

<b>Document Name</b>	<b>Brute-Force Post-Mitigation Validation (Windows Server 2022)</b>	<b>Version</b>	<b>1.3</b>
<b>Author</b>	<b>Anusha Ramu Chakravarthi</b>	<b>Date Created</b>	<b>19/04/2025</b>
<b>Attack Type</b>	<b>Brute-Force Testing (Post-Security Hardening)</b>	<b>Last Modified</b>	<b>27/04/2025</b>

## Document Description

This revised runbook is designed to validate the effectiveness of brute-force protection mechanisms implemented on Ubuntu 22.04 after initial testing. These include tools such as Fail2Ban, SSH hardening, WordPress login restrictions, and other mitigations. It aligns with the "Protect" and "Detect" functions of the NIST Cybersecurity Framework.

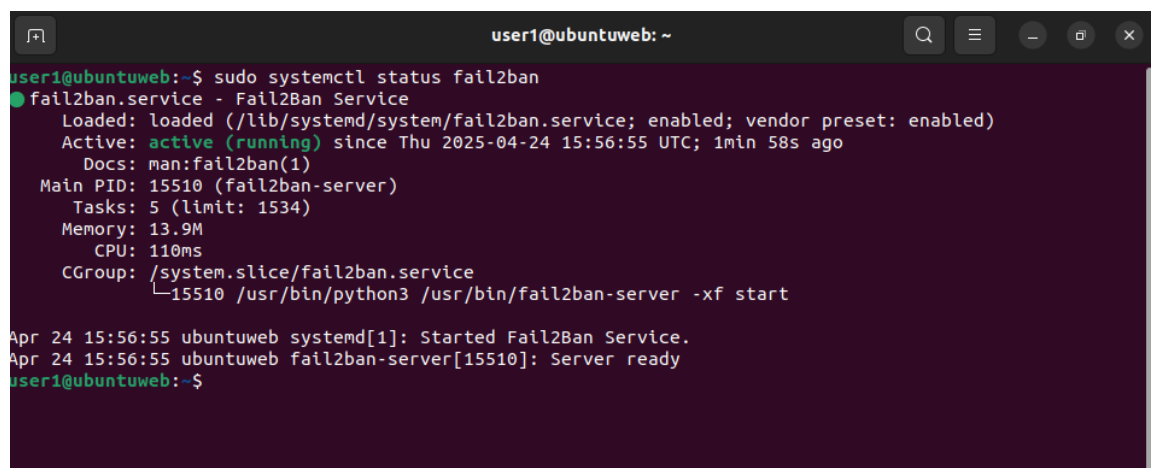
## Step 1

### Verify Security Controls Are Active

Ensure all configured brute-force protection mechanisms are active.

- Confirm **Fail2Ban** is installed and running:

```
sudo systemctl status fail2ban
```



```

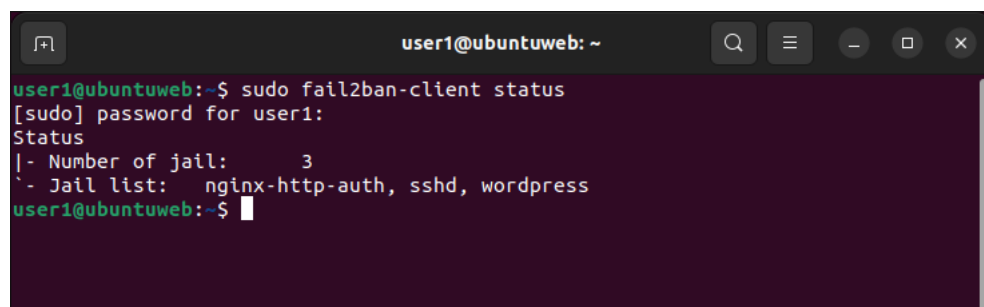
user1@ubuntuweb: ~
user1@ubuntuweb:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-04-24 15:56:55 UTC; 1min 58s ago
     Docs: man:fail2ban(1)
    Main PID: 15510 (fail2ban-server)
      Tasks: 5 (limit: 1534)
    Memory: 13.9M
       CPU: 110ms
    CGroup: /system.slice/fail2ban.service
            └─15510 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Apr 24 15:56:55 ubuntuweb systemd[1]: Started Fail2Ban Service.
Apr 24 15:56:55 ubuntuweb fail2ban-server[15510]: Server ready
user1@ubuntuweb:~$

```

- Verify Fail2Ban jail configuration for SSH and WordPress (apache/nginx).

```
sudo fail2ban-client status
```



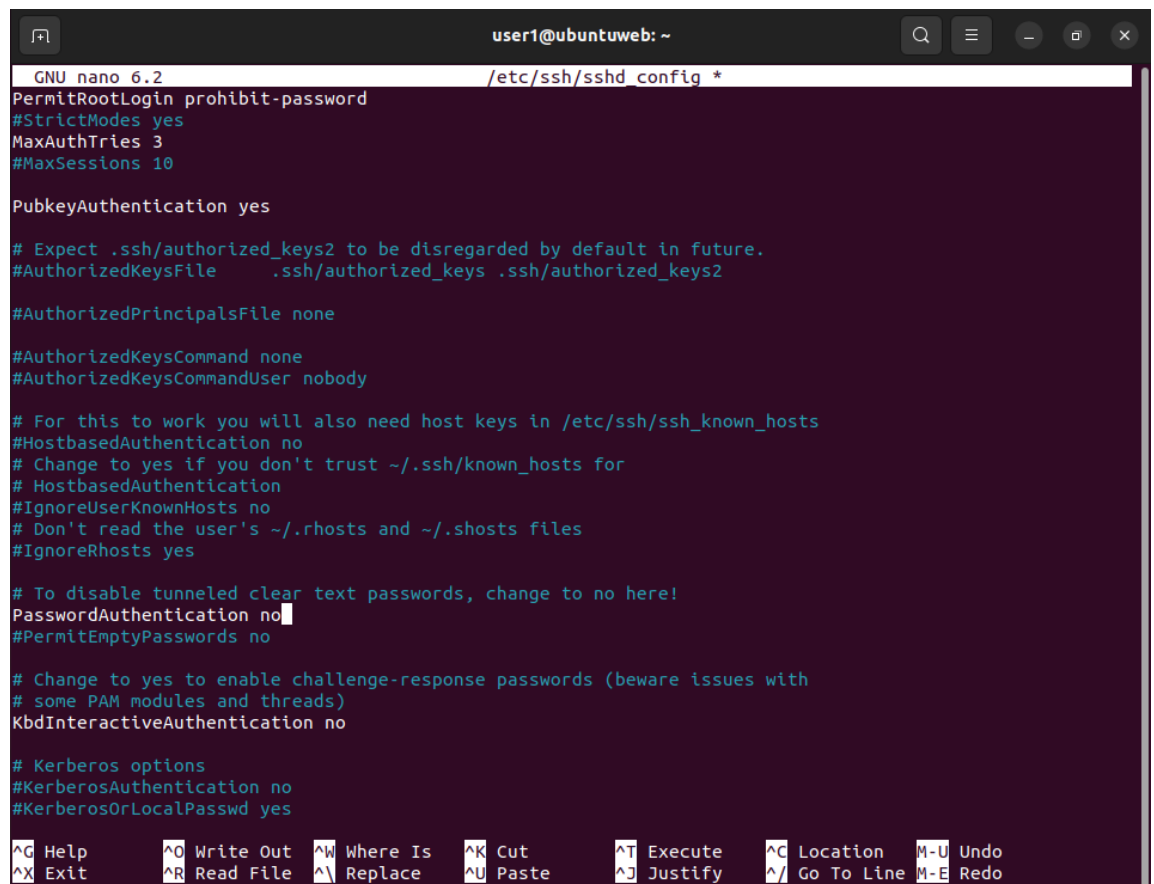
```

user1@ubuntuweb:~$ sudo fail2ban-client status
[sudo] password for user1:
Status
|- Number of jail:      3
  '- Jail list:  nginx-http-auth, sshd, wordpress
user1@ubuntuweb:~$

```

- Confirm SSH PasswordAuthentication is set to "no" (if applicable):

```
sudo nano /etc/ssh/sshd_config
```



```

GNU nano 6.2 /etc/ssh/sshd_config *
PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

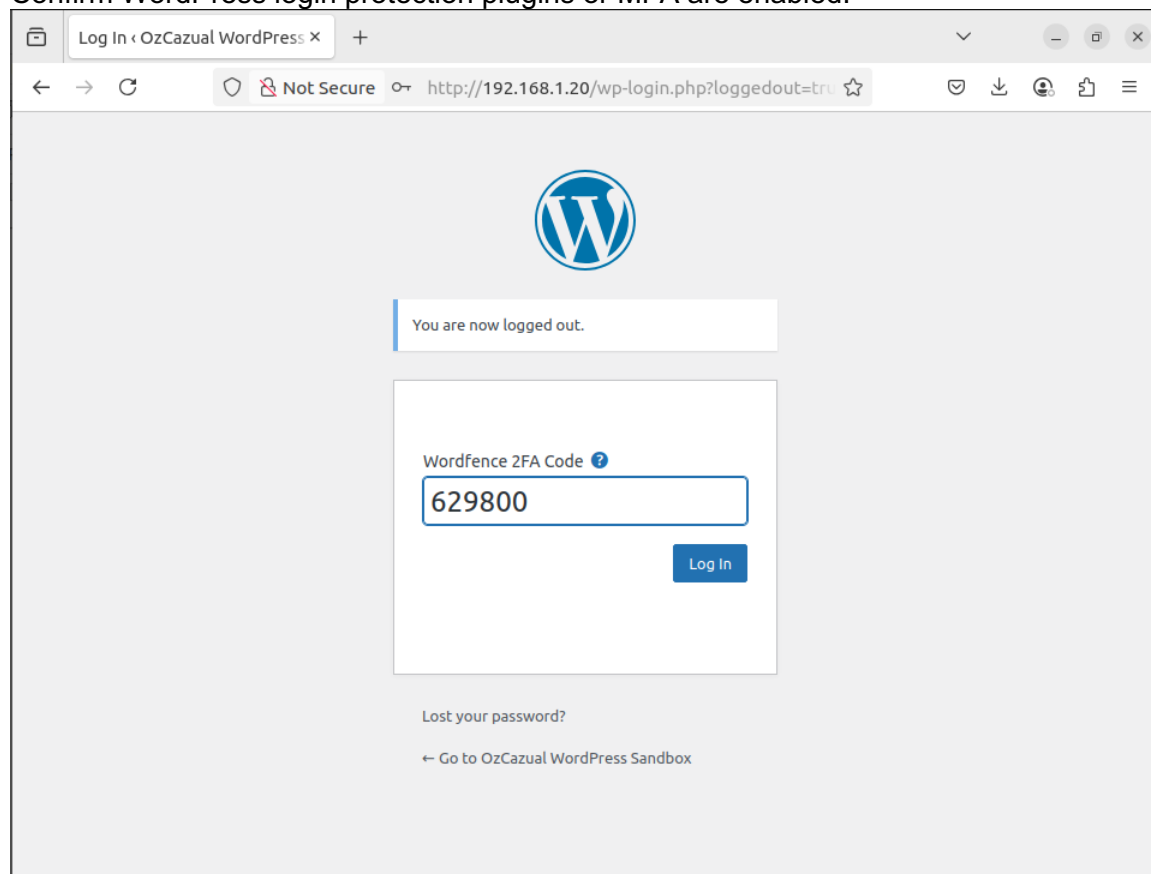
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes

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

```

- Confirm WordPress login protection plugins or MFA are enabled.



## Step 2

### Simulate SSH Brute-Force Attack (Controlled)

Run controlled brute-force attempts under the Fail2Ban threshold.

- Use Hydra to perform 3-4 failed SSH login attempts.
- Confirm Fail2Ban does not trigger before threshold is crossed.

```
hydra -L users.txt -P passwords.txt ssh://<target_IP>
```

```
user1@kali: ~  
user1@ubuntuweb: ~  
user1@ubuntuweb: ~  
user1@kali: ~  
[user1@kali]~  
$ hydra -L /usr/share/wordlists/users.txt -P /usr/share/wordlists/passwords.txt ssh://192.168.1.20 -vv  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret 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 2025-04-27 03:19:57  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prev  
ent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 352 login tries (l:22/p:16), ~22 tries per task  
[DATA] attacking ssh://192.168.1.20:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://admin@192.168.1.20:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.20:22  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "Weakpassword01" - 1 of 352 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "Weakpassword02" - 2 of 352 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "Weakpassword03" - 3 of 352 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "Weakpassword04" - 4 of 352 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "password1" - 5 of 352 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "userPass" - 6 of 352 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "pfsense" - 7 of 352 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "adminPass" - 8 of 352 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "Pqssword123!" - 9 of 352 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "!nf0tecH" - 10 of 352 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "testpass1" - 11 of 352 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "testpass2" - 12 of 352 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "testpass99" - 13 of 352 [child 12] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "123456" - 14 of 352 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "awesome!" - 15 of 352 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "password" - 16 of 352 [child 15] (0/0)  
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer  
[ERROR] ssh protocol error  
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer  
[ERROR] ssh protocol error
```

- Monitor /var/log/auth.log.

```
sudo tail -f /var/log/auth.log
```

```
user1@ubuntuweb: ~  
user1@ubuntuweb: ~  
user1@kali: ~  
Apr 26 17:21:00 ubuntuweb sshd[5684]: Received disconnect from 192.168.1.99 port 53222:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5684]: Disconnected from invalid user james 192.168.1.99 port 53222 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5686]: Received disconnect from 192.168.1.99 port 53234:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5686]: Disconnected from invalid user james 192.168.1.99 port 53234 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5708]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5708]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=  
192.168.1.99 user=testuser99  
Apr 26 17:21:00 ubuntuweb sshd[5688]: Received disconnect from 192.168.1.99 port 53250:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5688]: Disconnected from invalid user james 192.168.1.99 port 53250 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5698]: Failed password for invalid user james from 192.168.1.99 port 53330 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5691]: Failed password for invalid user james from 192.168.1.99 port 53286 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5690]: Failed password for invalid user james from 192.168.1.99 port 53282 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5694]: Failed password for invalid user james from 192.168.1.99 port 53302 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5696]: Failed password for invalid user james from 192.168.1.99 port 53316 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5710]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5712]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5712]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=  
192.168.1.99 user=testuser99  
Apr 26 17:21:00 ubuntuweb sshd[5710]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=  
192.168.1.99 user=testuser99  
Apr 26 17:21:00 ubuntuweb sshd[5700]: Failed password for invalid user james from 192.168.1.99 port 53360 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5701]: Failed password for invalid user james from 192.168.1.99 port 53366 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5690]: Received disconnect from 192.168.1.99 port 53282:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5690]: Disconnected from invalid user james 192.168.1.99 port 53282 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5691]: Received disconnect from 192.168.1.99 port 53286:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5691]: Disconnected from invalid user james 192.168.1.99 port 53286 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5694]: Received disconnect from 192.168.1.99 port 53302:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5694]: Disconnected from invalid user james 192.168.1.99 port 53302 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5696]: Received disconnect from 192.168.1.99 port 53316:11: Bye Bye [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5696]: Disconnected from invalid user james 192.168.1.99 port 53316 [preauth]  
Apr 26 17:21:00 ubuntuweb sshd[5714]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5715]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5704]: Failed password for invalid user james from 192.168.1.99 port 53374 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5718]: User testuser99 from 192.168.1.99 not allowed because not listed in AllowUsers  
Apr 26 17:21:00 ubuntuweb sshd[5622]: Failed password for invalid user james from 192.168.1.99 port 53198 ssh2  
Apr 26 17:21:00 ubuntuweb sshd[5715]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=
```

## Step 3

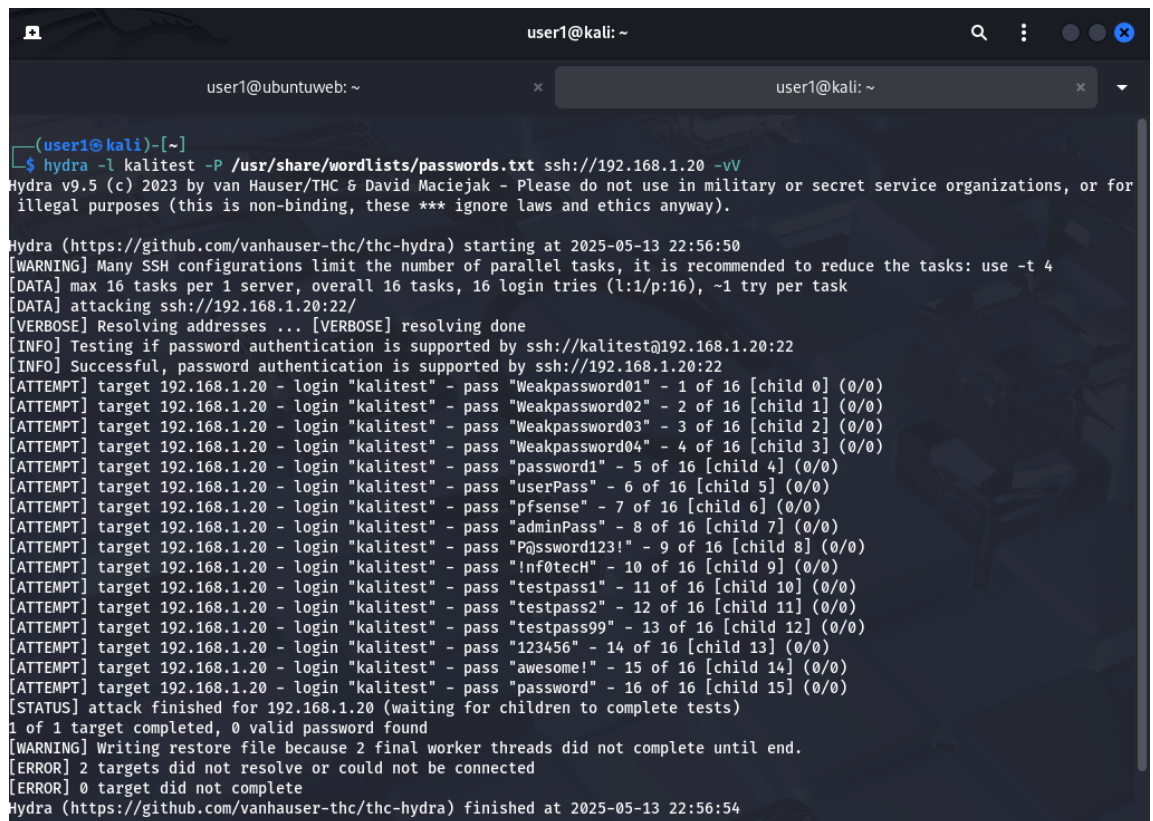
### Trigger Fail2Ban SSH Protection

Exceed login threshold to verify IP banning.

- Use **Hydra** or **manual SSH** attempts to fail logins repeatedly.

- Using **hydra**:

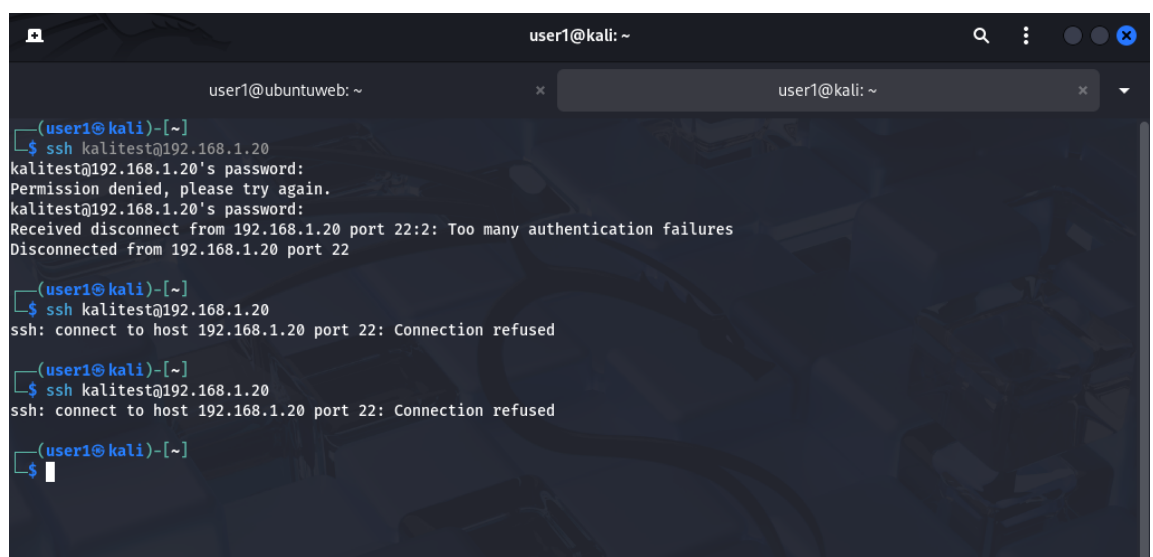
```
hydra -l <username> -P passwords.txt  
ssh://<target_IP>
```



```
(user1@kali)-[~]  
$ hydra -l kalitest -P /usr/share/wordlists/passwords.txt ssh://192.168.1.20 -vv  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret 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 2025-05-13 22:56:50  
[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, 16 login tries (l:1/p:16), ~1 try per task  
[DATA] attacking ssh://192.168.1.20:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://kalitest@192.168.1.20:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.20:22  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "Weakpassword01" - 1 of 16 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "Weakpassword02" - 2 of 16 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "Weakpassword03" - 3 of 16 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "Weakpassword04" - 4 of 16 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "password1" - 5 of 16 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "userPass" - 6 of 16 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "pfsense" - 7 of 16 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "adminPass" - 8 of 16 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "P@ssword123!" - 9 of 16 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "!nf0tech" - 10 of 16 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "testpass1" - 11 of 16 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "testpass2" - 12 of 16 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "testpass99" - 13 of 16 [child 12] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "123456" - 14 of 16 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "awesome!" - 15 of 16 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.20 - login "kalitest" - pass "password" - 16 of 16 [child 15] (0/0)  
[STATUS] attack finished for 192.168.1.20 (waiting for children to complete tests)  
1 of 1 target completed, 0 valid password found  
[WARNING] Writing restore file because 2 final worker threads did not complete until end.  
[ERROR] 2 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-13 22:56:54
```

- **Manual SSH with wrong user:**

```
ssh <username>@<target_IP>
```

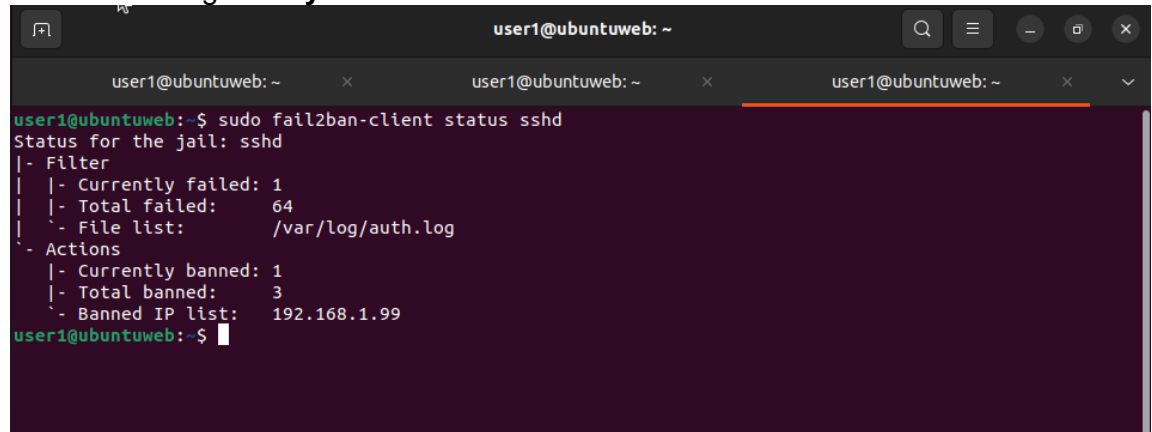


```
(user1@kali)-[~]  
$ ssh kalitest@192.168.1.20  
kalitest@192.168.1.20's password:  
Permission denied, please try again.  
kalitest@192.168.1.20's password:  
Received disconnect from 192.168.1.20 port 22: Too many authentication failures  
Disconnected from 192.168.1.20 port 22  
  
(user1@kali)-[~]  
$ ssh kalitest@192.168.1.20  
ssh: connect to host 192.168.1.20 port 22: Connection refused  
  
(user1@kali)-[~]  
$ ssh kalitest@192.168.1.20  
ssh: connect to host 192.168.1.20 port 22: Connection refused  
  
(user1@kali)-[~]  
$
```

- Check **Fail2Ban logs**:

```
sudo fail2ban-client status sshd
```

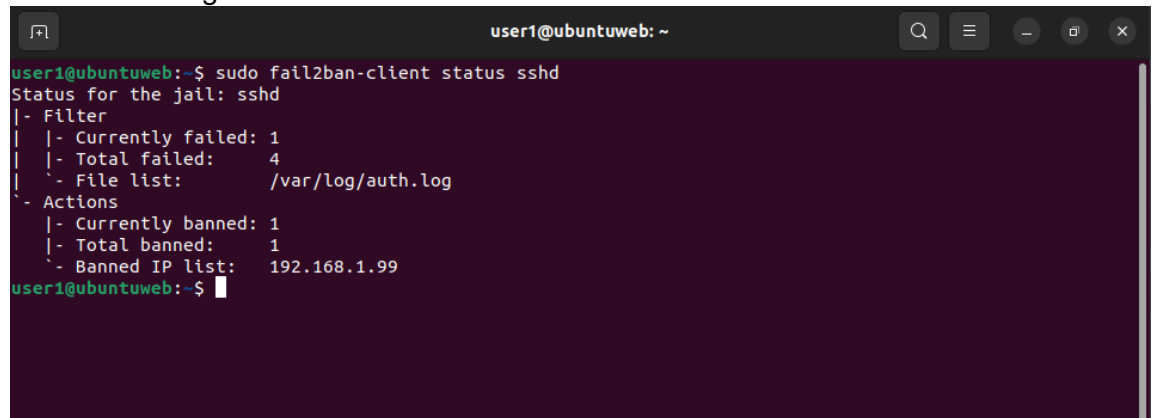
- Fail2ban logs for **Hydra**



A terminal window titled 'user1@ubuntuweb: ~' showing the output of the command 'sudo fail2ban-client status sshd'. The output displays the status for the jail 'sshd'. Under the 'Filter' section, it shows 'Currently failed: 1', 'Total failed: 64', and 'File list: /var/log/auth.log'. Under the 'Actions' section, it shows 'Currently banned: 1', 'Total banned: 3', and 'Banned IP list: 192.168.1.99'.

```
user1@ubuntuweb:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed:    64
|   '- File list:       /var/log/auth.log
'- Actions
    |- Currently banned: 1
    |- Total banned:    3
    '- Banned IP list:   192.168.1.99
user1@ubuntuweb:~$
```

- Fail2ban logs for **Manual SSH**



A terminal window titled 'user1@ubuntuweb: ~' showing the output of the command 'sudo fail2ban-client status sshd'. The output displays the status for the jail 'sshd'. Under the 'Filter' section, it shows 'Currently failed: 1', 'Total failed: 4', and 'File list: /var/log/auth.log'. Under the 'Actions' section, it shows 'Currently banned: 1', 'Total banned: 1', and 'Banned IP list: 192.168.1.99'.

```
user1@ubuntuweb:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed:    4
|   '- File list:       /var/log/auth.log
'- Actions
    |- Currently banned: 1
    |- Total banned:    1
    '- Banned IP list:   192.168.1.99
user1@ubuntuweb:~$
```

- Confirm attacker IP is banned.



- Check for corresponding logs and system response.

```
sudo tail -f /var/log/auth.log
```

#### ○ System response for Hydra

```
user1@ubuntuweb: ~
May 13 12:56:31 ubuntuweb sudo: user1 : TTY=pts/2 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/fail2ban.log
May 13 12:56:31 ubuntuweb sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 13 12:56:50 ubuntuweb sshd[1271]: exited MaxStartups throttling after 00:04:06, 3 connections dropped
May 13 12:56:50 ubuntuweb sshd[3323]: Invalid user kalitest from 192.168.1.99 port 45936
May 13 12:56:50 ubuntuweb sshd[3323]: Received disconnect from 192.168.1.99 port 45936:11: Bye Bye [preauth]
May 13 12:56:50 ubuntuweb sshd[3323]: Disconnected from invalid user kalitest 192.168.1.99 port 45936 [preauth]
May 13 12:56:51 ubuntuweb sshd[3334]: Invalid user kalitest from 192.168.1.99 port 46044
May 13 12:56:51 ubuntuweb sshd[3336]: Invalid user kalitest from 192.168.1.99 port 46062
May 13 12:56:51 ubuntuweb sshd[3337]: Invalid user kalitest from 192.168.1.99 port 46076
May 13 12:56:51 ubuntuweb sshd[3333]: Invalid user kalitest from 192.168.1.99 port 46040
May 13 12:56:51 ubuntuweb sshd[3340]: Invalid user kalitest from 192.168.1.99 port 46094
May 13 12:56:51 ubuntuweb sshd[3329]: Invalid user kalitest from 192.168.1.99 port 45994
May 13 12:56:51 ubuntuweb sshd[3332]: Invalid user kalitest from 192.168.1.99 port 46032
May 13 12:56:51 ubuntuweb sshd[3330]: Invalid user kalitest from 192.168.1.99 port 46010
May 13 12:56:51 ubuntuweb sshd[3335]: Invalid user kalitest from 192.168.1.99 port 46056
May 13 12:56:51 ubuntuweb sshd[3334]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:56:51 ubuntuweb sshd[3339]: Invalid user kalitest from 192.168.1.99 port 46090
May 13 12:56:51 ubuntuweb sshd[3336]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:56:51 ubuntuweb sshd[3336]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:56:51 ubuntuweb sshd[3337]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:56:51 ubuntuweb sshd[3334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:56:51 ubuntuweb sshd[3337]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:56:51 ubuntuweb sshd[3333]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:56:51 ubuntuweb sshd[3333]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:56:51 ubuntuweb sshd[3332]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:56:51 ubuntuweb sshd[3332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
```

#### ○ System response for Manual SSH

```
user1@ubuntuweb: ~
May 13 12:39:06 ubuntuweb sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/nano /etc/fail2ban/jail.local
May 13 12:39:06 ubuntuweb sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 13 12:40:12 ubuntuweb sudo: pam_unix(sudo:session): session closed for user root
May 13 12:40:47 ubuntuweb sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/systemctl restart fail2ban
May 13 12:40:47 ubuntuweb sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 13 12:40:48 ubuntuweb sudo: pam_unix(sudo:session): session closed for user root
May 13 12:41:00 ubuntuweb sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/fail2ban-client status
May 13 12:41:00 ubuntuweb sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 13 12:41:01 ubuntuweb sudo: pam_unix(sudo:session): session closed for user root
May 13 12:42:33 ubuntuweb sshd[3079]: Invalid user kalitest from 192.168.1.99 port 43942
May 13 12:42:41 ubuntuweb sshd[3079]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:42:41 ubuntuweb sshd[3079]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:42:42 ubuntuweb sshd[3079]: Failed password for invalid user kalitest from 192.168.1.99 port 43942 ssh2
May 13 12:42:49 ubuntuweb sshd[3079]: pam_unix(sshd:auth): check pass; user unknown
May 13 12:42:51 ubuntuweb sshd[3079]: Failed password for invalid user kalitest from 192.168.1.99 port 43942 ssh2
May 13 12:42:53 ubuntuweb sshd[3079]: error: maximum authentication attempts exceeded for invalid user kalitest from 192.168.1.99 port 43942 ssh2 [preauth]
May 13 12:42:53 ubuntuweb sshd[3079]: Disconnecting invalid user kalitest 192.168.1.99 port 43942: Too many authentication failures [preauth]
May 13 12:42:53 ubuntuweb sshd[3079]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99
May 13 12:43:20 ubuntuweb sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
May 13 12:43:20 ubuntuweb sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 13 12:43:20 ubuntuweb sudo: pam_unix(sudo:session): session closed for user root
May 13 12:45:59 ubuntuweb sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/usr/bin/cat /var/log/auth.log
user1@ubuntuweb: ~$
```

```
sudo tail -f /var/log/fail2ban.log
```

```
user1@ubuntuweb: ~  
user1@ubuntuweb: ~  
user1@ubuntuweb: ~  
user1@ubuntuweb:~$ sudo tail -f /var/log/fail2ban.log  
[sudo] password for user1:  
2025-05-13 12:52:47,045 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:52:47  
2025-05-13 12:52:47,050 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:52:47  
2025-05-13 12:52:47,050 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:52:47  
2025-05-13 12:52:47,052 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:52:47  
2025-05-13 12:52:47,158 fail2ban.actions [3061]: NOTICE [sshd] 192.168.1.99 already banned  
2025-05-13 12:52:47,158 fail2ban.actions [3061]: NOTICE [sshd] 192.168.1.99 already banned  
2025-05-13 12:52:47,158 fail2ban.actions [3061]: NOTICE [sshd] 192.168.1.99 already banned  
2025-05-13 12:52:47,158 fail2ban.actions [3061]: NOTICE [sshd] 192.168.1.99 already banned  
2025-05-13 12:52:47,181 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:52:47  
2025-05-13 12:55:47,020 fail2ban.actions [3061]: NOTICE [sshd] Unban 192.168.1.99  
2025-05-13 12:56:50,736 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:50  
2025-05-13 12:56:51,112 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,118 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,121 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,126 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,143 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,152 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,155 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,158 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1  
2:56:51  
2025-05-13 12:56:51,160 fail2ban.filter [3061]: INFO [sshd] Found 192.168.1.99 - 2025-05-13 1
```

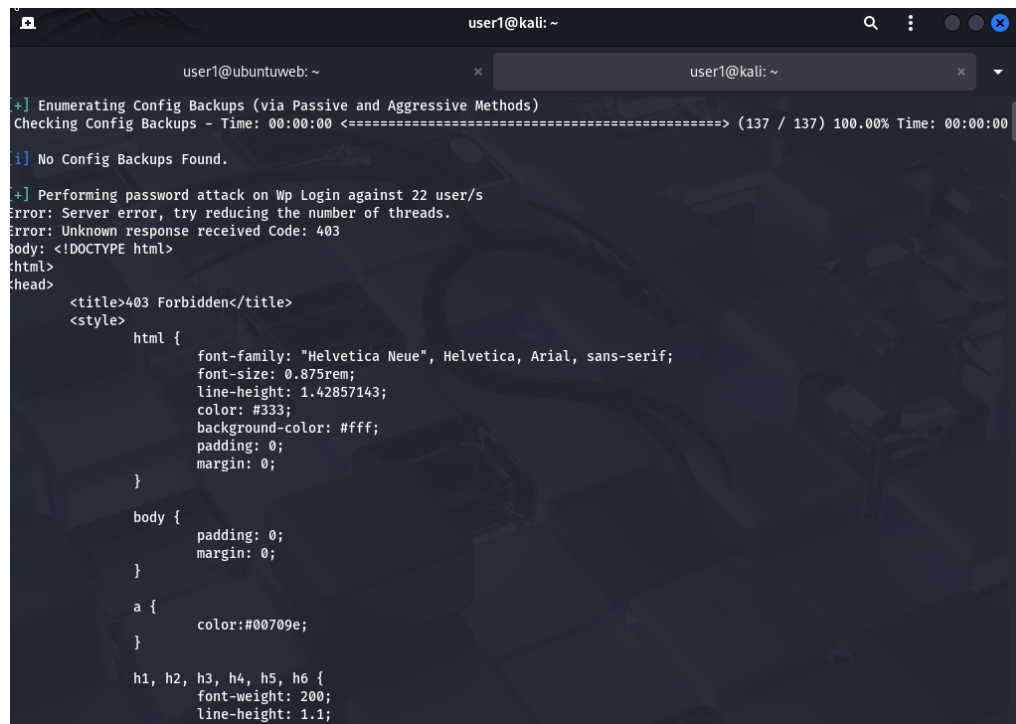
## Step 4

### Simulate WordPress Brute-Force with Login Protection

Attempt login to WordPress to validate plugin or application-layer protection.

- Use WPScan or Burp Suite for simulated login attempts.
- Monitor login behavior (rate limiting, CAPTCHAs, lockouts).

```
wpscan -v -t2 --url http://<target_IP> -U users.txt -P passwords.txt -force
```

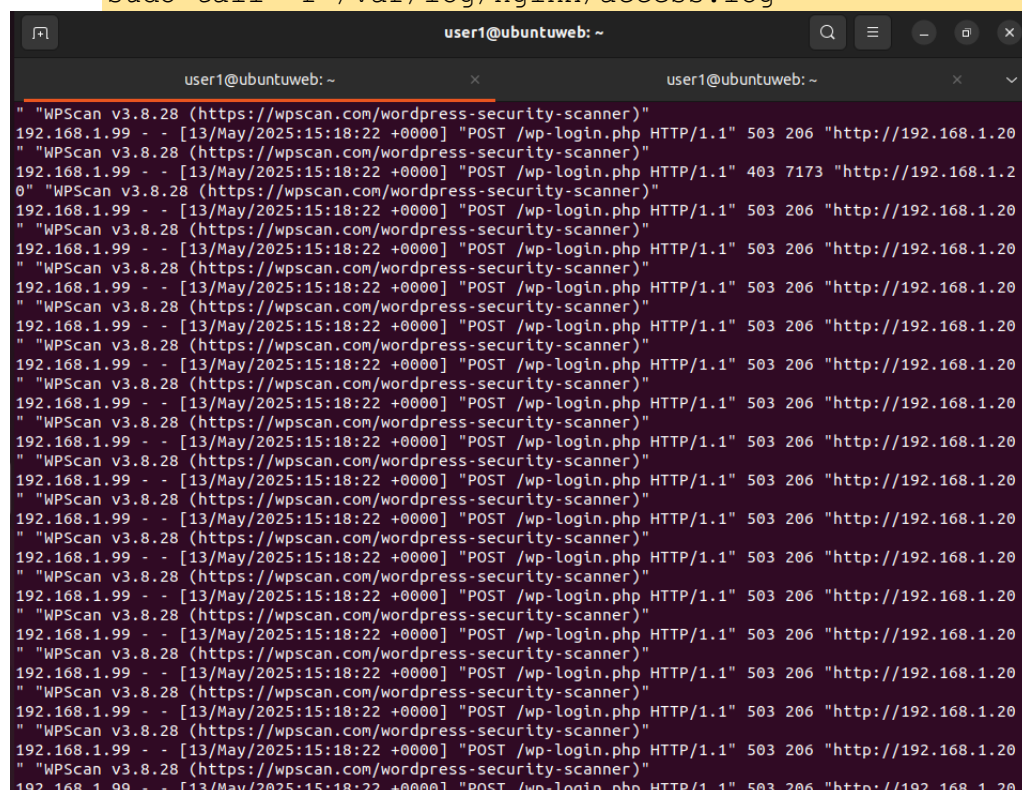


```
user1@kali: ~  
user1@ubuntuweb: ~  
+ ] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:00 <===== (137 / 137) 100.00% Time: 00:00:00  
i ] No Config Backups Found.  
+ ] Performing password attack on Wp Login against 22 user/s  
Error: Server error, try reducing the number of threads.  
Error: Unknown response received Code: 403  
Body: <!DOCTYPE html>  
<html>  
<head>  
<title>403 Forbidden</title>  
<style>  
    html {  
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;  
        font-size: 0.875rem;  
        line-height: 1.42857143;  
        color: #333;  
        background-color: #fff;  
        padding: 0;  
        margin: 0;  
    }  
  
    body {  
        padding: 0;  
        margin: 0;  
    }  
  
    a {  
        color: #00709e;  
    }  
  
    h1, h2, h3, h4, h5, h6 {  
        font-weight: 200;  
        line-height: 1.1;  
    }  
</style>  
</head>  
</html>
```

- Check web server access logs and plugin logs.

- **Web Server access logs:**

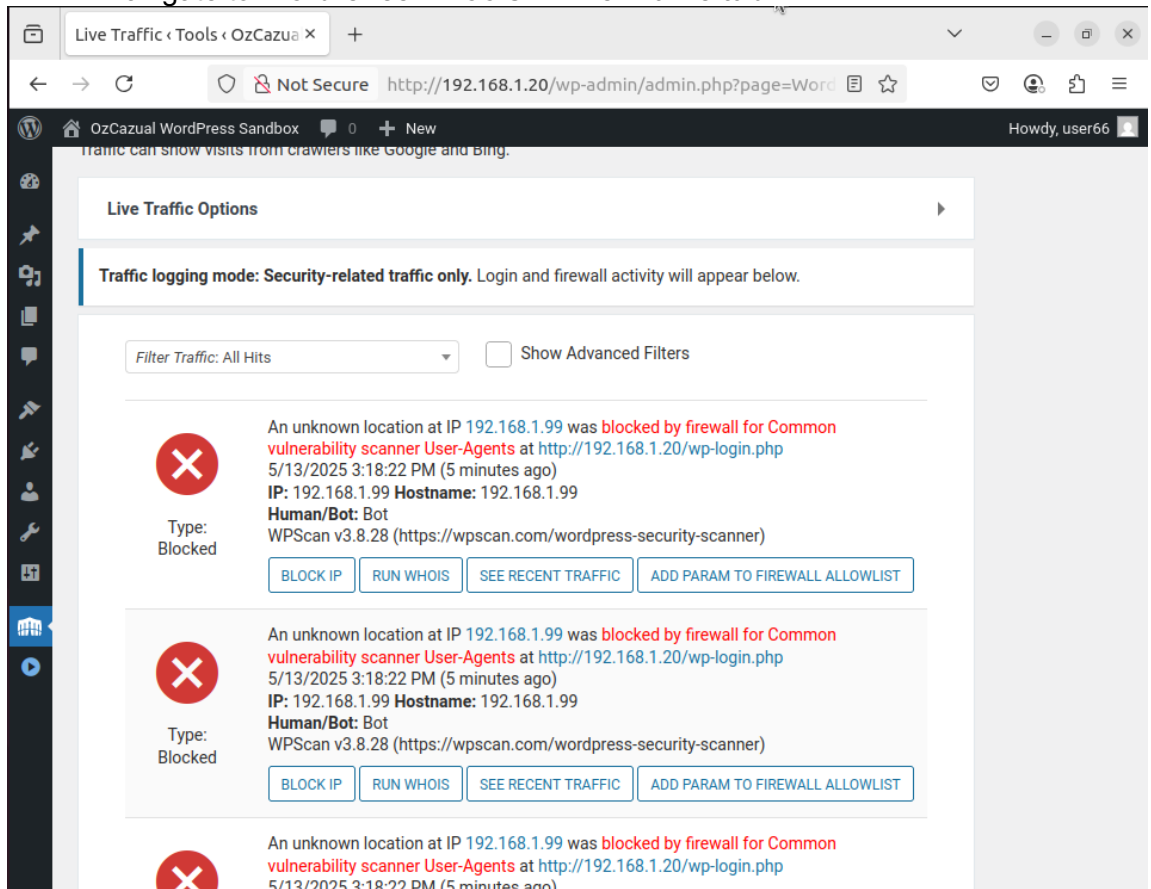
```
sudo tail -f /var/log/nginx/access.log
```



```
user1@ubuntuweb: ~  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 403 7173 "http://192.168.1.20"  
0 "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"  
"WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
192.168.1.99 - - [13/May/2025:15:18:22 +0000] "POST /wp-login.php HTTP/1.1" 503 206 "http://192.168.1.20"
```



- **Wordfence Plugin logs:**  
Login to WordPress.  
Navigate to **Wordfence > Tools > Live Traffic tab**



## Step 5

### Analyze Detection and Logs

Confirm all attacks are logged and responded to as expected.

- Review SSH logs: `/var/log/auth.log`
- Review Fail2Ban logs: `/var/log/fail2ban.log`
- Analyze `/var/log/nginx/access.log` or `apache2/access.log`
- Review **WordPress plugin logs** if available.

## Step 6

### Unban and Restore Access

Clear bans to restore access for additional testing.

- Unban test IPs using:  
`sudo fail2ban-client set sshd unbanip <attacker-ip>`
- Re-enable any disabled login protections (e.g., plugin lockouts).
- 

## Step 7

### Document Findings and Final Observations

Record test results and note system behavior.

- Log effectiveness of Fail2Ban and WordPress protections.
- Identify any weaknesses or bypass opportunities.
- Recommend configuration tuning where necessary.
- Export logs/screenshots as part of reporting.
- Refer **Test\_observations\_results\_ubuntu\_web\_server\_v1.pdf**