Task 2: Man-in-the-Middle (MitM) Attack using Ettercap

Objective

The objective of this task was to perform a Man-in-the-Middle (MitM) attack using Ettercap by attempting ARP poisoning in order to intercept network traffic between a victim machine and the network gateway.

Lab Environment

- Attacker Machine: Kali Linux (VMware)
- Network Interface: tun0 (TryHackMe VPN)
- Tool Used: Ettercap
- Analysis Tool: Wireshark
- Platform: TryHackMe Virtual Lab

Tool Installation

Ettercap was pre-installed on Kali Linux.
Version verification command:

```
ettercap --version
```

Methodology

Step 1: Launch Ettercap

Ettercap was started in graphical mode using the following command:

```
sudo ettercap -G
```

Step 2: Interface Configuration

- Primary interface selected: **tun0**
- Sniffing at startup: **Enabled**
- Bridged sniffing: **Disabled**

This configuration ensures that Ettercap listens on the TryHackMe VPN interface.

Step 3: Host Discovery

From the Ettercap menu:

```
Hosts → Scan for Hosts
```

After scanning, the host list showed multiple IP addresses including:

- Attacker machine
- Network gateway
- Target machine

Step 4: Target Assignment

From the Hosts List:

- The victim IP was added to **Target 1**
- The gateway IP was added to **Target 2**

This setup is required for launching a MitM attack.

Step 5: ARP Poisoning Attempt

The ARP poisoning attack was initiated using:

```
MitM → ARP Poisoning
```

Option selected:

- ✓ Sniff remote connections

Observation and Limitation

Although Ettercap was correctly configured, ARP poisoning could not be fully executed in the TryHackMe environment. This is because:

- TryHackMe VPN (tun0) operates in a **routed Layer-3 network**
- ARP poisoning requires a **Layer-2 broadcast domain**
- Layer-2 attacks like ARP spoofing are not supported over routed VPN tunnels

This limitation is inherent to cloud-based lab environments and not due to misconfiguration.

Traffic Analysis

To validate traffic monitoring, Wireshark was used on the same interface:

```
sudo wireshark
```

Interface selected: **tun0**

Although active ARP poisoning was not possible, network traffic was successfully observed and analyzed.

Result

- Ettercap was successfully configured on the tun0 interface
- Hosts were discovered and targets were assigned
- ARP poisoning was attempted but restricted due to VPN limitations
- The attack scenario demonstrated how MitM attacks would function in a real Layer-2 network

Conclusion

This task demonstrated the configuration and attempted execution of a Man-in-the-Middle attack using Ettercap. While full ARP poisoning was not feasible due to the routed nature of the TryHackMe VPN, the lab effectively highlighted the attack methodology and real-world constraints. In a traditional LAN environment, the same technique could be used to intercept sensitive network traffic.