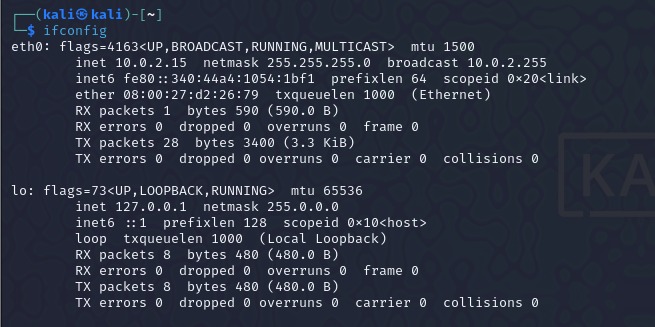
**Practical 2**

**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.

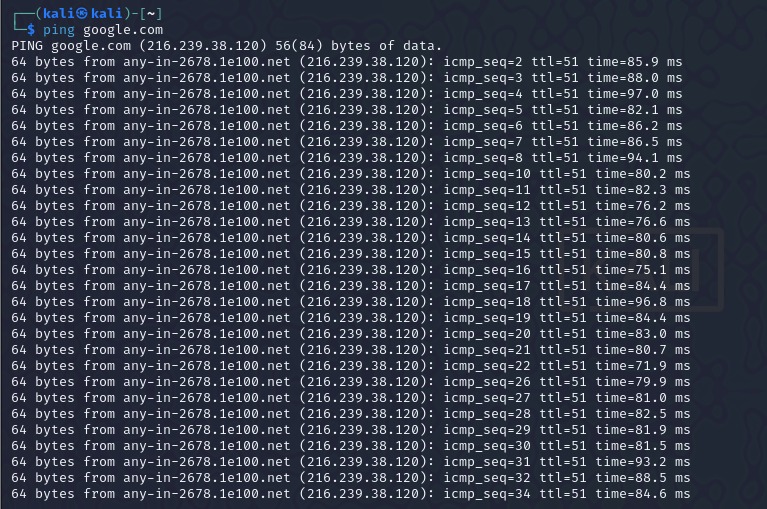
**(a).** ifconig

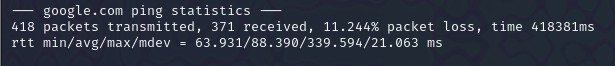
  
**Explanation:**

ifconfig is a command-line tool in Linux/Unix for managing network interfaces. It displays details like IP addresses, MAC addresses, and subnet masks. You can enable/disable interfaces (up/down) or assign IP addresses. For example, ifconfig eth0 192.168.1.10 sets an IP. Note: It's deprecated on modern systems and replaced by the ip command.

1. **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)).

**(a).** ping



  
 **Explanation:**

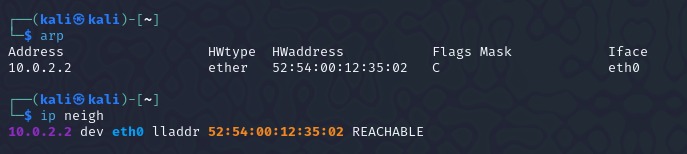
The ping command tests network connectivity between your system and another device by sending ICMP Echo Request packets and measuring response times. It's used to check if a host is reachable and to diagnose network issues.

**Section 2: ARP and Routing**

1. **Displaying ARP Table:**  
    Use the arp or ip neigh command to display the ARP table of your machine.

**(a).** arp

**(b).** ip neigh

  
**Explanation:**

**a) arp**

The arp command manages the ARP table, mapping IP addresses to MAC addresses in a local network. Use arp -a to view mappings, or add/remove entries with arp -s/arp -d. It’s mainly used for troubleshooting but is now deprecated.

**b) ip neigh**

The ip neigh command replaces arp for managing ARP and NDP entries. Use ip neigh to view neighbors, and add/remove entries as needed. It’s part of the modern ip suite for network management.

1. **Viewing the Routing Table:**  
    Use route -n or ip route to display the current routing table.

**(a).** route -n

**(b).** ip route

  
**Explanation:**

**a) route -n**

The route -n command displays the kernel's IP routing table with numerical addresses (no DNS lookups). It shows the destination, gateway, and network interface details, used to analyze or troubleshoot routing issues.

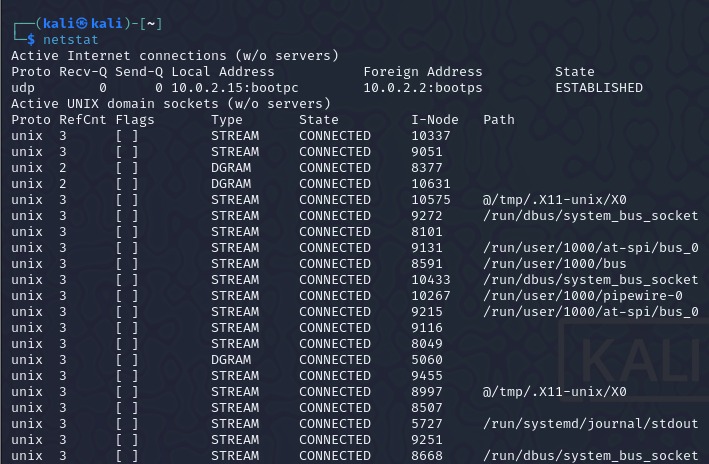
**b) ip route**

The ip route command is a modern replacement for route, used to view and manage the routing table. Use ip route show to display routes, and add/remove routes with ip route add/del. It's part of the ip suite for advanced network management.

**Section 3: Network Statistics and Sockets**

1. **Monitoring Active Connections:**  
    Use the netstat or ss command to display active TCP and UDP connections.

**(a).** netstat



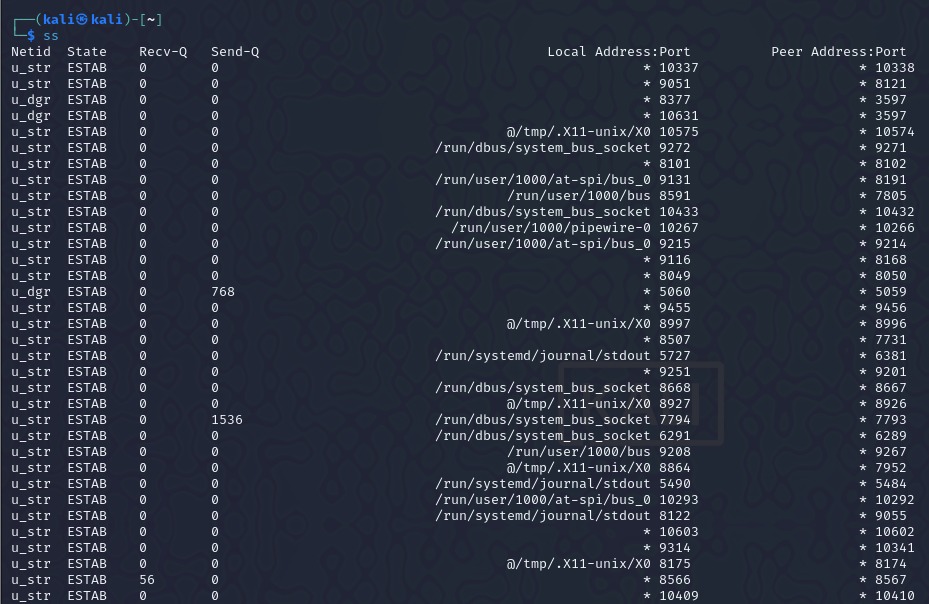
**Explanation:**

The netstat command displays network statistics and connection details in Linux/Unix. It helps monitor and troubleshoot network issues.

**Key Uses:**

1. **Show Active Connections:** netstat -an lists all open ports and connections.
2. **Display Listening Ports:** netstat -l shows services waiting for connections.
3. **View Interface Statistics:** netstat -i shows network interface usage.
4. **Routing Table:** netstat -r displays the system’s routing table.

**(b).** ss

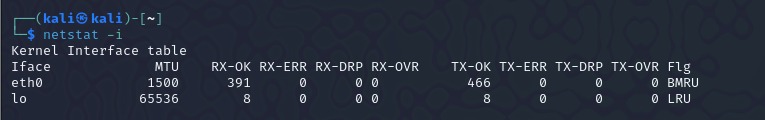


**Explanation:**

The ss command is a modern replacement for netstat, used to display socket statistics and monitor network connections more efficiently.

**Network Statistics:**  
 Use netstat -i or ip -s link to view detailed network interface statistics.

**(a).** netstat -i



**Explanation:**

The netstat -i command displays statistics for network interfaces on a Linux/Unix system. It provides details like packets sent/received, errors, and dropped packets for each interface.

**(b).** ip –s link

  
**Explanation:**

The ip -s link command displays detailed information and statistics for network interfaces in Linux.

**Key Details:**

1. **Interface Info**: Shows interface names, statuses (e.g., UP, DOWN), and MAC addresses.
2. **Statistics**: Provides packet-level details:
   * **RX (Receive)**: Packets, bytes, errors, dropped packets, etc.
   * **TX (Transmit)**: Packets, bytes, errors, dropped packets, etc.
3. **Use Case**: Useful for diagnosing network issues like packet loss or interface errors.

This command is part of the modern ip toolset for managing network configurations.

**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)).

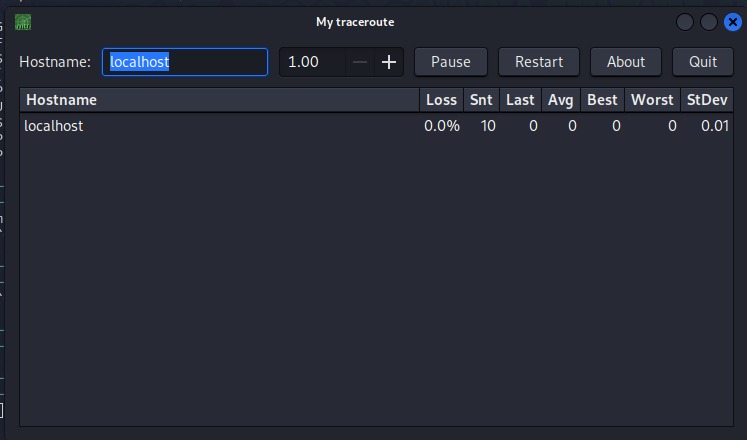
**(a).** traceroute

  
**Explanation:**

The traceroute command is used to trace the path that packets take from your system to a destination, typically a server or IP address. It helps diagnose network routing issues by showing each hop along the route and the time it takes to reach each hop.

1. **MTR Analysis:**  
    Use the mtr tool to perform a real-time network path analysis.

**(a).** mtr



**Explanation:**

The mtr (My Traceroute) command is a network diagnostic tool that combines the functionality of traceroute and ping. It provides a real-time, continuous analysis of the route and performance between your system and a destination.

**Key Features:**

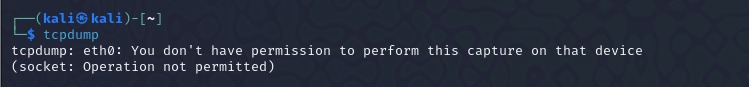
1. **Real-time Tracing**: Continuously shows the route and updates with round-trip times for each hop.
2. **Network Performance**: Displays packet loss and latency information for each hop.
3. **Usage**: mtr google.com shows the path and performance to google.com, updating in real-time.

It is more dynamic than traceroute and helps diagnose network issues effectively.

**Section 5: Advanced Commands**

1. **Packet Sniffing:**  
    Use the tcpdump command to capture packets on an interface. Filter packets for ICMP traffic only.

**(a).** tcpdump

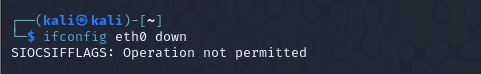


**Explanation:**

tcpdump is a command-line packet analyzer that captures and displays network traffic in real-time. It's widely used for network troubleshooting and monitoring.

1. **Network Interface Manipulation:**  
    Disable a specific interface using ifconfig down or ip link set down.

**(a).** ifconfig eth0 down



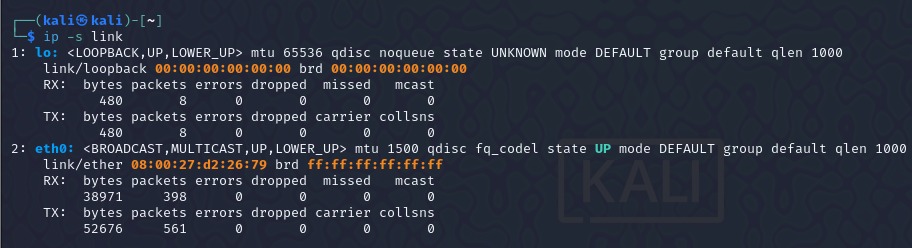
**Explanation:**

The command ifconfig eth0 down is used to disable the network interface eth0 on a Linux/Unix system.

**Effect:**

* **Disables Interface**: It brings down the specified network interface (eth0), causing it to stop sending or receiving traffic.
* **Example Use Case**: This can be used for troubleshooting or when you need to temporarily disconnect the interface from the network.

**(b).** ip –s link



**Explanation:**

The ip -s link command is used to display detailed information and statistics about network interfaces on a Linux/Unix system.

**Output Includes:**

1. **Interface Info**: Displays the name (e.g., eth0, lo), MAC address, and status (e.g., UP, DOWN).
2. **Statistics**: Shows the number of packets received (RX) and transmitted (TX), as well as errors, dropped packets, and more.
   * **RX**: Received packets, errors, dropped packets, etc.
   * **TX**: Transmitted packets, errors, dropped packets, etc.