Attack Simulation: VPN Traffic Capture Scenario

1. Initial Setup

- Ensure the VM has network connectivity.

- Confirm that your VPN is running and establishes a TUN interface (tun0 or tun1).

2. Verify Network Connectivity

Commands:

```
ping -c 3 facebook.com
```

```
ping -c 3 amazon.com
```

Purpose:

Ensure DNS and general internet access work before capturing traffic.

3. Identify VPN Interface

Command:

```
ip a
```

Purpose:

Find the TUN interface created by the VPN.

4. Start Traffic Capture on VPN Tunnel

Command:

```
sudo tcpdump -i tunX -n port 80
```

Purpose:

Capture HTTP traffic inside the VPN tunnel.

5. Generate HTTP Traffic

Commands:

```
curl http://example.com
```

Or visit:

http://example.com

Purpose:

Create HTTP packets so tcpdump can display them.

6. Expected tcpdump Output

Example:

```
IP 10.x.x.x > 93.184.216.34: Flags [S], seq..., ack...
```

Meaning:

The VM sends HTTP requests through the VPN and tcpdump captures them.

7. Key Points

- VPN uses a virtual tunnel interface (tunX).
- HTTP traffic is visible.
- HTTPS traffic is encrypted and cannot be inspected.
- The scenario demonstrates traffic monitoring inside a VPN tunnel.

End of Simulation.