Basic Networking Commands

ifconfig (Linux) or ipconfig (Windows): Displays the network interface configuration, including IP addresses, subnet masks, and other network details.

* netstat: Shows network connections, routing tables, and network interface statistics. Useful options include:
  + netstat -tuln: Displays listening ports and associated programs.
  + netstat -r: Shows the routing table.
* traceroute (Linux) or tracert (Windows): Traces the route that packets take from your computer to a destination IP address or domain, showing each hop along the way.
* nslookup (or dig on Linux): Performs DNS (Domain Name System) lookups to retrieve DNS records, including IP addresses associated with a domain.
* wget or curl: These tools are used to make HTTP requests and retrieve web content. They can be used to test connectivity and fetch data from URLs.
* ssh (Secure Shell): Connects to a remote server using the SSH protocol. It allows you to securely access and manage remote systems.
* ping (Packet Internet Groper): Sends ICMP echo requests to a target IP address or domain to check connectivity and measure round-trip time.
* arp (Address Resolution Protocol): Displays and manages the mapping between IP addresses and MAC addresses in a local network.
* ifup (Linux) or ifconfig /all (Windows): Brings up a network interface that is currently down.
* route (Linux) or route print (Windows): Shows or modifies the IP routing table, which determines how network traffic is directed.

Top - command to monitor CPU and memory usage

netstat -tuln | grep <port-number>

wget https://downloads.apache.org/tomcat/tomcat-10/v10.0.12/bin/apache-tomcat-10.0.12.tar.gz

wget <http://archive.ubuntu.com/ubuntu/pool/universe/t/tree/tree_1.7.0-3_amd64.deb>