a)

Installation

```
zakmii@zakmii-VirtualBox:~$ sudo apt install knockd iptables -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libip4tc2 libip6tc2 libxtables12
Suggested packages:
  firewalld
The following NEW packages will be installed:
  knockd
The following packages will be upgraded:
  iptables libip4tc2 libip6tc2 libxtables12
4 upgraded, 1 newly installed, 0 to remove and 430 not upgraded.
Need to get 556 kB of archives.
After this operation, 111 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 iptables amd64
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxtables12 a
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2 amd6
```

```
zakmii@zakmii-VirtualBox:~$ sudo nano /etc/default/knockd
zakmii@zakmii-VirtualBox:~$ sudo nano /etc/knockd.conf
zakmii@zakmii-VirtualBox:~$ clera^C
zakmii@zakmii-VirtualBox:~$ ^C
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p udp --dport 7000 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p udp --dport 8000 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p udp --dport 9000 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo systemctl restart knockd
zakmii@zakmii-VirtualBox:~$ sudo systemctl enable knockd
```

dropping port 22 and also accepting knock using tcp

```
zakmii@zakmii-VirtualBox:~$ sudo systemctl enable knockd
Synchronizing state of knockd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable knockd
Created symlink /etc/systemd/system/multi-user.target.wants/knockd.service → /lib/systemd/system/knockd.service.
zakmii@zakmii-VirtualBox:~$ hostname -I
10.0.2.15
zakmii@zakmii-VirtualBox:~$ knock -v 10.0.2.15 7000 8000 9000
hitting tcp 10.0.2.15:7000
hitting tcp 10.0.2.15:8000
hitting tcp 10.0.2.15:9000
```

knocking to open the port

```
zakmll@zakmll-VirtualBox:~$ knock -v 10.0.2.15 9000 8000 7000
hitting tcp 10.0.2.15:9000
hitting tcp 10.0.2.15:8000
hitting tcp 10.0.2.15:7000
```

knocking again in reverse order to close the port

```
 GNU nano 6.2                                    /etc/knockd.conf
[options]
        UseSyslog

[openSSH]
        sequence    = 7000,8000,9000
        seq_timeout = 10
        command     = /usr/sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9000,8000,7000
        seq_timeout = 10
        command     = /usr/sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[openHTTPS]
        sequence    = 12345,54321,24680,13579
        seq_timeout = 5
        command     = /usr/local/sbin/knock_add -i -c INPUT -p tcp -d 443 -f %IP%
        tcpflags    = syn
```

b)

-> TCP is more reliable and guarantees that the knock was delivered
-> allows filtering based on SYN flags

c)

default knocking sequence is 7000, 8000, 9000
It is not safe as can be guessed by every attacker

We should use more randomised and lengthy sequence