💻 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:

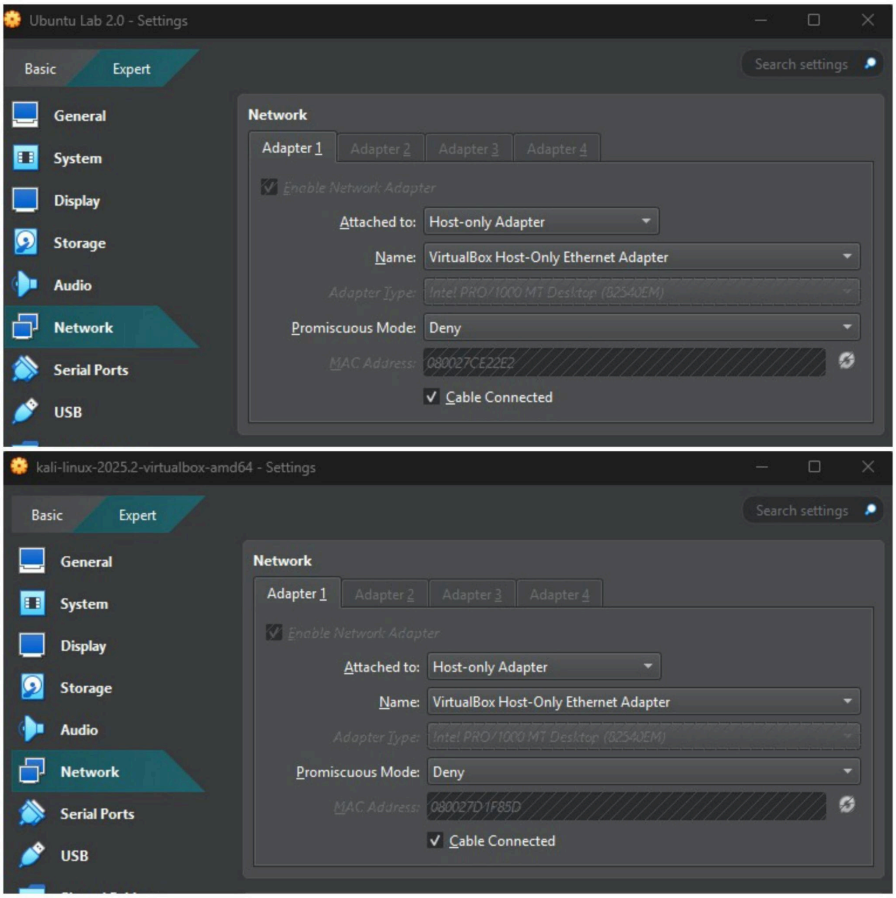
- 

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

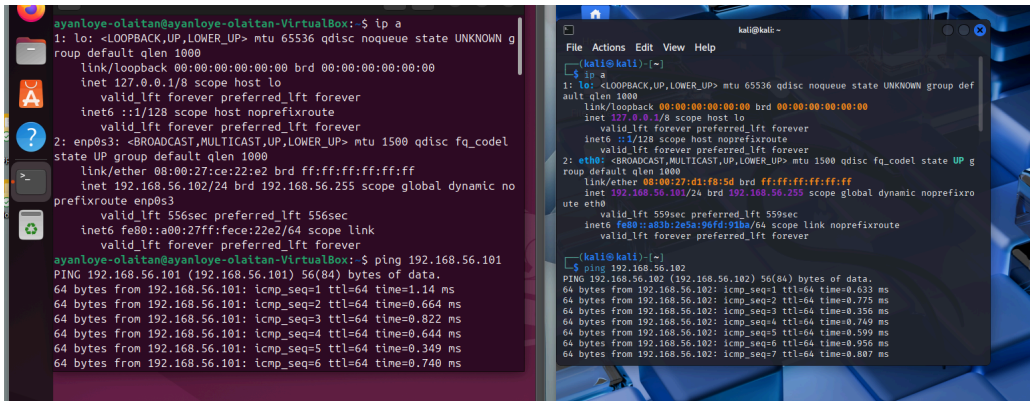
- 

  Image: Confirmed network connectivity between attacker and target machines.

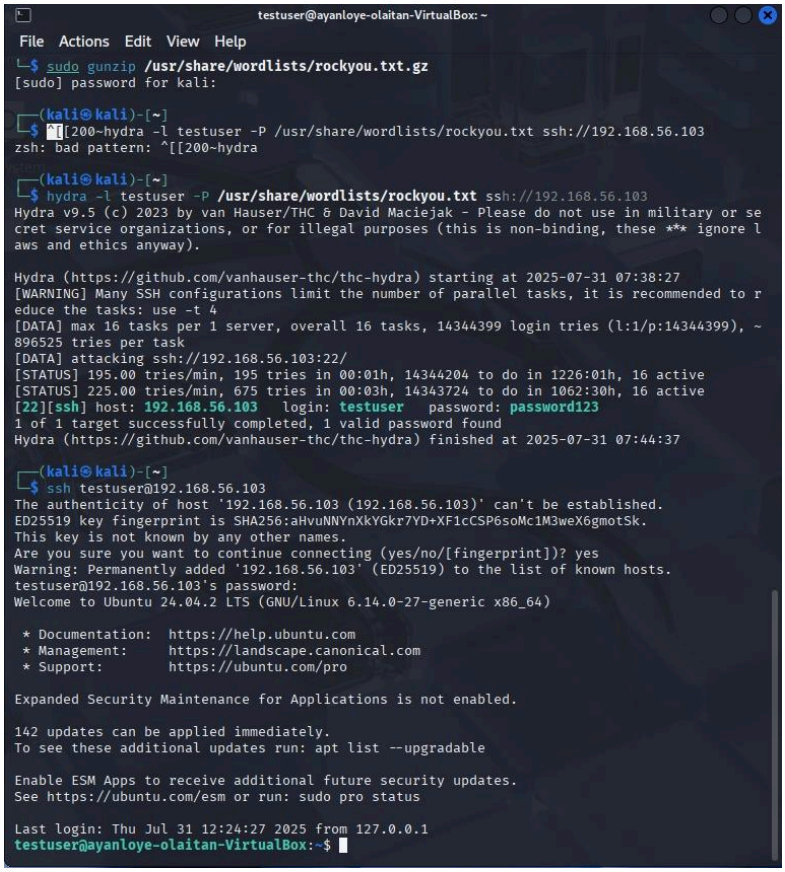
- 

Image: Hydra brute force attack successfully cracked SSH credentials.

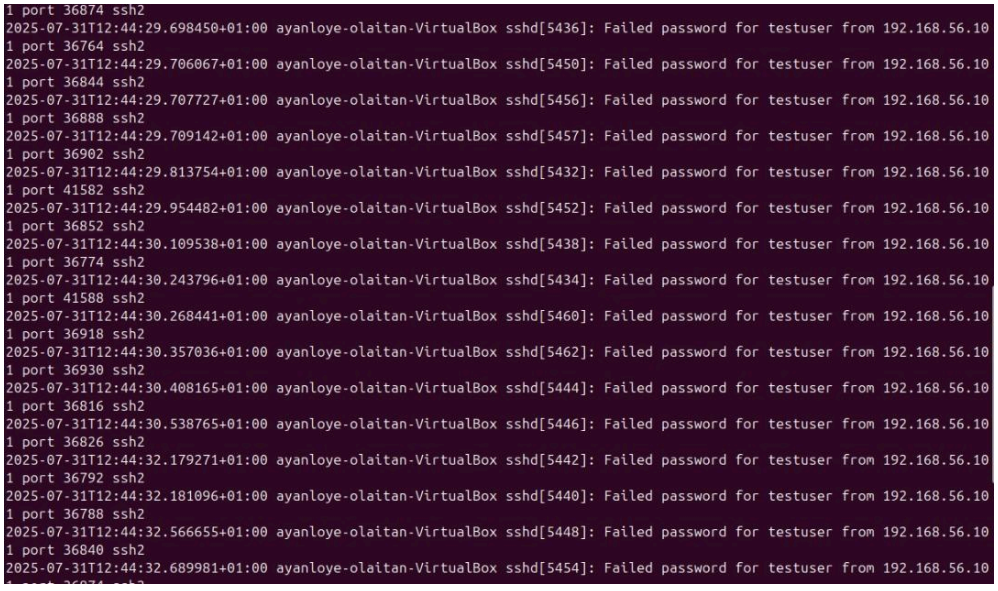
- 

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

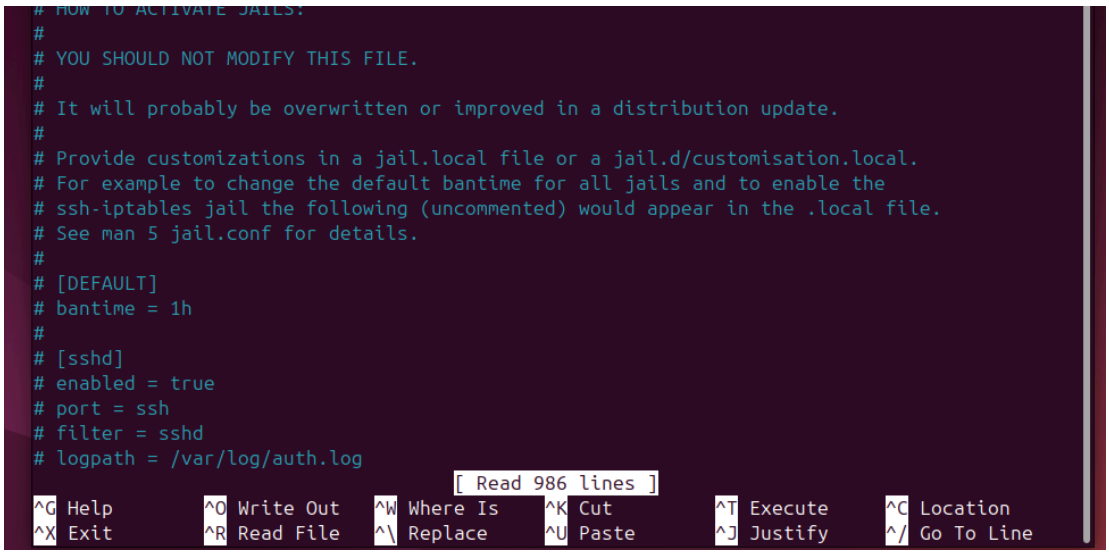
- 

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

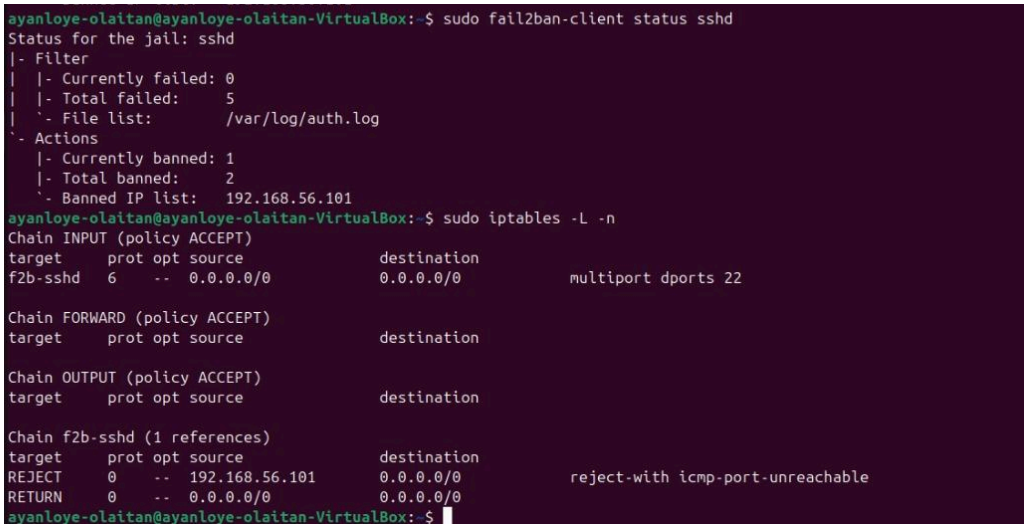
- 

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/rockyou.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

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