Experiment No: 2

Aim:

Detecting Suspicious Activity: Analyze network traffic to identify suspicious patterns, such as repeated connection attempts or unusual communication between hosts.

HTTPS Traffic Analysis (Wireshark):

Step 1: Start a Wireshark capture.

Step 2: Open a web browser and go to any HTTPS-based website.

Step 3: Stop the Wireshark capture.

Step 4: In the filter box, enter: 'ssl'

Step 5: Observe the first TLS packet - The destination IP is the target (server) IP.

TCP Traffic Analysis:

Step 1: Input filter: 'tcp.port == 80' to monitor only HTTP TCP traffic.

Step 2: Find the TCP [SYN] packet.

- Expand Ethernet:
  - Destination: Default Gateway MAC
  - Source: Your MAC address
- Expand IP:
  - Destination IP: e.g., Google
  - Source: Your local IP
- Expand TCP:
  - Flags: SYN (start of 3-way handshake)

Analyze TCP [SYN, ACK] Packet:

Step 1: Locate a TCP [SYN, ACK] packet.

- Ethernet:

- Destination: Your MAC address
    - Source: Default Gateway
- TCP:
    - Acknowledgement number: One higher than previous segment
    - Flags: [SYN, ACK] shows second step of handshake

Analyze SYN Flood Attack:

Step 1: Use 'hping.3' to flood the victim IP.

Step 2: Simultaneously, start capturing traffic on Wireshark.

Step 3: Use filter: 'tcp.flags.syn==1' to view SYN packets flood.

Step 4: Notice a lot of SYN packets with no time lag.

Analyze DoS Attacks:

Step 1: Use the 'macof' tool to flood the switch with MAC addresses.

Step 2: Observe IP addresses generating repeated traffic.

Step 3: For DDoS, use 'macof' to simulate fake IP addresses sending packets repeatedly.

Filtering Suspicious Activity:

Detecting Repeated Connection Attempts:

- Use TCP SYN filter: 'tcp.flags.syn==1 && tcp.flags.ack==0'
- Look for multiple attempts from the same source IP

Failed Login Attempts Filter (for SSH or RDP brute force):

- Filter: 'tcp.port==22 || tcp.port == 3389'

Detecting Unusual Communication Between Hosts:

- Go to Statistics -> Conversations
- Look at the IP and TCP/UDP connections
- Identify hosts with unusually high connections