**Proof of Concept (PoC) Report**

**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. The task involves enabling SSH, exploiting weak configurations through a brute-force attack, and mitigating the risks by hardening the SSH configuration.

**2. Objectives Setup:**

* Enable SSH and configure it to allow root login and password authentication.
* **Exploit:** Perform a brute-force attack on SSH using a tool like Hydra.
* **Mitigation:** Disable root login, enable key-based authentication, and configure fail2ban to prevent brute-force attacks.

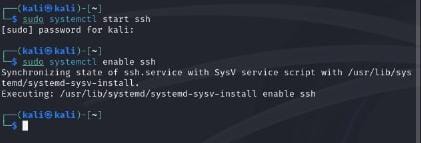
# 3. Setup

## 3.1. Enable SSH

SSH was enabled and set to start on boot using the systemctl command.

**Commands Used:**

sudo systemctl start ssh sudo systemctl enable ssh



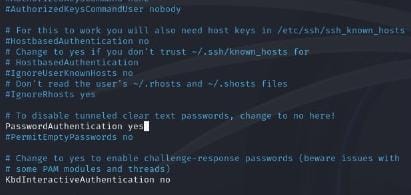
## 3.2 Allow Root Login and Password Authentication

The SSH configuration file (/etc/ssh/sshd\_config) was modified to allow root login and password authentication.

**Configuration Changes:**

PermitRootLogin yes

PasswordAuthentication yes



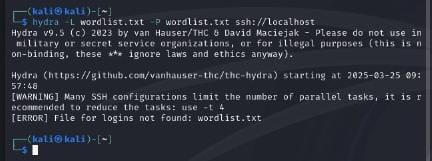
# 4. Exploitation

## 4.1 Brute-Force Attack

A brute-force attack was performed using Hydra to exploit the weak SSH configuration. The attack successfully identified a valid password for the user alan.

**Commands Used:**

hydra -l alan -P wordlist.txt ssh://localhost



# 5. Mitigation

## 5.1 Disable Root Login and Password Authentication

The SSH configuration was updated to disable root login and password authentication, enforcing key-based authentication instead.

**Configuration Changes:**

PermitRootLogin no

PasswordAuthentication no

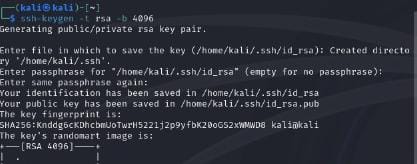


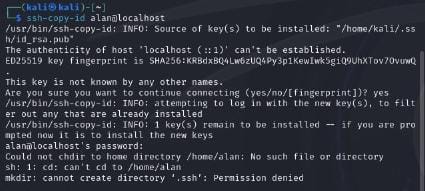
## 5.2 Enable Key-Based Authentication

Key-based authentication was set up by generating an SSH key pair and copying the public key to the authorized keys file.

**Commands used:**

ssh-keygen -t rsa -b 4096 ssh-copy-id alan@localhost





## 5.3 Verify Mitigation

After hardening the SSH configuration, attempts to log in as root or using a password were denied.

**Commands Used:**

ssh root@localhost



# 6. Conclusion

This PoC successfully demonstrated the risks of insecure SSH configurations and the effectiveness of hardening measures. By disabling root login, enforcing key-based authentication, and preventing brute-force attacks, the SSH service was secured.

## 7. Recommendations

* Regularly update SSH configurations to follow security best practices.
* Use tools like fail2ban to block repeated failed login attempts.
* Monitor SSH logs for suspicious activity.