SSH

SSH stands for Secure shell:

SSH is turned on by default on every Linux server operating system like centos,Ubuntu,or Suse Linux

we can check that is running by this command

```
=>ps aux | grep ssh
```

this command will show the ssh daemon if it is running on the system
typically ssh runs on port 22

SSH has many security features built in like

1) Shell access
2) File transfer (SCP and SFTP)
4) Executing remote commands
5) port forwarding and tunneling
6) Creating VPN
7) Forwarding X displays
8) Encrypted proxy browsing via socks protocols
9) And mounting remote directories

we can transfer file and zip then up at the same time with SCP. This helps a lot for backing up the system

co connect the system with ssh this command is used

```
=>ssh <username>@<hostname/hostIP>
```

we can also issue command after if we want to

```
=>ssh <username>@<hostname/hostIP> <command>
```

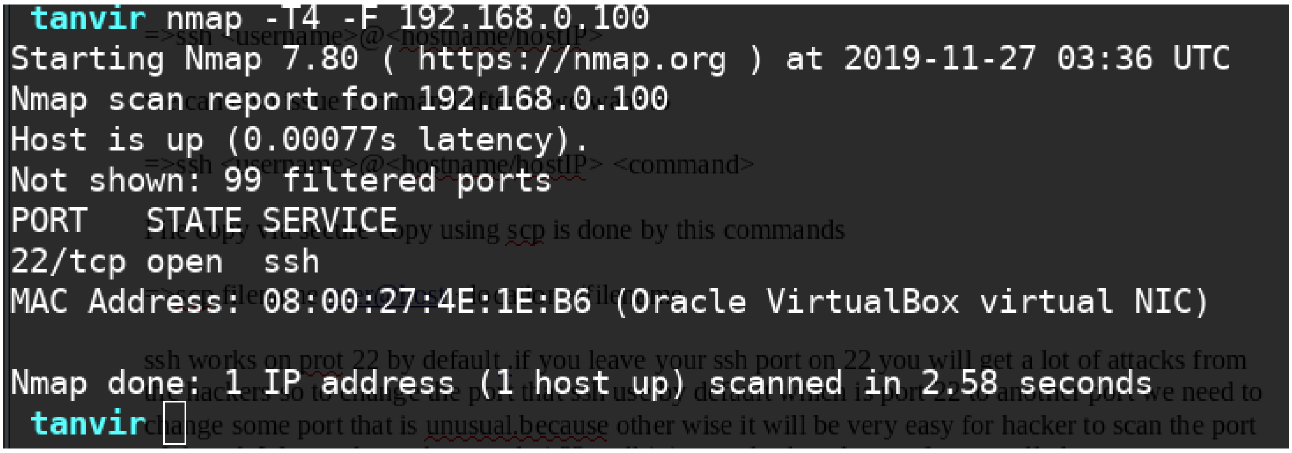
File copy via secure copy using scp is done by this commands

```
=>scp filename user@host:<location>/filename
```

ssh works on prot 22 by default .if you leave your ssh port on 22 you will get a lot of attacks from the hackers so to change the port that ssh use by default which is port 22 to another port we need to change some port that is unusual.because other wise it will be very easy for hacker to scan the port of the ssh.Want to know how to do it??.well it is mostly done by a software called nmap

my VM ip address is 192.168.0.100 to make a quick scan lets go to the host terminal and do a quick scan with nmap

```
=> nmap -T4 -F 192.168.0.100
```



```
 tanvir nmap -T4 -F 192.168.0.100
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-27 03:36 UTC
Nmap scan report for 192.168.0.100
Host is up (0.00077s latency).
Not shown: 99 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:4E:1E:B6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.58 seconds
 tanvir
```

we can see that we got the ssh port and the MAC address of the system .

To change the port of the ssh we will change a configuration filename

=>vim /etc/ssh/sshd_config

we scroll down and see the port nuber

we un comment the file and change it to 2237 and save and exit

now if you are using Selinux you may have to issue another command to make sure that Selinux knows that you are making aport change

=>semanage port -a -t ssh_port_t -p tcp 2237

to see the change
=> semanage port -l | grep ssh

it will show you the new port

now lets try connecting with port 22

we will see that the connection is refused

now lets scan the port with nmap again

=> nmap -T4 -F 192.168.0.100

we will see the port 22 is closed

now changing port will now work if you dont open in the firewall
so lets change the firewall settings

=>firewall-cmd –permanent –add-port=2237/tcp

now reload the firewalld

=>systemctl restart firewalld.service

and after that you can access the ssh with the new port.
=>ssh -p 2237 root@192.168.0.100

[public and private key]

but Changing the port is not the only thing that you should do you may want to use the two factor authentication like public and private key.

[public and private key goes here]

because if your ssh is compromised then the attacker can change your server into honeypot and steal users inforamtion.

[what is a honeypot?]
[honeypot goes here]