1. **Use the ping command to test the connectivity to a remote server (e.g., example.com).**

ping example.com

1. **Write a script to measure the round-trip time for each packet and analyze the results.**

TARGET=”example.com”

Ping -c 10 $TARGET | awk -F ‘/’ ‘END {print “Min RTT: “ $3 “ ms, Avg RTT: “ $5 “ ms, Max RTT: “ $7 “ ms”}’

1. **Use the traceroute to trace the route packets take to a destination**

traceroute example.com

1. **Analyze the output to identify any potential bottlenecks or points of failure in the route.**

**Analyze Traceroute Output**

When analyzing the output of the traceroute, look for:

* **High Latency**: Identify any hops with significantly higher response times.
* **Timeouts**: Any \* \* \* entries indicate that a hop did not respond. This may suggest a potential bottleneck or a firewall blocking ICMP packets.
* **Consistent Delays**: If a hop consistently shows delays, it could be a point of failure.

1. **Use the nslookup command to find the IP address of a given domain (e.g., example.com).**

nslookup example.com

1. **Use the netstat command to view active connections and listening ports on your machine.**

This command shows:

* -t: TCP connections
* -u: UDP connections
* -l: only listening ports
* -n: show numerical addresses instead of resolving hostnames

1. **Use the ifconfig (Linux) or ip a command to display network interface configurations.**

ip a

1. **Perform a basic network scan using nmap on your local network to identify active devices and open ports.**

nmap -sP 192.168.1.0/24

nmap -sn 192.168.1.0/24

1. **Create a report summarizing the devices found, their IP addresses, and the services running on the open ports.**

nmap -sV 192.168.1.0/24 > report.txt

1. **Capture network packets using tcpdump on a specific interface.**

Ifconfig

sudo tcpdump -I eth0 -w capture.pcap

1. **Analyze the captured packets for specific protocols (like HTTP or DNS) and summarize your findings.**

tcpdump -r capture.pcap -A -s 0 ‘tcp port 80’

1. **Use the whois command to gather registration information about a domain.**

whois

1. **Use the hostname command to display and change the hostname of your machine.**

hostname

sudo hostname shashank

1. **Use the finger command to gather information about users on a system.**

finger

1. **Use the who command to see who is currently logged into the system and the last command to view the login history.**

who

last