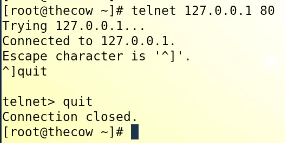
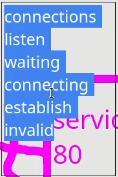
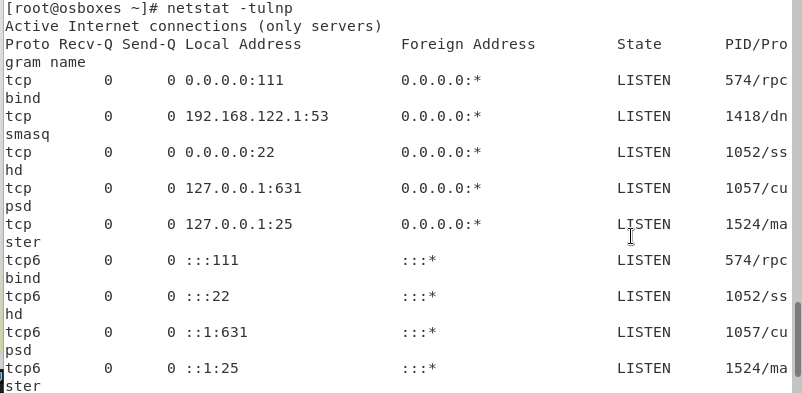
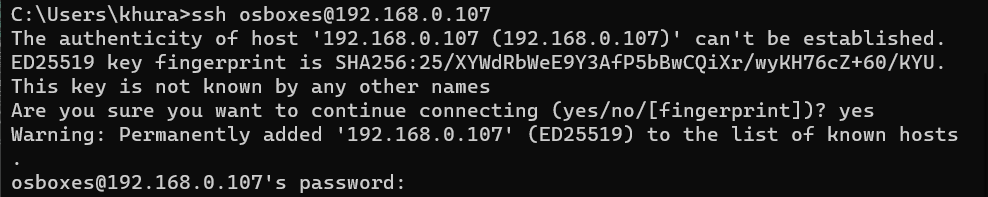
Lecture 05

**NW6-Ports-Sniffer-RPM**

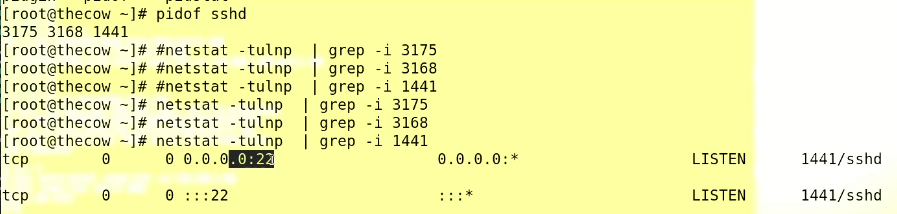
To open “tomcat” port which is 8080 à or any specific port , à its service must be started

* $ service tomcan start
* Tip:- to start a file in “less” mode à $ less <file\_name\_and\_path>
* $ less /etc/service
* Total ports à 0 .. 65535
  1. 1 .. 1023 à privileged ports à http, ftp, ssh etc
  2. 1024 ..65535 à non -privileged ports à not commonly used
* **nmap**
* Nmap (Network Mapper) is an open-source security tool used for network exploration, management, and security auditing. It can be used to discover hosts and services on a computer network, and to determine the operating system and version of the devices that are running on the network.

Nmap is available for most operating systems, including Windows, Linux, and macOS. It can be run from the command line or through a graphical user interface. It is widely used by network administrators and security professionals to assess the security of their networks and to identify potential vulnerabilities.

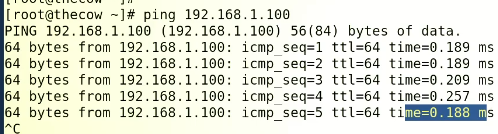
* $ nmap 127.0.0.1 à checks locally opened ports on a server
* **$ nmap <clint\_IP> à to check opened ports on a client.**
* $ nmap <domain\_IP> à it will check whole network i.e $ nmap 192.168.0.1/24
* Steps to check ports on home network
  1. $ ip rl à to know network IP à then run that IP for opened ports
* Another tool to check opened ports à “telnet”
* telnet checks specific IP address
* $ telnet 127.0.0.1 80
  1. 
  2. To check a client that port “80” is opened or not
  3. $ telnet <client\_IP>
* Another command to check specific port, à telnet checks the ports and returns.
* $ nc --> netcat
* $ nc 127.0.0.1 80
* **Remeber:-** “nc” command doesn’t show anything, if it shows nothing it means connection is established
* 
* Once telnet or nc confirms that the port is open à we can connect the remote machine as mentioned below, à in browser,
* 
* If telnet return that port is not opened or connection to specific port is refused, then we may not be able to connect the remote machine through browser
* To check opened ports and which client is connected,
* The command is,
* 
* $ netstat -an/-vatnp/-tulnp à different flags have different effects and results
* 
* To establish a remote connection with base machine and VM
* I used following steps as demonstrated by Sir Kazim Sheikh,
  1. Opened “cmd” on windows machine
  2. > ssh [osboxes@192.168.0.107](mailto:osboxes@192.168.0.107) à to login to my VM which is CentOS 7, “osboxes” is my VM machine name, “192.168.0.107” is IP of my VM
  3. I entered password of my VM and logged in remotely,,
  4. Text

     Description automatically generated
  5. The returned to my VM and typed command,
  6. $ netstat -an | grep 22 à to check the status of port “22” which is default port for “ssh” service, and found that connection is “ESTABLISHED” à base machine is connected via its IP à “192.168.0.103” and it is also displaying base machine’s PID “3501” to my VM.
  7. Table

     Description automatically generated with low confidence
  8. To check which port is assessed by a process,
  9. 
  10. sshd à here “d” means “deamon” which denotes that ssh is a “deamon” process.
  11. The flag “-tulnp” means
* "t" option displays TCP connections
* "u" option displays UDP connections
* "l" option displays only listening sockets
* "n" option displays numerical addresses (instead of resolving hostnames)
* "p" option displays the process ID (PID) and name of the program that owns the socket.
  1. “-vatnp”
* "v" option displays detailed information about the connections and sockets.
* "a" option shows both listening and non-listening sockets.
* "t" option displays TCP connections
* "n" option displays numerical addresses (instead of resolving hostnames)
* "p" option displays the process ID (PID) and name of the program that owns the socket.
  1. “-an”
* "a" option shows both listening and non-listening sockets.
* "n" option displays numerical addresses (instead of resolving hostnames)
  1. Tip:- “|grep -i ”

The "grep -i" command is used to search for a specified string or pattern in a file or the output of a command. The "grep" command stands for "global regular expression print" and it is used to search for lines in a file or output that match a specific pattern or string. The "-i" option tells grep to perform a case-insensitive search.

When used in combination with a pipe ("|"), the "grep -i" command can be used to filter the output of another command. For example, you can use it to find all processes listening on a specific port, by running the command "netstat -an | grep -i :80" which will display all the lines from the netstat output that contain the string ":80" (the default port for HTTP traffic) regardless of the case.

* ping
* 
* Ping is a monitoring tool à 64 bytes (by default) packed is sent to check à 188 mili second is the time consumed
* Ping checks a specific “IP” whether it is up or down à
* 
* $ ping -c 6 <IP-address> à to get the output 6 times only
* $ to increase packet size instead of 64 bytes,
* $ ping -s 1024 <ip-add> à “-s”” flag is for size of ping packet
* $ ping -i eth1 <IP\_add> à to use a specific “interface” for ping to go out
* **Query :- why ping does not have and port?**

The "ping" command is used to test the connectivity between two devices on a network. It works by sending Internet Control Message Protocol (ICMP) "echo request" packets to a target host and waiting for an "echo reply" in return. The "ping" command is designed to test the reachability and basic connectivity of a host on a network, rather than testing the availability of a specific service or port.

A port is a specific number assigned to a network service or application, such as HTTP (port 80) or SSH (port 22). The port number is used to direct incoming traffic to the correct service or application running on a host. When a host receives a packet on a specific port, it knows which service or application to pass that packet to.

Since the "ping" command is not checking for a specific service or application, it doesn't need to use a port number. Instead, it uses the ICMP protocol, which operates at a lower level than TCP or UDP. This allows the "ping" command to determine if a host is reachable and responding to ICMP packets, without needing to know about specific ports or services.

* 
* **ping works on layer 4 or transport layer**

**tracerout google.com**

Traceroute is a network troubleshooting tool used to display the route and measure the transit delays of packets across an Internet Protocol (IP) network. It can help identify the path that a packet takes from the source host to the destination host, as well as any intermediate routers or devices along the way. It works by sending a sequence of packets with gradually increasing time-to-live (TTL) values, and recording the IP address of each device that sends an ICMP "time exceeded" message in response. The resulting output shows the list of devices and the time it takes for a packet to reach each hop, which can be used to identify bottlenecks or connectivity issues along the route.

* The routers passed in the way to reach googl.com are called “hops”

$ tcpdump à packet sniffer or packet capturing tool.

* To check how many packets are in and out from a server or a n NIC
* $ tcpdump -vvv à CLI (wireshark) tool

Other Network Monitoring tools

* 1. Iptraf
  2. Ipref
  3. Wireshark
  4. nmon

Nagios: An open-source monitoring tool that can be used to monitor servers, network devices, and applications.

Wireshark: A free and open-source packet analyzer that can be used to capture, analyze, and troubleshoot network traffic.

PRTG Network Monitor: A comprehensive network monitoring tool that can be used to monitor servers, network devices, and applications.

SolarWinds Network Performance Monitor: A commercial network monitoring tool that provides real-time visibility into network performance and availability.

Zabbix: An open-source monitoring solution that can be used to monitor servers, network devices, and applications.

Splunk: A powerful log analysis tool that can be used to monitor and troubleshoot network issues

Cacti: A web-based network monitoring and graphing tool that uses SNMP to monitor network devices

Icinga: A open-source monitoring tool that can be used to monitor servers, network devices, and applications.

CloudWatch: A monitoring service from Amazon Web Services that can be used to monitor AWS resources and the applications you run on AWS

OpenNMS: An open-source network management platform that can be used to monitor network devices, servers, and applications.

These are some of the most widely used network monitoring tools, but there are many others available as well, each with its own unique set of features and capabilities.

**Package management**

* definition à to write files in the Hard Disk
* in Linux “rpm” is just like “exe” in Windows OS
* “rpm” stands for Redhat Package Manager

RPM (Red Hat Package Manager) is a package management system used by some Linux distributions, such as:

* 1. Red Hat Enterprise Linux (RHEL)
  2. Fedora
  3. CentOS
  4. Oracle Linux
  5. Scientific Linux
  6. SUSE Linux Enterprise Server (SLES)

Debian package (deb) is a package format used by some Linux distributions, such as:

1. Debian
2. Ubuntu
3. Linux Mint
4. Pop!\_OS
5. elementary OS
6. Kali Linux
7. Raspbian
8. Mint Debian
9. LMDE (Linux Mint Debian Edition)

$ rpm -ivh <package\_name>.rpm à

The command "rpm -ivh" is used to install an RPM package on a Linux system.

The options used in the command are:

* i : install
* v : verbose (show detailed information during the installation process)
* h : hash (show progress using a hash mark)
* $ dbpkg -i <package\_name>.deb
* To check total installed software in our CentOS system ,
* $ rpm -qa
* “-qa” à query all because in system there is a rpm database for managing a rpm package
* To install “zsh” package
* zsh (Z shell) is a Unix shell that is similar to the Bourne shell (sh) and the Bourne-Again shell (bash), but with additional features and improvements. It is often considered to be a more powerful and feature-rich alternative to the default shell on many Linux and UNIX systems.
* Some of the key features of zsh include:
* Auto-completion: zsh provides advanced auto-completion features for commands, options, and file paths, which can save time and reduce typing errors.
* Globbing: zsh supports advanced pattern matching for file names, known as "globbing," which allows for powerful and expressive commands.
* History: zsh has a powerful history mechanism that allows users to easily recall and reuse previous commands, and offers advanced search and editing capabilities.
* Plugins: zsh has a large number of plugins available that can add additional functionality, such as syntax highlighting, theme support, and more.
* Themes: zsh has a large number of themes available that can be used to customize the appearance of the shell,
* zsh is popular among developers and system administrators because of its advanced features and capabilities, and is often recommended for use in place of the default shell for increased productivity and efficiency.