POC TASKS

TASK 1: User & Permission Misconfigurations

1.1) Create Multiple Users

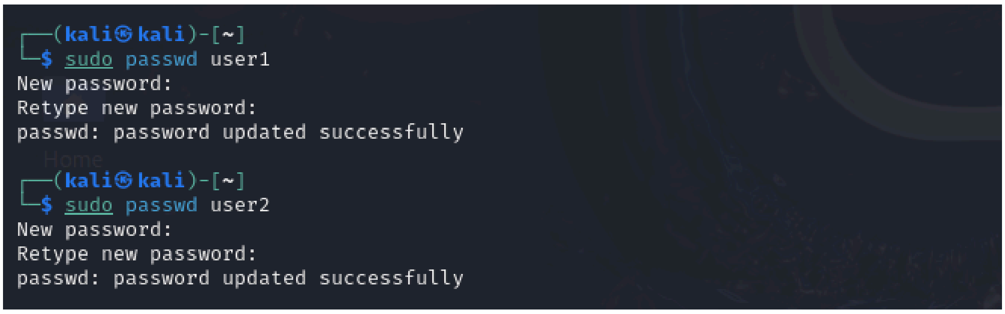
create user1 and user2:

sudo useradd -m user1

sudo useradd -m user2

sudo passwd user1 # Set password

sudo passwd user2 # Set password



```
┌──(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
```

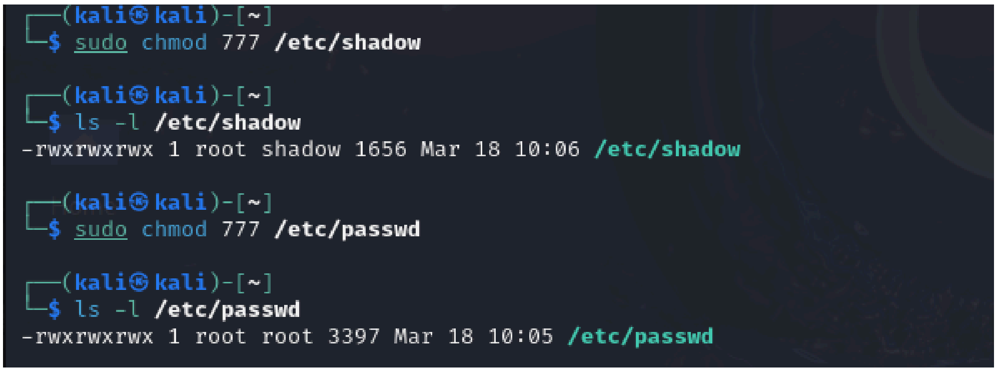
1.2) Assign Incorrect Permissions to Sensitive Files

»Make system files world-readable

sudo chmod 777 /etc/shadow

sudo chmod 777 /etc/passwd

ls -l /etc/shadow /etc/passwd



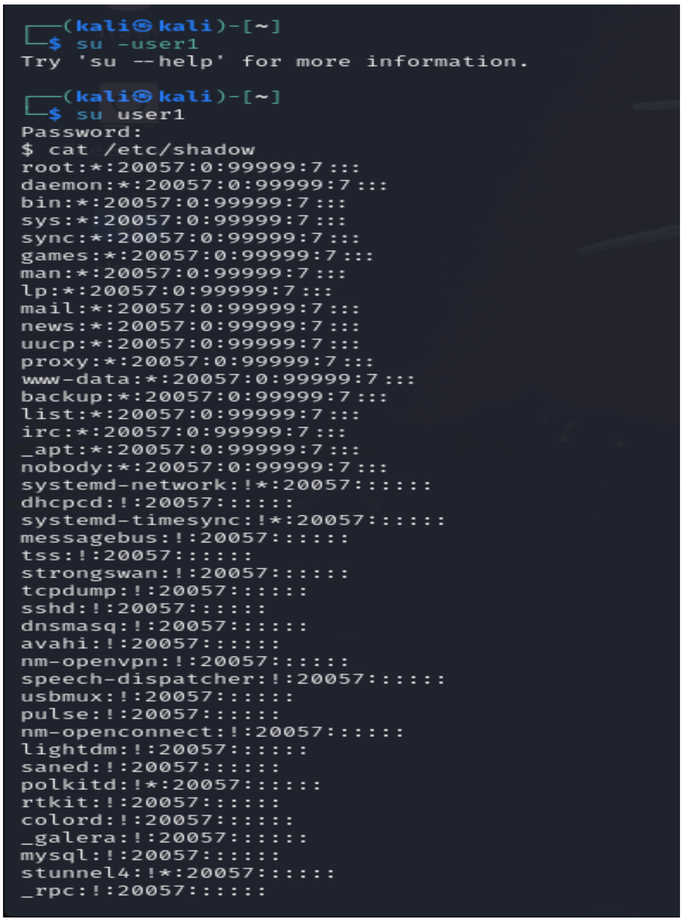
```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 777 /etc/shadow

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/shadow
-rwxrwxrwx 1 root shadow 1656 Mar 18 10:06 /etc/shadow

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

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd
-rwxrwxrwx 1 root root 3397 Mar 18 10:05 /etc/passwd
```

- Now, Any user can now read and modify password hashes.

1.3) Exploit: Access Sensitive System Files as Low-Privileged User

1.3.1) Switch to user1 (Low Privilege User)

su - user1

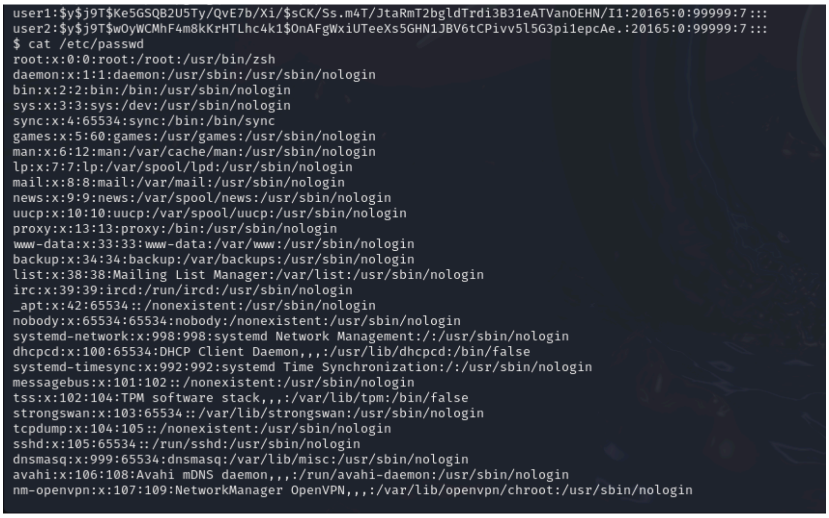


```
┌──(kali㉿kali)-[~]
└─$ su -user1
Try 'su --help' for more information.

┌──(kali㉿kali)-[~]
└─$ su user1
Password:
$ cat /etc/shadow
root:*:20057:0:99999:7:::
daemon:*:20057:0:99999:7:::
bin:*:20057:0:99999:7:::
sys:*:20057:0:99999:7:::
sync:*:20057:0:99999:7:::
games:*:20057:0:99999:7:::
man:*:20057:0:99999:7:::
lp:*:20057:0:99999:7:::
mail:*:20057:0:99999:7:::
news:*:20057:0:99999:7:::
uucp:*:20057:0:99999:7:::
proxy:*:20057:0:99999:7:::
www-data:*:20057:0:99999:7:::
backup:*:20057:0:99999:7:::
list:*:20057:0:99999:7:::
irc:*:20057:0:99999:7:::
_apt:*:20057:0:99999:7:::
nobody:*:20057:0:99999:7:::
systemd-network:!*:20057::::::
dhcpcd:!:20057::::::
systemd-timesync:!*:20057::::::
messagebus:!:20057::::::
tss:!:20057::::::
strongswan:!:20057::::::
tcpdump:!:20057::::::
sshd:!:20057::::::
dnsmasq:!:20057::::::
avahi:!:20057::::::
nm-openvpn:!:20057::::::
speech-dispatcher:!:20057::::::
usbmux:!:20057::::::
pulse:!:20057::::::
nm-openconnect:!:20057::::::
lightdm:!:20057::::::
saned:!:20057::::::
polkitd:!*:20057::::::
rtkit:!:20057::::::
colord:!:20057::::::
_galera:!:20057::::::
mysql:!:20057::::::
stunnel4:!*:20057::::::
_rpc:!:20057::::::
```

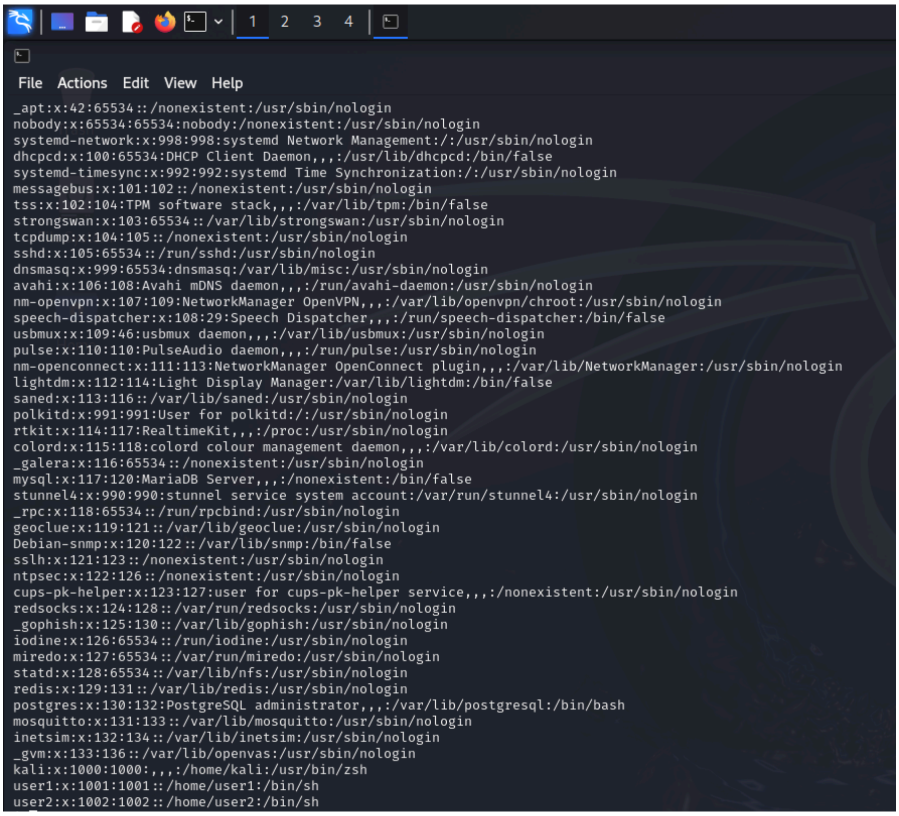
1.3.2) Now, as user1, try accessing the system files:

cat /etc/shadow

cat /etc/passwd



```
user1:$y$j9T$Ke5GSQB2U5Ty/QvE7b/Xi/$sCK/Ss.m4T/JtaRmT2bgldTrdi3B31eATVanOEHN/I1:20165:0:99999:7:::
user2:$y$j9T$wOyWCMhF4m8kKrHTLhc4k1$OnAFgWxiUTeeXs5GHN1JBV6tCPivv5l5G3pi1epcAe.:20165:0:99999:7:::
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```



```
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
pulse:x:110:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
nm-openconnect:x:111:113:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
lightdm:x:112:114:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
rtkit:x:114:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:115:118:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
_galera:x:116:65534::/nonexistent:/usr/sbin/nologin
mysql:x:117:120:MariaDB Server,,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:118:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:119:121::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:120:122::/var/lib/snmp:/bin/false
sslh:x:121:123::/nonexistent:/usr/sbin/nologin
ntpsec:x:122:126::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:123:127:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
redsocks:x:124:128::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:125:130::/var/lib/gophish:/usr/sbin/nologin
iodine:x:126:65534::/run/iodine:/usr/sbin/nologin
miredo:x:127:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:128:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:129:131::/var/lib/redis:/usr/sbin/nologin
postgres:x:130:132:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mosquitto:x:131:133::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:132:134::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:133:136::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
user1:x:1001:1001::/home/user1:/bin/sh
user2:x:1002:1002::/home/user2:/bin/sh
```

1.4) Mitigation: Fix Permission Issues & Secure Privileges

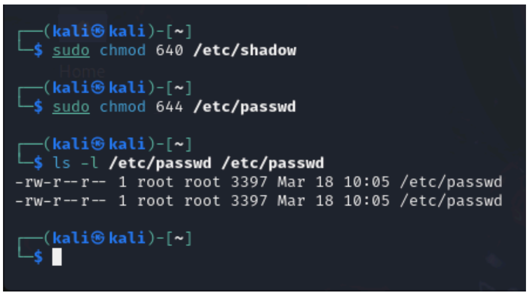
1.4.1) Restrict Permissions on System Files

Switch back to root and fix permissions:

sudo chmod 640 /etc/shadow

sudo chmod 644 /etc/passwd

ls -l /etc/shadow /etc/passwd



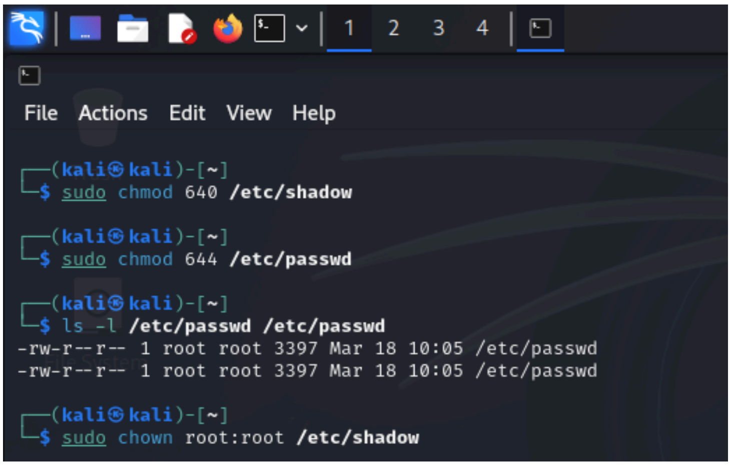
```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 640 /etc/shadow

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

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd /etc/passwd
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd

┌──(kali㉿kali)-[~]
└─$ 
```

Fixes:
/etc/shadow is now only readable by root.
/etc/passwd is world-readable but not writable.

1.4.1)Use chown to Assign Proper Ownership

Ensure system files are owned by root:

sudo chown root:root /etc/shadow
sudo chown root:root /etc/passwd



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

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

┌──(kali㉿kali)-[~]
└─$ ls -l /etc/passwd /etc/passwd
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd

┌──(kali㉿kali)-[~]
└─$ sudo chown root:root /etc/shadow
```

Fixes: Only root can modify these files.
