

TASK2:

Remote Access & SSH Hardening:

Setup:

1. To start the process, we first activate it using `sudo systemctl enable ssh`, followed by `sudo systemctl start ssh`.

```
(kali㉿kali)-[~]  
$ sudo systemctl enable ssh  
[sudo] password for kali:  
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh  
  
(kali㉿kali)-[~]  
$ sudo systemctl start ssh
```

2. Next, we update the SSH configuration to allow root login and enable password authentication by modifying the `/etc/ssh/sshd_config` file.

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

3. Now, update the `PermitRootLogin` and `PasswordAuthentication` parameters to `yes`.

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

4. We restart the SSH service.

```
(kali㉿kali)-[~]
$ sudo systemctl restart ssh
```

Exploitation: Brute forcing SSH

1. To brute-force SSH root login hydra is used.

```
(kali㉿kali)-[~]
$ hydra -l root -p kat.txt ssh://192.168.29.133
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-25 07:31:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
```

2. Root login and authentication are disabled, this is done by setting PermitRootLogin and PasswordAuthentication no.

3. To enhance authentication security, generate an SSH key pair on the client machine using `ssh-keygen -t rsa -b 4096`.

```
(kali㉿kali)-[~]
$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): yes
Enter passphrase for "yes" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in yes
Your public key has been saved in yes.pub
The key fingerprint is:
SHA256:2j2RHGX80V0vV0a/T/UdJD0e/OGkCKU3GFw11vwdSR4 kali@kali
The key's randomart image is:
+--[RSA 4096]--+
|    ... ++B+E=|
|    .o= XB=|
|    +.o = *@|
|    .ooo *o@|
|    S +. ..+=|
|    o . . o.|
|    . . o .|
|    .|
+---[SHA256]---+
```

4. Next, copy the key to the server with `ssh-copy-id user@` and finally , restarting the SSH server using `sudo systemctl restart ssh`.

```
(kali㉿kali)-[~]
$ ssh-copy-id user@192.168.62.133
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub"
```

Configure Fail2ban to prevent attacks:

1. To improve system security, install fail2ban using `sudo apt install fail2ban -y`. It helps helps to defend against brute-force attacks by detecting and blocking 3rd party login attempts.

```
(kali㉿kali)-[~]
$ sudo apt update && sudo apt install fail2ban -y
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
```

2. Atlast restart fail2ban to avoid SSH attacks.

```
(kali㉿kali)-[~]
$ sudo systemctl restart fail2ban
```

