

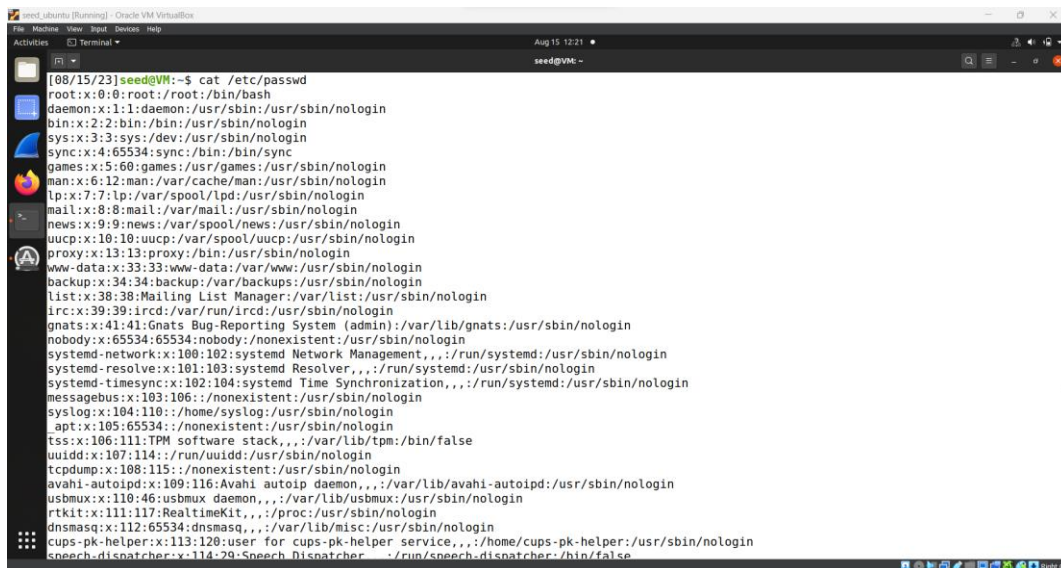
## LAB 5

### Secure Coding Lab

Ananthanarayanan S

CB.EN.P2CYS23007

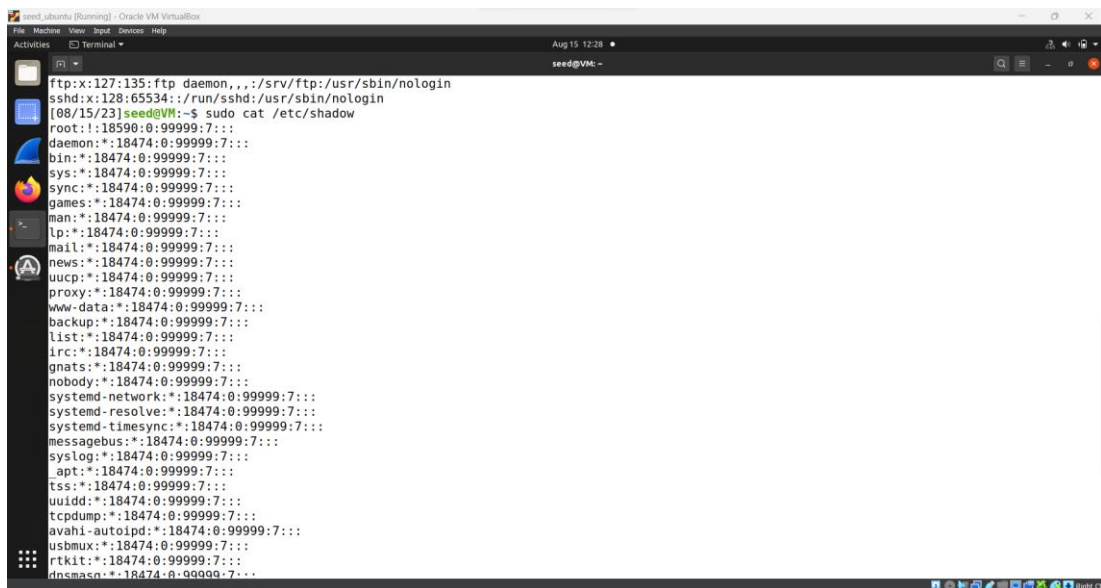
#### User information



```
[08/15/23]seed@VM:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/:/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:114:/:run/uidd:/usr/sbin/nologin
tcpdump:x:108:115:/:nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
```

Every user is listed in this line

#### Password information



```
[08/15/23]seed@VM:~$ sudo cat /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autoipd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
```

display the permission ,ownership size and timestamp

```
[08/15/23]seed@VM:~$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root 2886 Nov 24 2020 /etc/passwd
-rw-r----- 1 root shadow 1514 Nov 24 2020 /etc/shadow
```

---

user id, group id and group information

```
[08/15/23]seed@VM:~$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugindev),120(lpadmin),131(lxd),132(sambashare),136(docke
r)
```

---

## ADD USER

```
[08/15/23]seed@VM:~$ sudo adduser bob
Adding user `bob' ...
Adding new group `bob' (1001) ...
Adding new user `bob' (1001) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for bob
Enter the new value, or press ENTER for the default
  Full Name []: bob
  Room Number []: 1
  Work Phone []: 7874874949
  Home Phone []: 3977585755
  Other []:
Is the information correct? [Y/n] y
[08/15/23]seed@VM:~$
```

---

## Switch user

```
[08/15/23]seed@VM:~$ su bob
Password:
bob@VM: /home/seed$
```

---

## id

```
bob@VM: /home/seed$ id
uid=1001(bob) gid=1001(bob) groups=1001(bob)
```

---

## Change password

```
bob@VM: /home/seed$ passwd
Changing password for bob.
Current password:
New password:
Retype new password:
You must choose a longer password
New password:
Retype new password:
Bad: new and old password are too similar
New password:
Retype new password:
passwd: password updated successfully
```

---

```
bob@VM:/home/seed$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root 2950 Aug 15 13:02 /etc/passwd
-rw-r----- 1 root shadow 1644 Aug 15 13:08 /etc/shadow
bob@VM:/home/seed$
```

---

```
bob@VM:/home/seed$ sudo cat/etc/shadow
[sudo] password for bob:
Sorry, try again.
[sudo] password for bob:
Sorry, try again.
[sudo] password for bob:
bob is not in the sudoers file. This incident will be reported.
```

---

### Groups

```
bob@VM:/home/seed$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,seed
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:seed
floppy:x:25:
tape:x:26:
sudo:x:27:seed
audio:x:29:pulse
dip:x:30:seed
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
```

---

## Accesses control

```
bob@VM:/home/seed$ ls -l
total 76
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Desktop
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Documents
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Downloads
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Music
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Pictures
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Public
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Templates
drwxr-xr-x 2 seed seed 4096 Nov 24 2020 Videos
bob@VM:/home/seed$ ls -l mycat
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
bob@VM:/home/seed$ chmod +x mycat
chmod: changing permissions of 'mycat': Operation not permitted
bob@VM:/home/seed$ chmod 4755 mycat
chmod: changing permissions of 'mycat': Operation not permitted
bob@VM:/home/seed$ sudo chmod +x mycat
[sudo] password for bob:
bob is not in the sudoers file. This incident will be reported.
bob@VM:/home/seed$ sudo chmod 4755 mycat
[sudo] password for bob:
bob is not in the sudoers file. This incident will be reported.
bob@VM:/home/seed$ su seed
Password:
[08/15/23]seed@VM:~$ sudo chmod +x mycat
[08/15/23]seed@VM:~$ ls -l mycat
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
[08/15/23]seed@VM:~$ █
```

---

## Permissions on directories

```
[08/15/23]seed@VM:~$ ls -l Pictures
total 0
[08/15/23]seed@VM:~$ ls -l mycat
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
```

---

## Default permissions

```
[08/15/23]seed@VM:~$ umask
0002
[08/15/23]seed@VM:~$ touch mycat && ls -l mycat
touch: cannot touch 'mycat': Permission denied
[08/15/23]seed@VM:~$ umask
0002
[08/15/23]seed@VM:~$ touch myca && ls -l mycat
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
[08/15/23]seed@VM:~$ umask 0077
[08/15/23]seed@VM:~$ umask
0077
[08/15/23]seed@VM:~$ touch nee && ls -l new
ls: cannot access 'new': No such file or directory
[08/15/23]seed@VM:~$ touch nee && ls -l nee
-rw----- 1 seed seed 0 Aug 15 13:59 nee
[08/15/23]seed@VM:~$ █
```

---

Change ownership:

```
[08/15/23]seed@VM:~$ ls -l mycat
-rwsr-xr-x 1 4755 seed 43416 Aug 14 06:09 mycat
[08/15/23]seed@VM:~$ sudo chown bob mycat
[08/15/23]seed@VM:~$ ls -l mycat
-rwxr-xr-x 1 bob seed 43416 Aug 14 06:09 mycat
[08/15/23]seed@VM:~$
```

---

#### Full Access Control

```
[08/15/23]seed@VM:~$ getfacl mycat
# file: mycat
# owner: bob
# group: seed
user::rwx
group::r-x
other::r-x

[08/15/23]seed@VM:~$ setfacl -m user:bob:r mycat
setfacl: mycat: Operation not permitted
[08/15/23]seed@VM:~$ sudo setfacl -m user:bob:r mycat
[08/15/23]seed@VM:~$ getfacl mycat
# file: mycat
# owner: bob
# group: seed
user::rwx
user:bob:r--
group::r-x
mask::r-x
other::r-x
```

---

#### Run command as another user

```
[08/15/23]seed@VM:~$ whoami
seed
[08/15/23]seed@VM:~$ sudo -u bob whoami
bob
```

---

#### superuser privileges

```
[08/15/23]seed@VM:~$ sudo head /etc/shadow
root!:18590:0:99999:7:::
daemon*:18474:0:99999:7:::
bin*:18474:0:99999:7:::
sys*:18474:0:99999:7:::
sync*:18474:0:99999:7:::
games*:18474:0:99999:7:::
man*:18474:0:99999:7:::
lp*:18474:0:99999:7:::
mail*:18474:0:99999:7:::
news*:18474:0:99999:7:::
```

---

## Sudo configuration file

```
[08/15/23]seed@VM:~$ sudo head /etc/shadow
root!!:18590:0:99999:7:::
daemon*:18474:0:99999:7:::
bin*:18474:0:99999:7:::
sys*:18474:0:99999:7:::
sync*:18474:0:99999:7:::
games*:18474:0:99999:7:::
man*:18474:0:99999:7:::
lp*:18474:0:99999:7:::
mail*:18474:0:99999:7:::
news*:18474:0:99999:7:::
[08/15/23]seed@VM:~$ sudo cat/etc/sudoers
sudo: cat/etc/sudoers: command not found
[08/15/23]seed@VM:~$ su bob
Password:
bob@VM:/home/seed$ sude head /etc/shadow

Command 'sude' not found, did you mean:

  command 'sudo' from deb sudo (1.8.31-1ubuntu1.5)
  command 'sudo' from deb sudo-ldap (1.8.31-1ubuntu1.5)

Try: apt install <deb name>

bob@VM:/home/seed$ sudo head /etc/shadow
[sudo] password for bob:
bob is not in the sudoers file. This incident will be reported.
bob@VM:/home/seed$ cat /etc/shadow | grep bob
cat: /etc/shadow: Permission denied
bob@VM:/home/seed$ cat /etc/group | grep bob
bob:x:1001:
bob@VM:/home/seed$ █
```

---