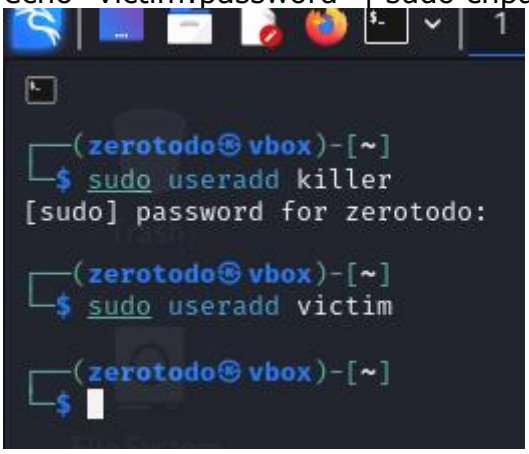
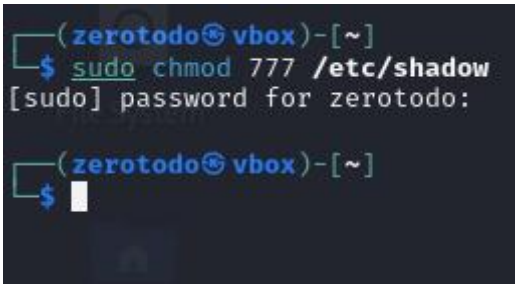
Tasks List For POC
PoC Task List: Linux Security - Exploitation & Hardening
Task 1: User & Permission Misconfigurations
Setup:

- Create multiple users (useradd , passwd).
  sudo useradd killer
  sudo useradd victim
  echo "attacker:password" | sudo chpasswd
  echo "victim:password" | sudo chpasswd



The attacker user will be used to exploit the misconfiguration.
The victim user is a normal system user.

- Assign incorrect permissions to sensitive files (chmod 777 /etc/shadow).
  sudo chmod 777 /etc/shadow
  sudo chmod 777 /etc/passwd



chmod 777 makes the files readable, writable, and executable by all users, which is a major security risk.
/etc/shadow contains hashed passwords, while /etc/passwd stores user account details.
✅ Exploit:
Demonstrate how a low-privileged user can access sensitive system files (e.g., /etc/passwd , /etc/shadow).

1. Switch to the attacker user:
   su attacker
   Attempt to read sensitive files

   cat /etc/shadow
   cat /etc/passwd

```
┌──(zerotodo㉿vbox)-[~]
└─$ su killer
Password:
$ cat/etc/shadow
sh: 1: cat/etc/shadow: Permission denied
$ cat /etc/shadow
root:!:20127:0:99999:7:::
daemon:*:20127:0:99999:7:::
bin:*:20127:0:99999:7:::
sys:*:20127:0:99999:7:::
sync:*:20127:0:99999:7:::
games:*:20127:0:99999:7:::
man:*:20127:0:99999:7:::
lp:*:20127:0:99999:7:::
mail:*:20127:0:99999:7:::
news:*:20127:0:99999:7:::
uucp:*:20127:0:99999:7:::
proxy:*:20127:0:99999:7:::
www-data:*:20127:0:99999:7:::
backup:*:20127:0:99999:7:::
list:*:20127:0:99999:7:::
irc:*:20127:0:99999:7:::
_apt:*:20127:0:99999:7:::
nobody:*:20127:0:99999:7:::
systemd-network:!*:20127::::::
dhcpcd:!:20127::::::
_galera:!:20127::::::
mysql:!:20127::::::
tss:!:20127::::::
strongswan:!:20127::::::
systemd-timesync:!*:20127::::::
_gophish:!:20127::::::
iodine:!:20127::::::
messagebus:!:20127::::::
tcpdump:!:20127::::::
miredo:!:20127::::::
_rpc:!:20127::::::
redis:!:20127::::::
mosquitto:!:20127::::::
redsocks:!:20127::::::
stunnel4:!*:20127::::::
sshd:!:20127::::::
dnsmasq:!:20127::::::
Debian-snmp:!:20127::::::
sslh:!:20127::::::
postgres:!:20127::::::
avahi:!:20127::::::
nm-openvpn:!:20127::::::
_gvm:!:20127::::::
speech-dispatcher:!:20127::::::
usbmux:!:20127::::::
cups-pk-helper:!:20127::::::
inetsim:!:20127::::::
```

Mitigation:

- Fix permission issues using `chmod`, `chown`.

  1. Restore correct permissions:

     sudo chmod 640 /etc/shadow

     sudo chmod 644 /etc/passwd

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

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

┌──(zerotodo㉿vbox)-[~]
└─$
```

2. Ensure proper file ownership:
   sudo chown root:shadow /etc/shadow
   sudo chown root:root /etc/passwdwd

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

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

┌──(zerotodo㉿vbox)-[~]
└─$
```

3.Secure sudo privileges using visudo:
   sudo /etc/passwdwd

```
┌──(zerotodo㉿vbox)-[~]
└─$ su killer
Password:
$ sudo /etc/passwd
[sudo] password for killer:
killer is not in the sudoers file.
$
```

- Limit sudo access only to trusted users.

  Remove unnecessary NOPASSWD entries.

Conclusion

This PoC highlights the dangers of misconfigured file permissions and how an attacker can exploit them. Proper file permissions, ownership settings, and sudo configuration are crucial for Linux system security.