

PROOF OF CONCEPT

LINUX SECURITY - EXPLOITATION & HARDENING

Task 2: Remote Access & SSH Hardening

1.EXECUTIVE SUMMARY

This PoC demonstrates the risks associated with insecure SSH configurations, such as allowing root login and password-based authentication. It includes enabling SSH, performing a brute-force attack, and then hardening the SSH configuration to prevent unauthorized access.

2.OBJECTIVES

- Setup: Enable SSH on a Linux machine, allow root login, and enable password authentication.
- Exploit: Perform a brute-force attack on SSH using tools like hydra or medusa.
- Mitigation: Disable root login, enable key-based authentication, and configure fail2ban to prevent brute-force attacks.

3. SETUP

3.1. Enable SSH and Configure Insecure Settings

1. Start and Enable SSH Service:

```
(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. Edit SSH Configuration to allow root login and password authentication:

```
(kali@kali)-[~]
$ sudo systemctl start ssh
[sudo] password for kali:

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

(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 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 2025-03-25 20:52:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: kat.txt
```

3.Restart SSH to apply changes:

```
(kali@kali)-[~]
$ sudo systemctl start ssh
[sudo] password for kali:

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

(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 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 2025-03-25 20:52:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: kat.txt
```

4) EXPLOIT:

4.1) Disable root login:

```
(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
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:BWqRnoTo3LPtY7BmtS8U8k/jXwtIJzs6a9grdHD6pTY kali@kali
The key's randomart image is:
+--[RSA 4096]--+
| . ...          |
|.. . 0.         |
|o .o.. .       |
| o =o+ . .     |
|  X ooS..      |
| * *.+=.       |
| . % 0+.. .    |
| * E.o. o .    |
| o ++B... .    |
+--[SHA256]-----+
```

4.2) Configure fail2ban:

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

Upgrading:
blueman          libldb2          libtalloc2       openssl           python3-ldb       python3-venv     samba-dsdb-modules
curl             libnss-winbind  libtdb1          openssl-provider-legacy python3-minimal   python3.13-tk    samba-lsbs
icu-devtools     libpam-winbind  libtevent0t64   python3           python3-nassl     samba            smbclient
libcurl3t64-gnutls libpython3-dev  libwbclient0    python3-aardwolf  python3-pycurl    samba-ad-dc      tdb-tools
libcurl4t64      libpython3-stdlib onboard         python3-arc4      python3-samba     samba-ad-provision winbind
libicu-dev       libsmbclient0  onboard-common  python3-dev       python3-samba     samba-common-bin
libjs-sphinxdoc libssl3t64     onboard-data    python3-donut     python3-tdb       samba-common-bin

Installing:
fail2ban

Installing dependencies:
libicu76      libpython3.13-dev  libpython3.13-stdlib python3.13      python3.13-minimal
libpython3.13 libpython3.13-minimal python3-systemd  python3.13-dev python3.13-venv
```

4.3) sudo systemctl enable fail2b:

```
(kali@kali)~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/sy
stemd/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'.
```