**Practical 2**

**Objective:**  
 Gain hands-on experience with networking commands and tools used in cybersecurity tasks like network monitoring, diagnostics, and reconnaissance.

**Section 1: Basic Network Diagnostics**

1. **Checking Network Interfaces:**  
    Use the ifconfig or ip a command to list all available network interfaces on your system.  
    **Question:** Identify the active interface and its IP address. What is the MAC address of your primary interface?
2. **Verifying Connectivity:**  
    Use the ping command to test the connectivity to a remote server (e.g., [google.com](https://pdpumail.pdpu.ac.in/owa/redir.aspx?C=C82eLSStCMNRdO6cdotcN3MPwojgV34Id_p_rNXK_Ne6_4hwlzDdCA..&URL=http%3a%2f%2fgoogle.com)).  
    **Question:** Capture and analyze the output. What do the time, TTL, and packet loss values indicate?

**Section 2: ARP and Routing**

1. **Displaying ARP Table:**  
    Use the arp or ip neigh command to display the ARP table of your machine.  
    **Question:** Identify the MAC address of the default gateway. Why is the ARP table important in networking?
2. **Viewing the Routing Table:**  
    Use route -n or ip route to display the current routing table.  
    **Question:** Find the default route. What is its significance in network traffic flow?

**Section 3: Network Statistics and Sockets**

1. **Monitoring Active Connections:**  
    Use the netstat or ss command to display active TCP and UDP connections.  
    **Question:** Identify the open ports and the services associated with them. Why is this information critical for cybersecurity?
2. **Network Statistics:**  
    Use netstat -i or ip -s link to view detailed network interface statistics.  
    **Question:** Identify any errors, dropped packets, or collisions. How can such issues affect network performance?

**Section 4: ICMP Tools**

1. **Traceroute Analysis:**  
    Use the traceroute command to trace the route to a popular website (e.g., [kali.org](https://pdpumail.pdpu.ac.in/owa/redir.aspx?C=27sraHANscmRPyYIGFoihNc9MGVIfR5RaBWScUMokaC6_4hwlzDdCA..&URL=https%3a%2f%2flinkprotect.cudasvc.com%2furl%3fa%3dhttp%253a%252f%252fkali.org%26c%3dE%2c1%2chJj9fqVRpYgsELSXzM2xwrAeCez_4IqKE5dCqvL14J7o44PeOsIt_PydO0MTbDzKVh5jYlbsUZGvBIhLR1aIR8HlYgQ8-S-D0XcQt0sAQMdg%26typo%3d1)).  
    **Question:** How many hops does it take to reach the destination? Identify any notable delays.
2. **MTR Analysis:**  
    Use the mtr tool to perform a real-time network path analysis.  
    **Question:** Compare the output with traceroute. What additional insights does mtr provide?

**Section 5: Advanced Commands**

1. **Packet Sniffing:**  
    Use the tcpdump command to capture packets on an interface. Filter packets for ICMP traffic only.  
    **Question:** Capture the output when performing a ping to a remote server. How can this data be useful in detecting a network attack?
2. **Network Interface Manipulation:**  
    Disable a specific interface using ifconfig down or ip link set down.  
    **Question:** What happens to the network connection? Re-enable the interface and verify connectivity.

**Section 6: Report Submission**

* Create a lab report with the following:
  + Command used
  + Output screenshot (where applicable)
  + Explanation of results