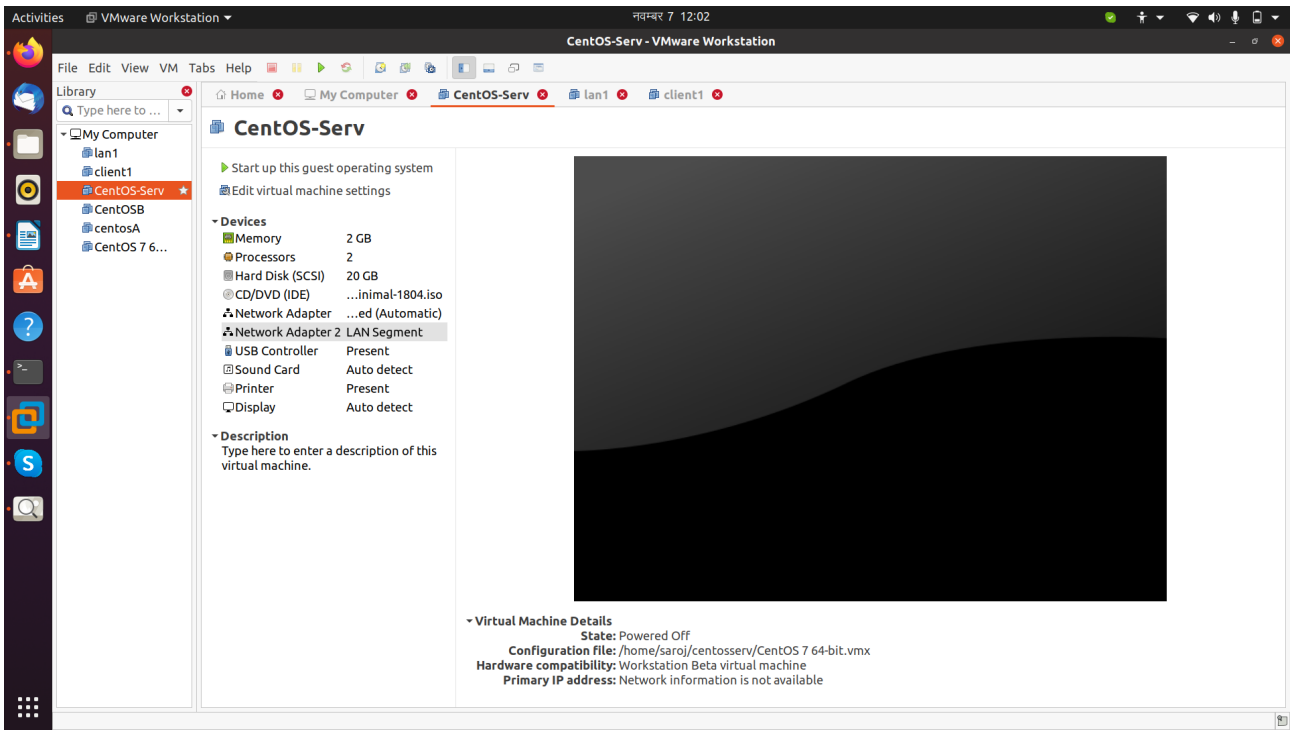
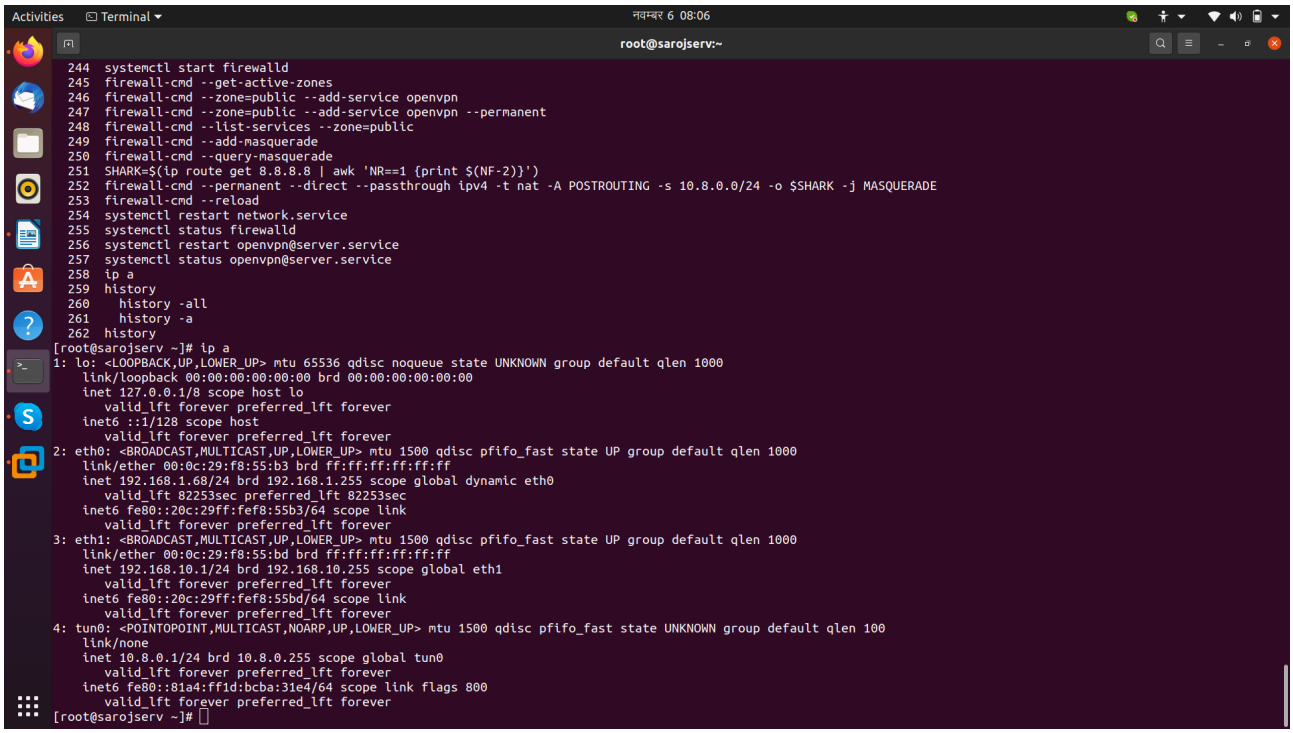
Q1 A)

```
ip a
  ifup ens33
   ip a
  ping google.com
  ip a
  hostname
 vi /etc/host
 vi /etc/hosts
 vi /etc/hostname
reboot
 vi /etc/default/grub
 grub2-mkconfig -o /boot/grub2/grub.cfg
  reboot
  ip a
  cd /etc/sysconfig/network-scripts/
  ls
 mv ifcfg-ens33 ifcfg-eth0
  ls
  cat ifcfg-eth0
 ls
 vi ifcfg-ens34
  mv ifcfg-ens34 ifcfg-eth1
  ls
  cat ifcfg-eth1
  vi ifcfg-eth0
  systemctl stop NetworkManager
  systemctl disable NetworkManager
  systemctl restart NetworkManager
  reboot
  ip a
  ping google.com
  yum install epel-release -y
  systemctl stop firewalld
  systemctl disable firewalld
  yum install iptables-services -y
  systemctl enable iptables
  systemctl start iptables
  systemctl status iptables
  systemctl stop iptables
  systemctl status iptables
```


Activities
VMware Workstation
नवम्बर 7 12:02
CentOS-Serv - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to ...
My Computer
lan1
client1
CentOS-Serv
CentOSB
centosA
CentOS 7 6...
Home
My Computer
CentOS-Serv
lan1
client1
CentOS-Serv
Start up this guest operating system
Edit virtual machine settings
Devices
Memory 2 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (IDE) ...inimal-1804.iso
Network Adapter ...ed (Automatic)
Network Adapter 2 LAN Segment
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered Off
Configuration file: /home/saroj/centosserv/CentOS 7 64-bit.vmx
Hardware compatibility: Workstation Beta virtual machine
Primary IP address: Network information is not available

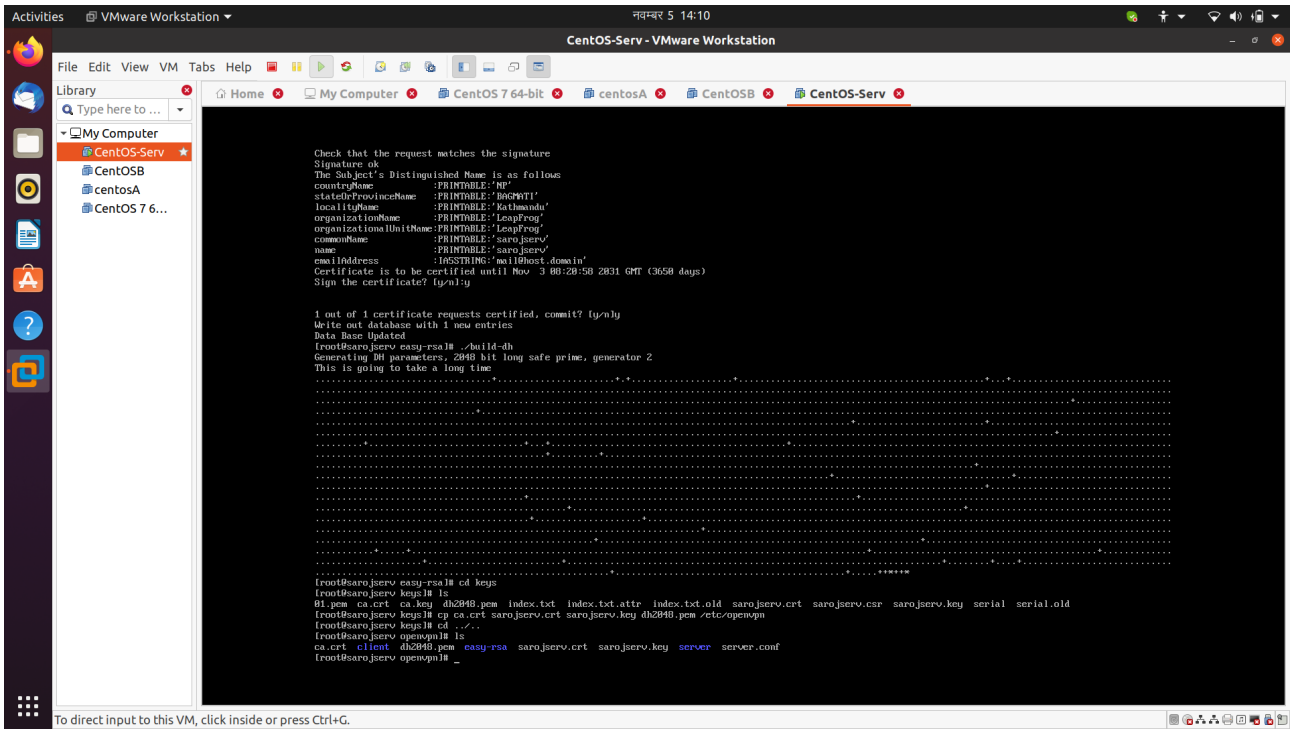

Activities
Terminal
नवम्बर 6 08:06
root@sarojserv:~
244 systemctl start firewalld
245 firewall-cmd --get-active-zones
246 firewall-cmd --zone=public --add-service openvpn
247 firewall-cmd --zone=public --add-service openvpn --permanent
248 firewall-cmd --list-services --zone=public
249 firewall-cmd --add-masquerade
250 firewall-cmd --query-masquerade
251 SHARK=$(ip route get 8.8.8.8 | awk 'NR==1 {print $(NF-2)}')
252 firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o $SHARK -j MASQUERADE
253 firewall-cmd --reload
254 systemctl restart network.service
255 systemctl status firewalld
256 systemctl restart openvpn@server.service
257 systemctl status openvpn@server.service
258 ip a
259 history
260 history -all
261 history -a
262 history
[root@sarojserv ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:0c:29:f8:55:b3 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.68/24 brd 192.168.1.255 scope global dynamic eth0
valid_lft 82253sec preferred_lft 82253sec
inet6 fe80::20c:29ff:fef8:55b3/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:0c:29:f8:55:bd brd ff:ff:ff:ff:ff:ff
inet 192.168.10.1/24 brd 192.168.10.255 scope global eth1
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fef8:55bd/64 scope link
valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
link/none
inet 10.8.0.1/24 brd 10.8.0.255 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::81a4:ff1d:bcba:31e4/64 scope link flags 800
valid_lft forever preferred_lft forever
[root@sarojserv ~]#

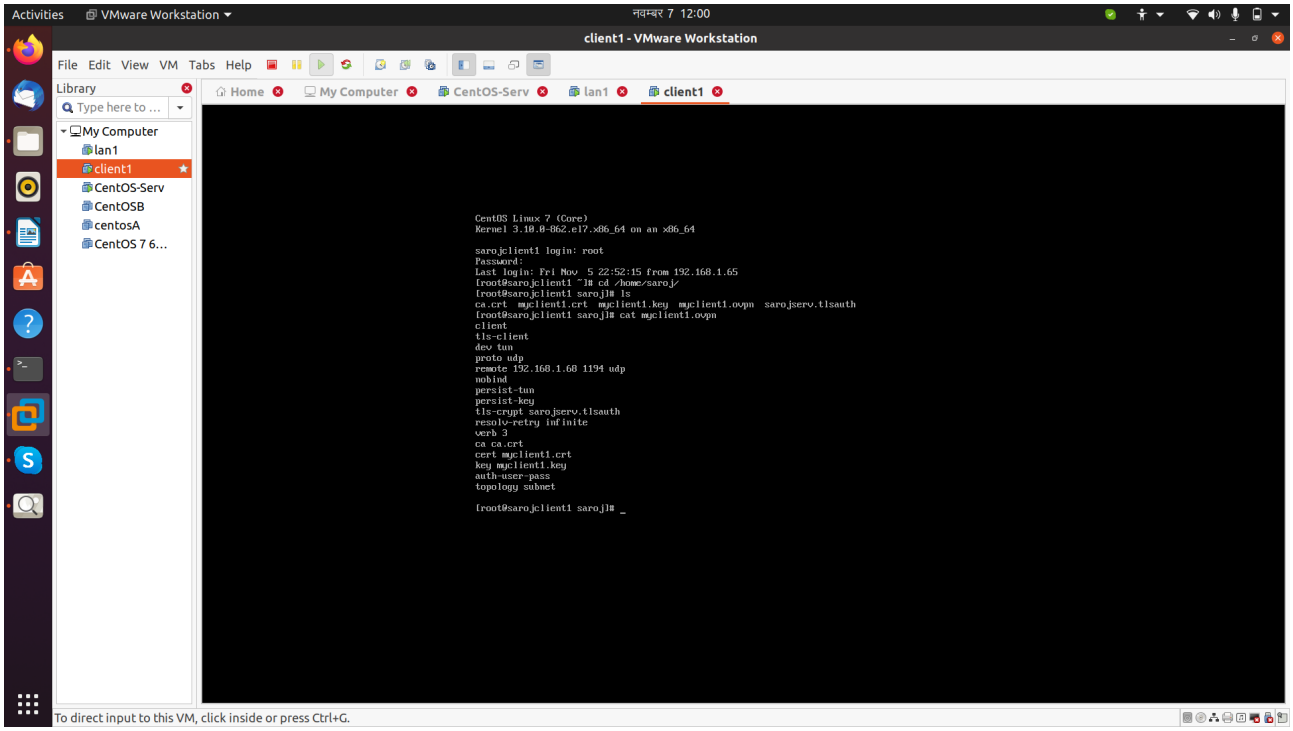
Q1 B)

```
yum install openvpn -y
cd /usr/share/doc/openvpn-2.4.11/sample/sample-config-files/
pwd
ls
cp server.conf /etc/openvpn
cd /etc/openvpn
ls
vi server.conf
yum install easy-rsa -y
mkdir -p /etc/openvpn/easy-rsa/keys
ls
yum install wget -y
wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
tar xfz /tmp/easyrsa
cd /tmp/easyrsa
cp -rf easy-rsa-old-2.3.3/easy-rsa/2.0/* /etc/openvpn/easy-rsa
pwd
ls
vi vars
source ./vars
./clean-all
./build-ca
./build-key-server $( hostname )
cd keys
ls
./build-dh
cd ..
source ./vars
./clean-all
./build-ca
./build-key-server $( hostname )
./build-dh
cd keys
ls
cp ca.crt sarojserv.crt sarojserv.key dh2048.pem /etc/openvpn
cd ../..
ls
restorecon -Rv /etc/openvpn
ln -s /lib/systemd/system/openvpn\@.service
/etc/systemd/system/multi-user.target.wants/openvpn\@server.service
ls
vi server.conf
ls
vi server.conf
ls
systemctl -f enable openvpn@server.service
systemctl -f start openvpn@server.service
systemctl start openvpn@server.service
systemctl status openvpn@server.service
vi server.conf
```

```
openvpn --keygen --secret /etc/openvpn/ta.key
openvpn --keygen --secret /etc/openvpn/easy-rsa/keys/ta.key
pwd
cd easy-rsa/
ls
cd keys/
ls
systemctl start openvpn@server.service
systemctl status openvpn@server.service
cd ../..
ls
vi server.conf
openvpn --genkey --secret /etc/openvpn/sarojserv.tlsauth
systemctl status openvpn@server.service
systemctl restart openvpn@server.service
systemctl status openvpn@server.service
ip a
source ./vars
pwd
cd easy-rsa/
pwd
ls
source ./vars
./build-key myclient1
cd keys
ls
ip a
ls
ls -l
cd
cd /home/
ls
cd saroj
ls
mkdir
mkdir client1key
ls
cd /etc/openvpn/
ls
cd easy-rsa/keys/
ls
cp ca.crt myclient1.crt myclient1.key /home/saroj/client1key/
cd /home/saroj/client1key/
ls
ll
chmod 644 myclient1.key
ll
scp ca.crt root@192.168.1.168:/home/saroj
scp myclient1.crt root@192.168.1.169:/home/saroj
ip a
scp myclient1.key root@192.168.1.69:/home/saroj
vi /etc/sysctl.conf
```

ls
sysctl -p
vi /etc/pam.d/openvpn
vi /etc/openvpn/server.conf
systemctl stop openvpn@server.service
systemctl start openvpn@server.service
systemctl status openvpn@server.service
systemctl stop firewalld
cd /etc/openvpn/
ls
scp sarojserv.tlsauth root@192.168.1.69:/home/saroj/
ls
ll
cp sarojserv.tlsauth /home/saroj/
cd /home/saroj/
ls
mv sarojserv.tlsauth client1key/
ls
cd client1key/
ls
ll
chmod 644 sarojserv.tlsauth
ll
scp sarojserv.tlsauth root@192.168.1.69:/home/saroj/



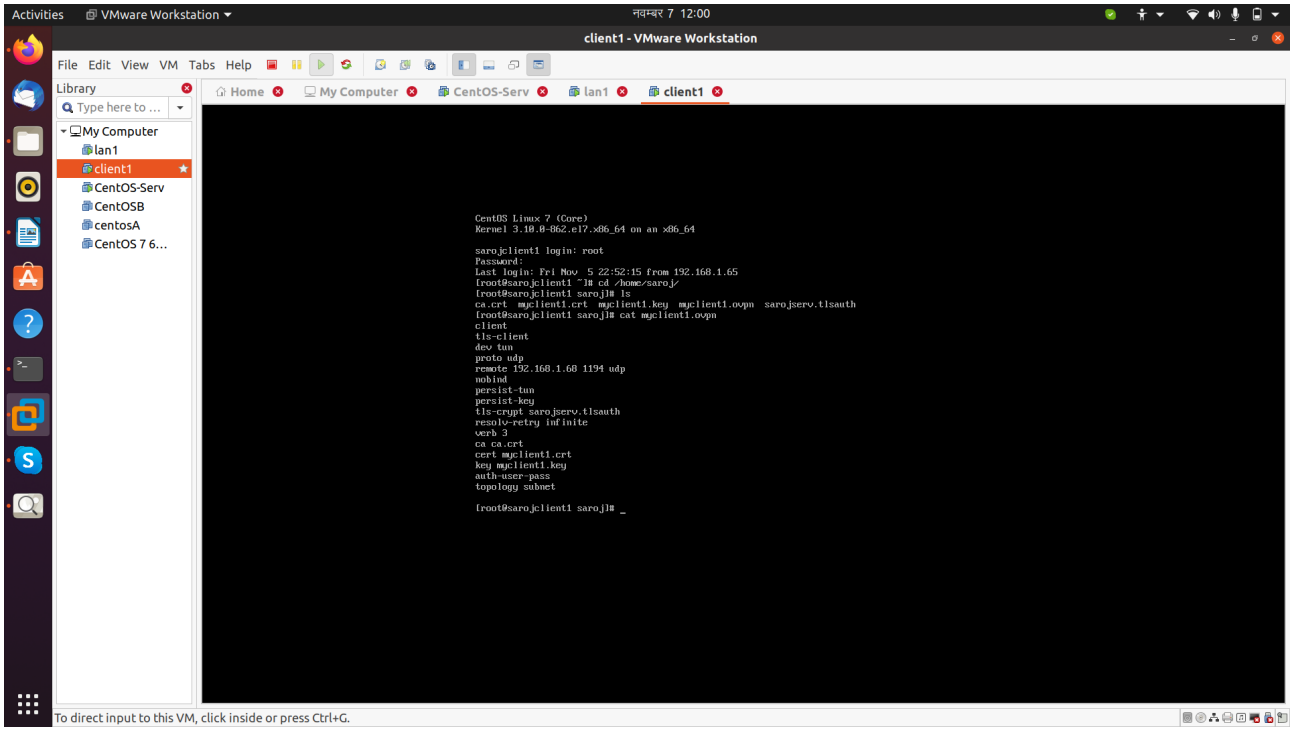


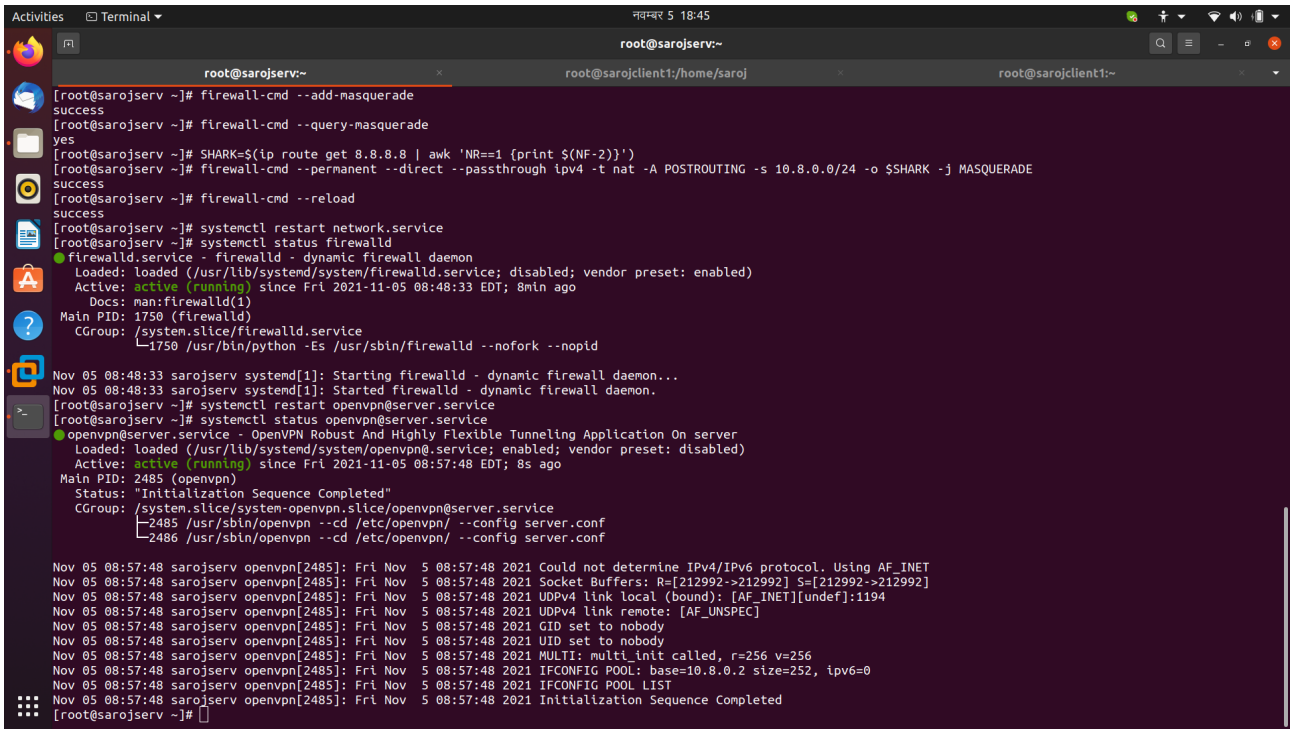
Q2

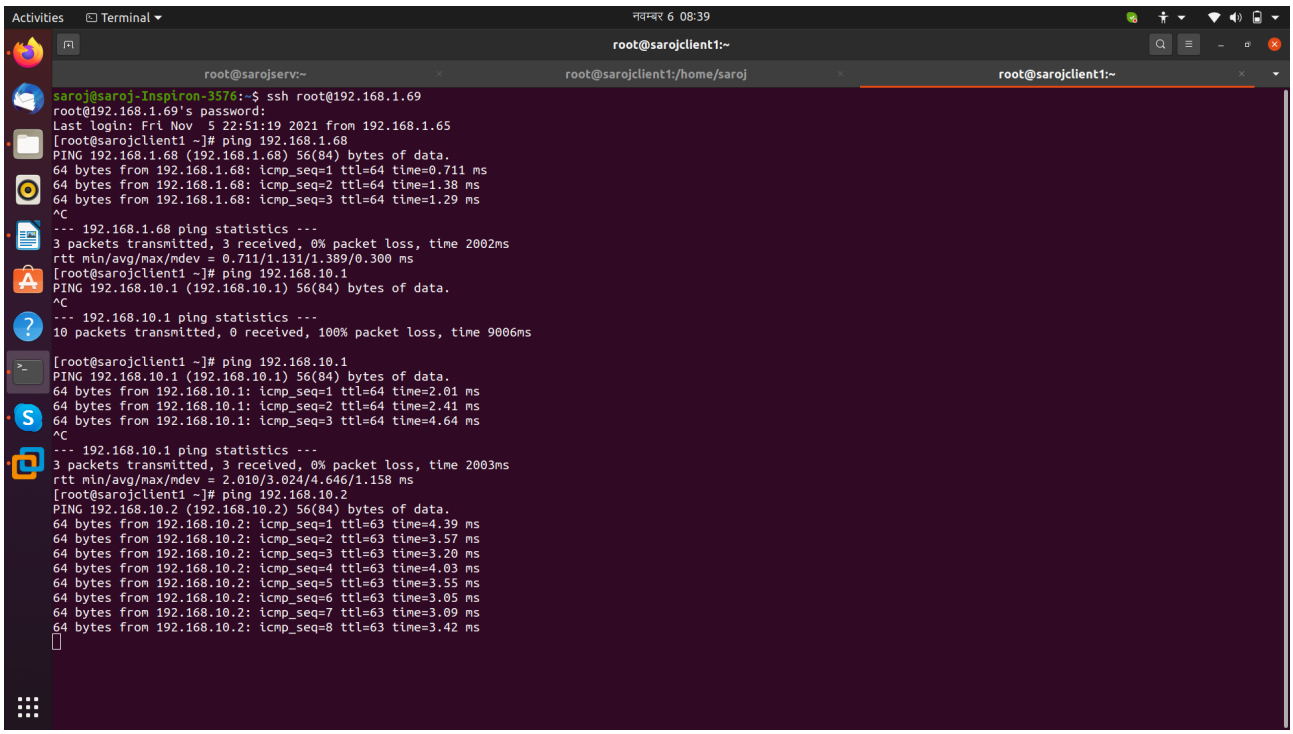
################Installed openvpn in Q1b refer in that#################################

systemctl stop openvpn@server.service
systemctl start openvpn@server.service
systemctl status openvpn@server.service
ip a

firewall-cmd --get-active-zones
systemctl start firewalld
firewall-cmd --get-active-zones
firewall-cmd --zone=public --add-service openvpn
firewall-cmd --zone=public --add-service openvpn --permanent
firewall-cmd --list-services --zone=public
firewall-cmd --add-masquerade
firewall-cmd --query-masquerade
SHARK=$(ip route get 8.8.8.8 | awk 'NR==1 {print $(NF-2)}')
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o $SHARK -j MASQUERADE
firewall-cmd --reload
systemctl restart network.service
systemctl status firewalld
systemctl restart openvpn@server.service
systemctl status openvpn@server.service
ip a


Activities
VMware Workstation
नवम्बर 7 12:00
client1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to ...
My Computer
lan1
client1
CentOS-Serv
CentOSB
centosA
CentOS 7 6...
Home
My Computer
CentOS-Serv
lan1
client1
CentOS Linux 7 (Core)
Kernel 3.10.0-862.el7.x86_64 on an x86_64
sarojclient1 login: root
Password:
Last login: Fri Nov 5 22:52:15 from 192.168.1.65
[root@sarojclient1 ~]# cd /home/saroj/
[root@sarojclient1 saroj]# ls
ca.crt myclient1.crt myclient1.key myclient1.ovpn sarojserv.tlsauth
[root@sarojclient1 saroj]# cat myclient1.ovpn
client
tls-client
dev tun
proto udp
remote 192.168.1.60 1194 udp
nobind
persist-tun
persist-key
tls-crypt sarojserv.tlsauth
resolv-retry infinite
verb 3
ca ca.crt
cert myclient1.crt
key myclient1.key
auth-user-pass
topology subnet
[root@sarojclient1 saroj]# _
To direct input to this VM, click inside or press Ctrl+G.


Activities
Terminal
नवम्बर 5 18:45
root@sarojserv:~
root@sarojserv:~
root@sarojclient1:/home/saroj
root@sarojclient1:~
[root@sarojserv ~]# firewall-cmd --add-masquerade
success
[root@sarojserv ~]# firewall-cmd --query-masquerade
yes
[root@sarojserv ~]# SHARK=$(ip route get 8.8.8.8 | awk 'NR==1 {print $(NF-2)}')
[root@sarojserv ~]# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o $SHARK -j MASQUERADE
success
[root@sarojserv ~]# firewall-cmd --reload
success
[root@sarojserv ~]# systemctl restart network.service
[root@sarojserv ~]# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
Active: active (running) since Fri 2021-11-05 08:48:33 EDT; 8min ago
Docs: man:firewalld(1)
Main PID: 1750 (firewalld)
CGroup: /system.slice/firewalld.service
└1750 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
Nov 05 08:48:33 sarojserv systemd[1]: Starting firewalld - dynamic firewall daemon...
Nov 05 08:48:33 sarojserv systemd[1]: Started firewalld - dynamic firewall daemon.
[root@sarojserv ~]# systemctl restart openvpn@server.service
[root@sarojserv ~]# systemctl status openvpn@server.service
openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; vendor preset: disabled)
Active: active (running) since Fri 2021-11-05 08:57:48 EDT; 8s ago
Main PID: 2485 (openvpn)
Status: "Initialization Sequence Completed"
CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
├2485 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf
└2486 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 Could not determine IPv4/IPv6 protocol. Using AF_INET
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 UDPv4 link local (bound): [AF_INET][undef]:1194
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 UDPv4 link remote: [AF_UNSPEC]
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 GID set to nobody
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 UID set to nobody
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 MULTI: multi_init called, r=256 v=256
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 IFCONFIG POOL: base=10.8.0.2 size=252, ipv6=0
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 IFCONFIG POOL LIST
Nov 05 08:57:48 sarojserv openvpn[2485]: Fri Nov 5 08:57:48 2021 Initialization Sequence Completed
[root@sarojserv ~]#



Q3

sudo su

yum -y install epel-release wget jq

curl -O https://copr.fedorainfracloud.org/coprs/jasonish/suricata-stable/repo/epel-7/jasonish-suricata-stable-epel-7.repo

yum -y install suricata

wget https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz

tar zxvf emerging.rules.tar.gz

rm /etc/suricata/rules/* -f

mv rules/*.rules /etc/suricata/rules/

rm -f /etc/suricata/suricata.yaml

wget -O /etc/suricata/suricata.yaml http://www.branchnetconsulting.com/wazuh/suricata.yaml

systemctl daemon-reload

systemctl enable suricata

systemctl start suricata

systemctl status suricata

curl http://testmyids.com

tail -n1 /var/log/suricata/fast.log