Ubuntu Security Lab Project Documentation

Objective:

- Simulate attacks (nmap scan, brute-force SSH attack) using Hydra and Nmap tools.
- Monitor and defend against attacks using Fail2Ban.
- Practice Blue Team skills: log inspection, detection, and automated banning.

Lab Environment:

- **Victim Machine:** Ubuntu VM (Static IP: 192.168.56.10)
- **Attacker Machine:** Cloned Ubuntu VM (Static IP: 192.168.56.20)
- Both VMs configured on an internal NAT network for isolated testing.

Steps Completed:

1. Environment Setup:

- Installed Ubuntu on both VMs.
- Configured static IP addresses via `/etc/netplan/01-network-manager-all.yaml`.
- Verified connectivity using ping.

Screenshot:

- P3 Pinged attacker and target machine to verify connectivity

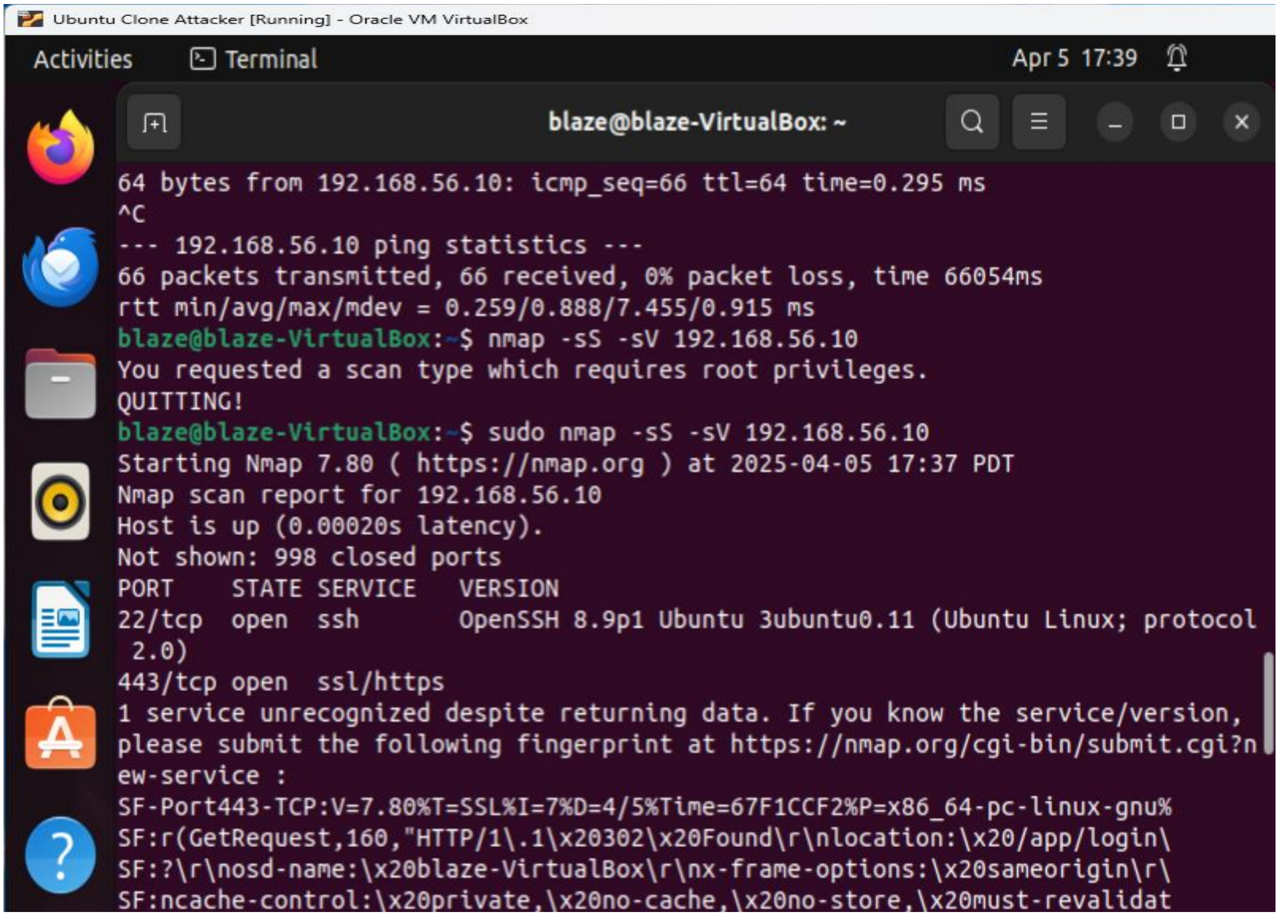
2. Reconnaissance Using Nmap:

- Performed a SYN scan (`nmap -sS`) and service version detection scan (`nmap -sV`) from attacker to victim.

- Identified open ports (22/SSH and 443/HTTPS).

Screenshot:

- P3 nmap scan of victims systems



Ubuntu Clone Attacker [Running] - Oracle VM VirtualBox
Activities
Terminal
Apr 5 17:39
blaze@blaze-VirtualBox: ~

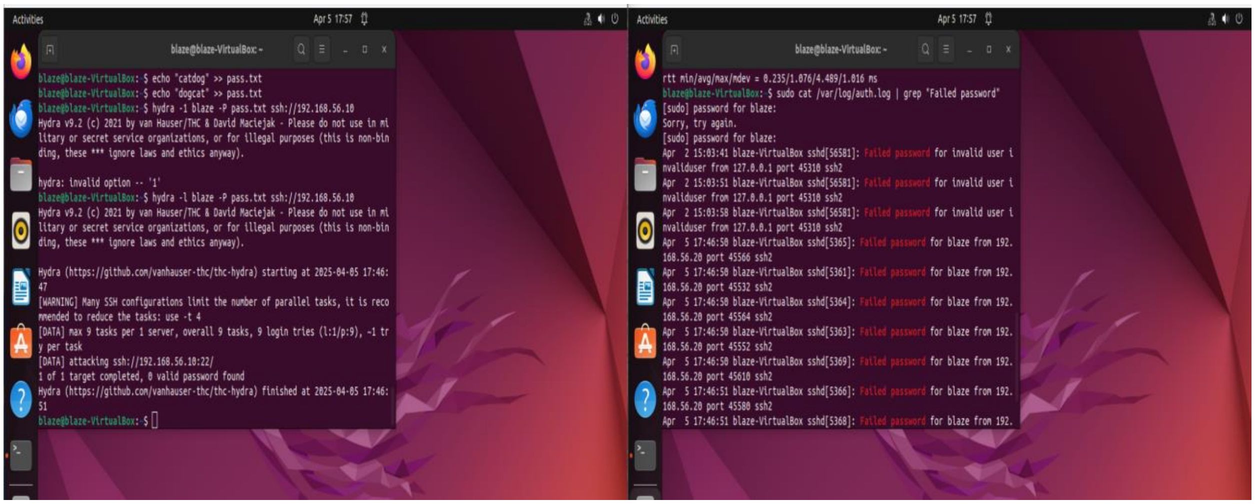
```
64 bytes from 192.168.56.10: icmp_seq=66 ttl=64 time=0.295 ms
^C
--- 192.168.56.10 ping statistics ---
66 packets transmitted, 66 received, 0% packet loss, time 66054ms
rtt min/avg/max/mdev = 0.259/0.888/7.455/0.915 ms
blaze@blaze-VirtualBox:~$ nmap -sS -sV 192.168.56.10
You requested a scan type which requires root privileges.
QUITTING!
blaze@blaze-VirtualBox:~$ sudo nmap -sS -sV 192.168.56.10
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 17:37 PDT
Nmap scan report for 192.168.56.10
Host is up (0.00020s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh       OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux; protocol
 2.0)
443/tcp open  ssl/https
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=4/5%Time=67F1CCF2%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,160,"HTTP/1\.1\x20302\x20Found\r\nlocation:\x20/app/login\
SF:?\r\nosd-name:\x20blaze-VirtualBox\r\nx-frame-options:\x20sameorigin\r\
SF:ncache-control:\x20private,\x20no-cache,\x20no-store,\x20must-revalidat
```

3. Attack Using Hydra (SSH Password Guessing):

- Created simple user and password files (`user.txt`, `pass.txt`).
- Ran Hydra SSH brute force attack against the victim.
- Observed multiple failed login attempts recorded in `/var/log/auth.log` on the victim.

Screenshot:

- Utilizing hydra (password guessing)



```
blaze@blaze-VirtualBox:~$ echo "catdog" >> pass.txt
blaze@blaze-VirtualBox:~$ echo "dogcat" >> pass.txt
blaze@blaze-VirtualBox:~$ hydra -1 blaze -P pass.txt ssh://192.168.56.10
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

hydra: invalid option -- '1'
blaze@blaze-VirtualBox:~$ hydra -l blaze -P pass.txt ssh://192.168.56.10
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-05 17:46:
47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 tr
y per task
[DATA] attacking ssh://192.168.56.10:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-05 17:46:
51
blaze@blaze-VirtualBox:~$
```

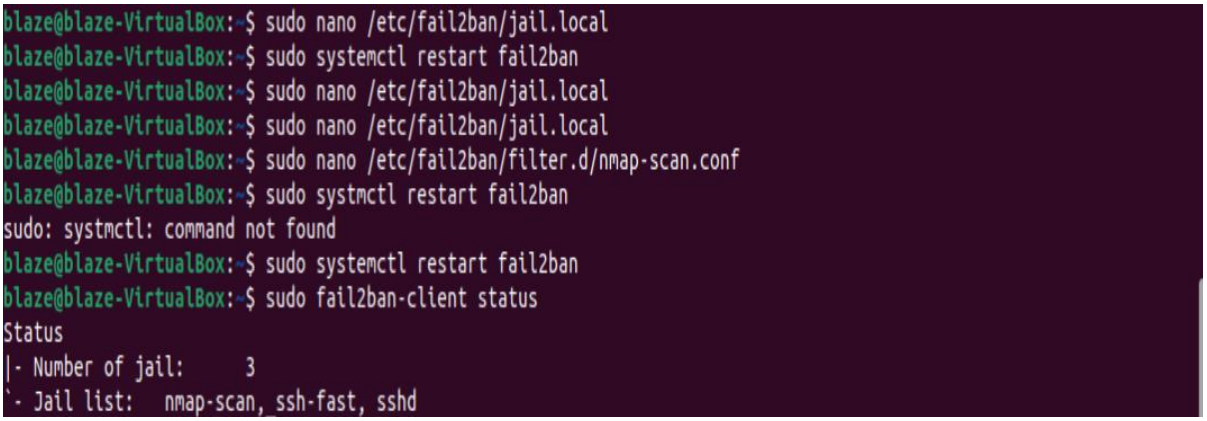
```
rtt min/avg/max/mdev = 0.235/1.076/4.489/1.016 ms
blaze@blaze-VirtualBox:~$ sudo cat /var/log/auth.log | grep "Failed password"
[sudo] password for blaze:
Sorry, try again.
[sudo] password for blaze:
Apr  2 15:03:41 blaze-VirtualBox sshd[56581]: Failed password for invalid user i
nvaliduser from 127.0.0.1 port 45310 ssh2
Apr  2 15:03:51 blaze-VirtualBox sshd[56581]: Failed password for invalid user i
nvaliduser from 127.0.0.1 port 45310 ssh2
Apr  2 15:03:58 blaze-VirtualBox sshd[56581]: Failed password for invalid user i
nvaliduser from 127.0.0.1 port 45310 ssh2
Apr  5 17:46:50 blaze-VirtualBox sshd[5365]: Failed password for blaze from 192.
168.56.20 port 45566 ssh2
Apr  5 17:46:50 blaze-VirtualBox sshd[5361]: Failed password for blaze from 192.
168.56.20 port 45532 ssh2
Apr  5 17:46:50 blaze-VirtualBox sshd[5364]: Failed password for blaze from 192.
168.56.20 port 45564 ssh2
Apr  5 17:46:50 blaze-VirtualBox sshd[5363]: Failed password for blaze from 192.
168.56.20 port 45552 ssh2
Apr  5 17:46:50 blaze-VirtualBox sshd[5369]: Failed password for blaze from 192.
168.56.20 port 45610 ssh2
Apr  5 17:46:51 blaze-VirtualBox sshd[5366]: Failed password for blaze from 192.
168.56.20 port 45580 ssh2
Apr  5 17:46:51 blaze-VirtualBox sshd[5368]: Failed password for blaze from 192.
```

4. Defense with Fail2Ban:

- Installed and configured Fail2Ban on the victim machine.
- Customized `/etc/fail2ban/jail.local` to:
  - Monitor SSH brute force attacks with default sshd jail.
  - Added a custom "ssh-fast" jail (lower thresholds).
  - Created a "nmap-scan" jail (attempted to detect nmap scans).
- Verified that jails were loaded and active.

Screenshot:

- Verifying fail2ban jail lists



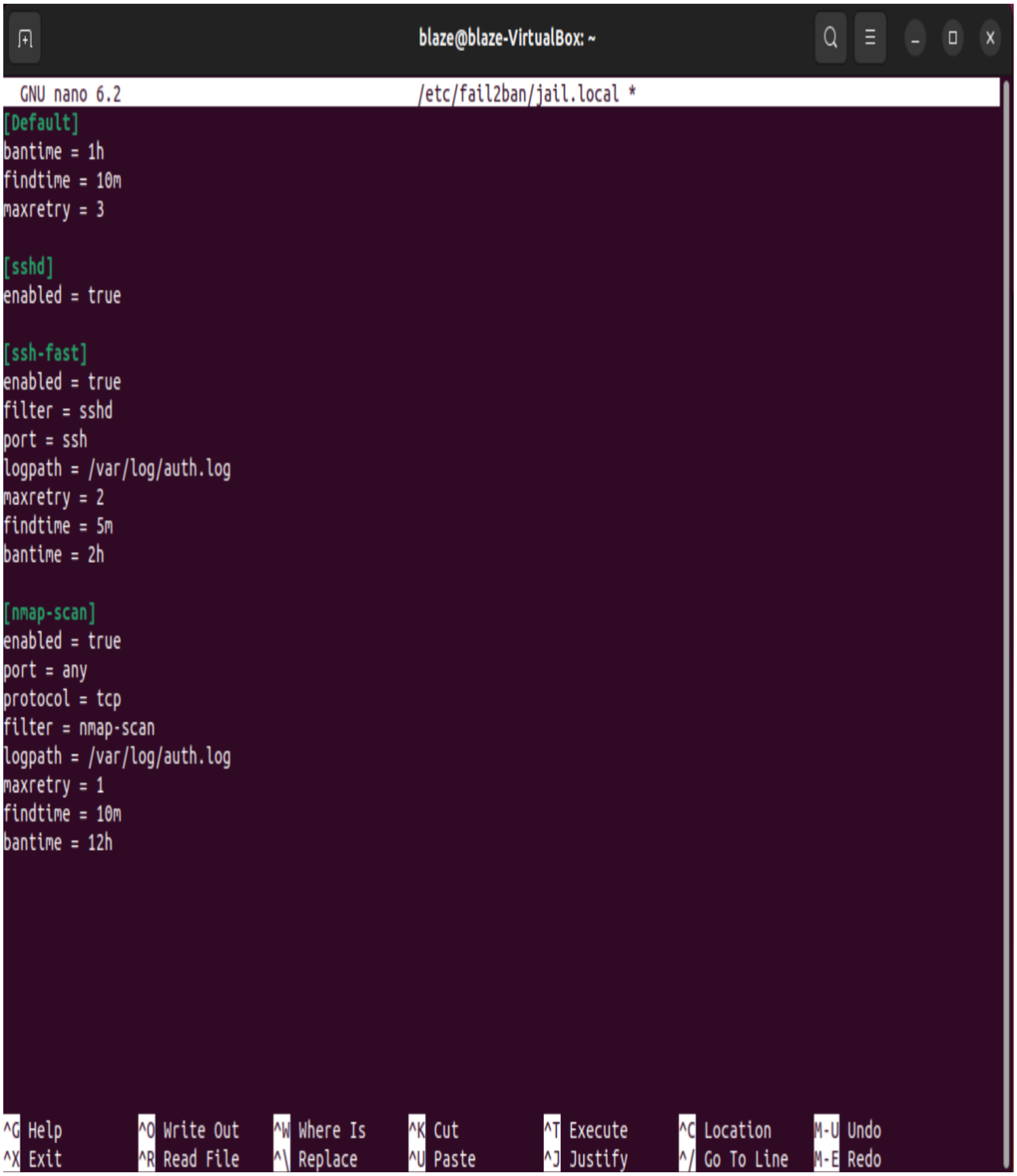
```
blaze@blaze-VirtualBox:~$ sudo nano /etc/fail2ban/jail.local
blaze@blaze-VirtualBox:~$ sudo systemctl restart fail2ban
blaze@blaze-VirtualBox:~$ sudo nano /etc/fail2ban/jail.local
blaze@blaze-VirtualBox:~$ sudo nano /etc/fail2ban/jail.local
blaze@blaze-VirtualBox:~$ sudo nano /etc/fail2ban/filter.d/nmap-scan.conf
blaze@blaze-VirtualBox:~$ sudo systmctl restart fail2ban
sudo: systmctl: command not found
blaze@blaze-VirtualBox:~$ sudo systemctl restart fail2ban
blaze@blaze-VirtualBox:~$ sudo fail2ban-client status
Status
|- Number of jail:      3
`- Jail list:   nmap-scan, ssh-fast, sshd
```

5. Adjusted Fail2Ban Sensitivity:

- Tuned `findtime`, `bantime`, and `maxretry` settings to quickly block brute-force attempts.
- Attempted brute-force after configuration to test sensitivity.

Screenshot:

- Editing fail2ban rules



```
  GNU nano 6.2                    /etc/fail2ban/jail.local *
[Default]
bantime = 1h
findtime = 10m
maxretry = 3

[sshd]
enabled = true

[ssh-fast]
enabled = true
filter = sshd
port = ssh
logpath = /var/log/auth.log
maxretry = 2
findtime = 5m
bantime = 2h

[nmap-scan]
enabled = true
port = any
protocol = tcp
filter = nmap-scan
logpath = /var/log/auth.log
maxretry = 1
findtime = 10m
bantime = 12h
```

Challenges Faced:

- Encountered issues with Fail2Ban custom jail for nmap scan detection.
- Troubleshooted log paths and jail configurations but nmap detection was not successful.
- Despite this, successful brute-force attempts were logged, and SSH bans were enforced.

Key Skills Practiced:

- Linux networking and static IP assignment.
- Using Nmap and Hydra for basic attack simulation.
- Log file analysis in `/var/log/auth.log`.
- Fail2Ban configuration and custom jail creation.
- Basic Blue Team defensive setup on Linux.

Potential Next Steps (Future Improvements):

- Refine custom filters for better detection of port scans.
- Implement other Fail2Ban filters (e.g., apache-auth, vsftpd).
- Set up email notifications for bans.
- Expand into Wazuh integration for enterprise-level monitoring.

End of Project Documentation