PROOF OF CONCEPT

LINUX SECURITY - EXPLOITATION & HARDENING

Task 4: SUID & 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 the SUID bit on /bin/bash, creating a script with root privileges, exploiting the misconfiguration, and then mitigating the issue by removing unnecessary SUID permissions and restricting script execution.

2. OBJECTIVES

- Setup: Set the SUID bit on /bin/bash and create a script running with root privileges.
- Exploit: Identify SUID misconfigurations using find and escalate privileges to root using /bin/bash -p.
- Mitigation: Remove unnecessary SUID permissions and restrict script execution to specific users.

3. SETUP

sudo chmod u+s /bin/bash ls -l /bin/bash echo -e "#!/bin/bash\necho 'Root Privileges Acquired'\nid" | sudo tee /root_script.sh # Create a script with root

privileges sudo chmod 4755 /root_script.sh ls -l /root_script.s

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod u+s /bin/bash
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ echo -e '#!/bin/bash\necho "You are root!"' > root_script.sh

┌──(kali㉿kali)-[~]
└─$ sudo chmod 4755 root_script.sh

┌──(kali㉿kali)-[~]
└─$ ls -l root_script.sh
-rwsr-xr-x 1 kali kali 33 Mar 25 21:40 root_script.sh
```

4) EXPLOIT

4.1) Find SUID misconfigurations:

```
┌──(kali㉿kali)-[~]
└─$ find / -perm -4000 2>/dev/null
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/chromium/chrome-sandbox

/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/bin/passwd
/usr/bin/mount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/fusermount3
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/umount
/usr/bin/chsh
/usr/bin/rsh-redone-rsh
/usr/bin/su
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/bash
/usr/bin/ntfs-3g
/usr/bin/kismet_cap_nrf_52840
/usr/bin/pkexec
/usr/bin/kismet_cap_nrf_mousejack
```

5) MITIGATION

5.1) Remove SUID:

5.2) Restrict script execution:

```
┌──(kali㉿kali)-[~]
└─$ chmod -s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted

┌──(kali㉿kali)-[~]
└─$ sudo chmod -s /bin/bash

┌──(kali㉿kali)-[~]
└─$ chmod 700 root_script.sh
```