Task - 5

Protocol Analysis

Objective: Capture live network packets and identify basic protocols and traffic types

Tools: Wireshark

Overview:

In this task, network traffic analysis was performed using Wireshark in a controlled penetration testing environment with Kali Linux as the attacker machine and Metasploitable 2 as the target system. Three separate packet captures were created: first, capturing the results of an Nmap scan on Metasploitable 2 to identify open ports, services, and versions; second, recording an FTP anonymous login session to demonstrate how credentials and commands are transmitted in plain text over unencrypted FTP; and third, capturing traffic while logging into the preinstalled Damn Vulnerable Web Application (DVWA) on Metasploitable 2, revealing usernames and passwords in plain text due to the use of unencrypted HTTP. These captures highlight common network protocols, expose insecure communication practices, and serve as the basis for further protocol-level analysis.

Protocols:

1.DNS (Domain Name System):

A protocol used to translate human-readable domain names into IP addresses. Common operations include DNS Query (request for resolution) and DNS Response (returns the resolved IP address or other records like MX, CNAME).

2.FTP (File Transfer Protocol):

A protocol for transferring files between a client and server over TCP (commonly on ports 21 for commands and 20 for data). FTP commands include USER (username), PASS (password), LIST (list files), RETR (download file), and STOR (upload file). The server responds with numeric codes such as 220 (service ready), 331 (username OK, need password), 230 (login successful), and 550 (file unavailable).

3.HTTP (Hypertext Transfer Protocol):

A protocol used for communication between clients (usually browsers) and web servers, typically on port 80 (HTTP) or 443 (HTTPS). Common methods include GET (retrieve data), POST (submit data to the server), HEAD (retrieve headers only), PUT (upload data), and DELETE (remove resource).

4.ARP (Address Resolution Protocol):

A link-layer protocol used to map an IP address to its corresponding MAC address within a local network. Common operations are ARP Request (“Who has IP x.x.x.x?”) and ARP Reply (“IP x.x.x.x is at MAC xx:xx:xx:xx:xx:xx”).

5.TCP (Transmission Control Protocol):

A connection-oriented transport protocol that ensures reliable data delivery. It operates over various ports, each associated with a specific service: 22 (SSH – secure shell access), 21/20 (FTP – file transfer), 445 (SMB – file sharing on Windows), 80 (HTTP – web traffic), 443 (HTTPS – secure web traffic), and 25 (SMTP – email sending)**.**

6.SSDP (Simple Service Discovery Protocol):

A network protocol based on HTTP over UDP (usually on port 1900) used for discovering devices and services on a local network, often in UPnP (Universal Plug and Play) environments.

Network Types:

As we are using the both attacker and victim machines in vmware we find the:

Network type: virtual LAN

Layer 3: since we are using our own virtual lan, the ip addresses private ip addresses are in the range of the 192.168.x.x/24

Layer 2: Ethernet frames from each machine using ARP