**Proof of Concept (PoC) Report**

**Task 4: SUID Misconfigurations & Privilege Escalation**

# 1. Executive Summary

This PoC demonstrates the risks associated with SUID (Set User ID) misconfigurations, which can allow low-privileged users to escalate their privileges to root. The task involves setting up SUID misconfigurations, exploiting them to gain root access, and mitigating the risks by removing unnecessary SUID permissions.

**2. Objectives Setup:**

* Install and configure a basic web server (Apache) and disable the firewall.
* Exploit: Use nmap and netcat to scan for open ports and services.
* Mitigation: Restrict access using ufw and implement iptables rules to block unnecessary traffic.

# 3. Setup

**3.1 Set SUID Bit on /bin/bash**

The SUID bit was set on /bin/bash to allow any user executing it to run it with the permissions of the file owner (root).

**Commands Used:**

sudo chmod u+s /bin/bash



**3.2 Create a Script with SUID Permissions**

A script named script.sh was created and given SUID permissions to run with root privileges.

**Commands Used:**

echo "echo 'Running as root!'" > script.sh sudo chmod 4755 script.sh



# 4. Exploitation

**4.1 Identify SUID Misconfigurations**

The find command was used to identify files with SUID permissions.

**Commands Used:**

find / -perm -4000 2>/dev/null



**4.2 Escalate Privileges to Root**

The SUID misconfiguration on /bin/bash was exploited to escalate privileges to root.

**Commands Used:**

/bin/bash -p



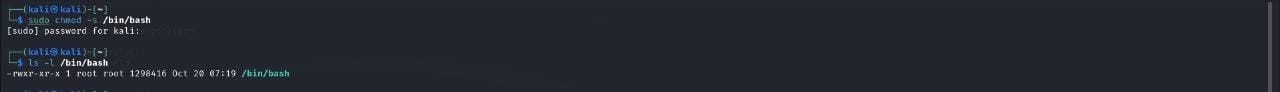
# 5. Mitigation

**5.1 Remove SUID Bit from /bin/bash**

The SUID bit was removed from /bin/bash to prevent privilege escalation.

**Commands Used:**

sudo chmod -s /bin/bash

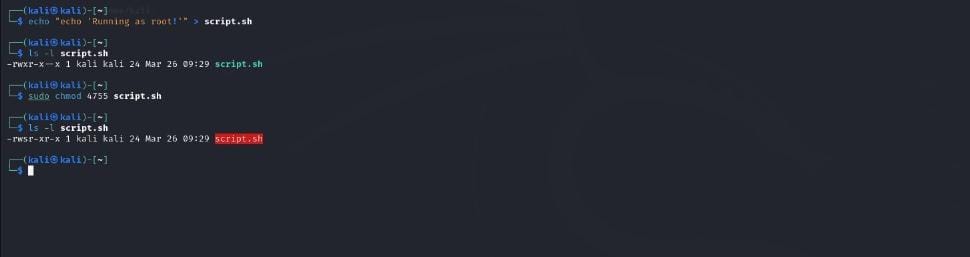


**5.2 Restrict Script Execution**

The script's permissions were modified to restrict execution to specific users.

**Commands Used:**

sudo chmod 750 script.sh sudo chown root:root script.sh



# 6. Conclusion

This PoC successfully demonstrated how SUID misconfigurations can lead to privilege escalation. By removing unnecessary SUID permissions and restricting script execution, the system was secured against such exploits.

# 7. Recommendations

* Regularly audit SUID/SGID files on the system.
* Remove SUID/SGID permissions from files that do not require them.
* Use tools like lynis or tripwire to monitor file permissions.