

PoC Task 2

Task 2: Remote Access & SSH Hardening

1) Setup:

1.1) Enable SSH:

`sudo systemctl enable ssh`

`sudo systemctl start ssh`

```
(kali㉿kali)-[~]
└─$ sudo chown root:root /etc/passwd

(kali㉿kali)-[~]
└─$ sudo visudo
visudo: /etc/sudoers.tmp unchanged

(kali㉿kali)-[~]
└─$ visudo
visudo: /etc/sudoers: Permission denied

(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
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
Created symlink '/etc/systemd/system/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.

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

(kali㉿kali)-[~]
└─$
```

```
(kali㉿kali)-[~]
└─$ sudo systemctl start ssh

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

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

(kali㉿kali)-[~]
└─$ hydra -l root -P rockyou.txt ssh://192.168.1.100
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 2025-03-18 10:36:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
```

1.2) Allow root login:

`sudo nano /etc/ssh/sshd_config`

Change PermitRootLogin yes

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#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

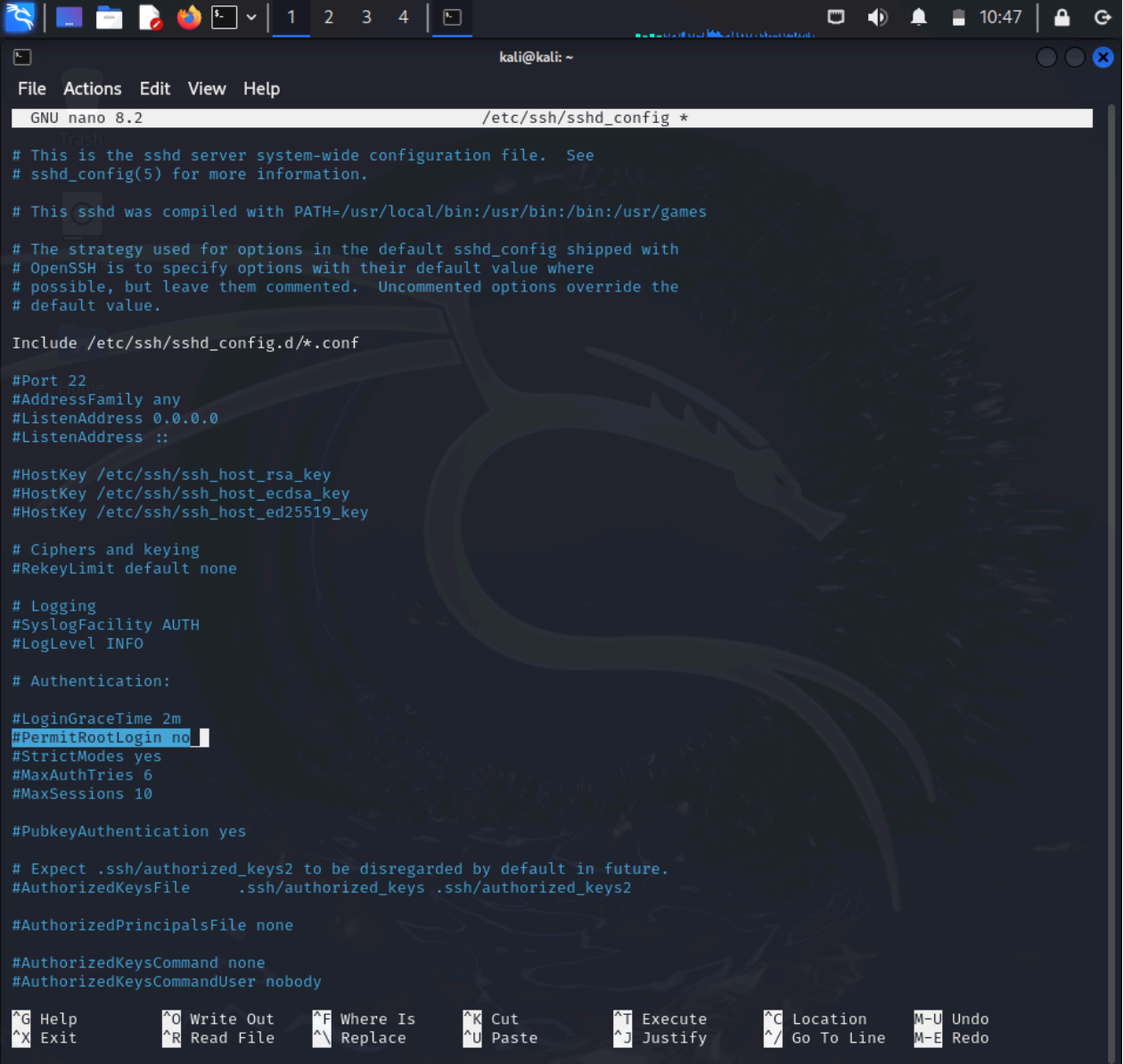
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

2) Exploit:

2.1) Disable root login:

`sudo nano /etc/ssh/sshd_config`

`# Set PermitRootLogin no`



```
GNU nano 8.2 /etc/ssh/sshd_config *
# 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 no
#StrictModes yes
#MaxAuthTries 6
#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

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

3) Enable key-based authentication:

ssh-keygen -t rsa

```
(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): kali
kali already exists.
Overwrite (y/n)? y
Enter passphrase for "kali" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kali
Your public key has been saved in kali.pub
The key fingerprint is:
SHA256:Yb6sh1D+A2HuCXIxUjSBxJS6pDJda/XjvD716aQwUo kali㉿kali
The key's randomart image is:
+--[RSA 4096]--+
| +0++         |
| + ..         |
| . .   o      |
| ... + =0 . .  |
| oo o X oE o   |
| = o * +oo+.   |
| .. + + B*o ...|
|    +.Bo oo    |
|    .oo+ ...   |
+--[SHA256]--+

(kali㉿kali)-[~]
$
```

4) Configure fail2ban:

4.1) sudo apt install fail2ban

```
(kali㉿kali)-[~]
$ sudo apt install fail2ban
The following packages were automatically installed and are no longer required:
  libpython3.12-dev python3.12-dev python3.12-venv ruby3.1-dev
  python3.12 python3.12-minimal ruby3.1 ruby3.1-doc
Use 'sudo apt autoremove' to remove them.

Upgrading:
  blueman          libnss-winbind    libwbclient0      python3-donut      python3-venv      samba-libs
  curl             libpam-winbind    onboard           python3-ldb         python3.13-tk      smbclient
  ldap-utils       libpython3-dev    onboard-common    python3-minimal    samba              tdb-tools
  libcurl3t64-gnutls libpython3-stdlib onboard-data       python3-nassl      samba-ad-dc        winbind
  libcurl4t64      libsmclient0      python3           python3-pycurl     samba-ad-provision samba-common
  libjs-sphinxdoc  libtalloc2        python3-aardwolf  python3-samba      samba-common       samba-common-bin
  libldap-common   libtdb1           python3-arc4      python3-talloc     samba-common-bin   samba-dsdb-modules
  libldb2          libtevent0t64     python3-dev       python3-tdb        samba-dsdb-modules

Installing:
  fail2ban

Installing dependencies:
  libldap2      libpython3.13-dev  libpython3.13-stdlib  python3.13  python3.13-minimal
  libpython3.13 libpython3.13-minimal python3-systemd      python3.13-dev  python3.13-venv

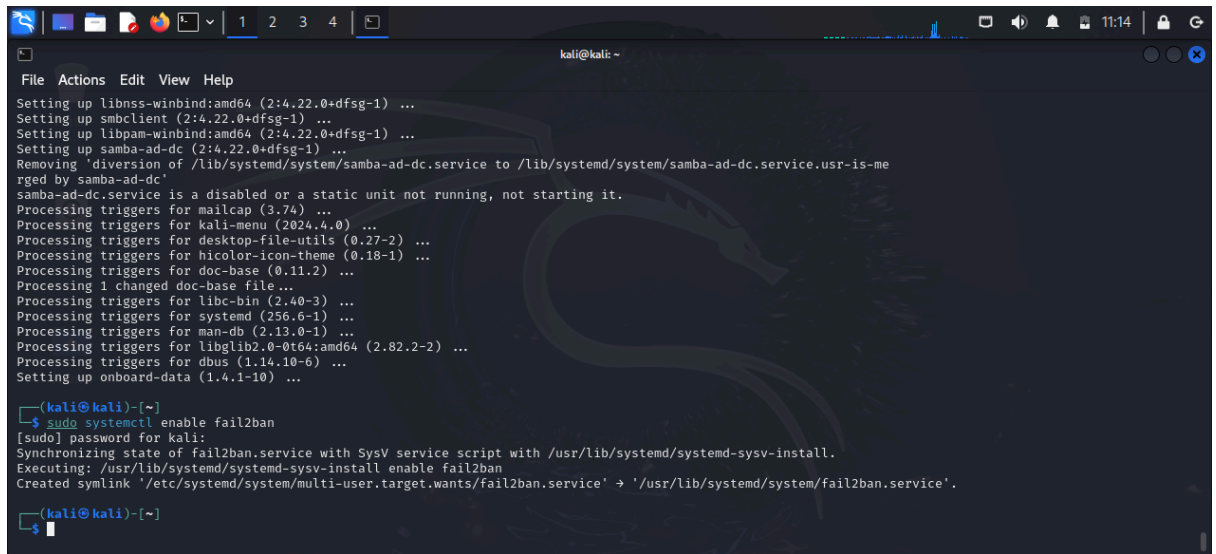
Suggested packages:
  mailx system-log-daemon monit python3.13-doc binfmt-support

REMOVING:
  winexe

Summary:
  Upgrading: 44, Installing: 11, Removing: 1, Not Upgrading: 1458
  Download size: 38.0 MB
  Space needed: 66.5 MB / 63.6 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-samba amd64 2:4.22.0+dfsg-1 [2,868 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 samba-common-bin amd64 2:4.22.0+dfsg-1 [1,330 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 smbclient amd64 2:4.22.0+dfsg-1 [498 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 samba-dsdb-modules amd64 2:4.22.0+dfsg-1 [335 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 python3-ldb amd64 2:2.11.0+samba4.22.0+dfsg-1 [73.2 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libldb2 amd64 2:2.11.0+samba4.22.0+dfsg-1 [175 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 libsmclient0 amd64 2:4.22.0+dfsg-1 [94.7 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 samba-ad-provision all 2:4.22.0+dfsg-1 [503 kB]
14% [9 samba-ad-provision 35.5 kB/503 kB 7%] [Waiting for headers]
```

4.2) sudo systemctl enable fail2ban

A terminal window on a Kali Linux system. The window title is 'kali@kali: ~'. The terminal shows the output of a system update command, including messages for updating libnss-winbind, smbclient, libpam-winbind, and samba-ad-dc. It also shows the removal of a diversion for samba-ad-dc.service. After the update, the user runs 'sudo systemctl enable fail2ban'. The terminal shows the password prompt, the synchronization of fail2ban.service with the SysV script, the execution of the enable command, and the creation of a symlink. The prompt returns to '(kali@kali)~'.

```
kali@kali: ~  
File Actions Edit View Help  
Setting up libnss-winbind:amd64 (2:4.22.0+dfsg-1) ...  
Setting up smbclient (2:4.22.0+dfsg-1) ...  
Setting up libpam-winbind:amd64 (2:4.22.0+dfsg-1) ...  
Setting up samba-ad-dc (2:4.22.0+dfsg-1) ...  
Removing diversion of /lib/systemd/system/samba-ad-dc.service to /lib/systemd/system/samba-ad-dc.service.usr-is-me  
rged by samba-ad-dc'  
samba-ad-dc.service is a disabled or a static unit not running, not starting it.  
Processing triggers for mailcap (3.74) ...  
Processing triggers for kali-menu (2024.4.0) ...  
Processing triggers for desktop-file-utils (0.27-2) ...  
Processing triggers for hicolor-icon-theme (0.18-1) ...  
Processing triggers for doc-base (0.11.2) ...  
Processing 1 changed doc-base file ...  
Processing triggers for libc-bin (2.40-3) ...  
Processing triggers for systemd (256.6-1) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for libglib2.0-0t64:amd64 (2.82.2-2) ...  
Processing triggers for dbus (1.14.10-6) ...  
Setting up onboard-data (1.4.1-10) ...  
  
(kali@kali)~  
$ sudo systemctl enable fail2ban  
[sudo] password for kali:  
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban  
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' -> '/usr/lib/systemd/system/fail2ban.service'.  
  
(kali@kali)~  
$
```