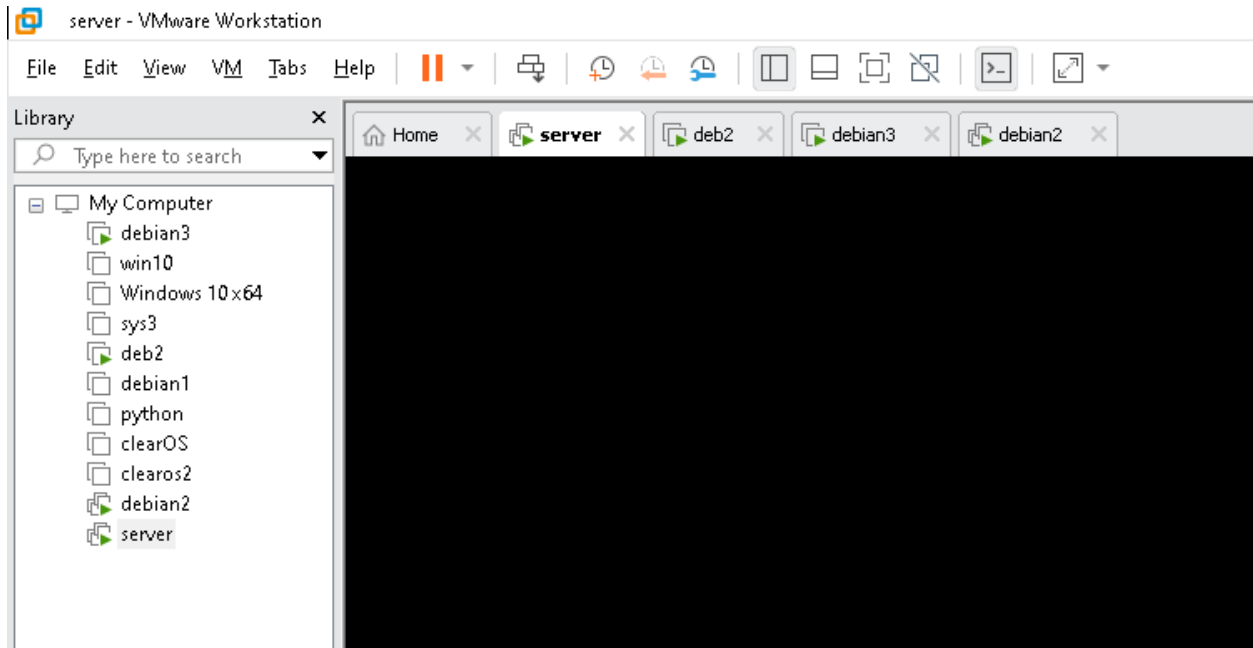


NDC- Iptables

Take 4 different machines

Make 1 server and put iptables rules in it.

Download links in all



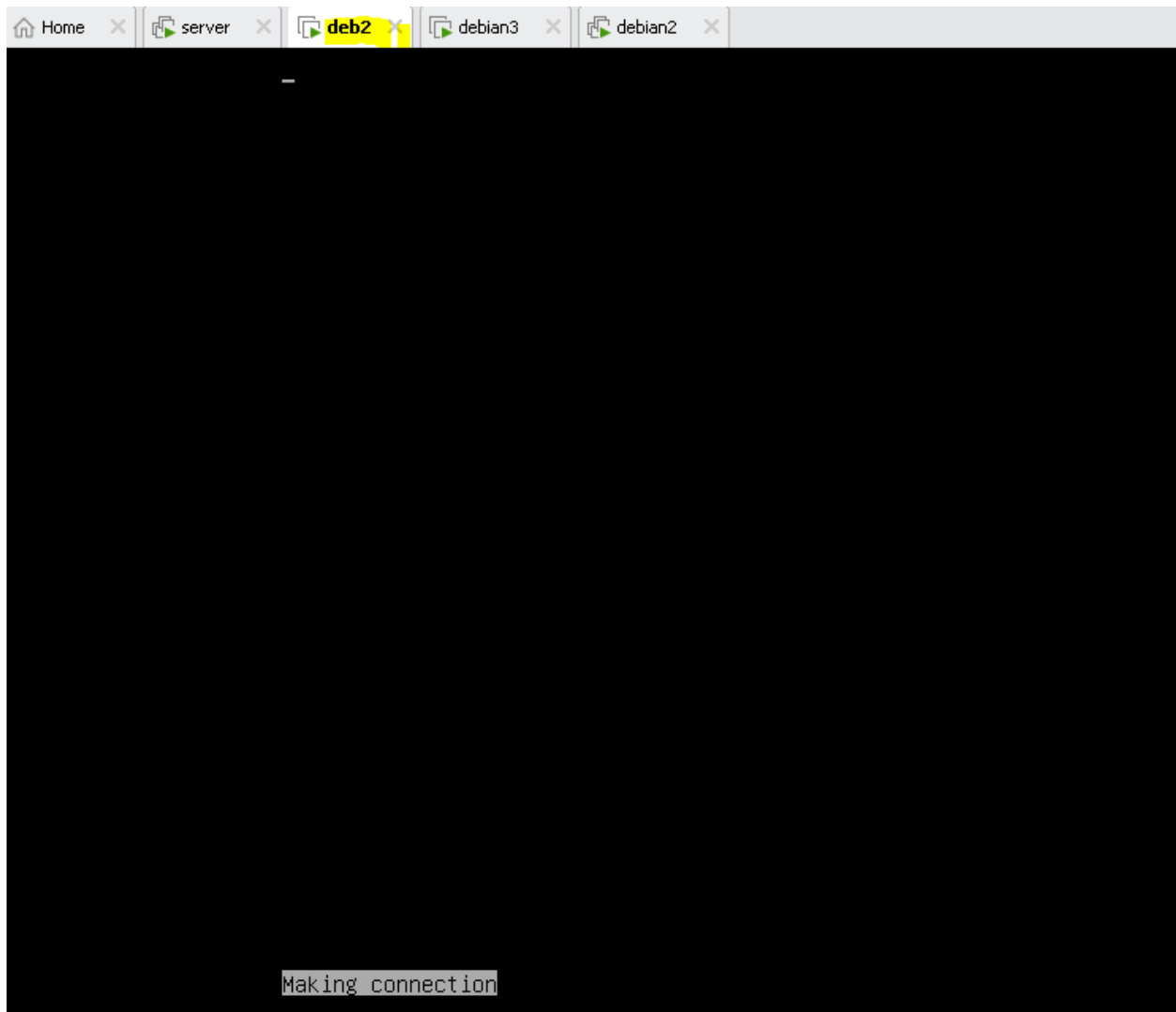
Configure Iptable

```
shuhari@debian: ~  
GNU nano 3.2 rules.sh  
#!/usr/bin/bash  
  
iptables -F  
  
iptables -A INPUT -s 192.168.80.1 -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -s 192.168.80.129 -p tcp --dport 80 -j DROP  
iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
iptables -A INPUT -s 192.168.80.129 -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -p tcp --dport 22 -j DROP  
iptables -A INPUT -s 31.13.79.35 -j DROP  
iptables -L
```

1) allow incoming HTTP traffic from any IP address(192.168.80.131)



but block incoming traffic from a specific IP address. (IP 192.168.80.129)



2) allow incoming traffic to all of ssh from a specific IP address(192.168.80.129)

```
shuhari@debian:~$ sudo ssh shuhari@192.168.80.135
[sudo] password for shuhari:
The authenticity of host '192.168.80.135 (192.168.80.135)' can't be established.
ECDSA key fingerprint is SHA256:1fPoJ0cLIFm1h4juzM1zmzQf0Gmw9VhJnxH10Xk4au0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.80.135' (ECDSA) to the list of known hosts.
shuhari@192.168.80.135's password:
Linux debian 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 30 23:03:38 2023
shuhari@debian:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
    00
    link/ether 00:0c:29:4a:59:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.135/24 brd 192.168.80.255 scope global dynamic ens33
        valid_lft 1767sec preferred_lft 1767sec
    inet6 fe80::20c:29ff:fe4a:5947/64 scope link
        valid_lft forever preferred_lft forever
shuhari@debian:~$
```

while blocking all other traffic.(192.168.80.131 cant login)

```
root@debian:~# ssh shuhari@192.168.80.135
^X^C
root@debian:~# 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:68:2b:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.131/24 brd 192.168.80.255 scope global dynamic ens33
        valid_lft 960sec preferred_lft 960sec
    inet6 fe80::20c:29ff:fe68:2b4f/64 scope link
        valid_lft forever preferred_lft forever
root@debian:~# _
```

3) Block www.facebook.com (from all)

