Network Security and Forensics

Lab Session 4

Submitted To:-

Dr. Lokesh Chauhan Sir

Submitted By:-

Saloni Rangari

M.Tech. AIDS

1) Use Cisco Packet Tracer tool to design and configure a small network.

a) Create a network topology with routers, switches, and end devices.

i) Assign IP addresses and configure routing protocols (e.g., RIP, OSPF).

1. **Open Cisco Packet Tracer**: Launch the application on your computer.
2. **Add Devices**:
   - Drag and drop the required devices (routers, switches, PCs) into the workspace. For example, add one router, multiple switches, and several PCs.
3. **Connect Devices**:
   - Use the connection tool (lightning bolt icon) to connect the devices. For example, connect the router to each switch using straight-through cables.
4. **Assign IP Addresses**:
   - Click on each PC, go to the **Desktop** tab, and select **IP Configuration**. Assign IP addresses, subnet masks, and default gateways according to your network design. For instance:
     - PC1: IP 192.168.1.2, Subnet Mask 255.255.255.0, Gateway 192.168.1.1
     - PC2: IP 192.168.1.3, Subnet Mask 255.255.255.0, Gateway 192.168.1.1
5. **Configure the Router**:
   - Click on the router, go to the **CLI** tab, and enter the following commands to assign IP addresses to the router interfaces:

```
bash

enable

configure terminal

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit
```

6. **Set Up Routing Protocols**:
   - For RIP:

```
bash

router rip

version 2

network 192.168.1.0
```

   - For OSPF:

```
bash
```

```
router ospf 1

network 192.168.1.0 0.0.0.255 area 0
```

ii) Simulate traffic between devices and analyze packet flow.

1. **Use the Simulation Mode**: Click on the **Simulation** tab to switch to simulation mode.
2. **Generate Traffic**:
   - Use the **ping** command from one PC to another to generate traffic. For example, from PC1, open the command prompt and type:

     ```
     bash

     ping 192.168.1.3
     ```
3. **Observe Packet Flow**:
   - In simulation mode, you can see the packets moving between devices. Click on the **Show All/None** button to view all packets, and then select specific protocols (like ICMP) to filter the view.

iii) Implement basic firewall rules and observe their effect.

1. **Access the Router's CLI**: Click on the router and go to the CLI tab.
2. **Configure Basic Access Control Lists (ACL)**:
   - To block traffic from a specific IP:

     bash

     ```
     access-list 1 deny 192.168.1.3

     access-list 1 permit any

     interface FastEthernet0/0

     ip access-group 1 in
     ```
3. **Test the Firewall Rules**:
   - Attempt to ping the blocked IP from another PC. Observe that the ping fails, indicating that the firewall rules are effective.

2) Capture and analyze network traffic using Wireshark.

a) Capture traffic on a local network (such as HTTP, DNS, or FTP traffic).

Start Capturing Traffic

1. **Open Wireshark**: Launch Wireshark on a computer connected to the network.
2. **Select the Network Interface**: Choose the appropriate network interface for capturing traffic.
3. **Start Capture**: Click on the shark fin icon or use Ctrl + E to start capturing packets.
4. **Generate Traffic**:
   - Perform actions such as browsing a website (HTTP), resolving domain names (DNS), or transferring files (FTP).

i) Identify different types of traffic, protocols, and their purposes.

1. **Apply Display Filters: Use filters to isolate specific types of traffic. For example:**
   - **For HTTP: http**
   - **For DNS: dns**
   - **For FTP: ftp**
2. **Analyze Protocols:**
   - **Click on individual packets to view their details in the packet details pane. Observe the source and destination IP addresses, port numbers, and protocol information.**
3. **Understand Purposes:**
   - **HTTP is used for web traffic, DNS resolves domain names to IP addresses, and FTP is used for file transfers.**

ii) Analyze the captured packets to understand how data travels through a network.

1. **Examine Packet Flow**: Look at the sequence of packets to understand how data is transmitted. Use the **Follow TCP Stream** feature to see the entire conversation between two endpoints.

2. **Check Headers**: Analyze packet headers to understand how data is encapsulated and transmitted. Pay attention to:

   - Source and destination IP addresses

   - TCP/UDP port numbers

   - Flags and sequence numbers in TCP packets

3. **Visualize Data Flow**: Use the **Statistics** menu in Wireshark to generate graphs and statistics about the captured traffic, helping to visualize data flow and identify bottlenecks.

4. **Document Findings**: Take notes on the types of traffic observed, their purposes, and any anomalies in the data flow.

iii) Discuss the implications of unsecured protocols and how perimeter devices can help secure them.

1. **Unsecured Protocols**: Discuss the risks associated with using unsecured protocols like HTTP and FTP, including vulnerabilities to eavesdropping and man-in-the-middle attacks.
2. **Perimeter Security Devices**: Explain how firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) can help secure network traffic by monitoring and controlling incoming and outgoing traffic based on predetermined security rules.
3. **Best Practices**: Recommend using secure alternatives (e.g., HTTPS instead of HTTP, SFTP instead of FTP) and implementing strong firewall rules to protect sensitive data during transmission.