Detecting and Blocking Unauthorized Access on Linux using Fail2Ban and Splunk

In this project, I demonstrate how to configure Fail2Ban to detect and prevent unauthorized SSH login attempts. The setup includes monitoring logs, configuring Splunk for centralized logging, and simulating brute-force attacks with Hydra.

Steps & Screenshots

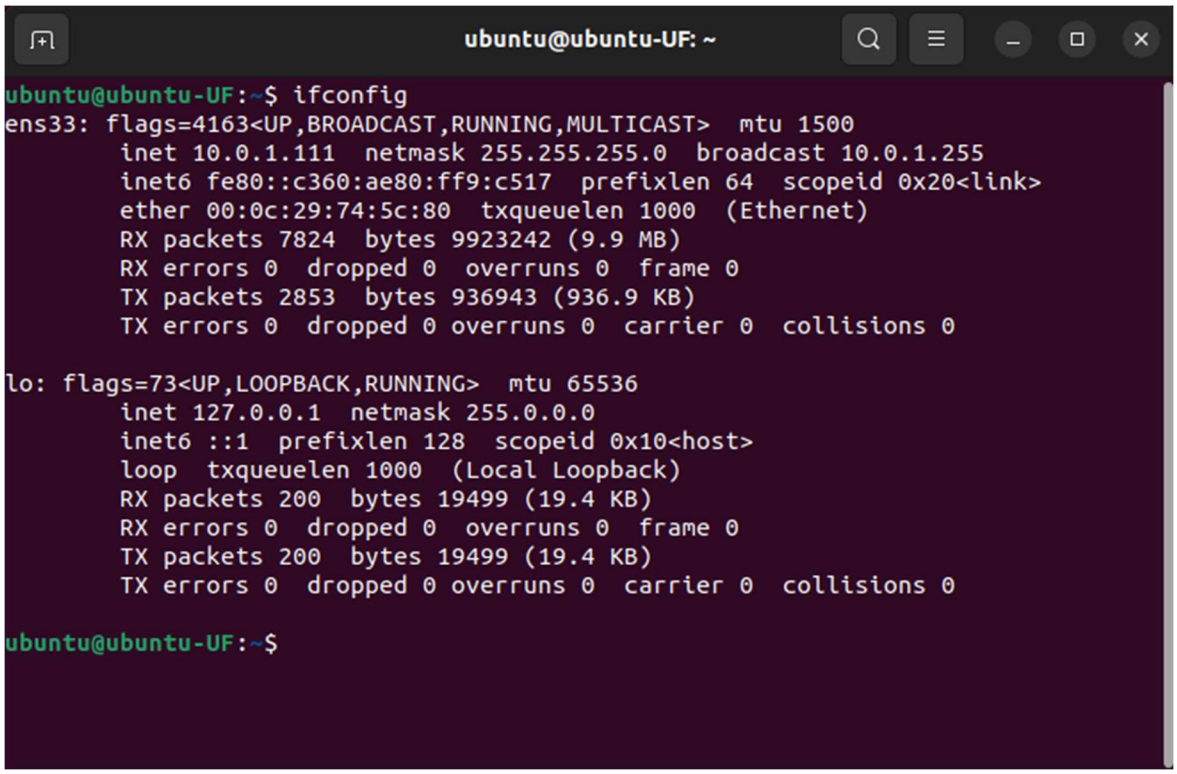


Figure 1Ubuntu IP (Victim PC)

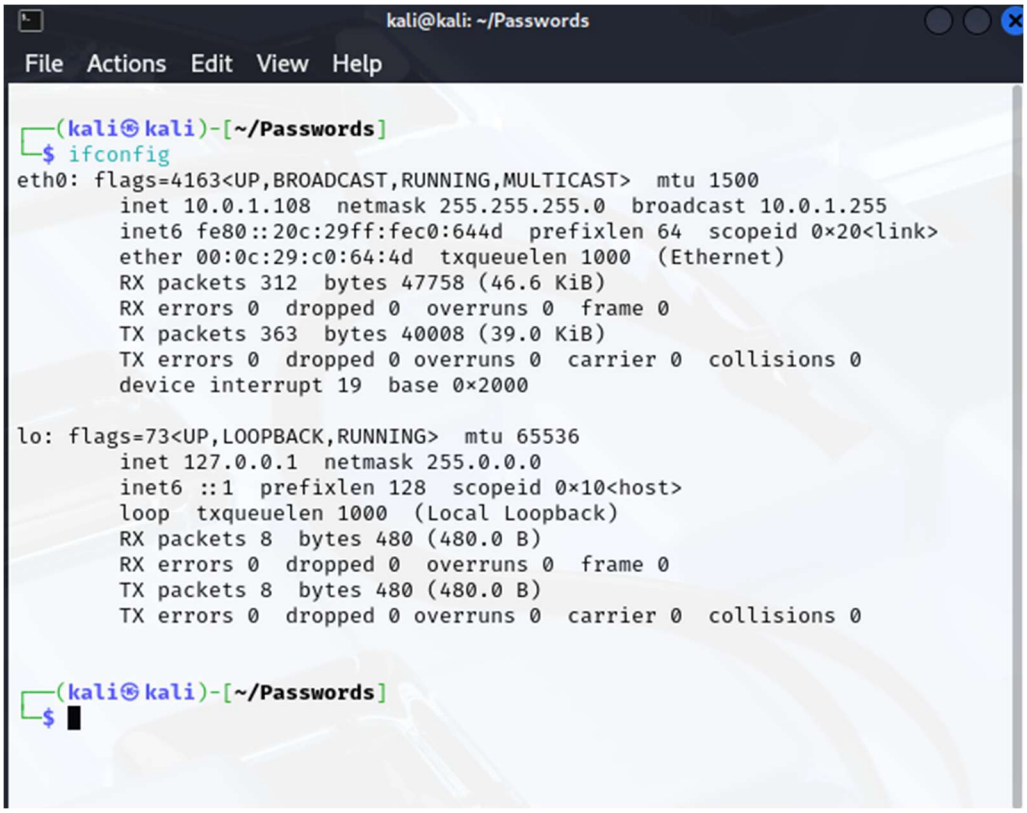


Figure 2 Attacker IP

Step 1: Install Required Tools

- Installed Splunk Universal Forwarder on the victim machine.

- Installed Fail2Ban on the victim machine to monitor unauthorized access.

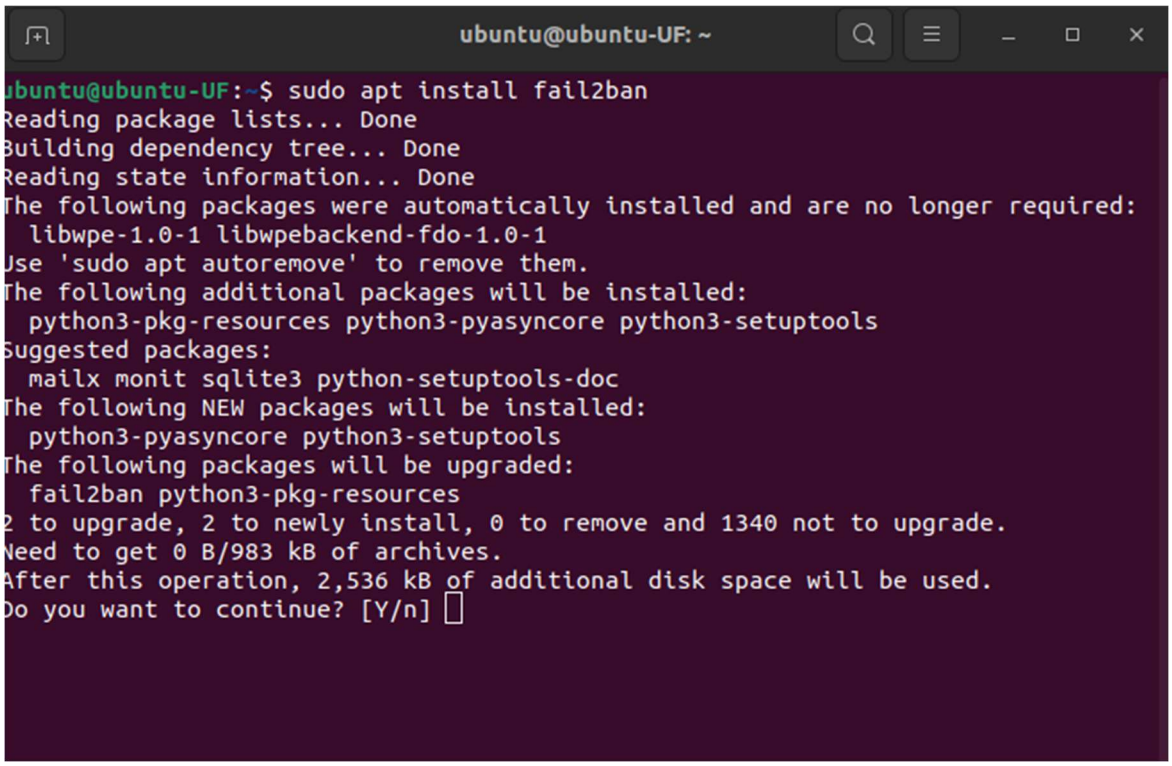


Figure 3 Fail2ban Installation

###Step 2: Install Fail2Ban & Configure

Fail2Ban is an open-source intrusion prevention software that helps protect servers from brute-force attacks, unauthorized access attempts, and suspicious activities by monitoring log files and banning malicious IP addresses. It works by dynamically blocking IP addresses that exhibit malicious behavior using firewall rules.

Configure:

sudo nano /etc/fail2ban/jail.local

Added the following lines to protect the SSH service:

[sshd]

enabled = true

port = ssh

logpath = /var/log/auth.log

maxretry = 3

bantime = 600

findtime = 600

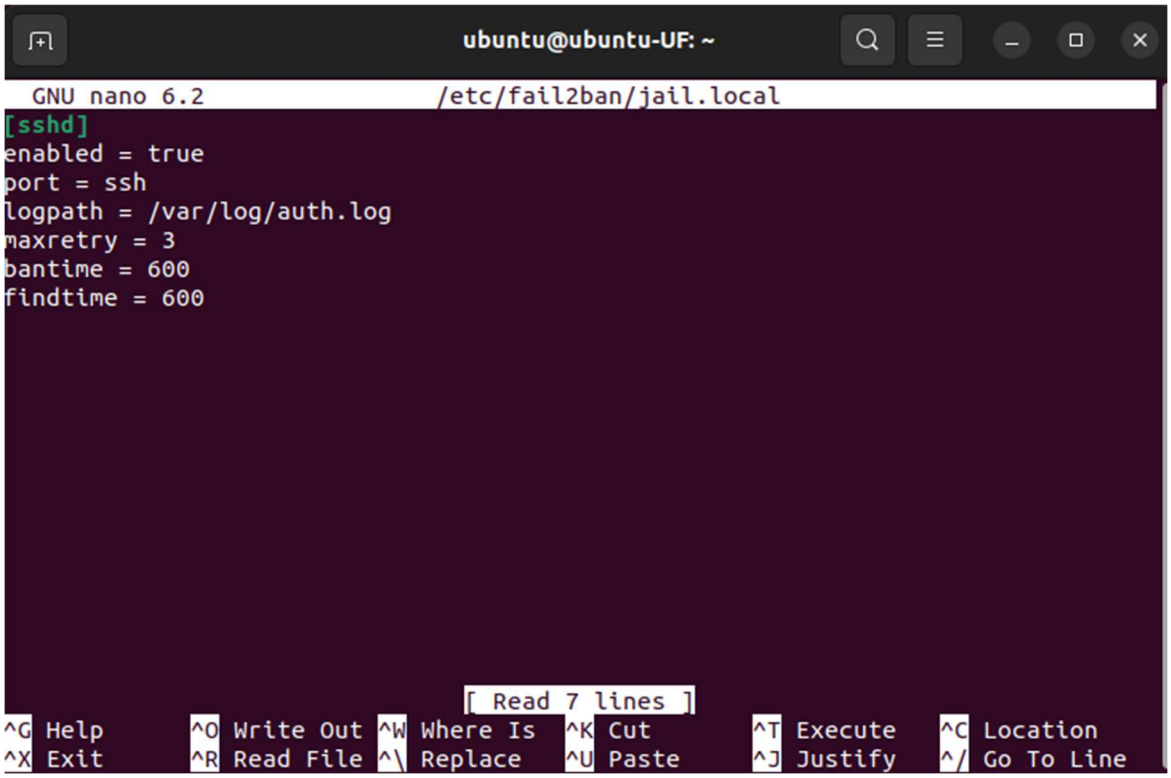


Figure 4 Fail2ban configuration

###Step 3: Created index and sourcetype in Splunk Server Dashboard

Index = fail2ban_logs

Sourcetype = fail2ban

###Step 4: Install hydra on Attack VM

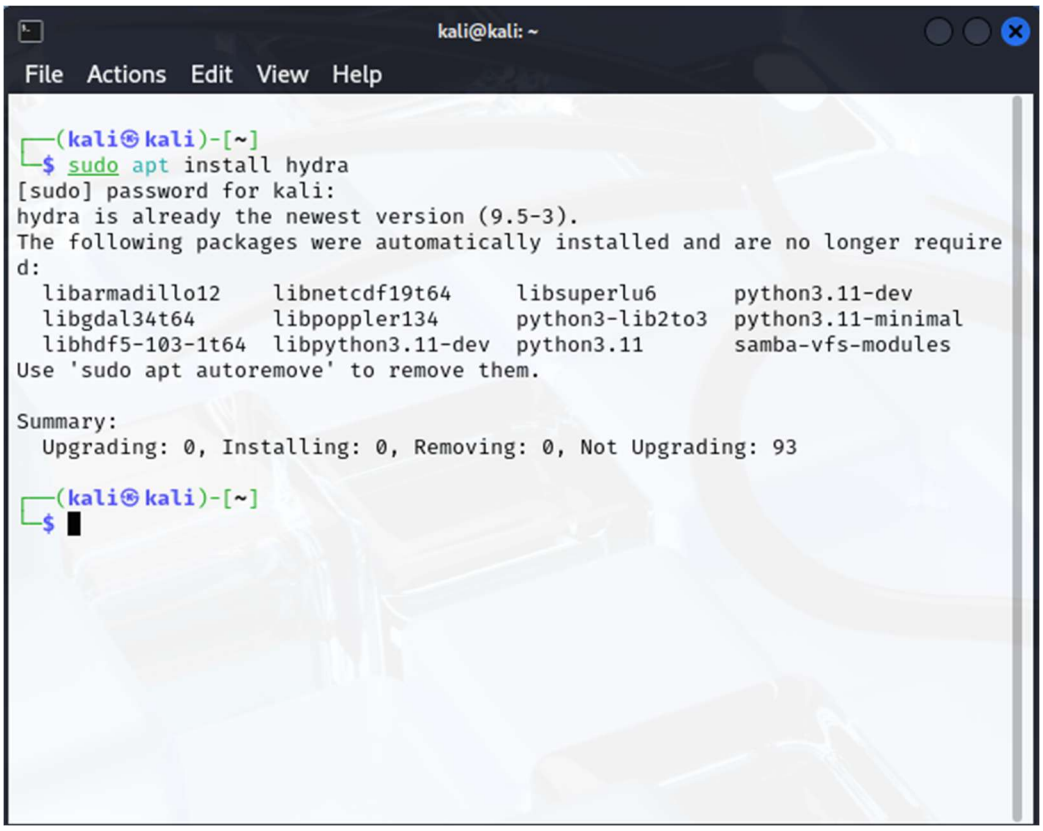


Figure 5 Hydra installation on Attacker PC

###Step 5: Created a dictionary folder as Passwords > passwords.txt

Figure 6 Dictionary List Folder

###Step 6: Perform the brute-force attack

"The following command attempts SSH login to the target machine using a dictionary attack:"

hydra -l admin(username) -P passwords.txt 10.0.1.111(target IP) ssh

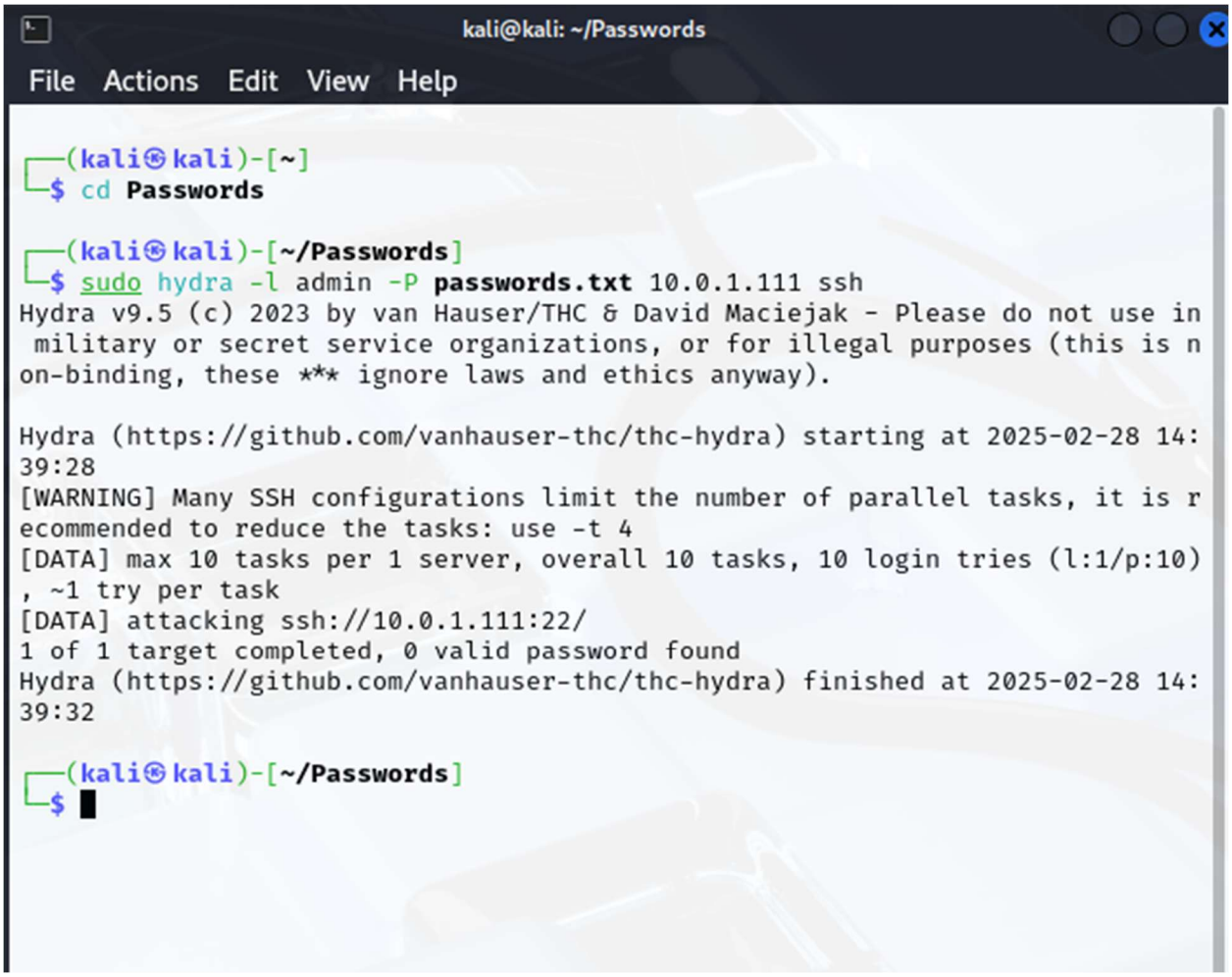


Figure 7 Brute-force simulate

###Step 7: Check the logs on Ubuntu VM (Victim PC)

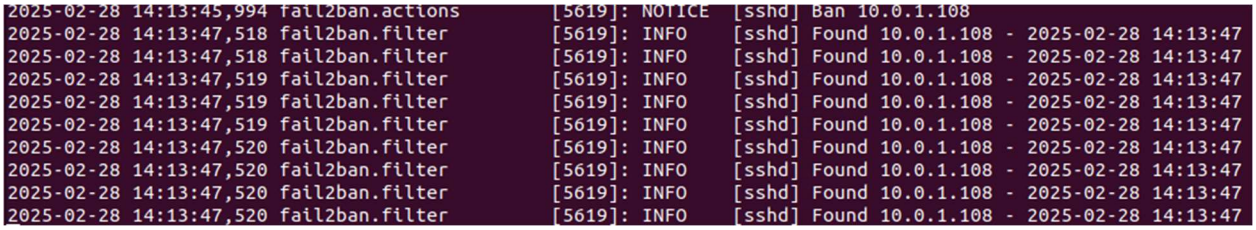
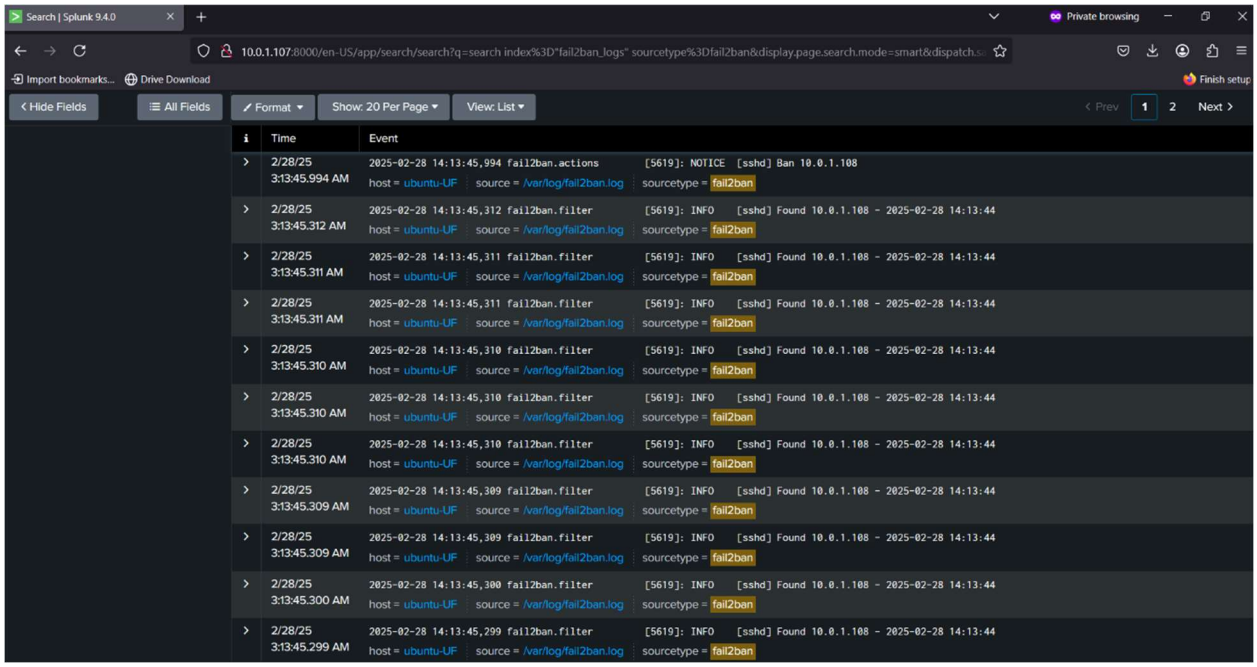


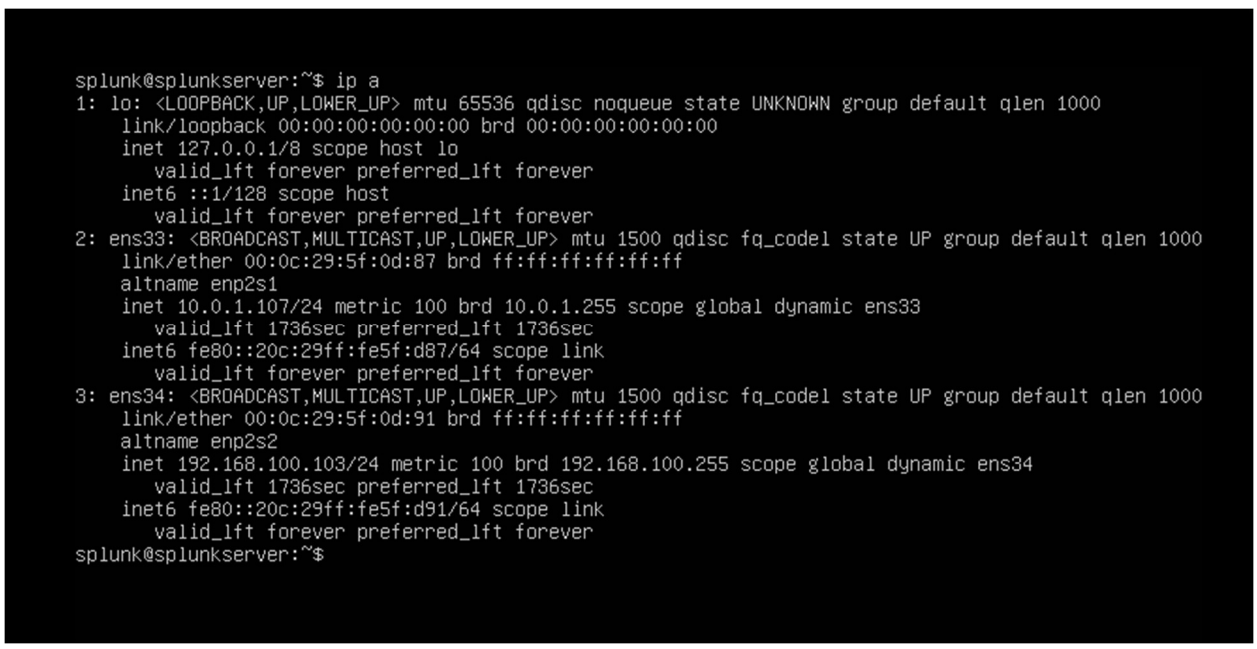
Figure 8 Ban notice logs on ubuntu

###Step 8: Check the logs on Splunk Dashboard



```
i  Time                 Event
>  2/28/25              2025-02-28 14:13:45,994 fail2ban.actions    [5619]: NOTICE  [sshd] Ban 10.0.1.108
   3:13:45.994 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,312 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.312 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,311 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.311 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,311 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.311 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,310 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.310 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,310 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.310 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,310 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.310 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,309 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.309 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,309 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.309 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,300 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.300 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
>  2/28/25              2025-02-28 14:13:45,299 fail2ban.filter     [5619]: INFO    [sshd] Found 10.0.1.108 - 2025-02-28 14:13:44
   3:13:45.299 AM       host = ubuntu-UF  source = /var/log/fail2ban.log  sourcetype = fail2ban
```

Figure 9 Ban logs on Splunk Server



```
splunk@splunkserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:0d:87 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.1.107/24 metric 100 brd 10.0.1.255 scope global dynamic ens33
       valid_lft 1736sec preferred_lft 1736sec
    inet6 fe80::20c:29ff:fe5f:d87/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:0d:91 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 192.168.100.103/24 metric 100 brd 192.168.100.255 scope global dynamic ens34
       valid_lft 1736sec preferred_lft 1736sec
    inet6 fe80::20c:29ff:fe5f:d91/64 scope link
       valid_lft forever preferred_lft forever
splunk@splunkserver:~$
```

Figure 10 Splunk Server IP

Conclusion:

This project successfully implemented Fail2Ban to detect and prevent brute-force attacks on an Ubuntu system. The logs were analyzed in Splunk, confirming that the attacker IP was automatically banned after multiple failed login attempts.