

Lab 4: Firewall and Log Analysis

Screenshot 1

```
sonal@serversunny:~/lab4$ sudo ufw enable
Firewall is active and enabled on system startup
sonal@serversunny:~/lab4$ sudo ufw status
Status: active
To                         Action      From
--                         ----       ---
22/tcp                      ALLOW      Anywhere
22/tcp (v6)                  ALLOW      Anywhere (v6)

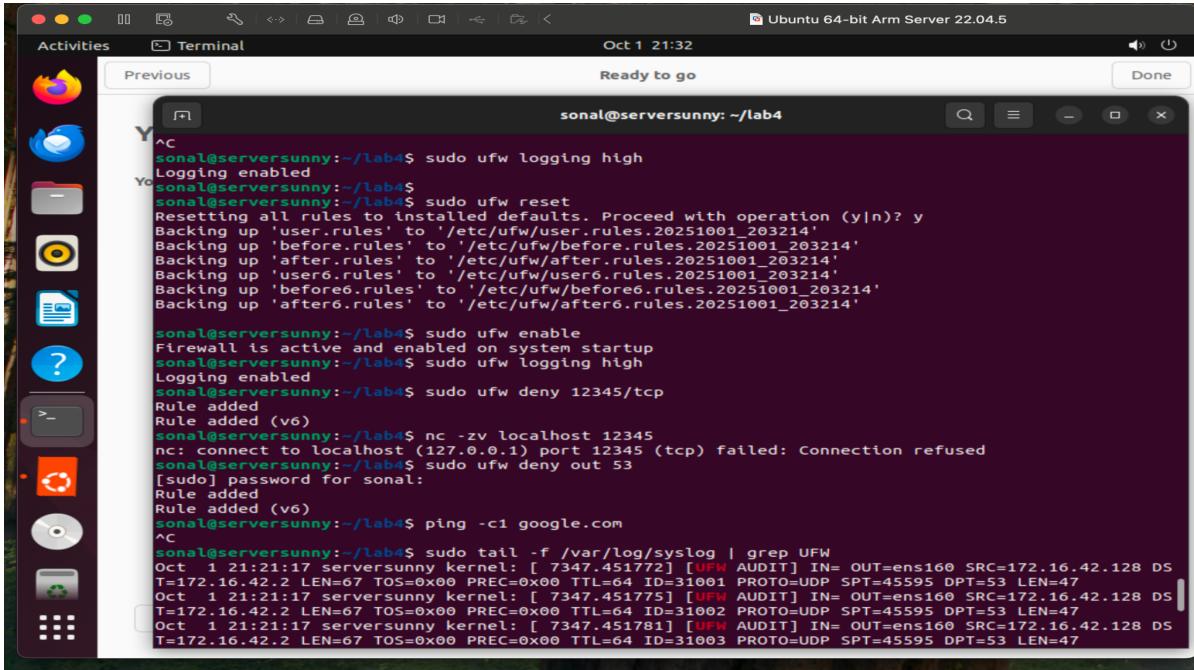
sonal@serversunny:~/lab4$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ----       ---
22/tcp                      ALLOW IN   Anywhere
22/tcp (v6)                  ALLOW IN   Anywhere (v6)

sonal@serversunny:~/lab4$ tail -f /var/log/ufw.log
tail: cannot open '/var/log/ufw.log' for reading: No such file or directory
tail: no files remaining
sonal@serversunny:~/lab4$ sudo ufw logging on
Logging enabled
sonal@serversunny:~/lab4$ tail -f /var/log/ufw.log
tail: cannot open '/var/log/ufw.log' for reading: No such file or directory
tail: no files remaining
sonal@serversunny:~/lab4$ sudo tail -f /var/log/syslog | grep UFW
^X
sudo ufw logging high
```

Here I enabled UFW (firewall) and checked its status. Then I turned on verbose mode and tried viewing log files, but they weren't available at first.

Screenshot 2

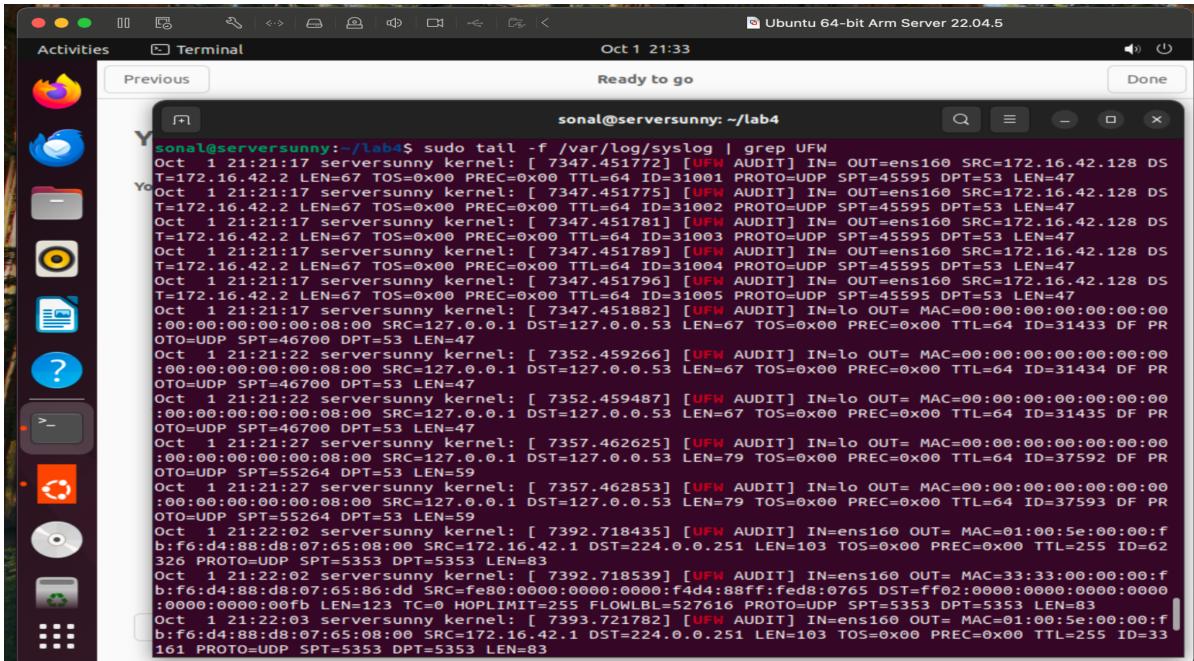


```
sonal@serversunny:~/lab4$ sudo ufw logging high
Logging enabled
sonal@serversunny:~/lab4$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y/n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20251001_203214'
Backing up 'before.rules' to '/etc/ufw/before.rules.20251001_203214'
Backing up 'after.rules' to '/etc/ufw/after.rules.20251001_203214'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20251001_203214'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20251001_203214'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20251001_203214'

sonal@serversunny:~/lab4$ sudo ufw enable
Firewall is active and enabled on system startup
sonal@serversunny:~/lab4$ sudo ufw logging high
Logging enabled
sonal@serversunny:~/lab4$ sudo ufw deny 12345/tcp
Rule added
Rule added (v6)
sonal@serversunny:~/lab4$ nc -zv localhost 12345
nc: connect to localhost (127.0.0.1) port 12345 (tcp) failed: Connection refused
sonal@serversunny:~/lab4$ sudo ufw deny out 53
[sudo] password for sonal:
Rule added
Rule added (v6)
sonal@serversunny:~/lab4$ ping -c1 google.com
^C
sonal@serversunny:~/lab4$ sudo tail -f /var/log/syslog | grep UFW
Oct 1 21:21:17 serversunny kernel: [ 7347.451772] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31001 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451775] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31002 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451781] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31003 PROTO=UDP SPT=45595 DPT=53 LEN=47
```

I reset the firewall, enabled logging, and denied access to port 12345. Then I tested with nc (netcat) and confirmed the connection was refused.

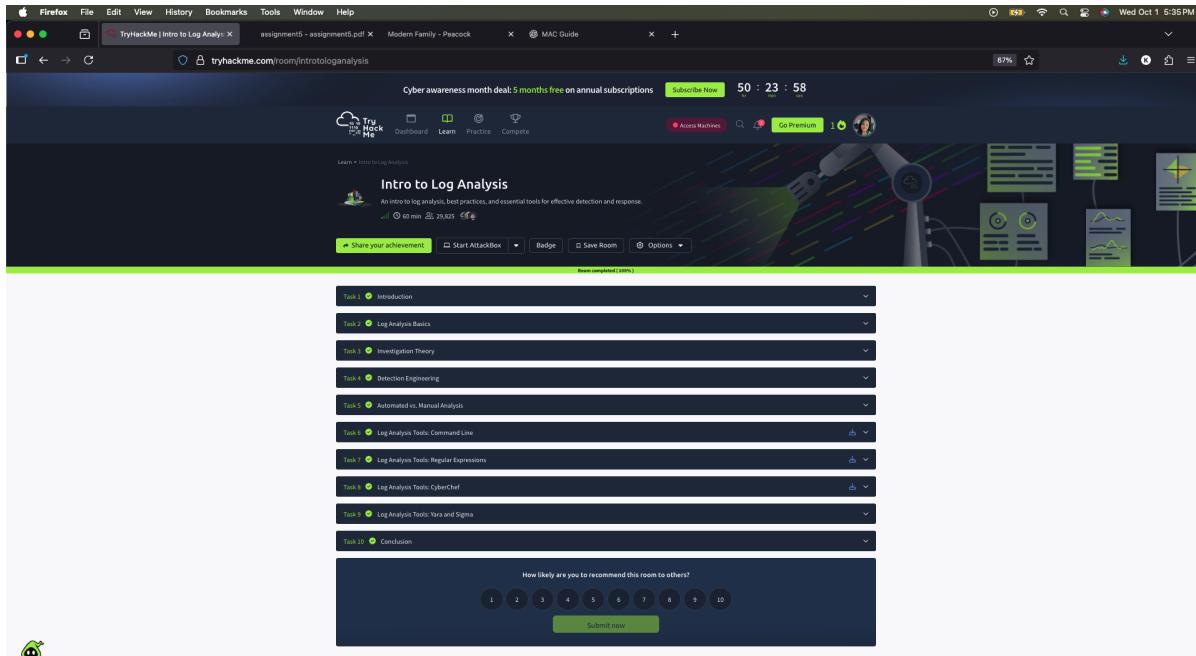
Screenshot 3



```
sonal@serversunny:~/lab4$ sudo tail -f /var/log/syslog | grep UFW
Oct 1 21:21:17 serversunny kernel: [ 7347.451772] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31001 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451775] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31002 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451781] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31003 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451796] [UFW AUDIT] IN= OUT=ens160 SRC=172.16.42.128 DS
T=172.16.42.2 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31005 PROTO=UDP SPT=45595 DPT=53 LEN=47
Oct 1 21:21:17 serversunny kernel: [ 7347.451882] [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00
:00:00:00:00:00 SRC=127.0.0.1 DST=127.0.0.53 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31433 DF PR
OTO=UDP SPT=46700 DPT=53 LEN=47
Oct 1 21:21:22 serversunny kernel: [ 7352.459266] [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00
:00:00:00:00:00 SRC=127.0.0.1 DST=127.0.0.53 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31434 DF PR
OTO=UDP SPT=46700 DPT=53 LEN=47
Oct 1 21:21:22 serversunny kernel: [ 7352.459487] [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00
:00:00:00:00:00 SRC=127.0.0.1 DST=127.0.0.53 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=31435 DF PR
OTO=UDP SPT=46700 DPT=53 LEN=47
Oct 1 21:21:27 serversunny kernel: [ 7357.462625] [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00
:00:00:00:00:00 SRC=127.0.0.1 DST=127.0.0.53 LEN=79 TOS=0x00 PREC=0x00 TTL=64 ID=37592 DF PR
OTO=UDP SPT=55264 DPT=53 LEN=59
Oct 1 21:21:27 serversunny kernel: [ 7357.462853] [UFW AUDIT] IN=lo OUT= MAC=00:00:00:00:00:00:00
:00:00:00:00:00 SRC=127.0.0.1 DST=127.0.0.53 LEN=79 TOS=0x00 PREC=0x00 TTL=64 ID=37593 DF PR
OTO=UDP SPT=55264 DPT=53 LEN=59
Oct 1 21:22:02 serversunny kernel: [ 7392.718435] [UFW AUDIT] IN=ens160 OUT= MAC=01:00:5e:00:00:f
b:f6:d4:88:d8:07:65:08:00 SRC=172.16.42.1 DST=224.0.0.251 LEN=103 TOS=0x00 PREC=0x00 TTL=255 ID=62
326 PROTO=UDP SPT=5353 DPT=5353 LEN=83
Oct 1 21:22:02 serversunny kernel: [ 7392.718539] [UFW AUDIT] IN=ens160 OUT= MAC=33:33:00:00:00:00:f
b:f6:d4:88:d8:07:65:08:00 SRC=fe80::0000:0000:f4d4:88ff:fed8:0765 DST=ff02:0000:0000:0000:0000
:0000:0000:00fb LEN=123 TC=0 HOPLIMIT=255 FLOWLBL=527616 PROTO=UDP SPT=5353 DPT=5353 LEN=83
Oct 1 21:22:03 serversunny kernel: [ 7393.721782] [UFW AUDIT] IN=ens160 OUT= MAC=01:00:5e:00:00:f
b:f6:d4:88:d8:07:65:08:00 SRC=172.16.42.1 DST=224.0.0.251 LEN=103 TOS=0x00 PREC=0x00 TTL=255 ID=33
161 PROTO=UDP SPT=5353 DPT=5353 LEN=83
```

Here I ran a ping test and checked logs with syslog. This showed UFW audit logs capturing blocked traffic, confirming that firewall rules were being enforced.

TryHackMe Log Analysis Completion



I also completed the TryHackMe 'Intro to Log Analysis' module, which covered basics, detection engineering, and log analysis tools.