Task 3: Network Traffic Analysis using Wireshark

Objective

The objective of this task was to capture and analyze network traffic during a Man-in-the-Middle testing scenario using Wireshark. The goal was to observe live network packets, identify active protocols, and understand traffic flow between the attacker machine and the target system.

Lab Environment

- Attacker Machine: Kali Linux (VMware)
- Network Interface: `tun0` (TryHackMe VPN)
- Target IP Address: **10.48.157.8**
- Tool Used: Wireshark
- Platform: TryHackMe Virtual Lab

Tool Installation

Wireshark comes pre-installed with Kali Linux.
Tool verification command:

```
wireshark --version
```

Methodology

Step 1: Launch Wireshark

Wireshark was launched with root privileges to allow packet capture:

```
sudo wireshark
```

Step 2: Interface Selection

- Selected Interface: **tun0**
- Reason: tun0 is the VPN interface used for communication with TryHackMe target machines.

Step 3: Traffic Generation

Since the tun0 interface is a routed VPN interface with minimal background traffic, network activity was manually generated using ICMP requests.

Command used:

```
ping 10.48.157.8
```

This ensured that packets were actively transmitted and received for analysis.

Step 4: Packet Filtering

The following Wireshark display filters were applied to analyze traffic:

ICMP traffic

```
icmp
```

Target-specific traffic

```
ip.addr == 10.48.157.8
```

These filters helped isolate relevant packets exchanged with the target machine.

Captured Logs (Sample)

```
No.    Time        Source        Destination      Protocol  Length  Info
1      0.000000    10.48.157.6   10.48.157.8      ICMP      98      Echo
(ping) request
2      0.031245    10.48.157.8   10.48.157.6      ICMP      98      Echo
(ping) reply
3      1.000342    10.48.157.6   10.48.157.8      ICMP      98      Echo
(ping) request
4      1.031678    10.48.157.8   10.48.157.6      ICMP      98      Echo
(ping) reply
```

(10.48.157.6 represents the attacker machine IP assigned by the VPN)

Observation

- ICMP echo request and reply packets were successfully captured.
- Traffic between the attacker machine and the target IP (10.48.157.8) was clearly visible.
- No Layer-2 traffic (ARP, LLMNR, NBT-NS) was observed due to the routed nature of the VPN.
- The tun0 interface only carried manually generated and targeted traffic.

Result

- Wireshark successfully captured live traffic on the tun0 interface.
- Target-specific communication was identified using filters.
- The task demonstrated effective packet capture and protocol analysis in a VPN-based lab environment.

Conclusion

This task demonstrated the use of Wireshark for analyzing network traffic in a controlled lab environment. Although broadcast and Layer-2 traffic were not present due to VPN routing, meaningful analysis was achieved by generating ICMP traffic manually. The captured packets confirmed successful communication with the target machine and validated the network monitoring setup.