# Proof of Concept (PoC) Report

# Task 4: SUID Misconfigurations & Privilege Escalation

## **1. Overview**

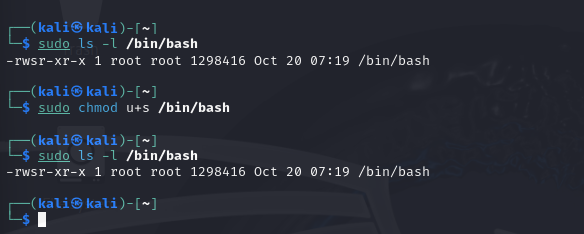
This Proof of Concept (PoC) report illustrates how misconfigured SUID (Set User ID) permissions can be exploited to gain unauthorized root access. The document provides a detailed walkthrough of discovering such vulnerabilities, escalating privileges, and implementing corrective actions to secure the system.

## **2. Understanding the Vulnerability**

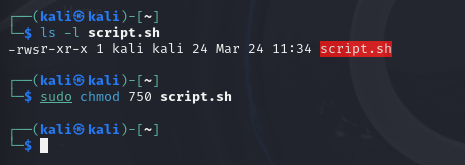
The SUID bit, when applied to an executable, allows it to run with the file owner's privileges instead of the user's. If misconfigured, this can lead to privilege escalation, where a standard user gains administrative control over the system.

## **3. Setting Up the Environment**

To replicate this security flaw, the following steps were performed:

**Applying the SUID bit to /bin/bash**

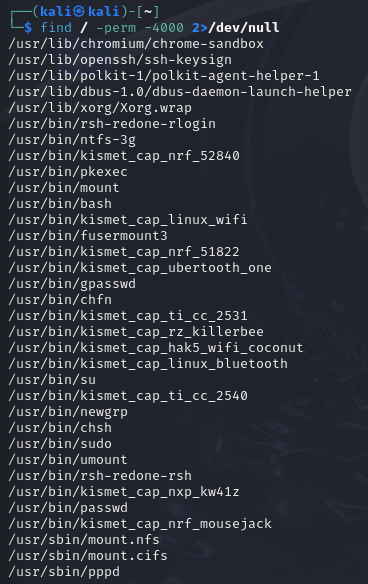
1. This modification enables any user running Bash to execute it with elevated privileges, which creates a security loophole.

**Creating a Privileged Script** 

## **4. Exploiting the Vulnerability**

### **Step 1: Locating SUID Misconfigurations**

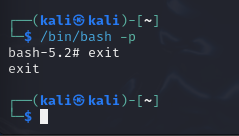
To identify files with SUID permissions, the following command is executed:



This scans the entire system for files that have the SUID bit set, suppressing error messages.

### **Step 2: Gaining Elevated Access via /bin/bash**

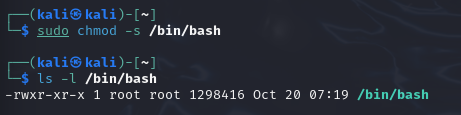
Upon discovering that /bin/bash has an SUID misconfiguration, privilege escalation can be achieved as follows:

****

The -p option ensures that the process retains its elevated privileges instead of dropping them.

## **5. Mitigating the Security Risk**

To prevent exploitation, implement these fixes:

**Disabling the SUID Bit on /bin/bash**

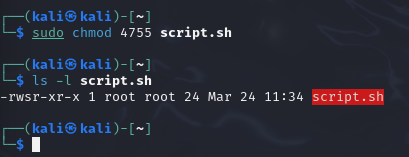
## 2. Restrict Script Execution

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 highlights how improperly configured SUID permissions can lead to privilege escalation. By removing unnecessary SUID settings and restricting script execution, such vulnerabilities can be effectively mitigated.