Question-4

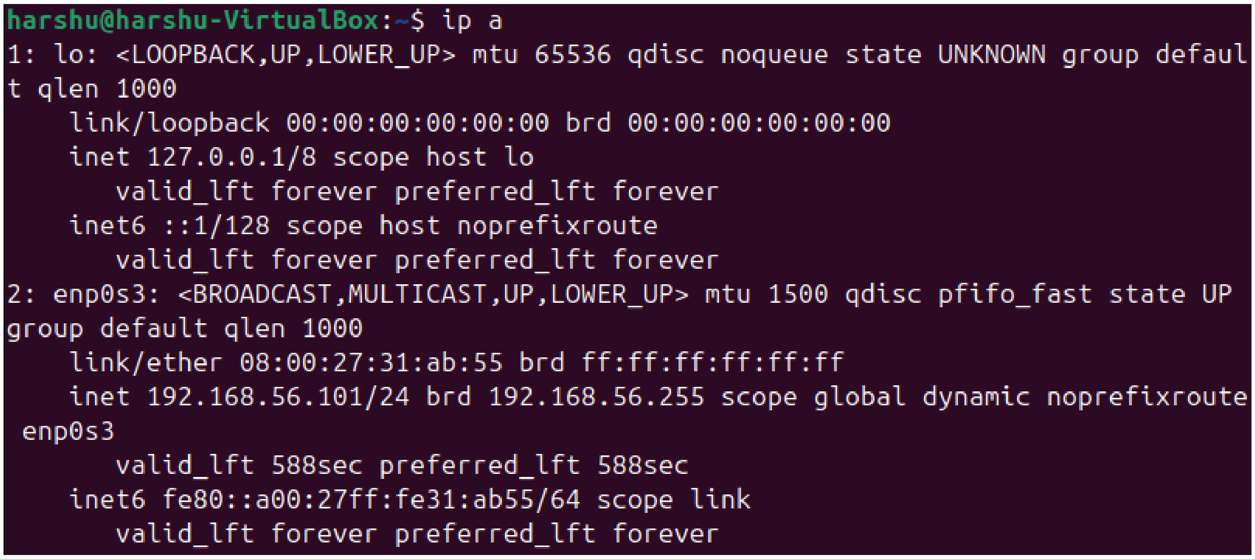
Part-A

For the connection between my vm and windows. We need to set the vm to Host-only mode so that both windows and vm communicate through each other. We can also set this into Bridge but this needs an external adapter.

After that, start Ubuntu on Virtual Machine(VM) and open the terminal.

—---

Run command, “ip a” to check the ip address of the VM for future purposes. Such as ssh my vm from windows.



```
harshu@harshu-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:31:ab:55 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute
 enp0s3
       valid_lft 588sec preferred_lft 588sec
    inet6 fe80::a00:27ff:fe31:ab55/64 scope link
       valid_lft forever preferred_lft forever
```

Image_1

—---

If knockd is not installed install it by following command:

- sudo apt update && sudo apt install knockd -y

Then, start it by this command:

- sudo systemctl start knockd

If already installed:
Check if knock is actively running by the following command

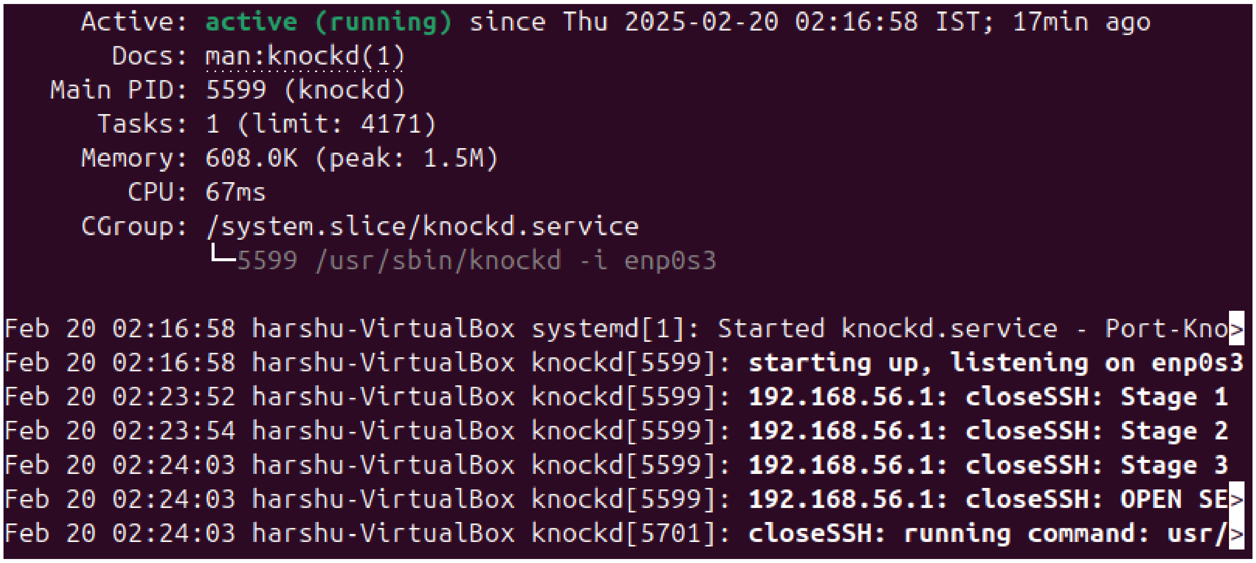
- sudo systemctl status knockd

If not try to restart and enable knockd by following command:

- sudo systemctl start knockd

- sudo systemctl enable knockd

My output after running - “sudo systemctl status knockd”



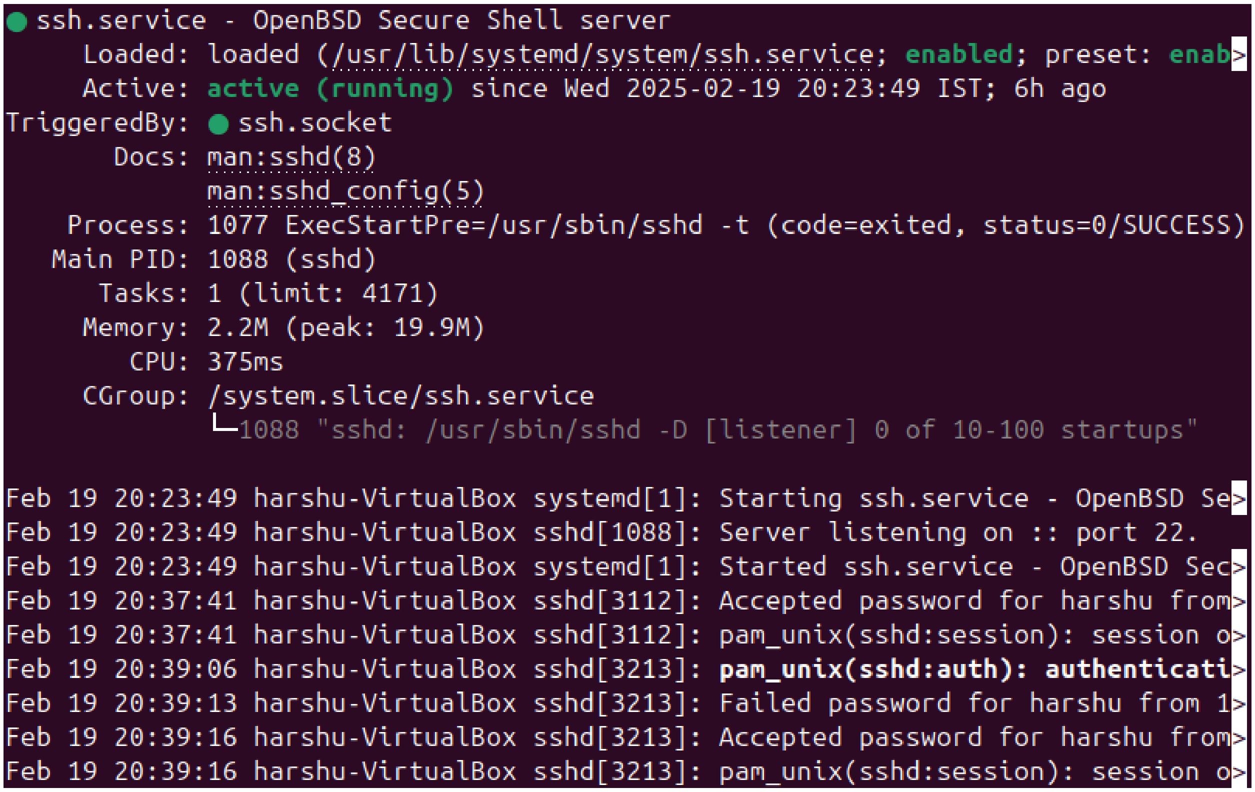
```
     Active: active (running) since Thu 2025-02-20 02:16:58 IST; 17min ago
       Docs: man:knockd(1)
   Main PID: 5599 (knockd)
      Tasks: 1 (limit: 4171)
     Memory: 608.0K (peak: 1.5M)
        CPU: 67ms
     CGroup: /system.slice/knockd.service
             └─5599 /usr/sbin/knockd -i enp0s3

Feb 20 02:16:58 harshu-VirtualBox systemd[1]: Started knockd.service - Port-Kno>
Feb 20 02:16:58 harshu-VirtualBox knockd[5599]: starting up, listening on enp0s3
Feb 20 02:23:52 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 1
Feb 20 02:23:54 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 2
Feb 20 02:24:03 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 3
Feb 20 02:24:03 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: OPEN SE>
Feb 20 02:24:03 harshu-VirtualBox knockd[5701]: closeSSH: running command: usr/>
```

Image_2

—---

Check if the ssh is actively running by this command

- sudo systemctl status ssh



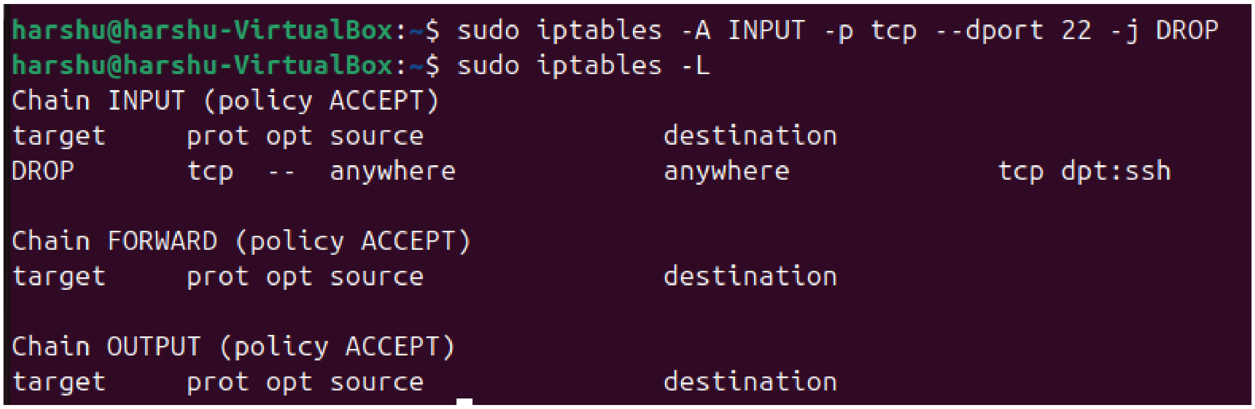
```
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
     Active: active (running) since Wed 2025-02-19 20:23:49 IST; 6h ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1077 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1088 (sshd)
      Tasks: 1 (limit: 4171)
     Memory: 2.2M (peak: 19.9M)
        CPU: 375ms
     CGroup: /system.slice/ssh.service
             └─1088 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 19 20:23:49 harshu-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Se>
Feb 19 20:23:49 harshu-VirtualBox sshd[1088]: Server listening on :: port 22.
Feb 19 20:23:49 harshu-VirtualBox systemd[1]: Started ssh.service - OpenBSD Sec>
Feb 19 20:37:41 harshu-VirtualBox sshd[3112]: Accepted password for harshu from>
Feb 19 20:37:41 harshu-VirtualBox sshd[3112]: pam_unix(sshd:session): session o>
Feb 19 20:39:06 harshu-VirtualBox sshd[3213]: pam_unix(sshd:auth): authenticati>
Feb 19 20:39:13 harshu-VirtualBox sshd[3213]: Failed password for harshu from 1>
Feb 19 20:39:16 harshu-VirtualBox sshd[3213]: Accepted password for harshu from>
Feb 19 20:39:16 harshu-VirtualBox sshd[3213]: pam_unix(sshd:session): session o>
```

Image_3
My ssh is actively running as shown above
—--

Run this command before knocking:

- sudo iptables -A INPUT -p tcp --dport 22 -j DROP

This command **blocks SSH (port 22) by default**, ensuring that SSH access is closed until a successful knock sequence occurs.



```
harshu@harshu-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
harshu@harshu-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Image_4

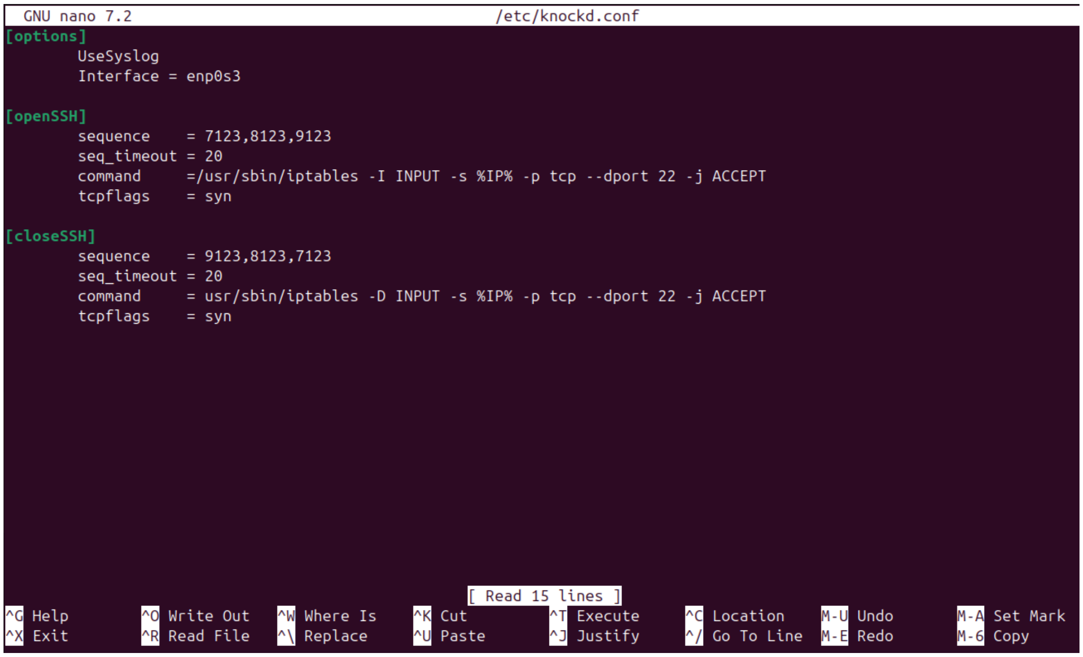
Blocking SSH (port 22) by default prevents brute-force attacks and ensures security. Since knockd dynamically modifies iptables rules, keeping SSH open would make knocking ineffective. By initially blocking SSH, only a correct knock sequence can open it, ensuring controlled access.

—---

enp0s3 is the network interface name used in Linux systems (especially on Ubuntu/Debian) to refer to a specific Ethernet adapter. It is responsible for handling network communication, such as sending and receiving data over the internet or a local network.

As you can see in image 1 my system network interface is enp0s3. So, When configuring knockd, it needs to listen on the correct network interface. If you set it to an incorrect interface, it won't detect port knocking. So, make Interface = enp0s3 in .config file.

Explaining config file:
1. Sequence - Defines the sequence of ports that must be "knocked" in order to open the SSH port.
2. seq_Timeout - Specifies the time window (in seconds) in which the knocking sequence must be completed.
3. Command - Defines the command that should be executed after a correct knock sequence.
- In my file it run, /usr/sbin/iptables -A INPUT -I %IP% -p tcp --dport 22 -j ACCEPT
- This rule **opens SSH (port 22) only for the knocking client's IP**.
4. Tcpflags - Specifies which **TCP flags** should be checked for knocking.



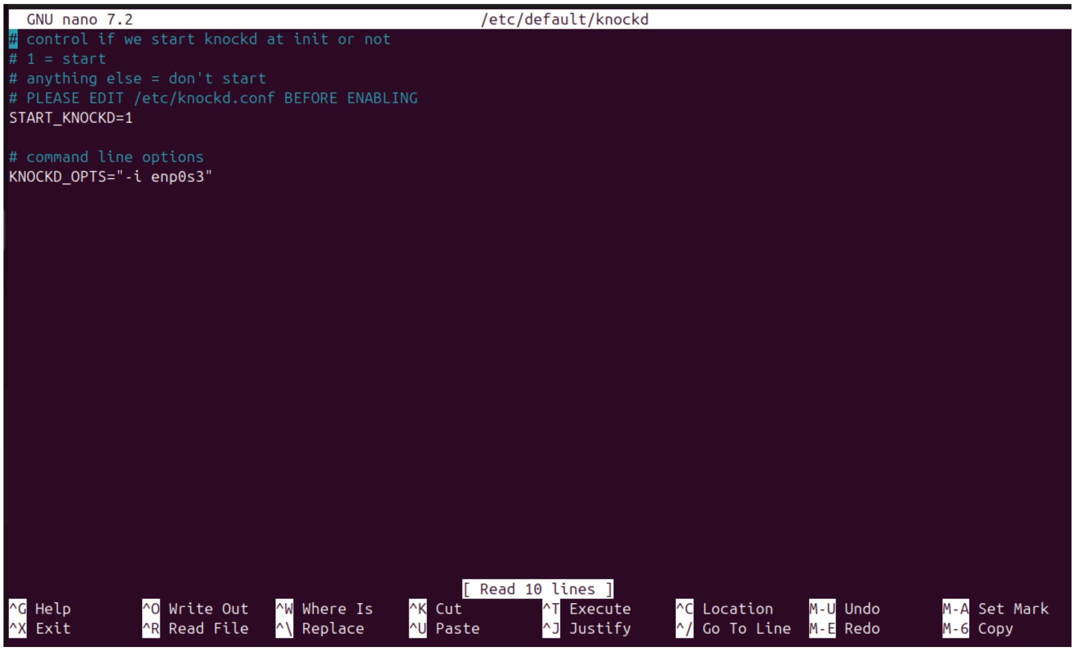
```
  GNU nano 7.2                                      /etc/knockd.conf
[options]
        UseSyslog
        Interface = enp0s3

[openSSH]
        sequence    = 7123,8123,9123
        seq_timeout = 20
        command     =/usr/sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9123,8123,7123
        seq_timeout = 20
        command     = usr/sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

                                               [ Read 15 lines ]
```

Image_5

—---

The /etc/default/knockd file contains environment variables that modify how knockd starts.

Make START_KNOCKD=1 - by this knockd **will start** automatically.
change eth0 to enp0s3 in /etc/default/knockd because your system does not have eth0, and knockd would fail if it tries to listen on a non-existent interface. Using enp0s3 ensures it works on your VM. This tells knockd to listen on enp0s3 instead of eth0.



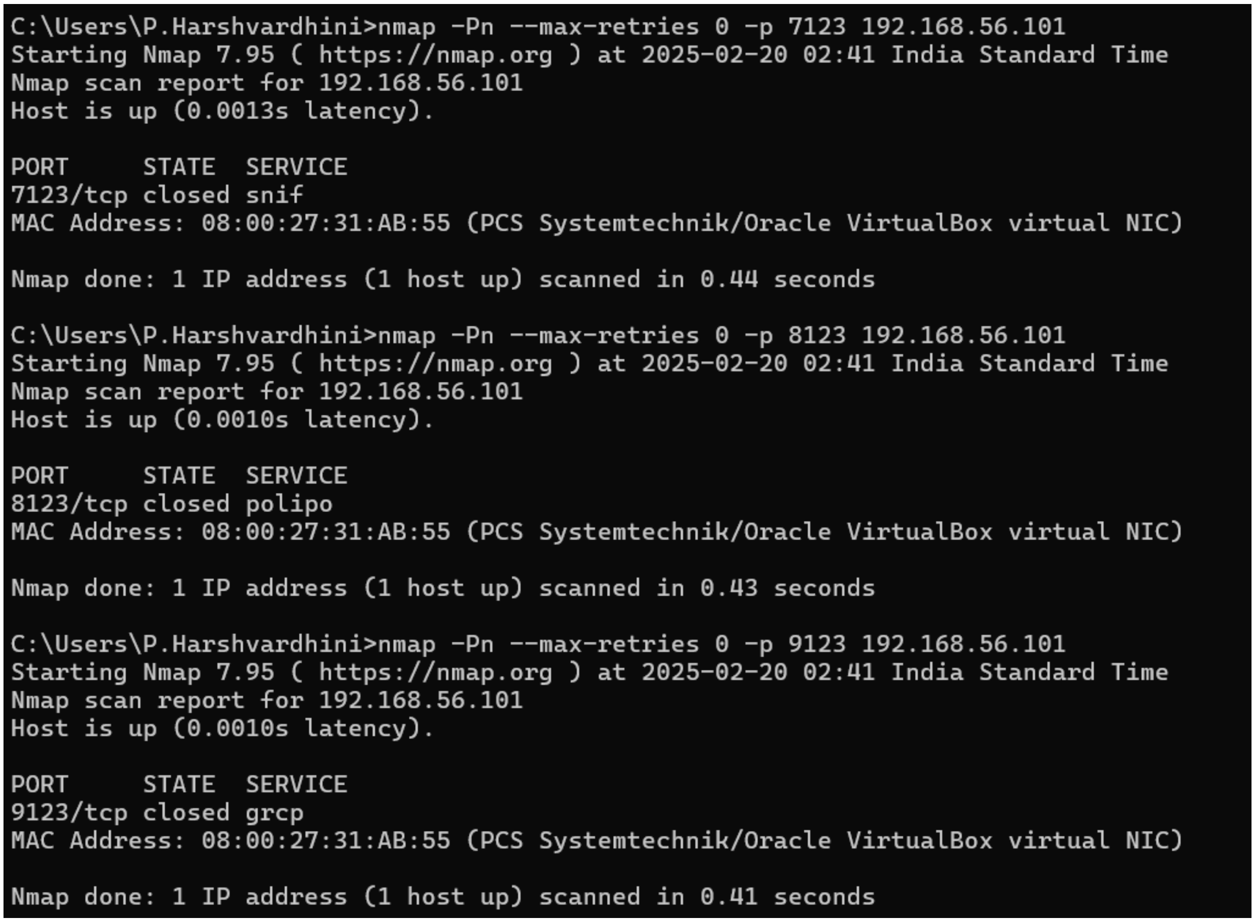
```
  GNU nano 7.2                                   /etc/default/knockd
# control if we start knockd at init or not
# 1 = start
# anything else = don't start
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
KNOCKD_OPTS="-i enp0s3"

                                    [ Read 10 lines ]
```

Image_6

—---

Opening the SSH Session

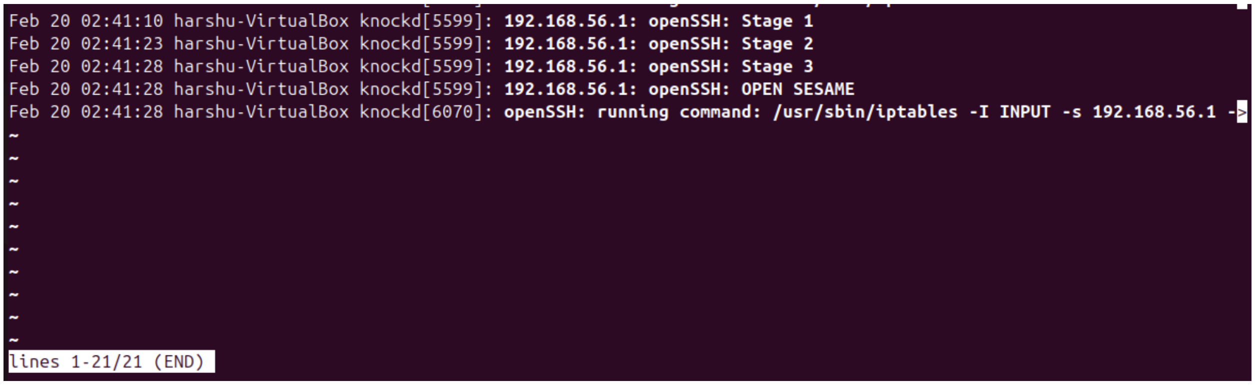
Using Nmap in Windows CMD, I sent the predefined sequence to trigger knockd on the server.



```
C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 7123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:41 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0013s latency).

PORT     STATE  SERVICE
7123/tcp closed snif
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 8123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:41 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
8123/tcp closed polipo
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 9123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:41 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
9123/tcp closed grcp
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Image_7

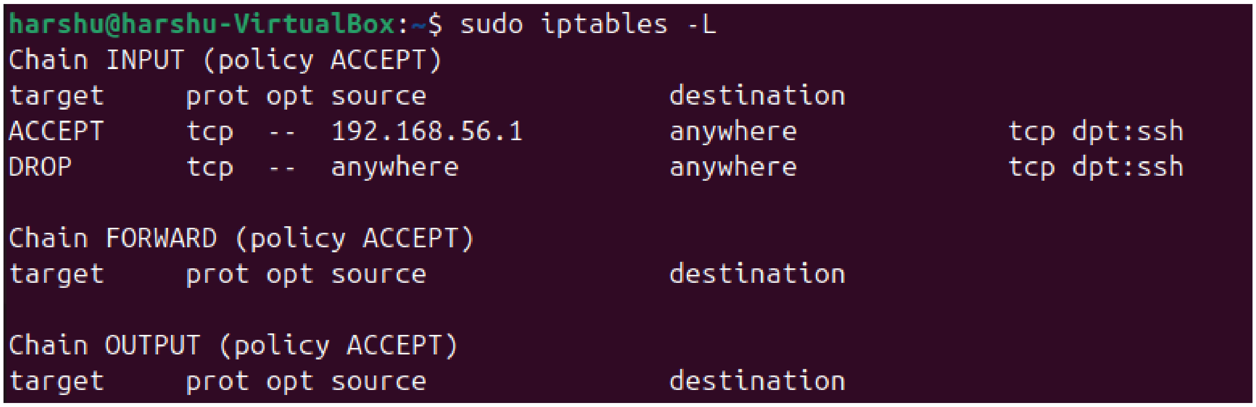
—---



```
Feb 20 02:41:10 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 1
Feb 20 02:41:23 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 2
Feb 20 02:41:28 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 3
Feb 20 02:41:28 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: OPEN SESAME
Feb 20 02:41:28 harshu-VirtualBox knockd[6070]: openSSH: running command: /usr/sbin/iptables -I INPUT -s 192.168.56.1 ->
~
~
~
~
~
~
~
~
~
~
lines 1-21/21 (END)
```

Image_8

Verification on the server (sudo systemctl status knockd) confirmed that knockd successfully registered the knock sequence. By opening port 22 SSH.



```
harshu@harshu-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.56.1         anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

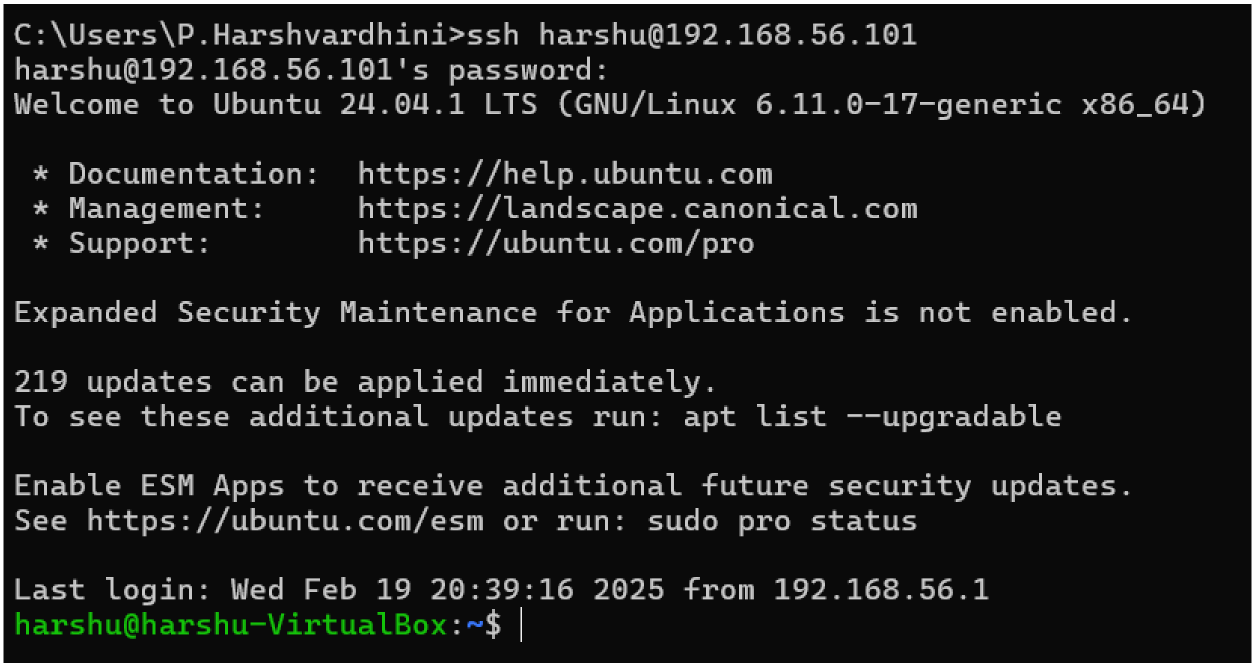
Image_9

Running “sudo iptables -L” showed that an ACCEPT rule was added for SSH (port 22). This confirmed that the knock sequence successfully modified firewall rules to allow SSH connections.

Now try doing ssh also from windows by the following command
Connected to the VM using:

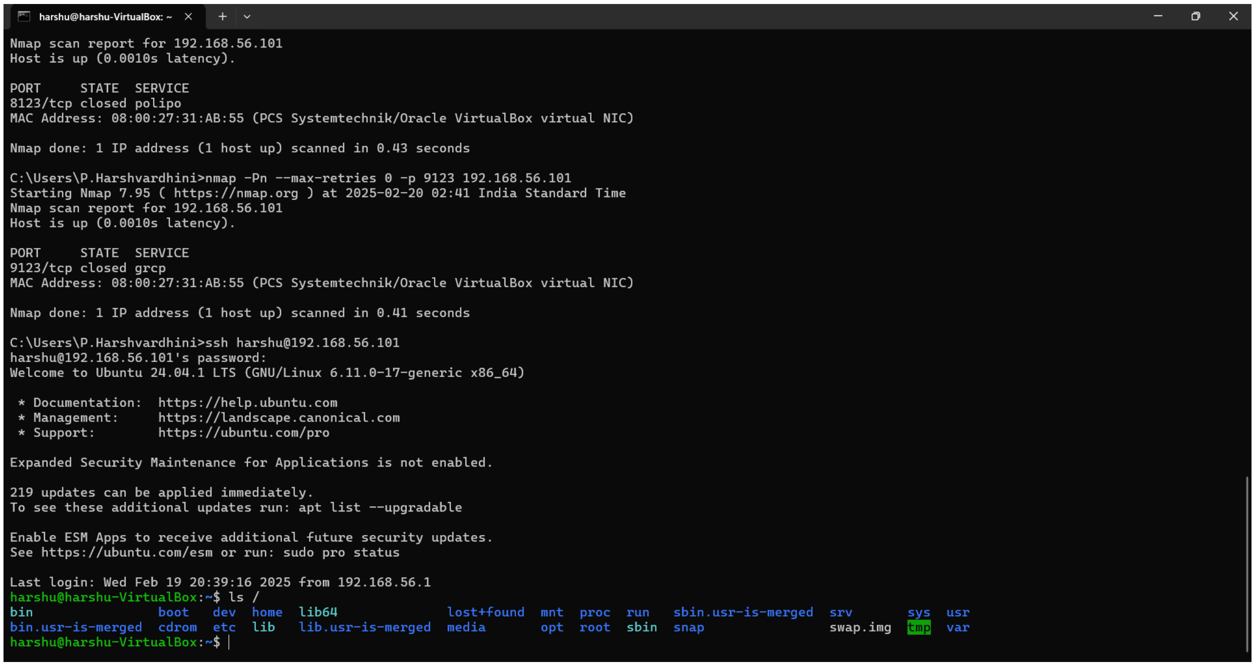
- harshu@192.168.56.101

As you can see below Welcome message means able to access vm through windows.

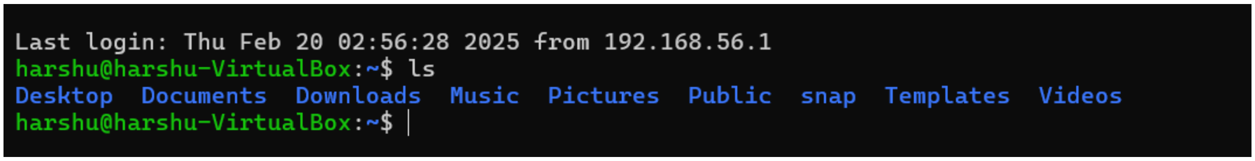


```
C:\Users\P.Harshvardhini>ssh harshu@192.168.56.101
harshu@192.168.56.101's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

219 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Feb 19 20:39:16 2025 from 192.168.56.1
harshu@harshu-VirtualBox:~$ 
```

Image_9 - Connected successfully



```
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
8123/tcp closed polipo
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 9123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:41 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
9123/tcp closed grcp
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

C:\Users\P.Harshvardhini>ssh harshu@192.168.56.101
harshu@192.168.56.101's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

219 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Feb 19 20:39:16 2025 from 192.168.56.1
harshu@harshu-VirtualBox:~$ ls /
bin                boot   dev  home  lib64              lost+found  mnt  proc  run   sbin.usr-is-merged  srv       sys  usr
bin.usr-is-merged  cdrom  etc  lib   lib.usr-is-merged  media       opt  root  sbin  snap                swap.img  tmp  var
harshu@harshu-VirtualBox:~$ |
```



```
Last login: Thu Feb 20 02:56:28 2025 from 192.168.56.1
harshu@harshu-VirtualBox:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
harshu@harshu-VirtualBox:~$ |
```

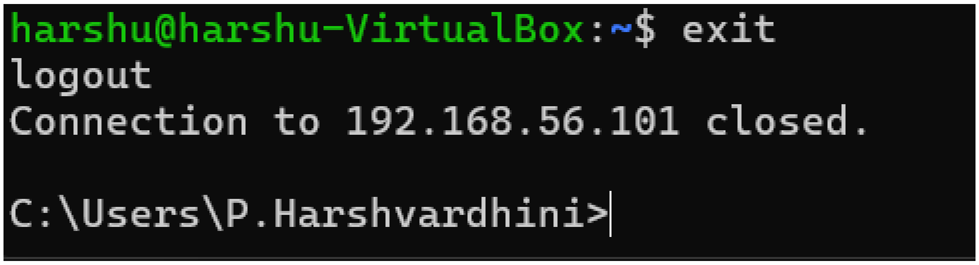
Image_10
Successfully accessed the VM and listed all directories, confirming SSH access was granted.

—---

Closing the SSH Session

Exited the SSH session using command

- exit

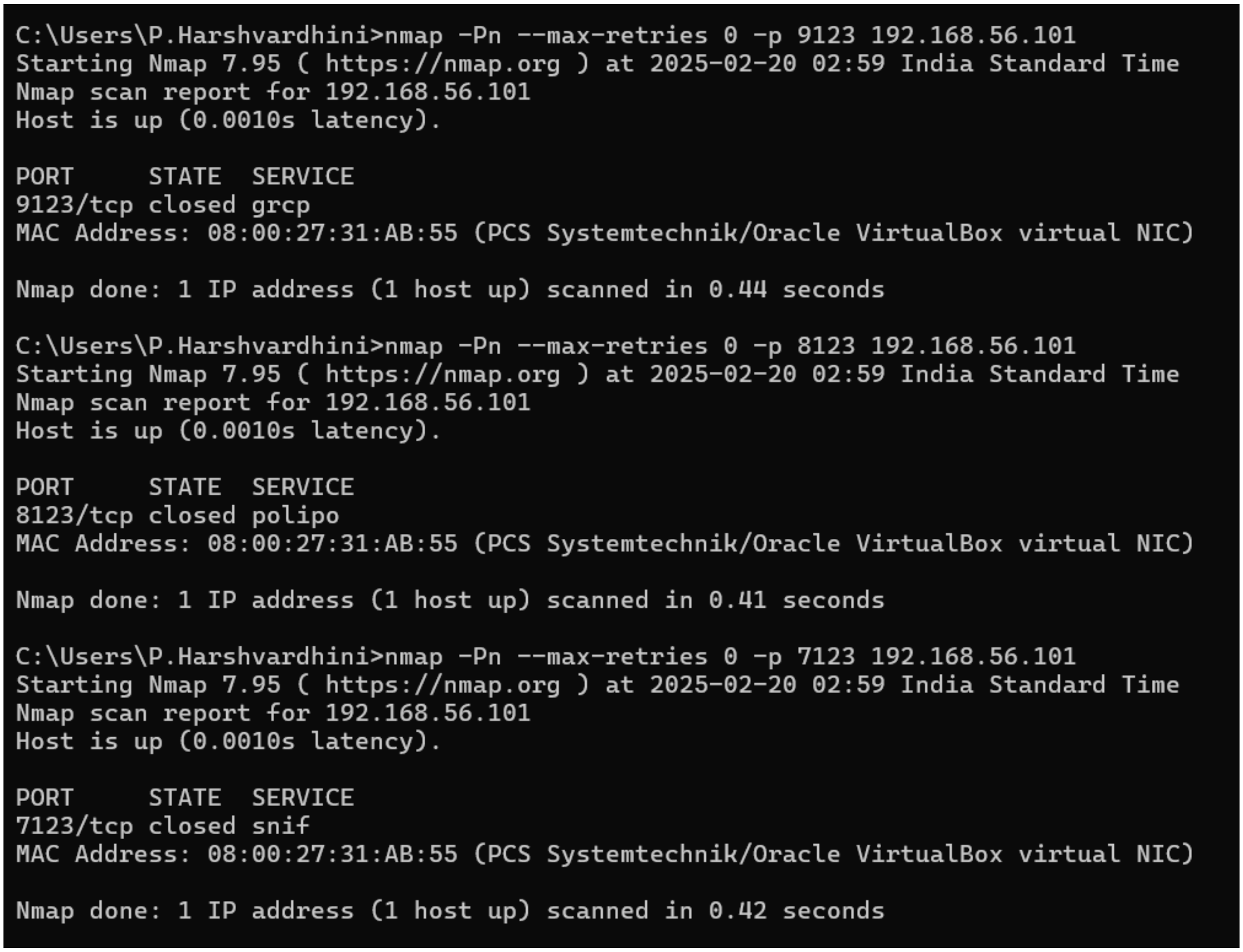


```
harshu@harshu-VirtualBox:~$ exit
logout
Connection to 192.168.56.101 closed.

C:\Users\P.Harshvardhini>
```

Image_11

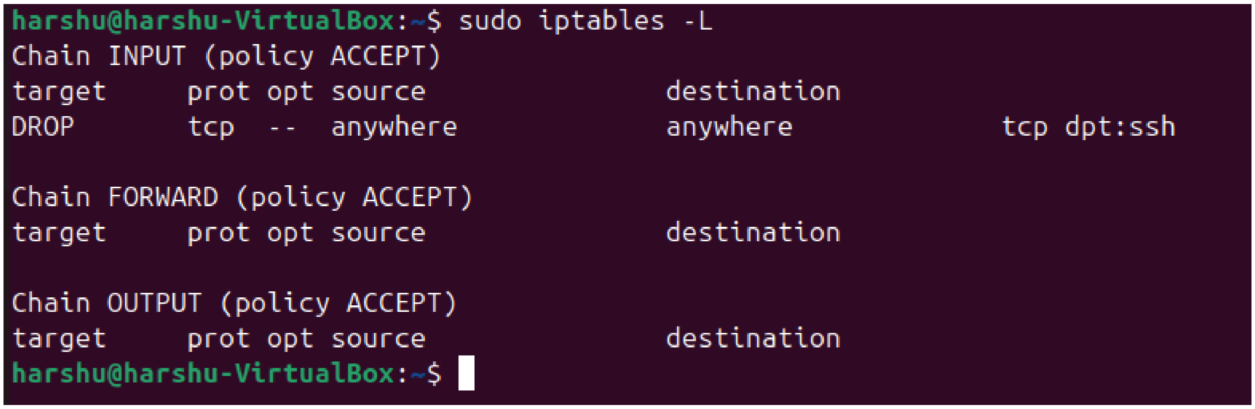
—---

Send the **closing knock sequence** from Windows CMD.
Closing the port 22 ssh.



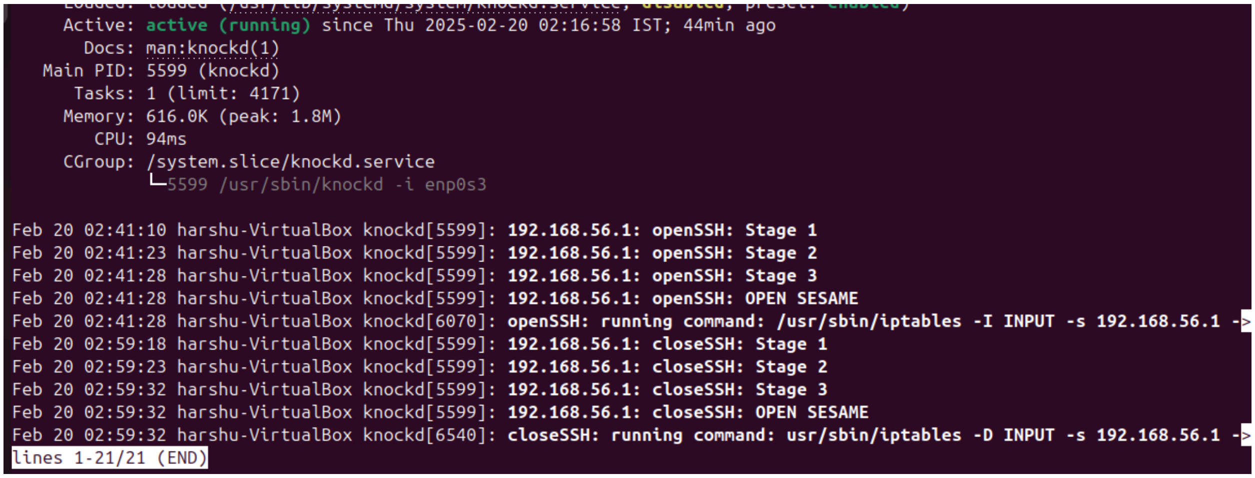
```
C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 9123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:59 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
9123/tcp closed grcp
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 8123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:59 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
8123/tcp closed polipo
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

C:\Users\P.Harshvardhini>nmap -Pn --max-retries 0 -p 7123 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 02:59 India Standard Time
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
7123/tcp closed snif
MAC Address: 08:00:27:31:AB:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

—---



```
harshu@harshu-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
harshu@harshu-VirtualBox:~$
```

Image_12
Verified that knockd removed the ACCEPT rule in iptables, effectively blocking SSH again.



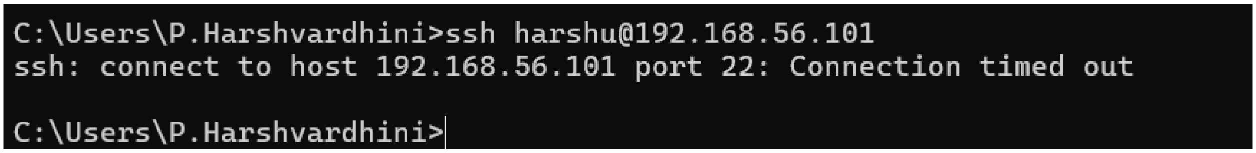
```
   Loaded: loaded (/usr/lib/systemd/system/knockd.service; disabled; preset: enabled)
   Active: active (running) since Thu 2025-02-20 02:16:58 IST; 44min ago
     Docs: man:knockd(1)
 Main PID: 5599 (knockd)
    Tasks: 1 (limit: 4171)
   Memory: 616.0K (peak: 1.8M)
      CPU: 94ms
   CGroup: /system.slice/knockd.service
           └─5599 /usr/sbin/knockd -i enp0s3

Feb 20 02:41:10 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 1
Feb 20 02:41:23 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 2
Feb 20 02:41:28 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: Stage 3
Feb 20 02:41:28 harshu-VirtualBox knockd[5599]: 192.168.56.1: openSSH: OPEN SESAME
Feb 20 02:41:28 harshu-VirtualBox knockd[6070]: openSSH: running command: /usr/sbin/iptables -I INPUT -s 192.168.56.1 ->
Feb 20 02:59:18 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 1
Feb 20 02:59:23 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 2
Feb 20 02:59:32 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: Stage 3
Feb 20 02:59:32 harshu-VirtualBox knockd[5599]: 192.168.56.1: closeSSH: OPEN SESAME
Feb 20 02:59:32 harshu-VirtualBox knockd[6540]: closeSSH: running command: usr/sbin/iptables -D INPUT -s 192.168.56.1 ->
lines 1-21/21 (END)
```

Image_13

As you can see closed successfully after running sudo systemctl status knockd

—--

After closing, not able to access the server through ssh as you can see below, means successfully closed as you can see below.



```
C:\Users\P.Harshvardhini>ssh harshu@192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection timed out

C:\Users\P.Harshvardhini>
```

Image_14

Part-B

- TCP ensures that all the data packets will be received without getting lost and reaching in the correct order. Basically it is reliable. On the other hand, UDP does not guarantee the delivery of all the packets and is lost making it difficult to maintain the correct sequence.
- Many networks do not support UDP packets and block them, restricting it from knocking.
- Further tcp provide option of error checking but there is no such facility for udp.

Part-C

- As the default of port sequence in port 22 is 7000, 8000, 9000. Thus these values are already known to others so, changing the port sequence adds more security to our port knocking. So changing it would be a better option rather than using the default sequence.