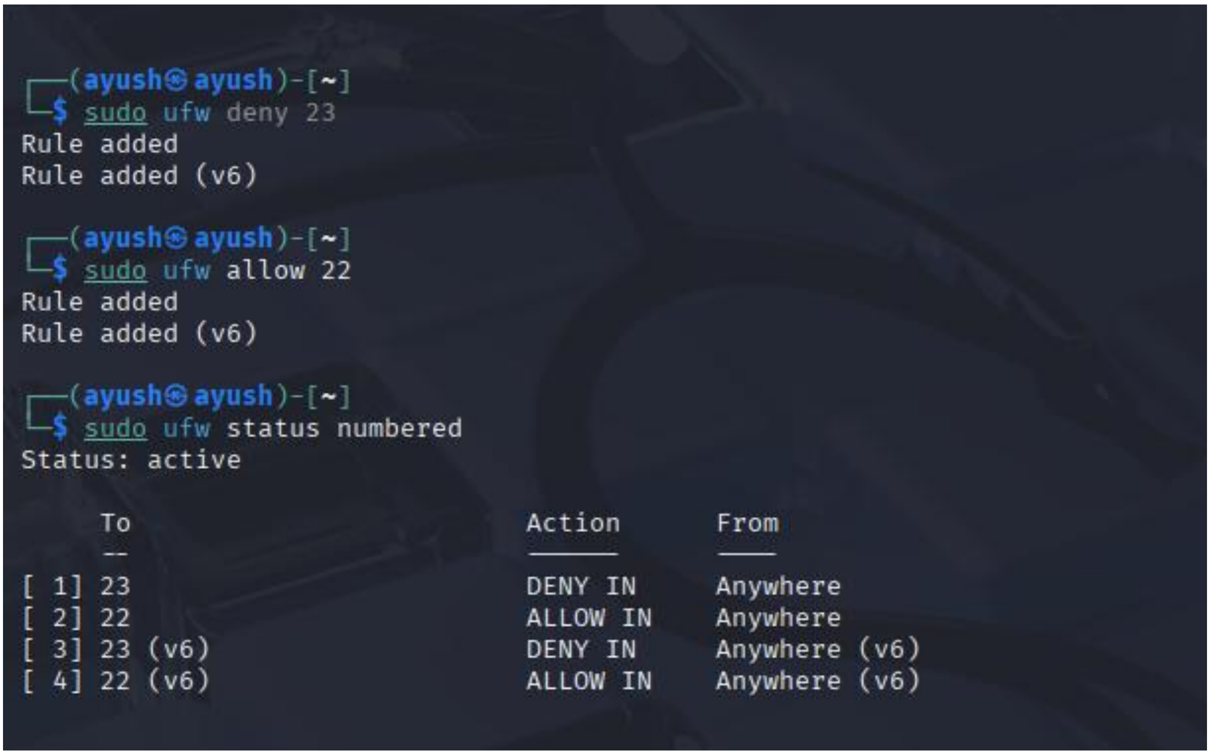
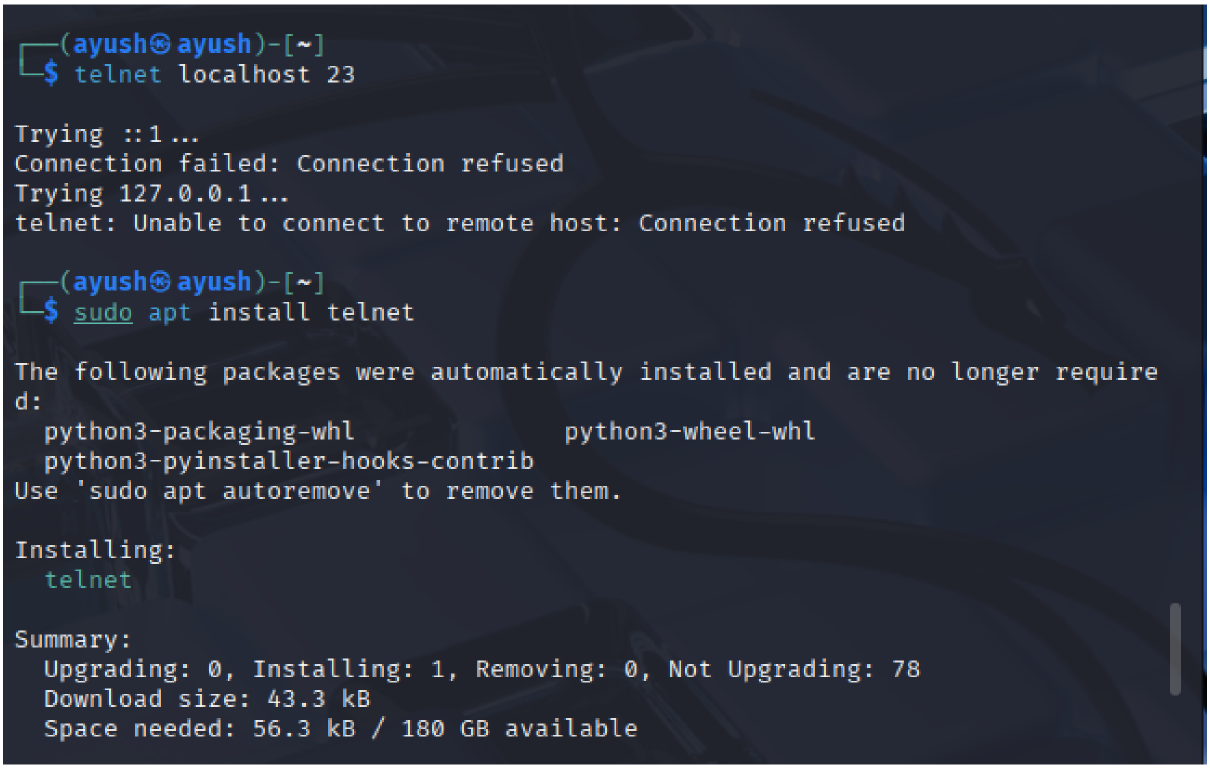
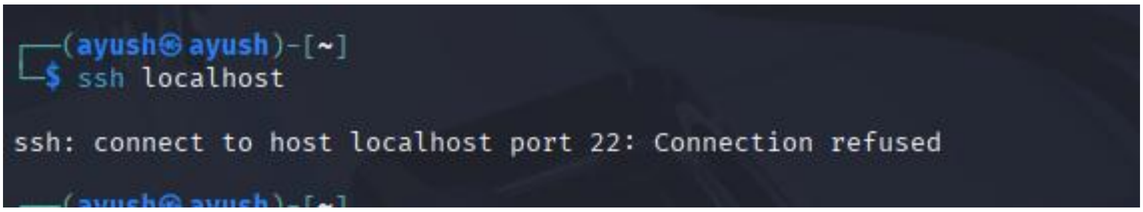


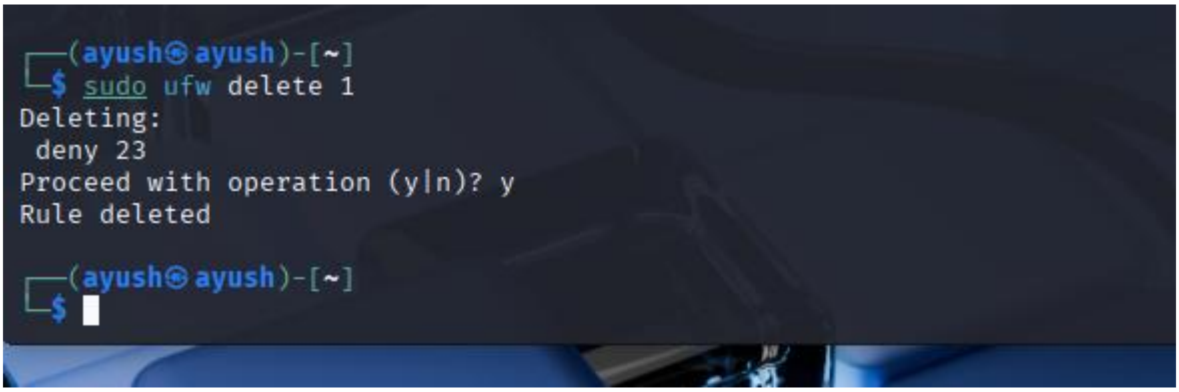
```
┌──(ayush㉿ayush)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 23 (v6)                    DENY IN     Anywhere (v6)
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
```



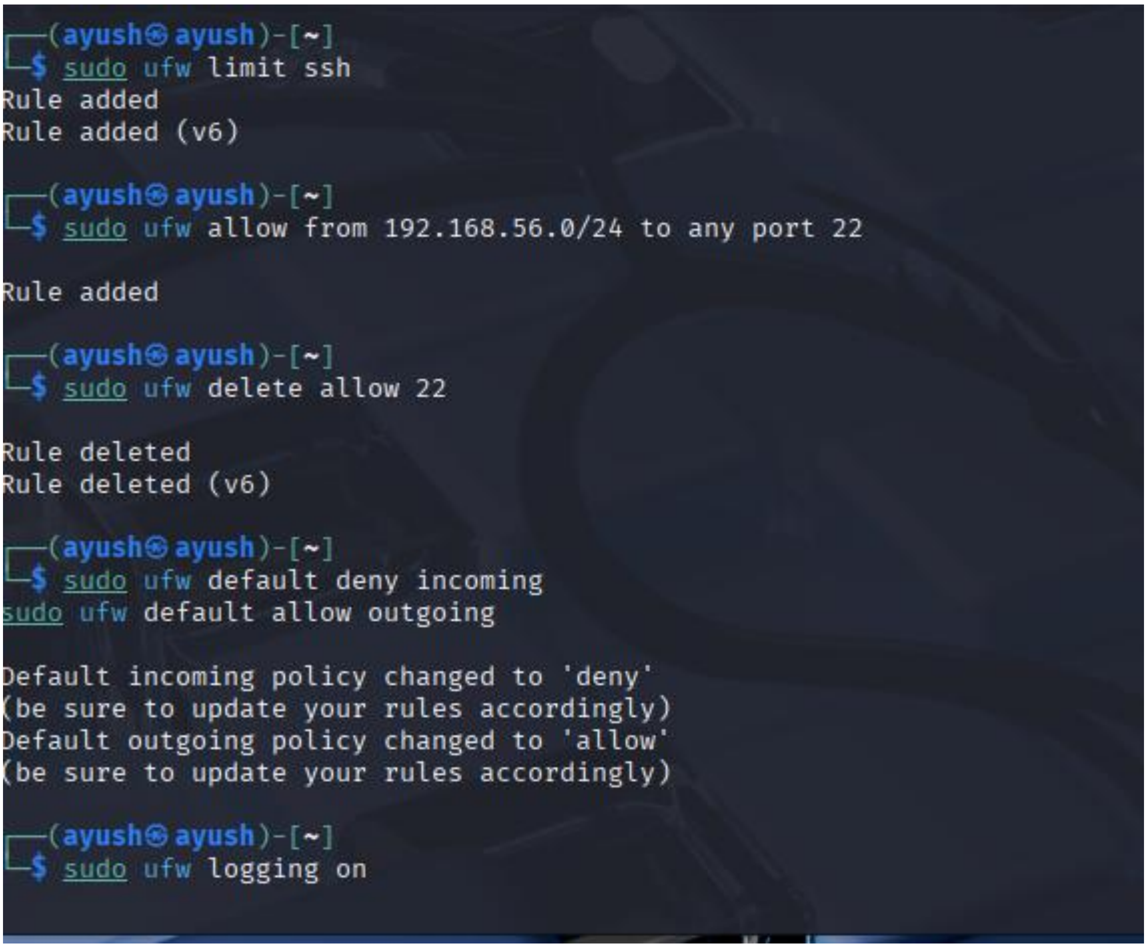
```
┌──(ayush㉿ayush)-[~]
└─$ telnet localhost 23

Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(ayush㉿ayush)-[~]
└─$ sudo apt install telnet

The following packages were automatically installed and are no longer require
d:
  python3-packaging-whl              python3-wheel-whl
  python3-pyinstaller-hooks-contrib
Use 'sudo apt autoremove' to remove them.

Installing:
  telnet

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 78
  Download size: 43.3 kB
  Space needed: 56.3 kB / 180 GB available
```



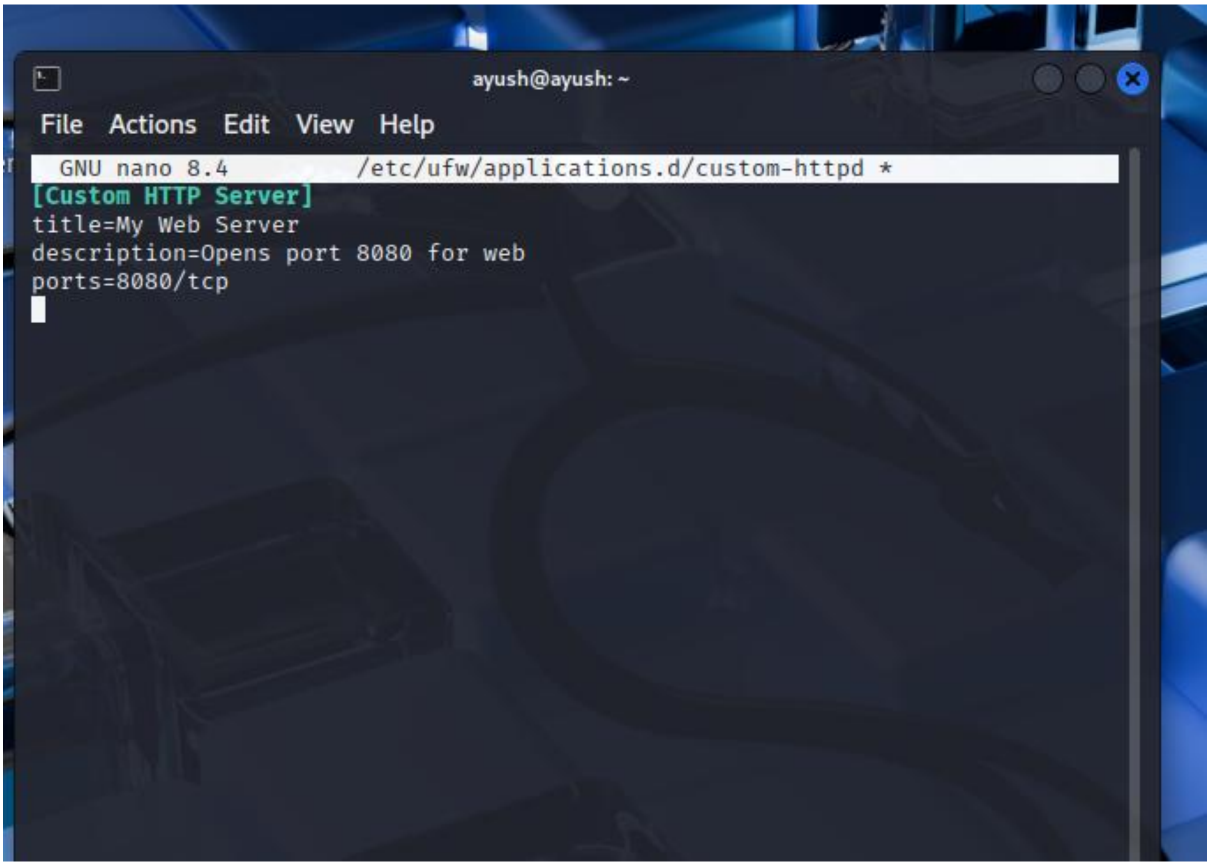
```
┌──(ayush㉿ayush)-[~]
└─$ ssh localhost

ssh: connect to host localhost port 22: Connection refused

┌──(ayush㉿ayush)-[~]
```



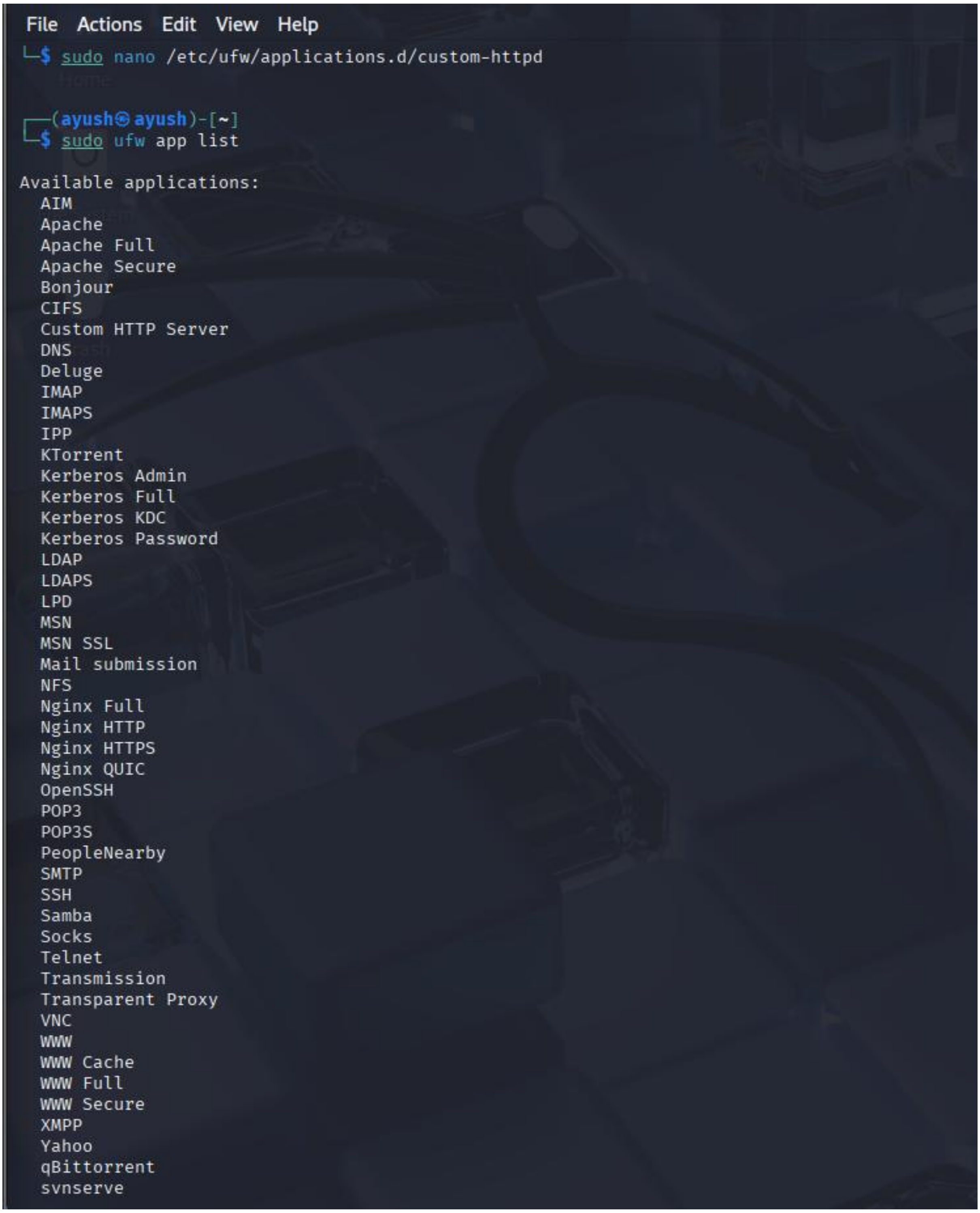
```
┌──(ayush㉿ayush)-[~]
└─$ sudo ufw delete 1
Deleting:
 deny 23
Proceed with operation (y|n)? y
Rule deleted

┌──(ayush㉿ayush)-[~]
└─$ 
```



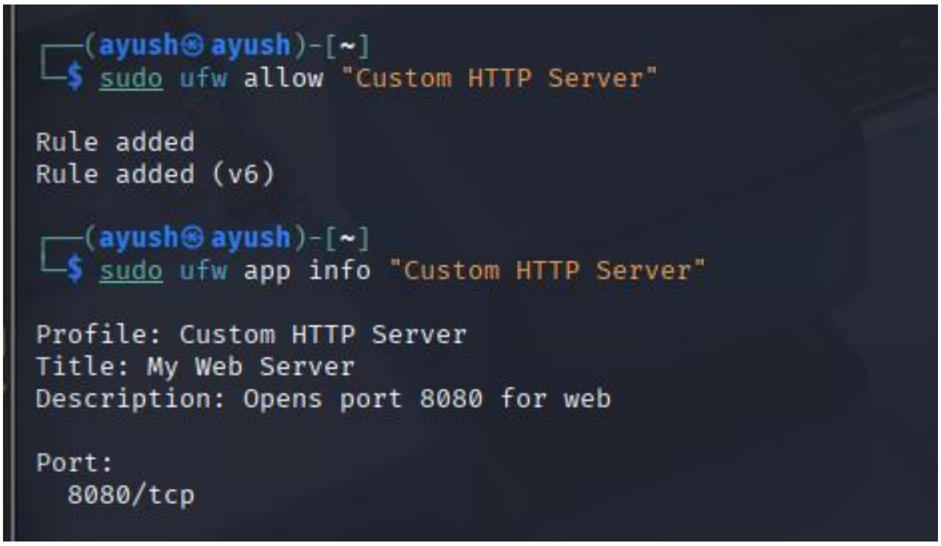
```
┌──(ayush㉿ayush)-[~]
└─$ sudo ufw limit ssh
Rule added
Rule added (v6)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw allow from 192.168.56.0/24 to any port 22

Rule added

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw delete allow 22

Rule deleted
Rule deleted (v6)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw default deny incoming
sudo ufw default allow outgoing

Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw logging on
```



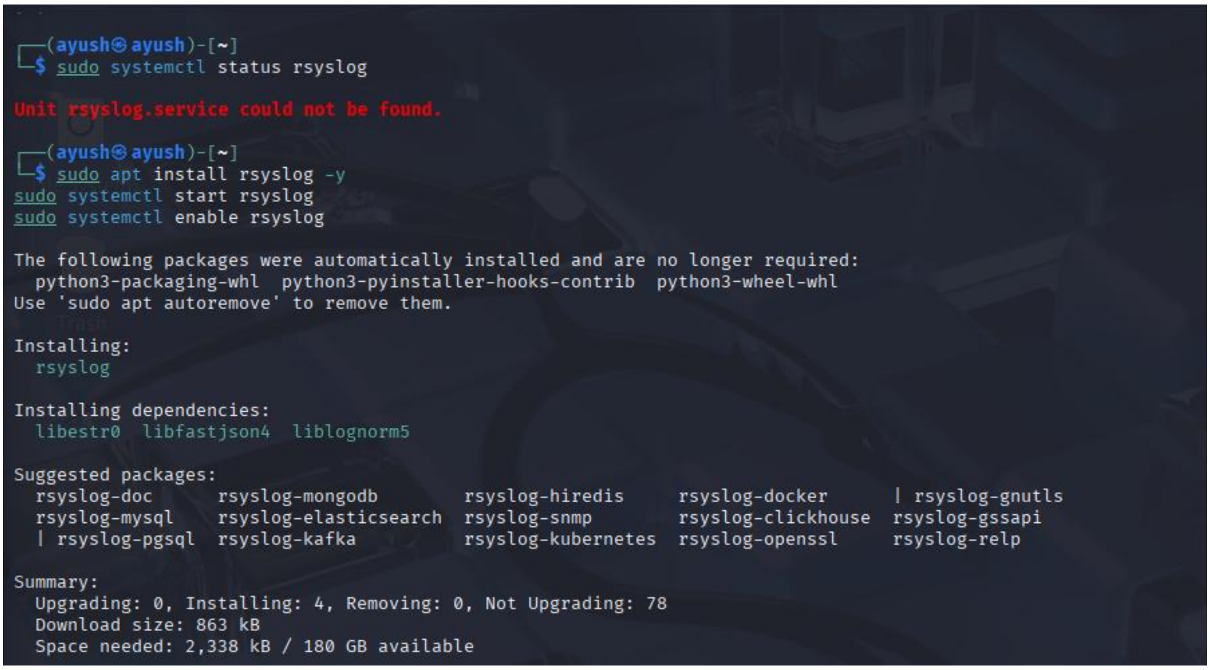
```
  GNU nano 8.4          /etc/ufw/applications.d/custom-httpd *
[Custom HTTP Server]
title=My Web Server
description=Opens port 8080 for web
ports=8080/tcp
```



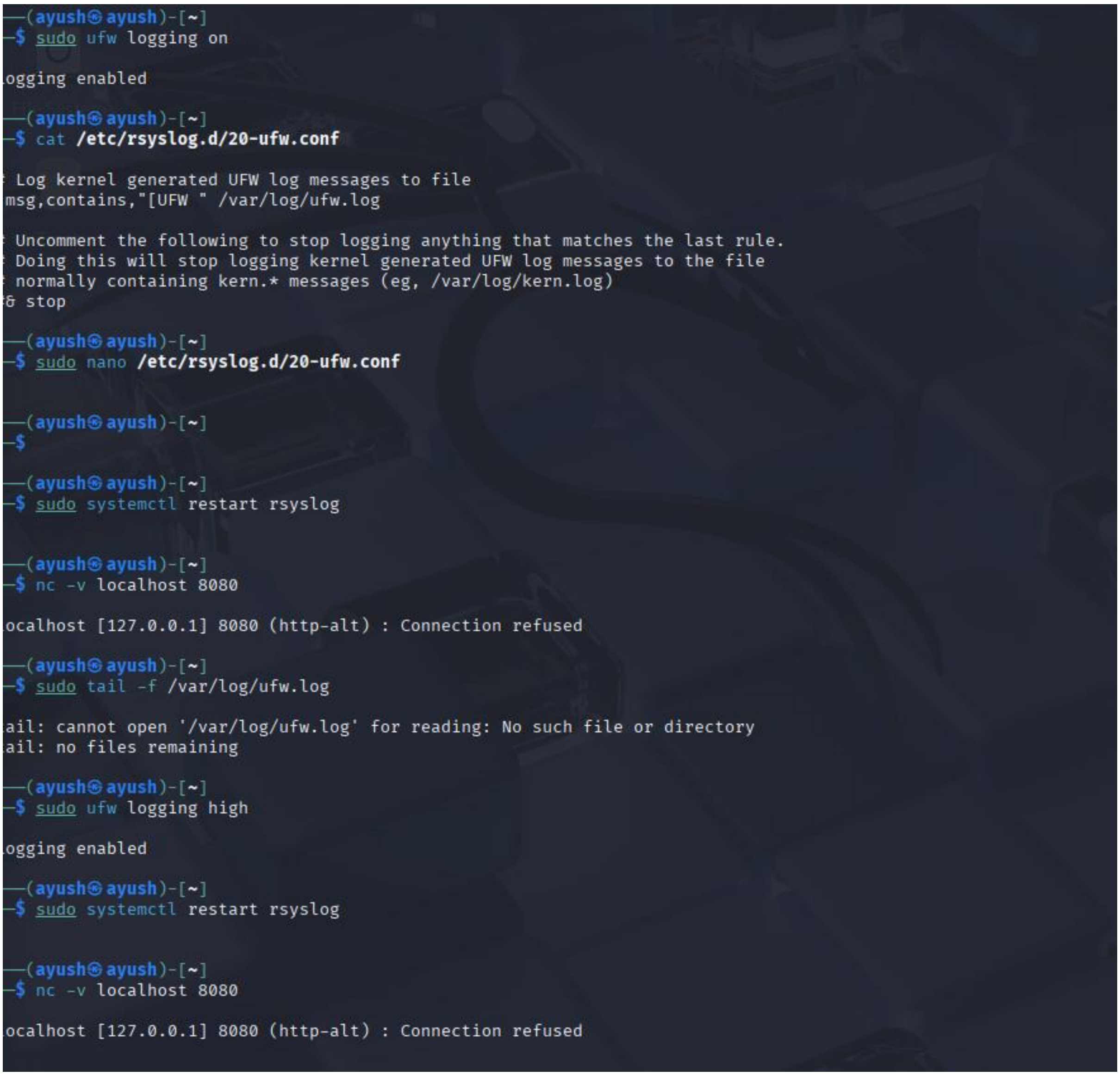
```
└─$ sudo nano /etc/ufw/applications.d/custom-httpd

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw app list

Available applications:
  AIM
  Apache
  Apache Full
  Apache Secure
  Bonjour
  CIFS
  Custom HTTP Server
  DNS
  Deluge
  IMAP
  IMAPS
  IPP
  KTorrent
  Kerberos Admin
  Kerberos Full
  Kerberos KDC
  Kerberos Password
  LDAP
  LDAPS
  LPD
  MSN
  MSN SSL
  Mail submission
  NFS
  Nginx Full
  Nginx HTTP
  Nginx HTTPS
  Nginx QUIC
  OpenSSH
  POP3
  POP3S
  PeopleNearby
  SMTP
  SSH
  Samba
  Socks
  Telnet
  Transmission
  Transparent Proxy
  VNC
  WWW
  WWW Cache
  WWW Full
  WWW Secure
  XMPP
  Yahoo
  qBittorrent
  svnserve
```



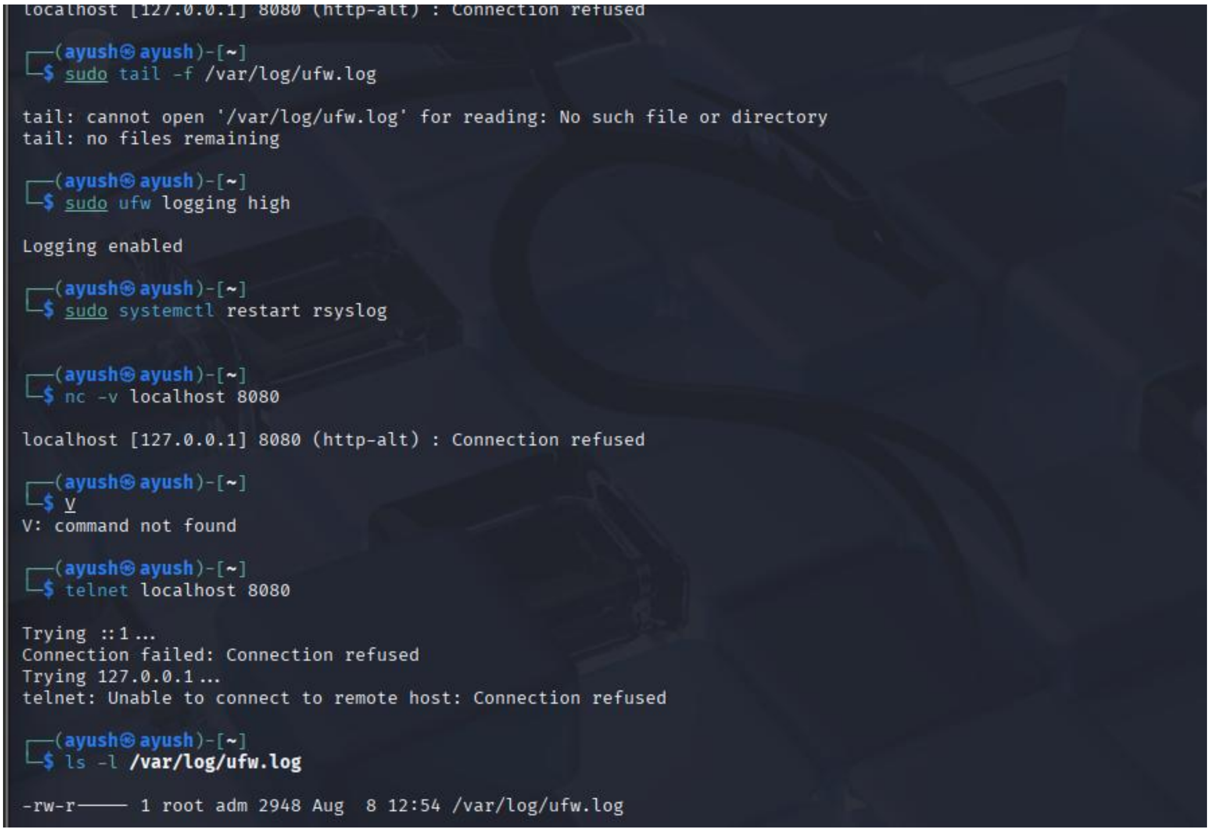
```
┌──(ayush㉿ayush)-[~]
└─$ sudo ufw allow "Custom HTTP Server"

Rule added
Rule added (v6)

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw app info "Custom HTTP Server"

Profile: Custom HTTP Server
Title: My Web Server
Description: Opens port 8080 for web

Port:
  8080/tcp
```



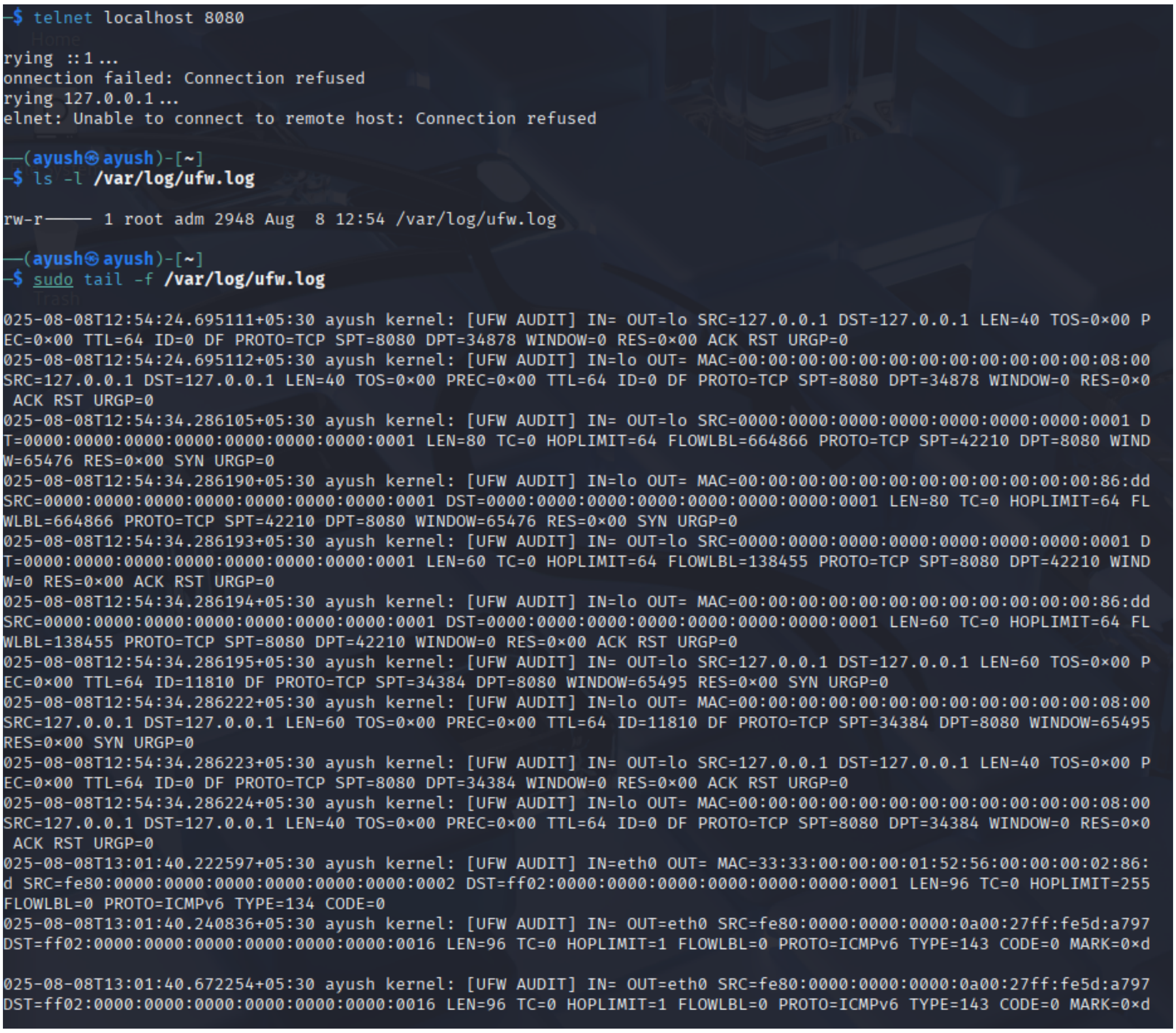
```
┌──(ayush㉿ayush)-[~]
└─$ sudo systemctl status rsyslog

Unit rsyslog.service could not be found.

┌──(ayush㉿ayush)-[~]
└─$ sudo apt install rsyslog -y
sudo systemctl start rsyslog
sudo systemctl enable rsyslog

The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
  rsyslog

Installing dependencies:
  libestr0  libfastjson4  liblognorm5

Suggested packages:
  rsyslog-doc       rsyslog-mongodb        rsyslog-hiredis     rsyslog-docker      | rsyslog-gnutls
  rsyslog-mysql     rsyslog-elasticsearch  rsyslog-snmp        rsyslog-clickhouse  rsyslog-gssapi
  | rsyslog-pgsql  rsyslog-kafka          rsyslog-kubernetes  rsyslog-openssl     rsyslog-relp

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 78
  Download size: 863 kB
  Space needed: 2,338 kB / 180 GB available
```



```
─(ayush㉿ayush)-[~]
─$ sudo ufw logging on

ogging enabled

─(ayush㉿ayush)-[~]
─$ cat /etc/rsyslog.d/20-ufw.conf

: Log kernel generated UFW log messages to file
msg,contains,"[UFW " /var/log/ufw.log

: Uncomment the following to stop logging anything that matches the last rule.
: Doing this will stop logging kernel generated UFW log messages to the file
: normally containing kern.* messages (eg, /var/log/kern.log)
& stop

─(ayush㉿ayush)-[~]
─$ sudo nano /etc/rsyslog.d/20-ufw.conf


─(ayush㉿ayush)-[~]
─$

─(ayush㉿ayush)-[~]
─$ sudo systemctl restart rsyslog


─(ayush㉿ayush)-[~]
─$ nc -v localhost 8080

ocalhost [127.0.0.1] 8080 (http-alt) : Connection refused

─(ayush㉿ayush)-[~]
─$ sudo tail -f /var/log/ufw.log

ail: cannot open '/var/log/ufw.log' for reading: No such file or directory
ail: no files remaining

─(ayush㉿ayush)-[~]
─$ sudo ufw logging high

ogging enabled

─(ayush㉿ayush)-[~]
─$ sudo systemctl restart rsyslog


─(ayush㉿ayush)-[~]
─$ nc -v localhost 8080

ocalhost [127.0.0.1] 8080 (http-alt) : Connection refused
```



```
localhost [127.0.0.1] 8080 (http-alt) : Connection refused

┌──(ayush㉿ayush)-[~]
└─$ sudo tail -f /var/log/ufw.log

tail: cannot open '/var/log/ufw.log' for reading: No such file or directory
tail: no files remaining

┌──(ayush㉿ayush)-[~]
└─$ sudo ufw logging high

Logging enabled

┌──(ayush㉿ayush)-[~]
└─$ sudo systemctl restart rsyslog


┌──(ayush㉿ayush)-[~]
└─$ nc -v localhost 8080

localhost [127.0.0.1] 8080 (http-alt) : Connection refused

┌──(ayush㉿ayush)-[~]
└─$ V
V: command not found

┌──(ayush㉿ayush)-[~]
└─$ telnet localhost 8080

Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(ayush㉿ayush)-[~]
└─$ ls -l /var/log/ufw.log

-rw-r----- 1 root adm 2948 Aug  8 12:54 /var/log/ufw.log
```



```
—$ telnet localhost 8080

rying ::1 ...
onnection failed: Connection refused
rying 127.0.0.1 ...
elnet: Unable to connect to remote host: Connection refused

—(ayush㉿ayush)-[~]
—$ ls -l /var/log/ufw.log

rw-r———— 1 root adm 2948 Aug  8 12:54 /var/log/ufw.log

—(ayush㉿ayush)-[~]
—$ sudo tail -f /var/log/ufw.log

025-08-08T12:54:24.695111+05:30 ayush kernel: [UFW AUDIT] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=40 TOS=0×00 P
EC=0×00 TTL=64 ID=0 DF PROTO=TCP SPT=8080 DPT=34878 WINDOW=0 RES=0×00 ACK RST URGP=0
025-08-08T12:54:24.695112+05:30 ayush kernel: [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
SRC=127.0.0.1 DST=127.0.0.1 LEN=40 TOS=0×00 PREC=0×00 TTL=64 ID=0 DF PROTO=TCP SPT=8080 DPT=34878 WINDOW=0 RES=0×0
 ACK RST URGP=0
025-08-08T12:54:34.286105+05:30 ayush kernel: [UFW AUDIT] IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 D
T=0000:0000:0000:0000:0000:0000:0000:0001 LEN=80 TC=0 HOPLIMIT=64 FLOWLBL=664866 PROTO=TCP SPT=42210 DPT=8080 WIND
W=65476 RES=0×00 SYN URGP=0
025-08-08T12:54:34.286190+05:30 ayush kernel: [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:86:dd
SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=80 TC=0 HOPLIMIT=64 FL
WLBL=664866 PROTO=TCP SPT=42210 DPT=8080 WINDOW=65476 RES=0×00 SYN URGP=0
025-08-08T12:54:34.286193+05:30 ayush kernel: [UFW AUDIT] IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 D
T=0000:0000:0000:0000:0000:0000:0000:0001 LEN=60 TC=0 HOPLIMIT=64 FLOWLBL=138455 PROTO=TCP SPT=8080 DPT=42210 WIND
W=0 RES=0×00 ACK RST URGP=0
025-08-08T12:54:34.286194+05:30 ayush kernel: [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:86:dd
SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=60 TC=0 HOPLIMIT=64 FL
WLBL=138455 PROTO=TCP SPT=8080 DPT=42210 WINDOW=0 RES=0×00 ACK RST URGP=0
025-08-08T12:54:34.286195+05:30 ayush kernel: [UFW AUDIT] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0×00 P
EC=0×00 TTL=64 ID=11810 DF PROTO=TCP SPT=34384 DPT=8080 WINDOW=65495 RES=0×00 SYN URGP=0
025-08-08T12:54:34.286222+05:30 ayush kernel: [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0×00 PREC=0×00 TTL=64 ID=11810 DF PROTO=TCP SPT=34384 DPT=8080 WINDOW=65495
RES=0×00 SYN URGP=0
025-08-08T12:54:34.286223+05:30 ayush kernel: [UFW AUDIT] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=40 TOS=0×00 P
EC=0×00 TTL=64 ID=0 DF PROTO=TCP SPT=8080 DPT=34384 WINDOW=0 RES=0×00 ACK RST URGP=0
025-08-08T12:54:34.286224+05:30 ayush kernel: [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
SRC=127.0.0.1 DST=127.0.0.1 LEN=40 TOS=0×00 PREC=0×00 TTL=64 ID=0 DF PROTO=TCP SPT=8080 DPT=34384 WINDOW=0 RES=0×0
 ACK RST URGP=0
025-08-08T13:01:40.222597+05:30 ayush kernel: [UFW AUDIT] IN=eth0 OUT= MAC=33:33:00:00:00:01:52:56:00:00:00:02:86:
d SRC=fe80:0000:0000:0000:0000:0000:0000:0002 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=96 TC=0 HOPLIMIT=255
FLOWLBL=0 PROTO=ICMPv6 TYPE=134 CODE=0
025-08-08T13:01:40.240836+05:30 ayush kernel: [UFW AUDIT] IN= OUT=eth0 SRC=fe80:0000:0000:0000:0a00:27ff:fe5d:a797
DST=ff02:0000:0000:0000:0000:0000:0000:0016 LEN=96 TC=0 HOPLIMIT=1 FLOWLBL=0 PROTO=ICMPv6 TYPE=143 CODE=0 MARK=0×d

025-08-08T13:01:40.672254+05:30 ayush kernel: [UFW AUDIT] IN= OUT=eth0 SRC=fe80:0000:0000:0000:0a00:27ff:fe5d:a797
DST=ff02:0000:0000:0000:0000:0000:0000:0016 LEN=96 TC=0 HOPLIMIT=1 FLOWLBL=0 PROTO=ICMPv6 TYPE=143 CODE=0 MARK=0×d
```