



SSH Brute-Force Attack Simulation and Mitigation Lab

Environment: Kali Linux (attacker), Ubuntu Server (target), VirtualBox

Overview:

SSH brute-force attacks are a common tactic used by attackers to gain unauthorized access to systems. Organizations risk major data breaches and system compromise if these attacks go unnoticed. This lab replicates a real-world scenario and demonstrates how to proactively defend against such threats. It was executed within a self-built virtual home lab environment consisting of Kali Linux (attacker) and Ubuntu (defender) virtual machines connected via a host-only network.

Project Objective:

To understand and simulate brute-force attack methods and to implement and validate SSH defense mechanisms using log monitoring, alerting, and banning unauthorized access attempts.

Implementation Steps:

Phase 1: Virtual Lab Setup

- Installed VirtualBox and created two VMs:
 - **Ubuntu VM:** Target machine
 - **Kali Linux VM:** Attacking machine
- Configured both on a private Host-Only network to simulate an isolated environment.
- Verified IP connectivity between the machines using ping.

Phase 2: Brute Force Attack Simulation

- Installed and enabled the OpenSSH server on Ubuntu.
- Created a user (testuser) with a known weak password.
- From Kali Linux, ran the following Hydra command:
`hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://<Ubuntu_IP>`
- Successfully cracked the SSH password using brute force.
- Observed authentication logs on Ubuntu using:
`sudo grep 'Failed password' /var/log/auth.log`

Phase 3: Defense - Fail2Ban Configuration

- Installed Fail2Ban on Ubuntu:

```
sudo apt install fail2ban
```

- Created and edited /etc/fail2ban/jail.local:
[sshd]
enabled = true
port = ssh
logpath = /var/log/auth.log
maxretry = 5
bantime = 3600
findtime = 600
- Restarted Fail2Ban:
sudo systemctl restart fail2ban
- Simulated multiple failed login attempts from Kali.
- Confirmed IP banning via:
sudo fail2ban-client status sshd

Evidence of Completion:

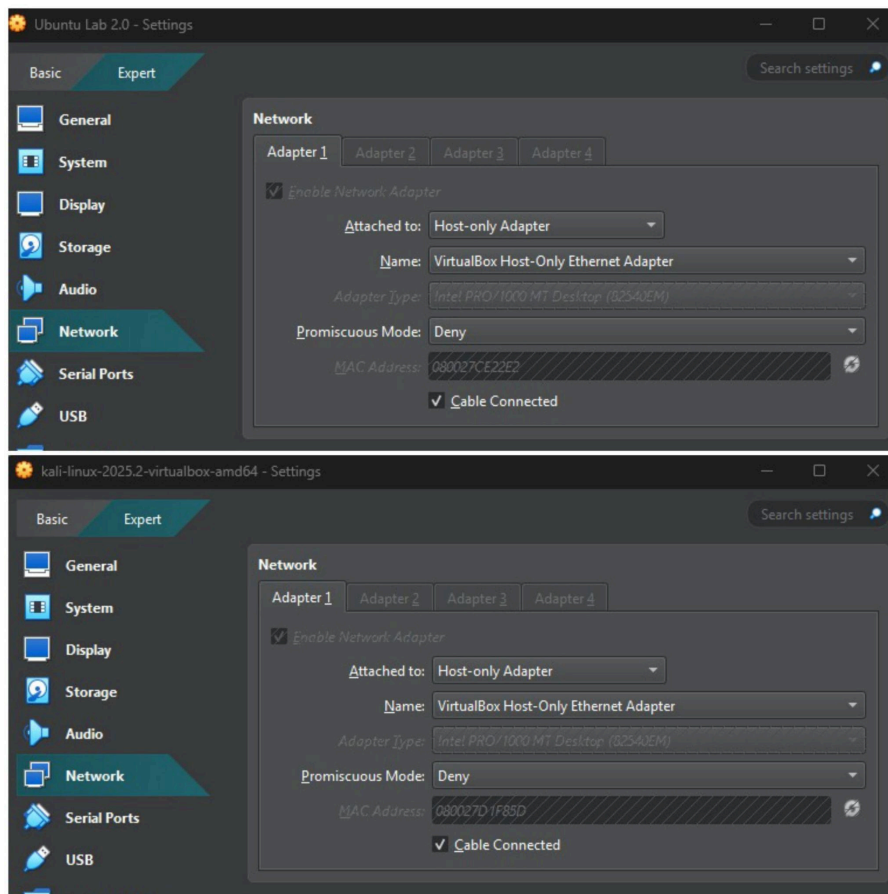


Image: Configured VirtualBox Host-Only Adapter (vboxnet0) for isolated lab environment.

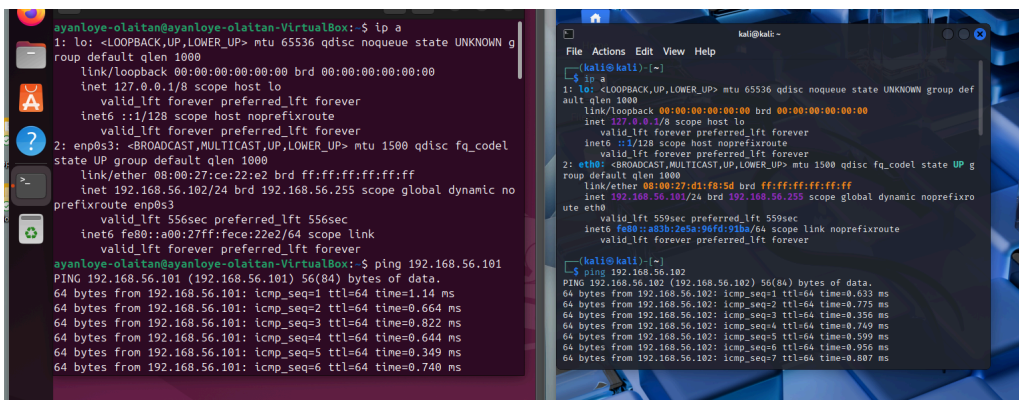


Image: Confirmed network connectivity between attacker and target machines.

```
testuser@ayanloye-olaitan-VirtualBox: ~  
File Actions Edit View Help  
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz  
[sudo] password for kali:  
  
(kali@kali)-[~]  
└─$ [200-hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103  
zsh: bad pattern: "[200-hydra  
  
(kali@kali)-[~]  
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se  
cret service organizations, or for illegal purposes (this is non-binding, these ** ignore l  
aws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-31 07:38:27  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r  
educe the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~  
896525 tries per task  
[DATA] attacking ssh://192.168.56.103:22/  
[STATUS] 195.00 tries/min, 195 tries in 00:01h, 14344204 to do in 1226:01h, 16 active  
[STATUS] 225.00 tries/min, 675 tries in 00:03h, 14343724 to do in 1062:30h, 16 active  
[22][ssh] host: 192.168.56.103 login: testuser password: password123  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-31 07:44:37  
  
(kali@kali)-[~]  
└─$ ssh testuser@192.168.56.103  
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.  
ED25519 key fingerprint is SHA256:aHvuNNYnKxYGkr7YD+XF1cCSP6soMc1M3weX6gmotSk.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.  
testuser@192.168.56.103's password:  
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-27-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
142 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
Last login: Thu Jul 31 12:24:27 2025 from 127.0.0.1  
testuser@ayanloye-olaitan-VirtualBox:~$
```

Image: Hydra brute force attack successfully cracked SSH credentials.

```
1 port 36874 ssh2  
2025-07-31T12:44:29.698450+01:00 ayanloye-olaitan-VirtualBox sshd[5436]: Failed password for testuser from 192.168.56.10  
1 port 36764 ssh2  
2025-07-31T12:44:29.706067+01:00 ayanloye-olaitan-VirtualBox sshd[5450]: Failed password for testuser from 192.168.56.10  
1 port 36844 ssh2  
2025-07-31T12:44:29.707727+01:00 ayanloye-olaitan-VirtualBox sshd[5456]: Failed password for testuser from 192.168.56.10  
1 port 36888 ssh2  
2025-07-31T12:44:29.709142+01:00 ayanloye-olaitan-VirtualBox sshd[5457]: Failed password for testuser from 192.168.56.10  
1 port 36902 ssh2  
2025-07-31T12:44:29.813754+01:00 ayanloye-olaitan-VirtualBox sshd[5432]: Failed password for testuser from 192.168.56.10  
1 port 41582 ssh2  
2025-07-31T12:44:29.954482+01:00 ayanloye-olaitan-VirtualBox sshd[5452]: Failed password for testuser from 192.168.56.10  
1 port 36852 ssh2  
2025-07-31T12:44:30.109538+01:00 ayanloye-olaitan-VirtualBox sshd[5438]: Failed password for testuser from 192.168.56.10  
1 port 36774 ssh2  
2025-07-31T12:44:30.243796+01:00 ayanloye-olaitan-VirtualBox sshd[5434]: Failed password for testuser from 192.168.56.10  
1 port 41588 ssh2  
2025-07-31T12:44:30.268441+01:00 ayanloye-olaitan-VirtualBox sshd[5460]: Failed password for testuser from 192.168.56.10  
1 port 36918 ssh2  
2025-07-31T12:44:30.357036+01:00 ayanloye-olaitan-VirtualBox sshd[5462]: Failed password for testuser from 192.168.56.10  
1 port 36930 ssh2  
2025-07-31T12:44:30.408165+01:00 ayanloye-olaitan-VirtualBox sshd[5444]: Failed password for testuser from 192.168.56.10  
1 port 36816 ssh2  
2025-07-31T12:44:30.538765+01:00 ayanloye-olaitan-VirtualBox sshd[5446]: Failed password for testuser from 192.168.56.10  
1 port 36826 ssh2  
2025-07-31T12:44:32.179271+01:00 ayanloye-olaitan-VirtualBox sshd[5442]: Failed password for testuser from 192.168.56.10  
1 port 36792 ssh2  
2025-07-31T12:44:32.181096+01:00 ayanloye-olaitan-VirtualBox sshd[5440]: Failed password for testuser from 192.168.56.10  
1 port 36788 ssh2  
2025-07-31T12:44:32.566655+01:00 ayanloye-olaitan-VirtualBox sshd[5448]: Failed password for testuser from 192.168.56.10  
1 port 36840 ssh2  
2025-07-31T12:44:32.689981+01:00 ayanloye-olaitan-VirtualBox sshd[5454]: Failed password for testuser from 192.168.56.10  
1 port 36774 ssh2
```

Image: Authentication logs on Ubuntu showing failed SSH login attempts from Kali.

```
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
# port = ssh
# filter = sshd
# logpath = /var/log/auth.log
```

[Read 986 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line

Image: Fail2Ban configuration to detect and ban brute force SSH attempts.

```
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| '- File list: /var/log/auth.log
'- Actions
  |- Currently banned: 1
  |- Total banned: 2
  '- Banned IP list: 192.168.56.101
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target prot opt source destination multiport dports 22
f2b-sshd 6 -- 0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain f2b-sshd (1 references)
target prot opt source destination reject-with icmp-port-unreachable
REJECT 0 -- 192.168.56.101 0.0.0.0/0
RETURN 0 -- 0.0.0.0/0 0.0.0.0/0
```

Image: Fail2Ban successfully detected intrusion and banned the attacker's IP address.


Skills Demonstrated:

- Cybersecurity attack and defense methodologies
- Log analysis and monitoring
- Virtual environment setup
- SSH configuration
- Network troubleshooting
- Linux system administration

Key Takeaways:

- Learned how brute-force SSH attacks are executed and how vulnerable systems can be exploited.
- Gained hands-on experience mitigating such attacks using Fail2Ban.
- Understood the value of log monitoring and proactive intrusion prevention in cybersecurity.

Project Status:

-  Completed — Includes setup, attack simulation, incident detection, and automated defense implementation.

Next Steps:

- Expand blue team tools to include UFW.
- Simulate other types of attacks (port scanning, dictionary attacks on other services).
- Deploy similar defensive mechanisms for web applications or FTP.

Appendix: Full Command Reference Table

Command	Explanation	System
ping <Ubuntu_IP>	Check network connectivity from Kali to Ubuntu	Kali
hydra -l testuser -P /usr/share/wordlists/rocky u.txt ssh://<Ubuntu_IP>	Brute-force SSH using known password list	Kali
ip a	Verify Kali IP address for ban confirmation	Kali
sudo apt update && sudo apt install hydra	Install Hydra tool	Kali

<code>sudo apt update && sudo apt install openssh-server</code>	Install OpenSSH server on Ubuntu	Ubuntu
<code>sudo systemctl enable ssh && sudo systemctl start ssh</code>	Enable and start SSH service	Ubuntu
<code>sudo adduser testuser</code>	Create test user for attack simulation	Ubuntu
<code>sudo grep 'Failed password' /var/log/auth.log</code>	View failed login attempts	Ubuntu
<code>sudo tail -f /var/log/auth.log</code>	Live monitor login attempts	Ubuntu
<code>sudo apt install fail2ban</code>	Install Fail2Ban to monitor and ban IPs	Ubuntu
<code>sudo nano /etc/fail2ban/jail.local</code>	Create/edit Fail2Ban jail config	Ubuntu
<code>sudo systemctl restart fail2ban</code>	Apply Fail2Ban config changes	Ubuntu
<code>sudo fail2ban-client status sshd</code>	View Fail2Ban status for SSH	Ubuntu
<code>sudo fail2ban-client status</code>	View overall Fail2Ban jail summary	Ubuntu
<code>sudo fail2ban-client set sshd unbanip <Kali_IP></code>	Unban Kali IP for retesting	Ubuntu
<code>sudo iptables -L</code>	View IP ban rules via iptables	Ubuntu
<code>sudo cat /var/log/fail2ban.log</code>	View Fail2Ban's activity log	Ubuntu