PROOF OF CONCEPT

LINUX SECURITY - EXPLOITATION & HARDENING

Task 1: User & Permission Misconfigurations

1.EXECUTIVE SUMMARY

This PoC demonstrates how incorrect permissions on sensitive system files (e.g., /etc/shadow) can allow low-privileged users to access critical information. The task involves creating users, misconfiguring file permissions,exploiting the misconfiguration, and then mitigating the issue by restoring proper permissions and ownership.

2. OBJECTIVES

- **Setup: Create users and assign incorrect permissions to sensitive files.**
- **Exploit: Demonstrate how a low-privileged user can access sensitive files.**
- **Mitigation: Fix the permission issues and prevent unauthorized access.**

3. SETUP

3.1. Create Multiple Users

Two users, user1 and user2, were created using the useradd command, and passwords were assigned using the passwd command.

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd user1

┌──(kali㉿kali)-[~]
└─$ sudo useradd user2

┌──(kali㉿kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

3.2. Assign Incorrect Permissions

The permissions for the /etc/shadow file were changed to 777 (read, write, and execute for everyone), making it accessible to all users.

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 777 /etc/shadow

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3378 Mar 25 20:04 /etc/passwd

┌──(kali㉿kali)-[~]
└─$ sudo chmod 777 /etc/passwd

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd
-rwxrwxrwx 1 root root 3378 Mar 25 20:04 /etc/passwd
```

4. EXPLOITATION

4.1. Access Sensitive File as Low-Privileged User

```
┌──(kali㉿kali)-[/home/kali]
└─PS> su - user1
Password:
$ cat /etc/shadow
root:!:20171:0:99999:7:::
daemon:*:20171:0:99999:7:::
bin:*:20171:0:99999:7:::
sys:*:20171:0:99999:7:::
sync:*:20171:0:99999:7:::
games:*:20171:0:99999:7:::
man:*:20171:0:99999:7:::
lp:*:20171:0:99999:7:::
mail:*:20171:0:99999:7:::
news:*:20171:0:99999:7:::
uucp:*:20171:0:99999:7:::
proxy:*:20171:0:99999:7:::
www-data:*:20171:0:99999:7:::
backup:*:20171:0:99999:7:::
list:*:20171:0:99999:7:::
irc:*:20171:0:99999:7:::
_apt:*:20171:0:99999:7:::
nobody:*:20171:0:99999:7:::
systemd-network:!*:20171::::::
```

5. MITIGATION

Fix Permission Issues & Secure Privileges

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 640 /etc/shadow
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo chmod 644 /etc/shadow

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd /etc/passwd
-rwxrwxrwx 1 root root 3378 Mar 25 20:04 /etc/passwd
-rwxrwxrwx 1 root root 3378 Mar 25 20:04 /etc/passwd
```