Network Monitoring:

NMAP:

yum install nmap* -y

1. ping whole N/W

nmap -sP <N/W-ip>/subnet

2. to check open ports

nmap -sT -p 80,443 <N/W-ip>/subnet ; # T=tcp connect

3. 3 way handshake on TCP

nmap -sS -p 80,443 <n/w-ip>/subnet ; # S=stealthy,sysscan

4. to display top 1000 ports open for a specific host

nmap -sT <any-ip>

nmap -sS <any-ip>

5. to check open ports for a specific host

nmap -O <any-ip>

6. to check smb info, traceroute, DNS, NFS and more

nmap -A <any-ip> ; # try different host or n/w ip

7. Decovey IP address:

#nmap -sS -D <source-ip_Decovey> <destination-ip>

TCPDUMP:

yum install tcpdump -y

1. # tcpdump

2. display packets in DNS format

tcpdump -I enp0s3 ; # enp0s3 = name of your ethernet interface

3. to limit your output

 # tcpdump -c 8 -i enp0s3

4. display in Ascii format

tcpdump -A -i enp0s3

5. Hexadecimal format

tcpdump -xx -i enp0s3

6. to display available interfaces

tcpdump -D

7. to save captured packets in a target file (.pcap)

tcpdump -w <filepath>.pcap -i enp0s3

8. to read a .pcap file

tcpdump -r <filepath>.pcap

9. to display packet details in IP format

tcpdump -n -i enp0s3

10. capture packets only on TCP protocols

tcpdump -i enp0s3 tcp

11. to monitor a specific port

tcpdump -i enp0s3 port 443

Example: ssh root@<ipaddr> -p24865

12. Packets transferred to a specific source IP address.

tcpdump -i enp0s3 <source-ip>

Check with # ssh root@<source-ip>

tcpdump -i enp0s3 <destination-ip>

NETSTAT:

netstat –help or # netstat -h

1. -a -all : Show both listening and non-listening sockets. With the –interfaces option, show interfaces that are not up

netstat -a | more ; # To show both listening and non-listening sockets.

2. List all tcp ports.

netstat -at ; #To list all tcp ports.

3. List all udp ports.

netstat -au ; #To list all udp ports.

4. List only listening ports.

netstat -l ; #To list only the listening ports.

5. List only listening TCP ports.

netstat -lt ; # To list only the listening tcp ports.

6. List only listening UDP ports.

netstat -lu ; # To list only the listening udp ports.

7. List only the listening UNIX ports

netstat -lx ; #To list only the listening UNIX ports.

8. List the statistics for all ports.

netstat -s ; # To list the statistics for all ports.

9. List the statistics for TCP (or) UDP ports.

netstat -st(TCP) ; # To list the statistics for TCP ports.

netstat -su(UDP) ; # List the statistics for UDP ports.

10. Display PID and program names in the output.

netstat -pt ; # To display the PID and program names.

11. Print the netstat information continuously.

netstat will print information continuously every few seconds.

netstat -c ; # To print the netstat information continuously.

12. The non-supportive address families in the system.

netstat --verbose ; # To get the non-supportive address families in the system.

13. The kernel routing information.

netstat -r ; # To get the kernel routing information.

14. The port on which a program is running.

netstat -ap | grep ssh ; # To get the port on which a program is running.

15. Which process is using a particular port:

netstat -an | grep ':80' ; # To get the process which is using the given port.

16. List of network interfaces.

netstat -i ; # To get the list of network interfaces.

17. Display extended information on the interfaces

(similar to ifconfig) using netstat -ie:

netstat -ie ; # To display extended information on the interfaces