.3. Scope of the project

The scope of the project to achieve the HTTP protocol scanning using Wireshark and obtaining username and password credentials from the given web URL and the same can be obtained using Wireshark tool.

2. System Description

2.1. Target System Description

The target system comprises of the following computing capabilities such as:
Operating System: Windows/Linux
Minimum RAM: 8 GB
Internet Connectivity: LAN/Ethernet/Wi-Fi
Hypervisor: VM WARE Pro
HDD: 100 GB

The computer system needs to be either Windows operating system or Linux operating system, basically, Linux is preferred and the most famous open-source OS KALI LINUX for the project deployment and target system.
The requirement of the internet access should be provided in order to scan the HTTP protocols using open-source tools such as Wireshark. Along with these, a web browser compatible with the OS version and system requirements should be available to access the web URL and for generating traffic on the system by which the Wireshark shall be able to scan the network traffic more precisely.

2.2. Assumptions and Dependencies (If Applicable)

- The target system has been managed by the hypervisor namely Oracle Virtual Box or VM Ware, which might need more memory as per the requirement to run the system smoothly without any issues.
- Availability of the Antivirus on the host system shall be there which can prevent the necessary operations to get carried out.
- The disk type used in this operation should be of NTFS File system and should have minimum disk capacity of about 25 GB to get the operation running smoothly on the system.
- The network analysts should have proper understanding about the HTTP protocol request methodologies and the procedures to run the HTTP scan.
- The network analysts should understand the architecture of the system before starting the inspection of the internet traffic, especially, the type of network connectivity such

as VPN connectivity and NIC (Network Interface Card) to carry out the process to get the desired output of the project at the end.

3. Analysis Report

The analysis report of the project is mentioned as per the following procedures which must be followed to get the desired output:

- Go to Kali Machine, post this start a web browser (Firefox) with the URL: http://testphp.vulnweb.com/.
- Start Wireshark network analyser tool.
- Open your URL in the browser and start Wireshark scanning.
- Go to login page and enter credentials.
- Now Stop the Wireshark scanning and save your packet file.
- Now check GET POST protocol in Wireshark.
- Encode the html file.
- Get the credentials.
- Save and Exit

3.1. System snapshots and full analysis report

Step 1: Open Kali Linux in a Virtual Machine with the help of a hypervisor software VM WARE.

Figure 1: Desktop of Kali Machine

Step 2: Now start Wireshark Protocol Analyzer and simultaneously start the Firefox Web Browser and input the Web URL on the Firefox and visit the web page.

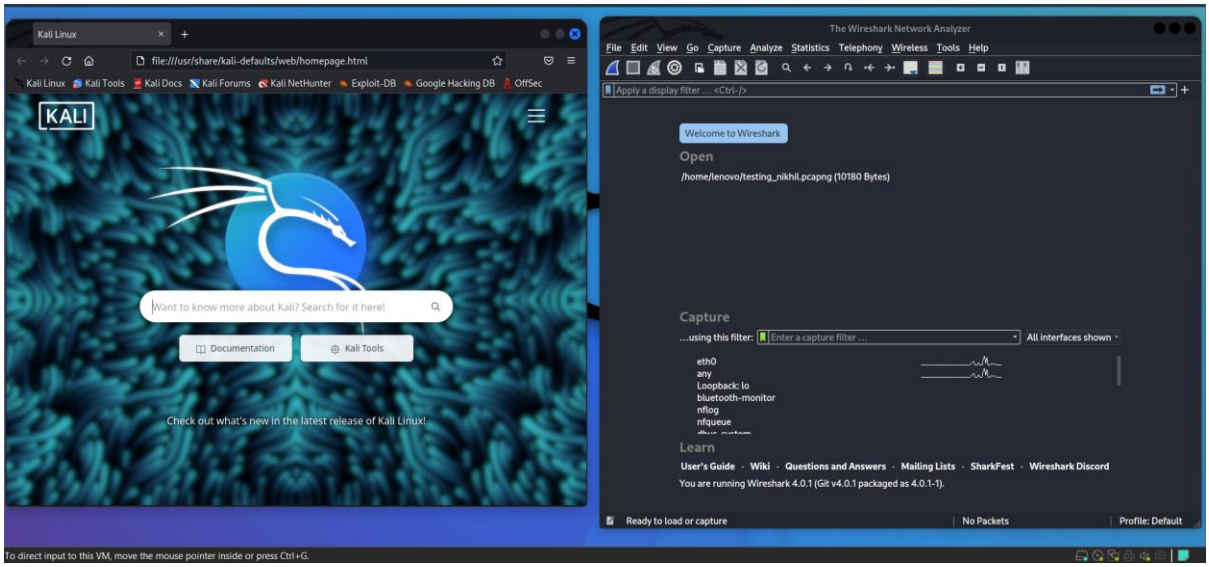

Figure 2: Firefox and Wireshark Window

Step 3: Now visit the Web URL and go to login page of the web page and enter user credentials.
Simultaneously, start the Wireshark network scanning by taking the Network interface as eth0 and check the scanning of the various protocols such as TCP, HTTP, ICMP, BGP, etc.

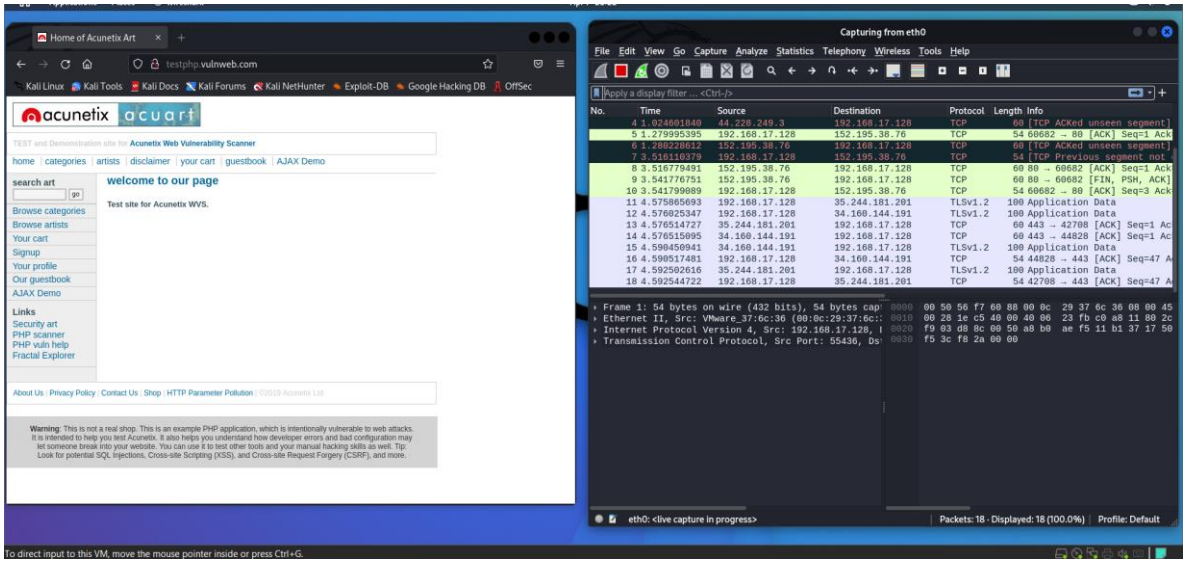

Figure 3: Opening WEB URL AND WIRESHARK TOOL.

Step 4: Now Enter the username and password and click on Login button on the web page.

Enter the username as Nikhil and password as any random password and click on Login button to POST the request to the web server of the HTTP.

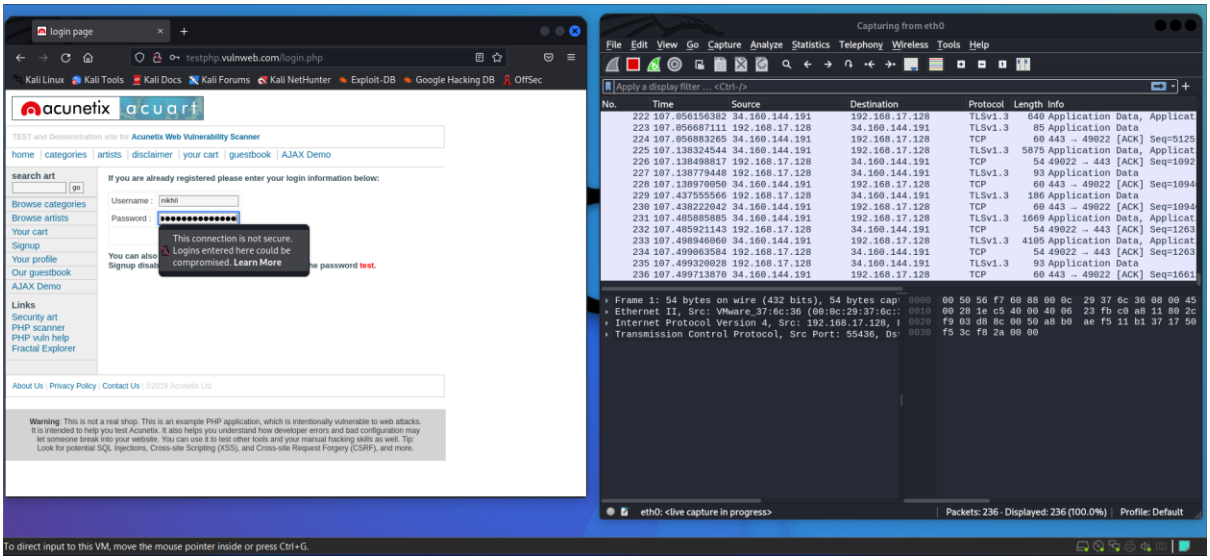

Figure 4: Entering Username and Password

Step 5: Now in the Wireshark, use the Wireshark filter options to filter out the HTTP protocol and inspect the network traffic of the HTTP protocol.

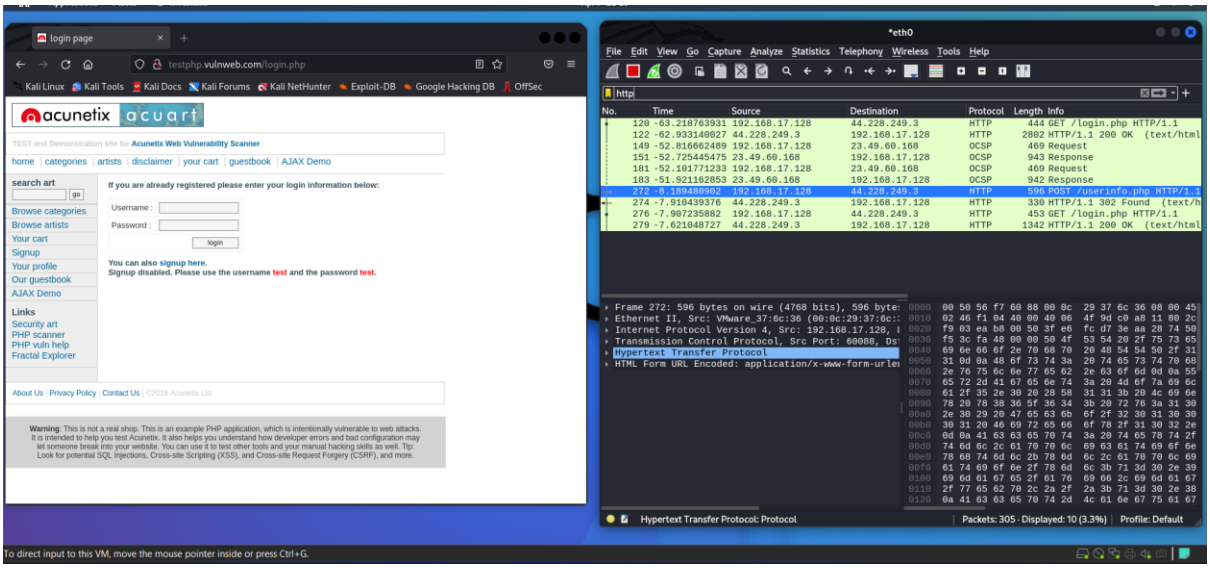

Figure 5: Inspecting HTTP Traffic.

Step 6: Now select the POST protocol, as we have entered the user information which will be sent to the web server using the POST protocol and check the user credentials by expanding the protocol.

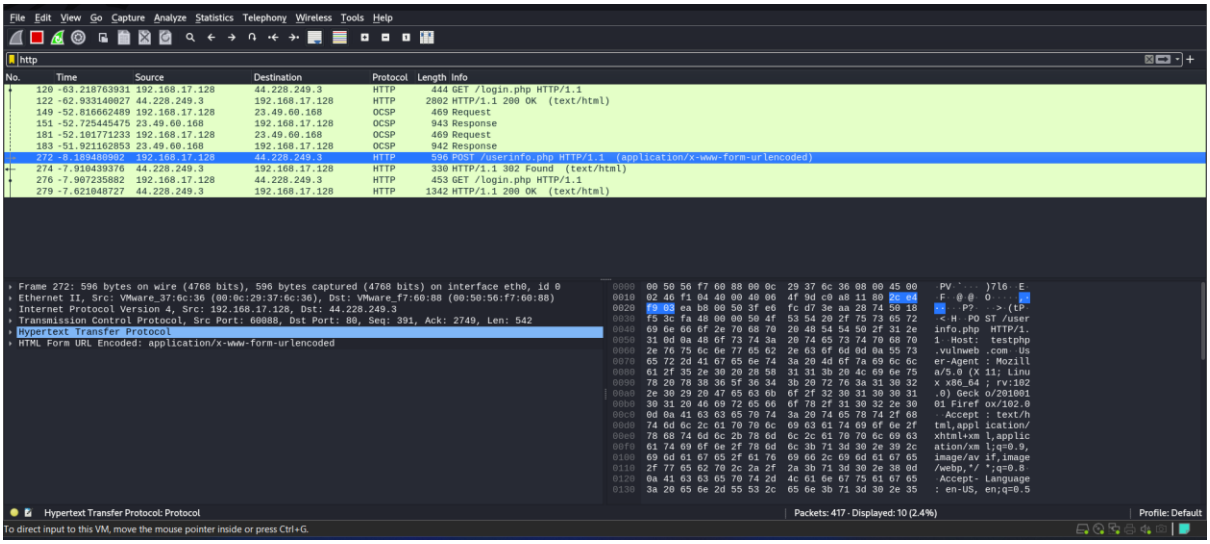

Figure 6: Inspecting POST Protocol.

Step 7: Now you can see the desired output as username and password along with the http inspection of the protocol during the web transmission.
The whole operation will be saved in a file with an extension of. pcap which can be checked in any OS with Wireshark installed in it.

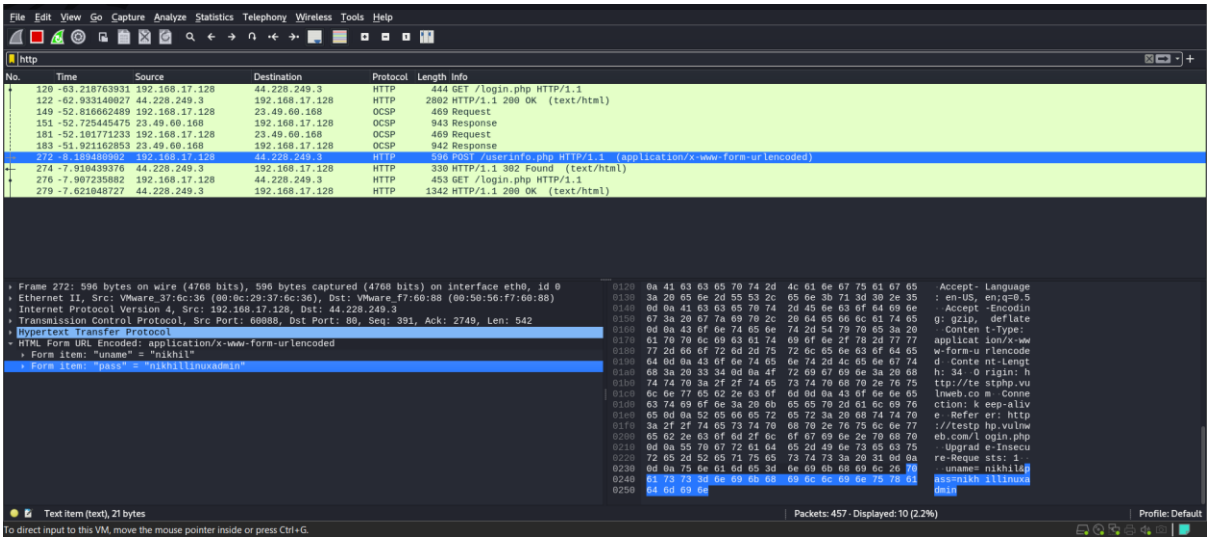

Figure 7: Final Output.

GITHUB LINK OF PROJECT: https://github.com/nikhil473/int301-nikhil

4. References

- https://www.wireshark.org/docs/
- https://wiki.wireshark.org/Hyper_Text_Transfer_Protocolrk.org
- https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/
- https://www.kali.org/tools/wireshark/