# 🛡️ SSH Firewall Hardening and Logging with UFW in a Virtual Home Lab

**Overview:**
This case study demonstrates firewall-level SSH brute-force mitigation using UFW (Uncomplicated Firewall) and Linux log auditing. The goal was to monitor, detect, and respond to unauthorized SSH access attempts through proper UFW configuration and analysis of system logs.

**Project Objective**:
To simulate brute-force SSH attacks and configure a firewall (UFW) on Ubuntu to detect, block, and log unauthorized connection attempts, demonstrating basic blue team defensive strategies and network access control.

**Tools & Technologies Used:**

- VirtualBox
- Ubuntu Server (Defender)
- Kali Linux (Attacker)
- Hydra (SSH brute-force tool)
- OpenSSH
- UFW (Uncomplicated Firewall)
- Linux logging tools

## Implementation Steps:

### Phase 1: Virtual Lab Preparation

- Ubuntu and Kali Linux VMs already connected via a Host-Only Adapter.
- Verified IP communication using ping <Ubuntu_IP> from Kali.

### Phase 2: UFW Setup and SSH Hardening

- Enabled UFW on Ubuntu:
  ```
  sudo ufw enable
  ```

- Allowed SSH connections explicitly:
  ```
  sudo ufw allow ssh
  ```

- Verified firewall status:
  ```
  sudo ufw status verbose
  ```

- Ensured logging was set to a suitable level:

*sudo ufw logging on*
*sudo ufw status verbose*

## Phase 3: SSH Brute-Force Attack Simulation

- Ran brute force attack from Kali:
  *hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://<Ubuntu_IP>*

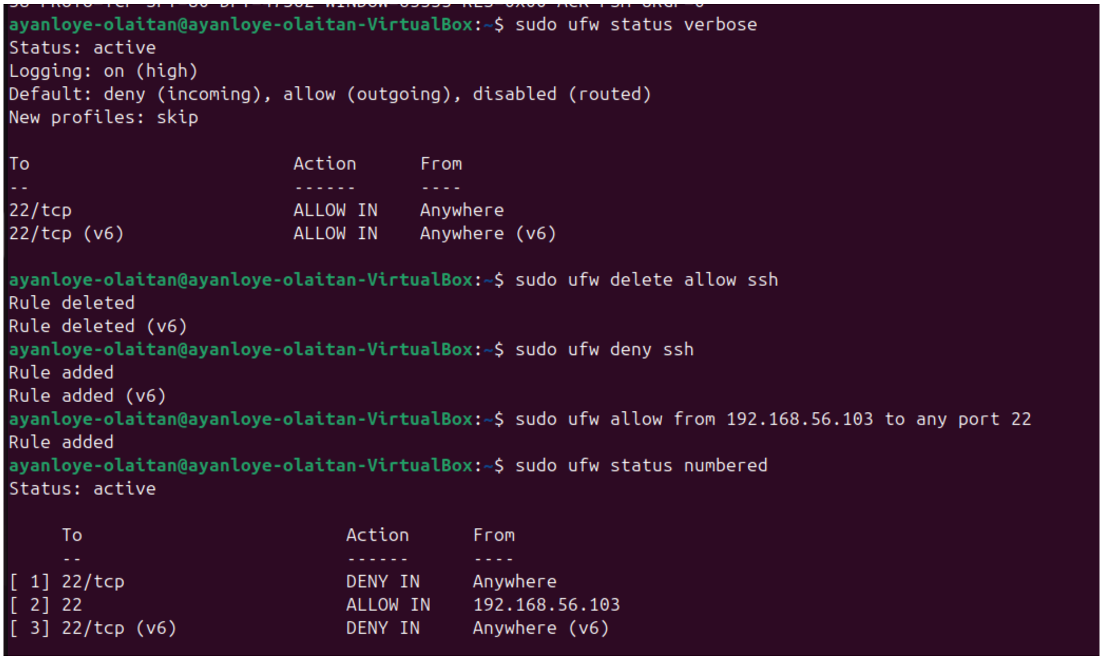
- Observed repeated connection attempts and failure logs.

## Phase 4: Firewall and Logging Verification

- Verified that UFW logs were generated:
  *sudo tail -f /var/log/ufw.log*

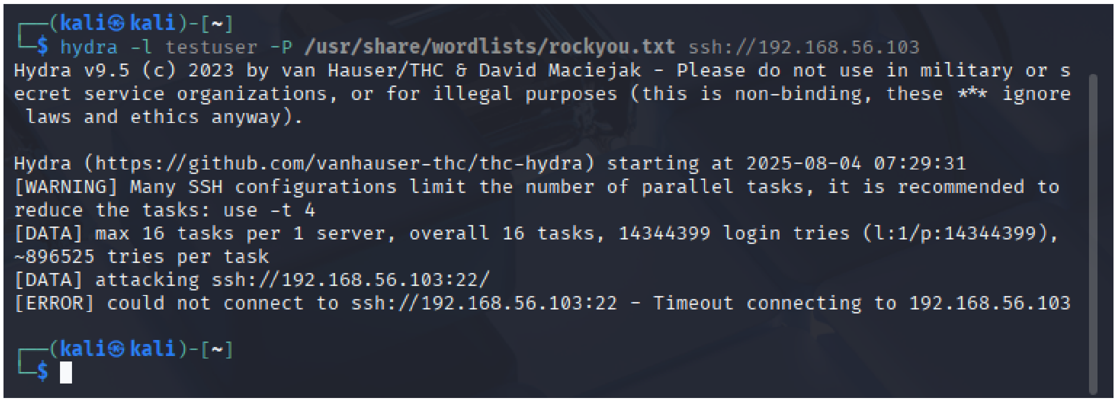
- Observed audit entries involving SSH connection attempts.
- Noted that while UFW logged the attempts, it did not automatically block brute-force IPs.

## Evidence of Completion:

- 

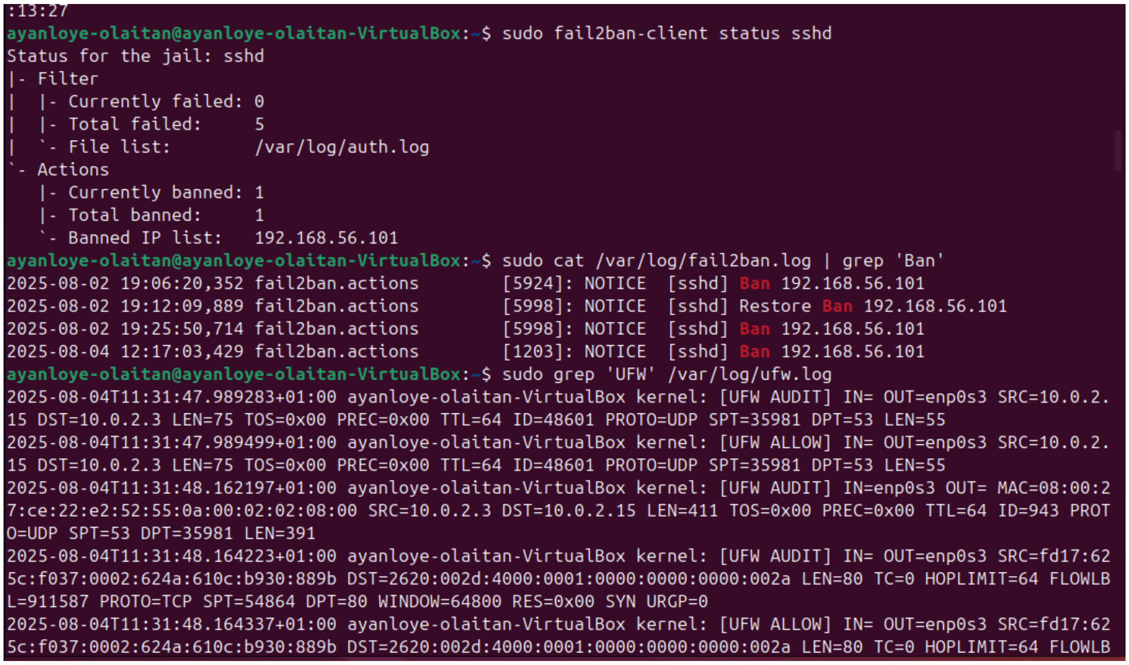
```
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo ufw status verbose
Status: active
Logging: on (high)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

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

ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo ufw delete allow ssh
Rule deleted
Rule deleted (v6)
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo ufw deny ssh
Rule added
Rule added (v6)
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo ufw allow from 192.168.56.103 to any port 22
Rule added
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     DENY IN     Anywhere
[ 2] 22                         ALLOW IN    192.168.56.103
[ 3] 22/tcp (v6)                DENY IN     Anywhere (v6)
```

  **Image:** UFW status and rules

- 

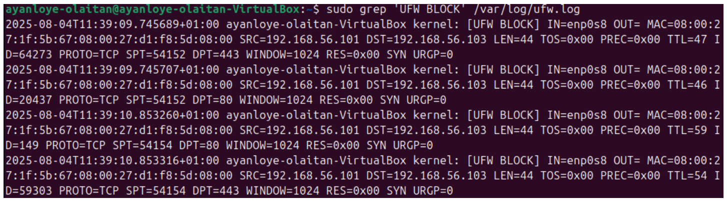
```
┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
ecret service organizations, or for illegal purposes (this is non-binding, these *** ignore
 laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-04 07:29:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce 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/
[ERROR] could not connect to ssh://192.168.56.103:22 - Timeout connecting to 192.168.56.103

┌──(kali㉿kali)-[~]
└─$ 
```

**Image:** Brute-force attempt from Kali using Hydra

- 

```
:13:27
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:     1
   `- Banned IP list:   192.168.56.101
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo cat /var/log/fail2ban.log | grep 'Ban'
2025-08-02 19:06:20,352 fail2ban.actions        [5924]: NOTICE  [sshd] Ban 192.168.56.101
2025-08-02 19:12:09,889 fail2ban.actions        [5998]: NOTICE  [sshd] Restore Ban 192.168.56.101
2025-08-02 19:25:50,714 fail2ban.actions        [5998]: NOTICE  [sshd] Ban 192.168.56.101
2025-08-04 12:17:03,429 fail2ban.actions        [1203]: NOTICE  [sshd] Ban 192.168.56.101
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo grep 'UFW' /var/log/ufw.log
2025-08-04T11:31:47.989283+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW AUDIT] IN= OUT=enp0s3 SRC=10.0.2.
15 DST=10.0.2.3 LEN=75 TOS=0x00 PREC=0x00 TTL=64 ID=48601 PROTO=UDP SPT=35981 DPT=53 LEN=55
2025-08-04T11:31:47.989499+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW ALLOW] IN= OUT=enp0s3 SRC=10.0.2.
15 DST=10.0.2.3 LEN=75 TOS=0x00 PREC=0x00 TTL=64 ID=48601 PROTO=UDP SPT=35981 DPT=53 LEN=55
2025-08-04T11:31:48.162197+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW AUDIT] IN=enp0s3 OUT= MAC=08:00:2
7:ce:22:e2:52:55:0a:00:02:02:08:00 SRC=10.0.2.3 DST=10.0.2.15 LEN=411 TOS=0x00 PREC=0x00 TTL=64 ID=943 PROT
O=UDP SPT=53 DPT=35981 LEN=391
2025-08-04T11:31:48.164223+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW AUDIT] IN= OUT=enp0s3 SRC=fd17:62
5c:f037:0002:624a:610c:b930:889b DST=2620:002d:4000:0001:0000:0000:0000:002a LEN=80 TC=0 HOPLIMIT=64 FLOWLB
L=911587 PROTO=TCP SPT=54864 DPT=80 WINDOW=64800 RES=0x00 SYN URGP=0
2025-08-04T11:31:48.164337+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW ALLOW] IN= OUT=enp0s3 SRC=fd17:62
5c:f037:0002:624a:610c:b930:889b DST=2620:002d:4000:0001:0000:0000:0000:002a LEN=80 TC=0 HOPLIMIT=64 FLOWLB
```

**Image:** /var/log/ufw.log entries showing audit and access logs

- 

```
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo grep 'UFW BLOCK' /var/log/ufw.log
2025-08-04T11:39:09.745689+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW BLOCK] IN=enp0s8 OUT= MAC=08:00:2
7:1f:5b:67:08:00:27:d1:f8:5d:08:00 SRC=192.168.56.101 DST=192.168.56.103 LEN=44 TOS=0x00 PREC=0x00 TTL=47 I
D=64273 PROTO=TCP SPT=54152 DPT=443 WINDOW=1024 RES=0x00 SYN URGP=0
2025-08-04T11:39:09.745707+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW BLOCK] IN=enp0s8 OUT= MAC=08:00:2
7:1f:5b:67:08:00:27:d1:f8:5d:08:00 SRC=192.168.56.101 DST=192.168.56.103 LEN=44 TOS=0x00 PREC=0x00 TTL=46 I
D=20437 PROTO=TCP SPT=54152 DPT=80 WINDOW=1024 RES=0x00 SYN URGP=0
2025-08-04T11:39:10.853260+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW BLOCK] IN=enp0s8 OUT= MAC=08:00:2
7:1f:5b:67:08:00:27:d1:f8:5d:08:00 SRC=192.168.56.101 DST=192.168.56.103 LEN=44 TOS=0x00 PREC=0x00 TTL=59 I
D=149 PROTO=TCP SPT=54154 DPT=80 WINDOW=1024 RES=0x00 SYN URGP=0
2025-08-04T11:39:10.853316+01:00 ayanloye-olaitan-VirtualBox kernel: [UFW BLOCK] IN=enp0s8 OUT= MAC=08:00:2
7:1f:5b:67:08:00:27:d1:f8:5d:08:00 SRC=192.168.56.101 DST=192.168.56.103 LEN=44 TOS=0x00 PREC=0x00 TTL=54 I
D=59303 PROTO=TCP SPT=54154 DPT=443 WINDOW=1024 RES=0x00 SYN URGP=0
```

**Image:** IP being blocked or dropped by firewall

## Skills Demonstrated:

- Linux firewall configuration (UFW)
- SSH service protection strategies
- System log analysis and monitoring
- Network access control
- Practical understanding of brute-force detection

## Key Takeaways:

- Host-based firewalls are essential for controlling access but may not respond dynamically to threats.
- UFW can audit connection attempts, but integration with tools like Fail2Ban is needed for automated IP blocking.
- System logs are critical for visibility into network behavior and potential malicious activity.

## Project Status:

- ✅ **Completed** — Virtual lab, firewall configuration, brute-force simulation, and log analysis successfully conducted.

## Next Steps:

- Integrate UFW with Fail2Ban for layered defense.
- Simulate firewall-based responses to port scans.

## Appendix: Key Command Reference

| **Command** | **Explanation** | **System** |
|---|---|---|
| sudo ufw enable | Enables the UFW firewall | Ubuntu |
| sudo ufw allow ssh | Allows incoming SSH traffic | Ubuntu |
| sudo ufw status verbose | Shows current firewall rules | Ubuntu |
| sudo ufw logging on | Enables logging for UFW | Ubuntu |
| sudo tail -f /var/log/ufw.log | Live monitor UFW logs | Ubuntu |
| sudo journalctl -u ufw | View detailed UFW journal | Ubuntu |

| | | |
|---|---|---|
| | logs | |
| sudo adduser testuser | Creates a user for testing SSH access | Ubuntu |
| hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://<Ubuntu_IP> | Performs brute-force SSH attack | Kali |
| ping <Ubuntu_IP> | Verifies network connectivity | Kali |