FCS- assignment - 1.2

Q4.a

```
fcs24@fcs01:~$ sudo apt-get install knockd
[sudo] password for fcs24:
Sorry, try again.
[sudo] password for fcs24:
Sorry, try again.
[sudo] password for fcs24:
Reading package lists... Done
Building dependency tree
Reading state information... Done
knockd is already the newest version (0.7-1ubuntu3.20.04.1).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
fcs24@fcs01:~$
```

- installing knockd

```
[options]
        UseSyslog

[openSSH]
        sequence    = 10005,10006,10007
        seq_timeout = 5
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 10007,10006,10005
        seq_timeout = 5
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

- configuring knockd by changing user sequence from default to 10005,10006,10007 for openssh, and reversed sequence for closedSSh
- And changing command for iptables rule by insering only some ip which are alllowed to use ssh port , otherswise we removed all other application or program such as ssh to whitelisted to use port 22.

```
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.42  netmask 255.255.252.0  broadcast 192.168.3.255
        inet6 fe80::20c:29ff:fef8:7cd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f8:7c:d2  txqueuelen 1000  (Ethernet)
        RX packets 52057406  bytes 4233358599 (4.2 GB)
        RX errors 0  dropped 2813231  overruns 0  frame 0
        TX packets 92370  bytes 8826211 (8.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1234  bytes 123408 (123.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1234  bytes 123408 (123.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

fcs24@fcs01:~$
```

- using ifconfig to get network interface which required in next step
- configuring knock sudo nano /etc/default/knockd

```
  GNU nano 4.8
# 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 ens32"
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1234  bytes 123408 (123.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

fcs24@fcs01:~$ sudo nano /etc/default/knockd
fcs24@fcs01:~$ sudo nano /etc/default/knockd
fcs24@fcs01:~$ sudo systemctl start knockd
fcs24@fcs01:~$
```

- starting knockd service using systelctl

```
fcs24@fcs01:~$ sudo nano /etc/default/knockd
fcs24@fcs01:~$ sudo systemctl start knockd
fcs24@fcs01:~$ 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
fcs24@fcs01:~$
```

- enable knockd service

```
fcs24@fcs01:~$ sudo systemctl status knockd
● knockd.service - Port-Knock Daemon
     Loaded: loaded (/lib/systemd/system/knockd.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-10-12 23:29:34 UTC; 1 day 15h ago
       Docs: man:knockd(1)
   Main PID: 855360 (knockd)
      Tasks: 1 (limit: 2273)
     Memory: 1.4M
     CGroup: /system.slice/knockd.service
             └─855360 /usr/sbin/knockd -i ens32

Oct 12 23:36:34 fcs01 knockd[855748]: openSSH: running command: /sbin/iptables -I INPUT -s 192.168.57.142 -p tcp --dport 22 -j ACCEPT
Oct 12 23:40:07 fcs01 knockd[855360]: 192.168.57.142: closeSSH: Stage 1
Oct 12 23:40:07 fcs01 knockd[855360]: 192.168.57.142: closeSSH: Stage 2
Oct 12 23:40:07 fcs01 knockd[855360]: 192.168.57.142: closeSSH: Stage 3
Oct 12 23:40:07 fcs01 knockd[855360]: 192.168.57.142: closeSSH: OPEN SESAME
Oct 14 14:25:31 fcs01 knockd[855360]: 192.168.57.142: openSSH: Stage 1
Oct 14 14:25:31 fcs01 knockd[855360]: 192.168.57.142: openSSH: Stage 2
Oct 14 14:25:31 fcs01 knockd[855360]: 192.168.57.142: openSSH: Stage 3
Oct 14 14:25:31 fcs01 knockd[855360]: 192.168.57.142: openSSH: OPEN SESAME
Oct 14 14:25:31 fcs01 knockd[916287]: openSSH: running command: /sbin/iptables -I INPUT -s 192.168.57.142 -p tcp --dport 22 -j ACCEPT
fcs24@fcs01:~$
```

```
fcs24@fcs01:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Apache Full                ALLOW IN    Anywhere
[ 2] 20/tcp                     ALLOW IN    Anywhere
[ 3] 21/tcp                     ALLOW IN    Anywhere
[ 4] Apache Full (v6)           ALLOW IN    Anywhere (v6)
[ 5] 20/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] 21/tcp (v6)                ALLOW IN    Anywhere (v6)

fcs24@fcs01:~$
```

- removing ssh from whitelisted programs
- now in ip tables rules we are allowing only specific ip that can access 22 tcp port
- and if that user send reverse sequence then that ip rule is remove from the table

Q4-b Why should one prefer doing this over TCP instead of UDP?

- Because udp is stateless protocol
- While sending packets using udp the packet might dropped or come in unorder way.
- Since knockd what particular sequence hits , that cannot be possible using udp.

Q4-c What is the default choice of ports in the knockd configuration. Is it safe?

- no it is not safe , since it is default configuraion everyone knows the sequence, hence the we can say that anyone can hit same sequence if it is default one, and get the access.
- It is like you lock your house door with pinlock , but since their is default pinlock code you didnt change, everyone have little knowledge about it can unlock it.