COMPUTER NETWORKS INDUSTRY PROBLEM-1

TEAM MEMBER 1-BHARGAV M V

SRN:PES1UG20CS660

TEAM MEMBER 1-MAHESH SHRIPAD BHAT

SRN:PES1UG20CS661

TEAM MEMBER 1-P CHAITANYA P S

SRN:PES1UG20CS669

PROBLEM STATEMENT:

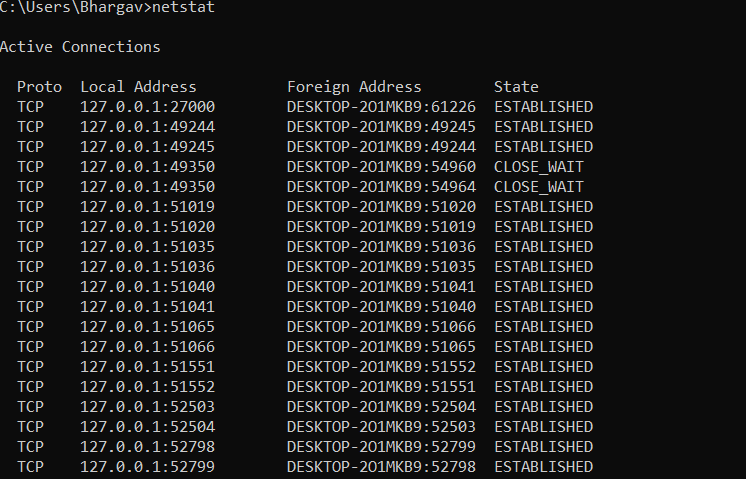
Web Server monitoring techniques  
An organization has deployed a Windows based web server on its network. The network  
administrator has to identify the appropriate techniques for analyzing the below parameters.  
1.TCP traffic (Incoming TCP Syn requests, TCP reset connections, TCP established connections,  
TCP half open connections)  
2.Technique to monitor specific application requests on Web server  
3.Technique to monitor HTTP Get requests to on Web server  
4.Server bandwidth  
5.Port status of the web server  
A combination of different types of tools like Wireshark, nmap, netstat is to be used with  
appropriate commands and filters identified for achieving the required output.  
Deliverable:  
1. Technique to monitor TCP SYN requests to the web server with wireshark output  
2. Technique to monitor TCP reset connections sent to and from the Web Server with wireshark  
output  
3. Technique to monitor established open connections on a Web Server with netstat output  
4. Technique to monitor TCP half open connections on the Web Server with netstat output  
5. Technique to monitor requests to a specific application on the Web server with wireshark output  
6. Technique to monitor HTTP GET requests to the web server with wireshark output  
7. Technique to monitor server bandwidth with netstat output  
8. Technique to monitor the port status of a Web Server with nmap output

NETSTAT:

the **netstat** command (short for “network statistics”) is used to display protocol statistics and current TCP/IP network connections.

We will test netstat without passing any argument

Display all the current connections,

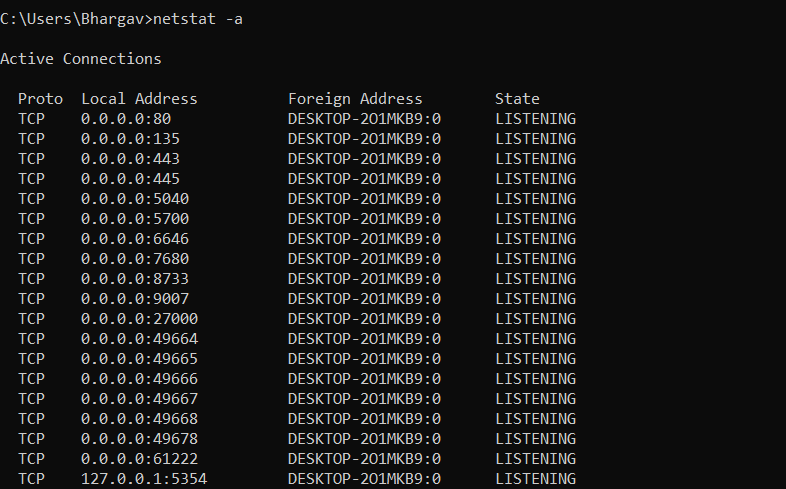


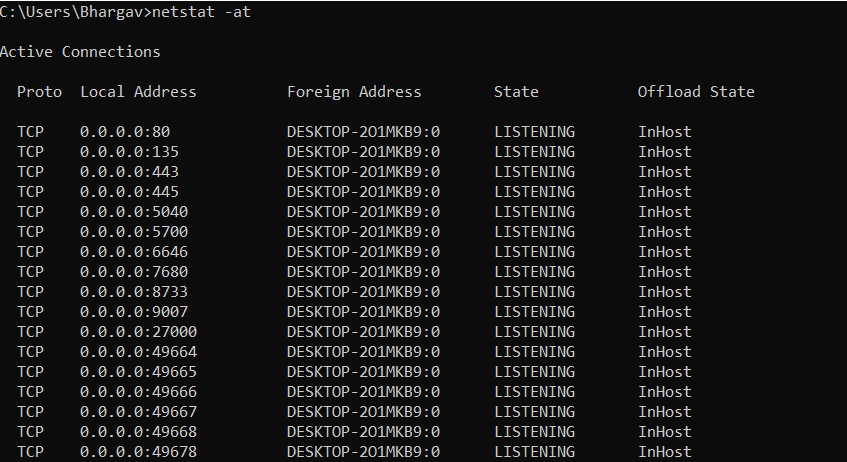
If u want to exit the search ctrl+c

If we write netstat -a

,it will dislplay the connections and lists the ports (listening ports)

Netstat -at will list all tcp connections and netstat -au will list all udp connections





Protocol is of two types ,UDP and TCP

UDP is connectionless protocol

TCP is connection oriented protocol

LOCAL ADDRESS:

* + 1. Is the representing the machine, 135 is representing port number

Local address contains the address and port number of all the local end of socket

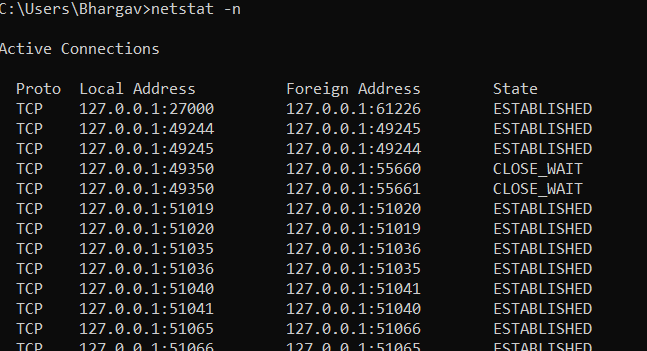
Foreign address contains the address and port number of all the remote end of socket

Format is same as in the local address

netstat -n

display all ip address and port number in numerical form

after typing netstat -n



127.0.0.1:1589

127.0.0.1 represents the IP address of local end of socket

1589 represents port number

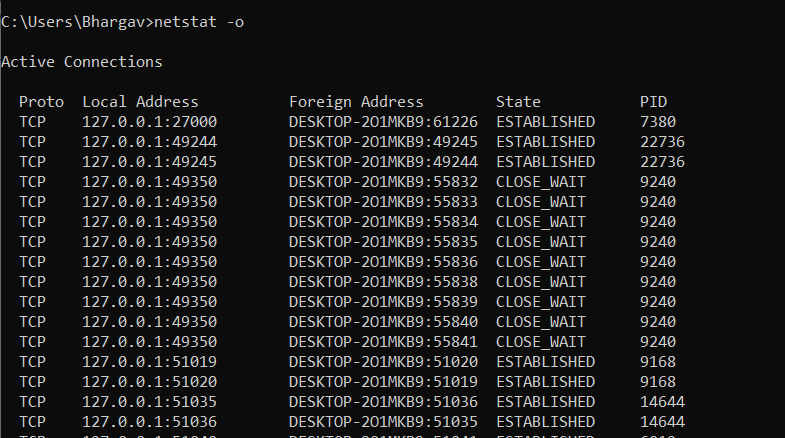
127.0.0.1:9930

127.0.0.1 represents the IP address of remote end of socket

1589 represents port number

netstat -o

if u want to \*\*\* process ID

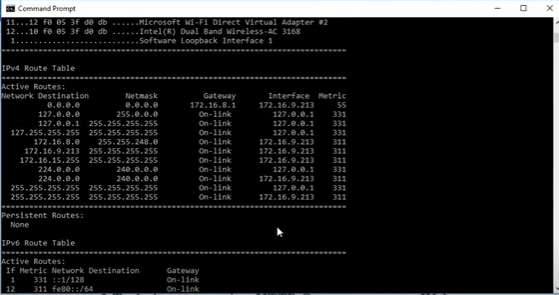


Here we can see local address ,foreign address

PID represents process id

Netstat -r

For routing table



It gives information about

Active routes: network destination, Netmask ,Gateway,Interface,Metric

The basic differernce between IPV4 and IPV6 is that ipv6 is unique ,it depends on device.

We can observe different states

ESTABLISHED :

SOCKET HAS AN ESTABLISHED CONNECTION

TIME\_WAIT:

Socket is waiting for close action

Socket is not being used

CLOSE\_WAIT:

Remote end has shut down

Waiting for socket to end

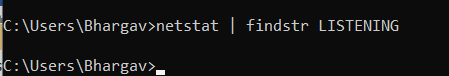
LISTENING state:

Socket is listening

UNKOWN STATE:

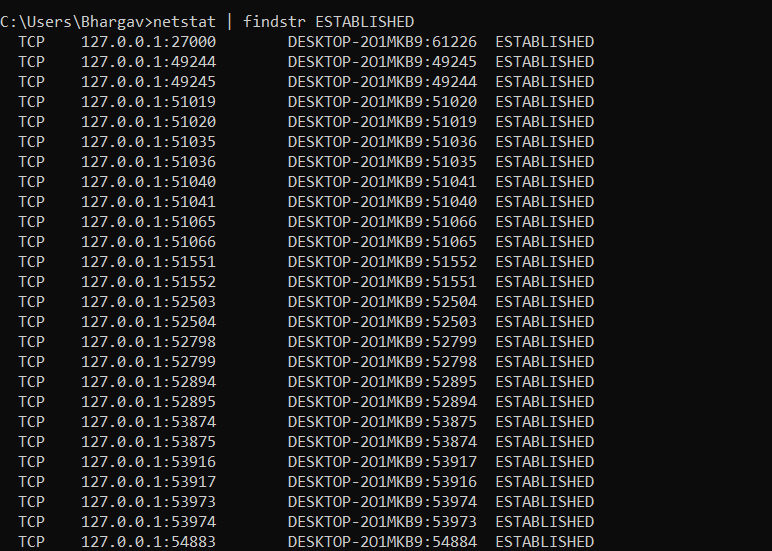
Socket is unknown state

netstat | findstr LISTENING lists all the listening connections



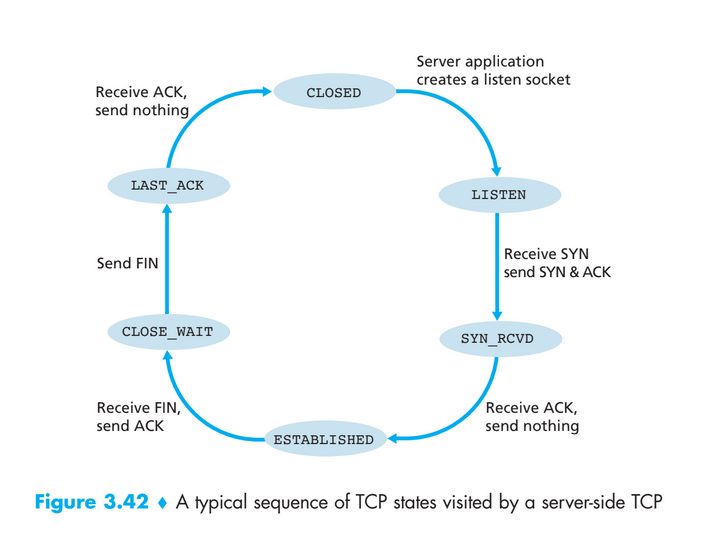
netstat | findstr ESTABLISHED:

command used to find the established connections on the server



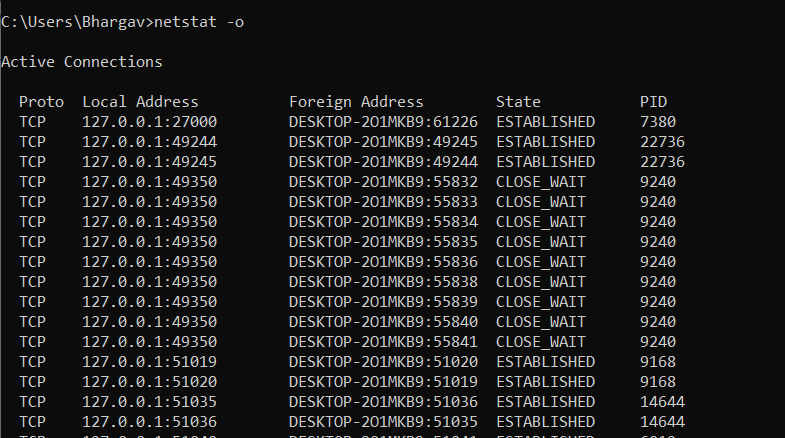
netstat | findstr SYN\_RECV

command used to find the half open tcp connections on the server





Using netstat -o to see which process id has many open connections and thus we can conclude that the process id with many open connections uses a lot of bandwidth .

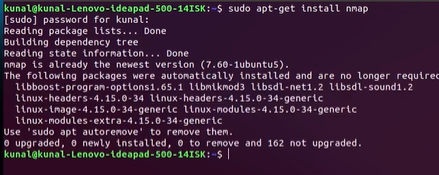


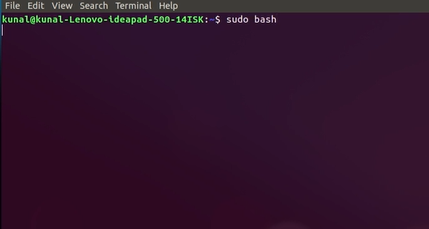
Here PID 9240 uses a lot of bandwidth as it has many connections.

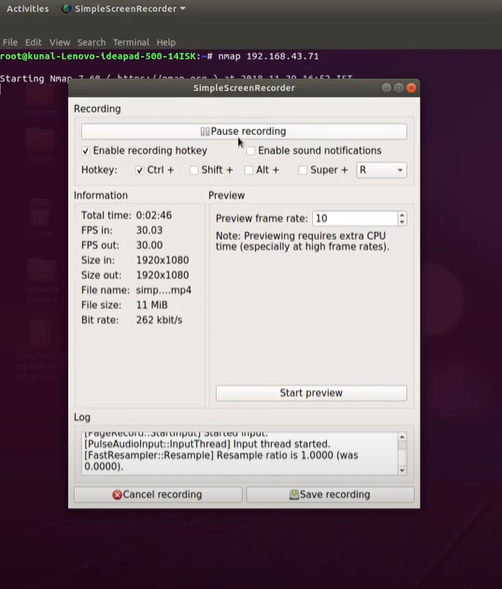
NMAP:

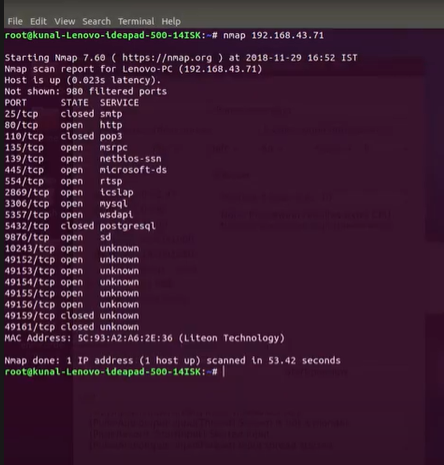
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

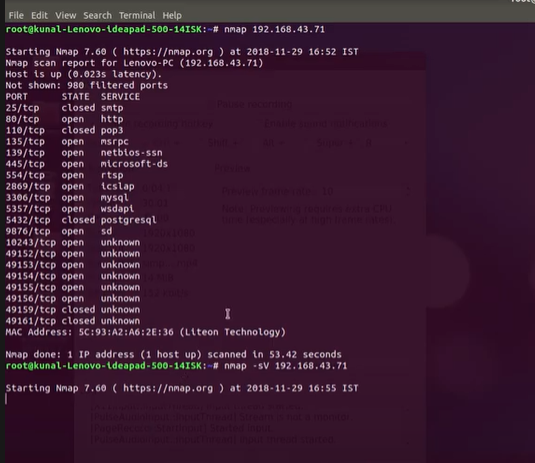
Installing nmap

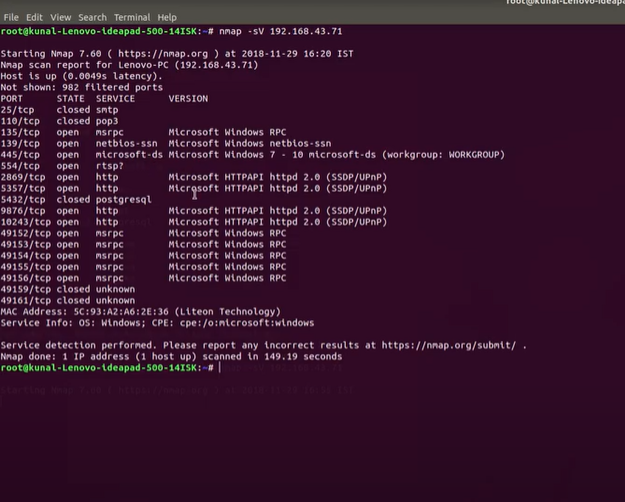


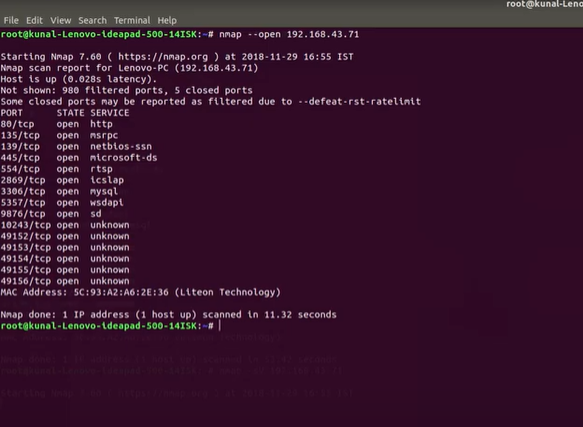


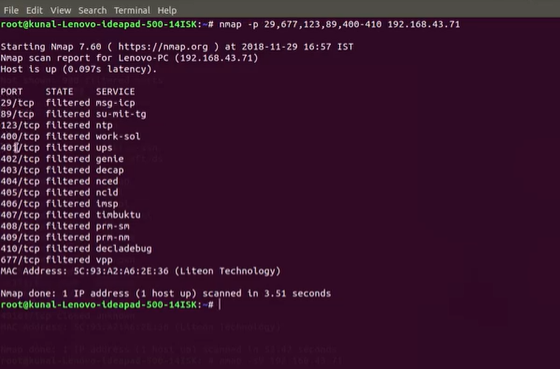




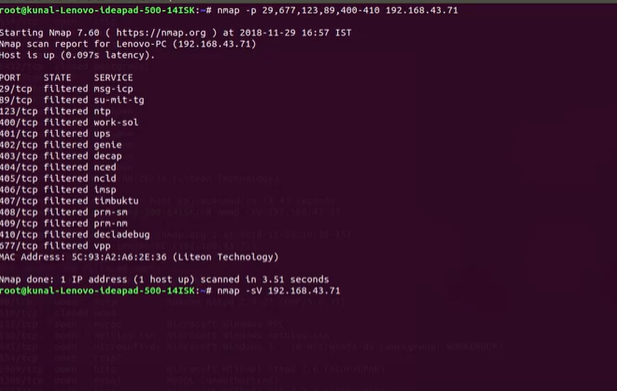


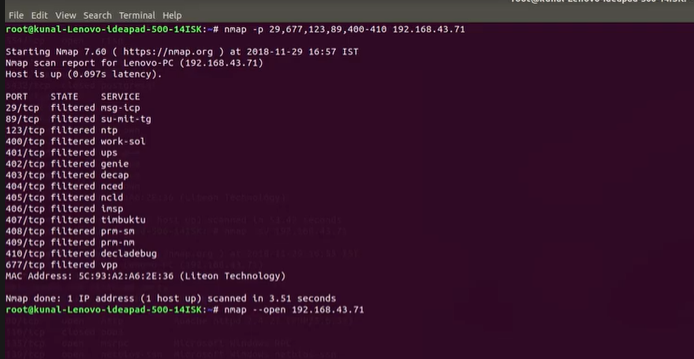


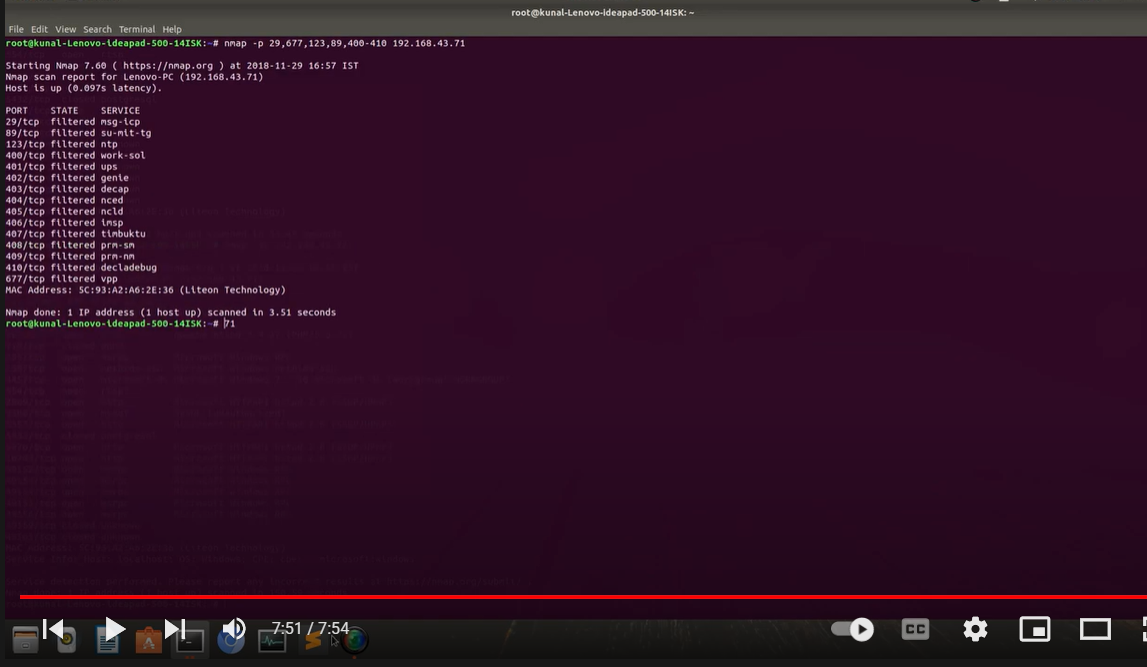


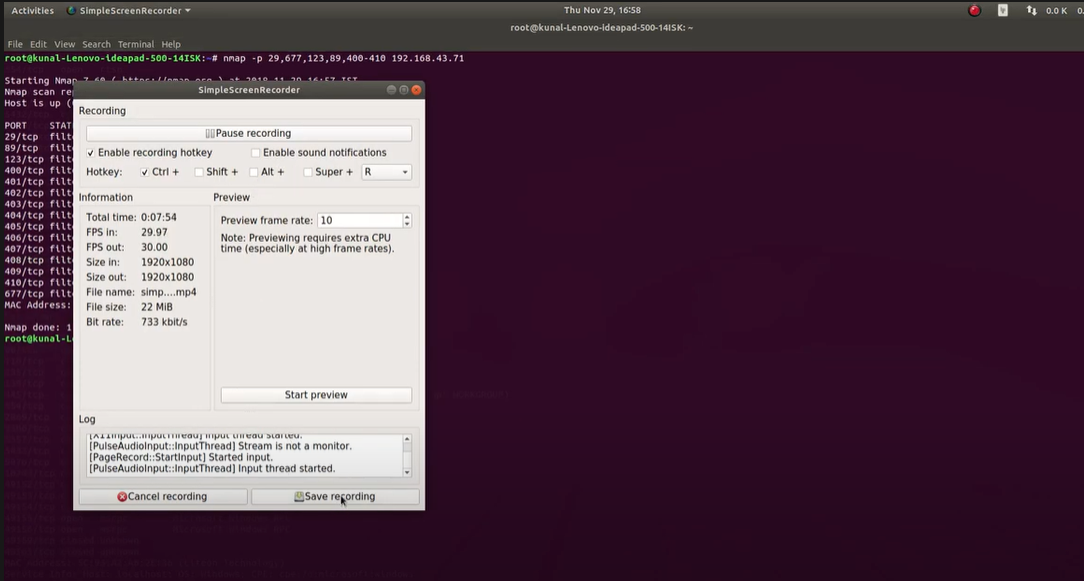


nmap -sv 192.168.43.71

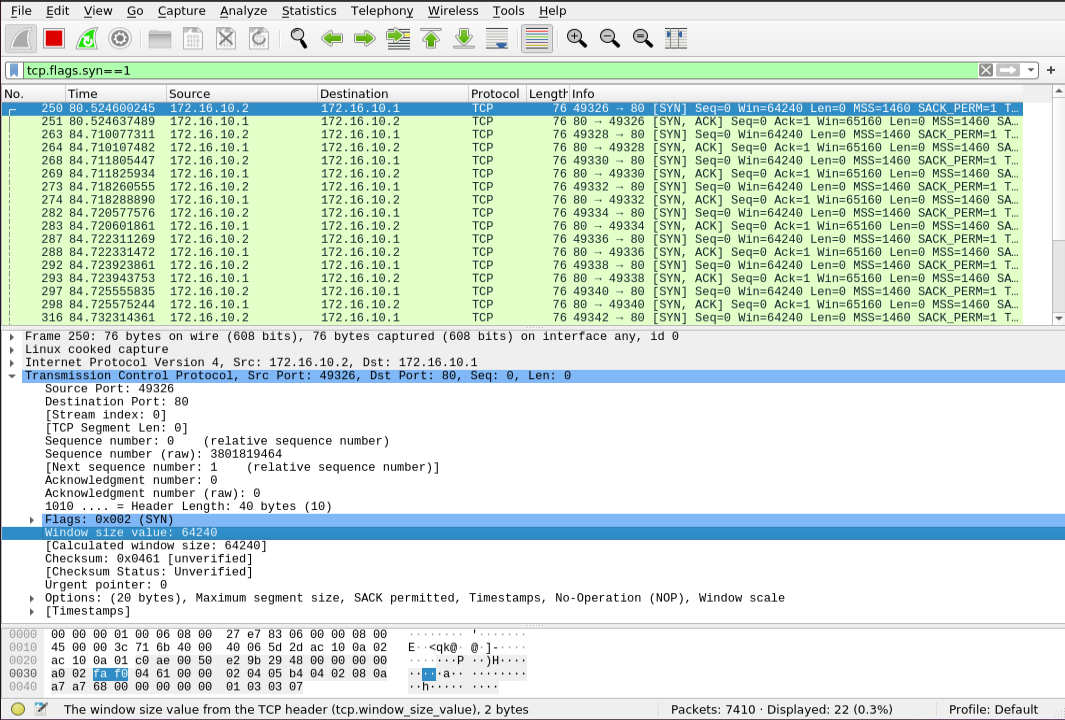




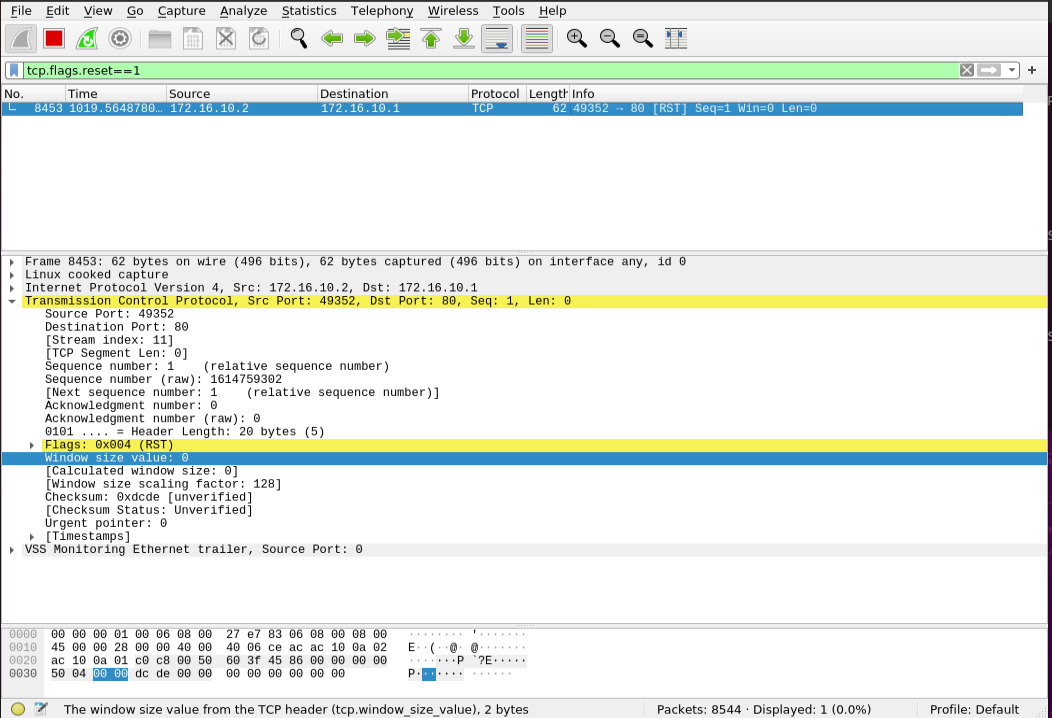




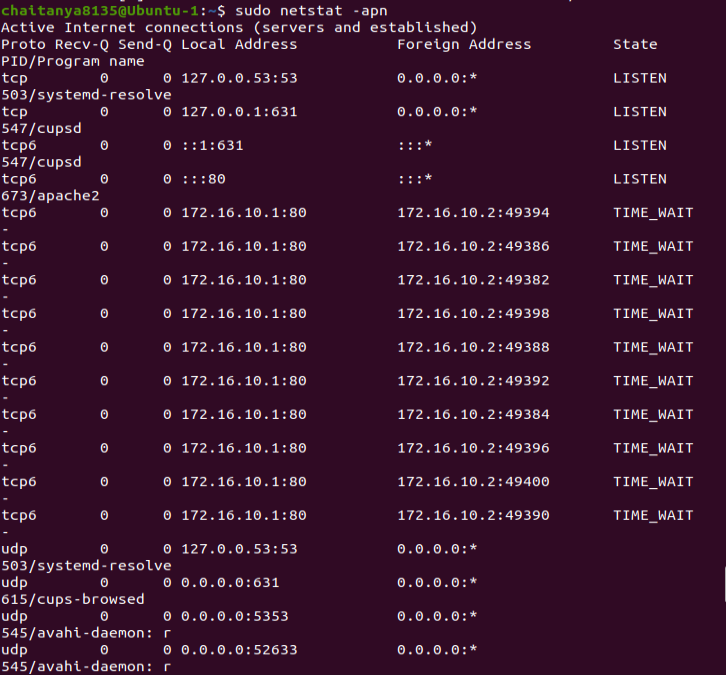
Monitoring TCP SYN requests to web server(using filter: tcp.flags.syn==1)



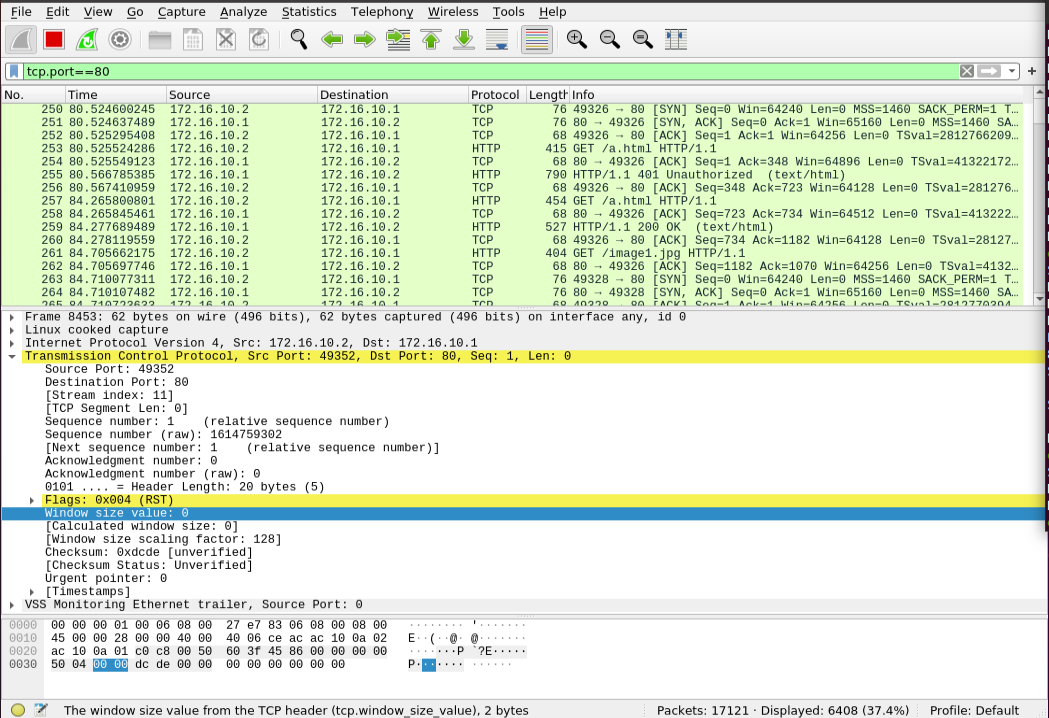
Monitoring TCP reset request to web server(using filter: tcp.flags.reset==1)



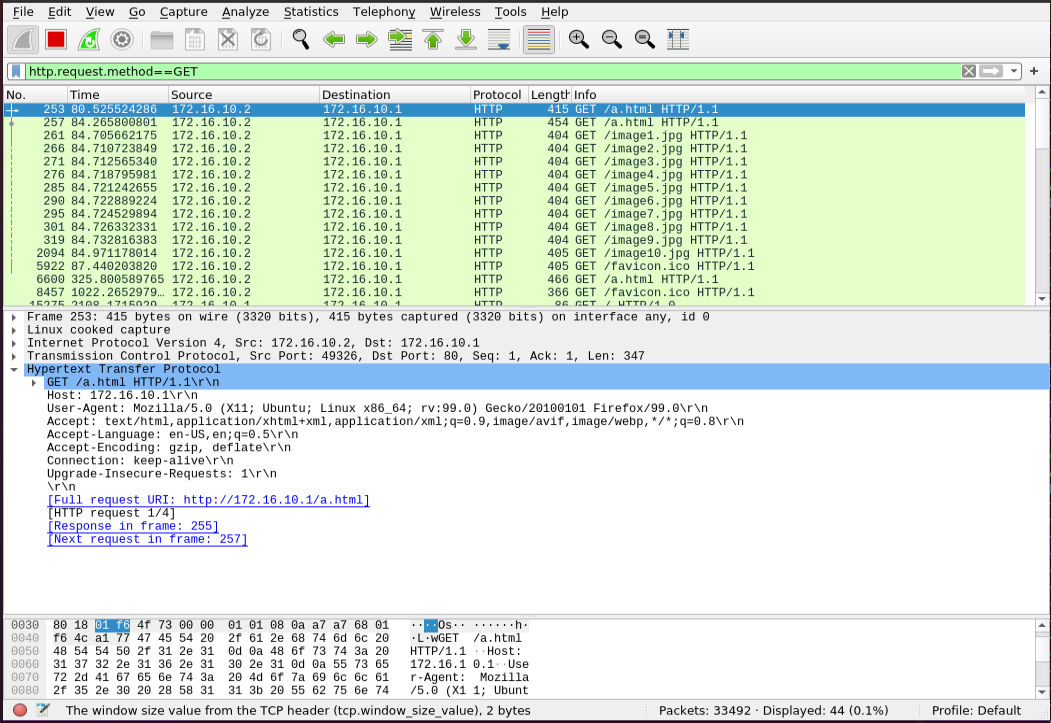
Monitoring established open and half open connections on the web server



Monitoring requests to a specific application(using filter: tcp.port == <port No of application>)



Monitoring HTTP GET requests to the web server(using filter: http.request.method==GET)



Port status using nmap

