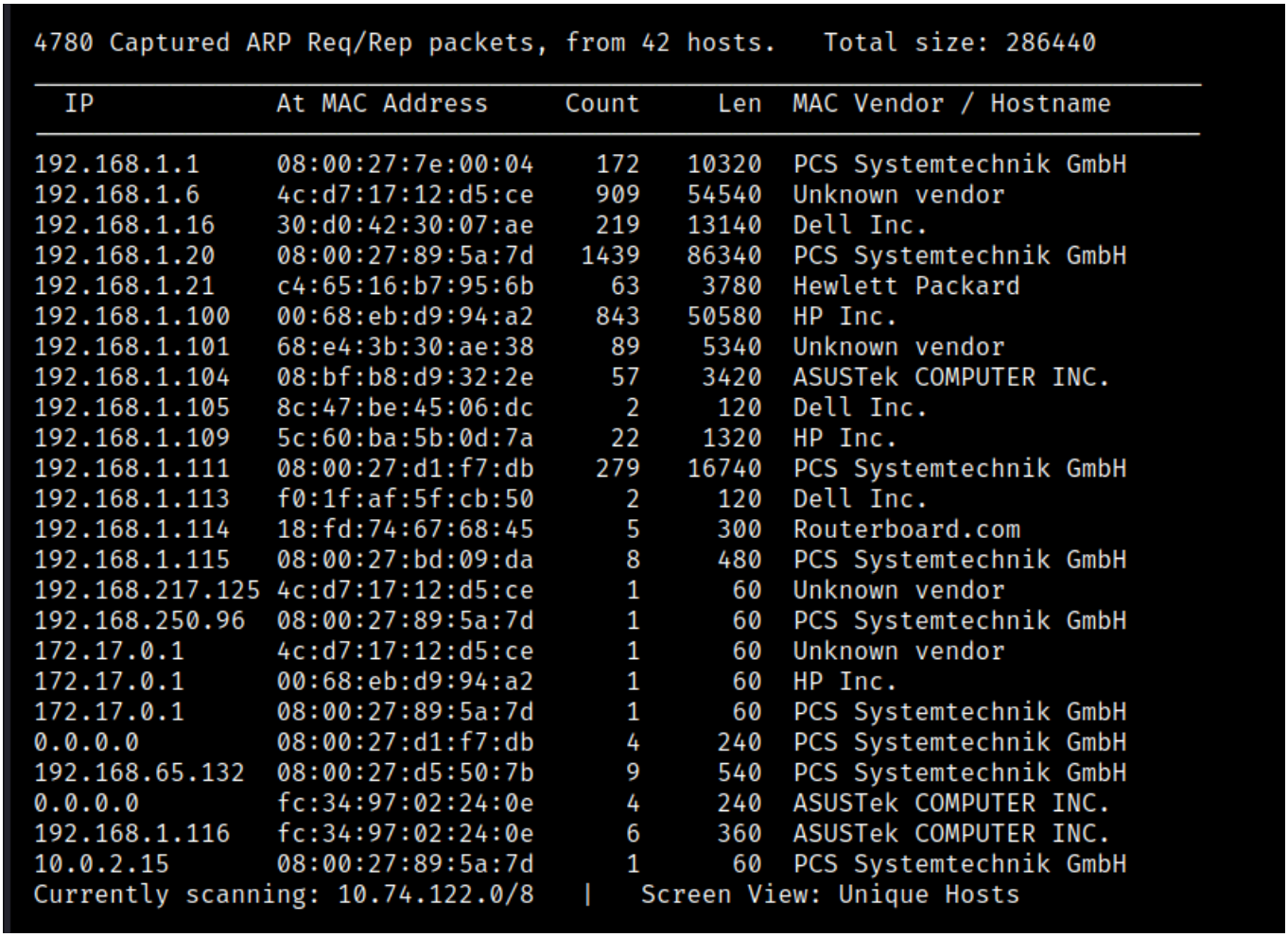
Informe del parcial III

Fase 1 Reconocimiento de las ips nivel general del pool 192.168.1.0/24



```
4780 Captured ARP Req/Rep packets, from 42 hosts.   Total size: 286440
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     08:00:27:7e:00:04    172   10320  PCS Systemtechnik GmbH
192.168.1.6     4c:d7:17:12:d5:ce    909   54540  Unknown vendor
192.168.1.16    30:d0:42:30:07:ae    219   13140  Dell Inc.
192.168.1.20    08:00:27:89:5a:7d   1439   86340  PCS Systemtechnik GmbH
192.168.1.21    c4:65:16:b7:95:6b     63    3780  Hewlett Packard
192.168.1.100   00:68:eb:d9:94:a2    843   50580  HP Inc.
192.168.1.101   68:e4:3b:30:ae:38     89    5340  Unknown vendor
192.168.1.104   08:bf:b8:d9:32:2e     57    3420  ASUSTek COMPUTER INC.
192.168.1.105   8c:47:be:45:06:dc      2     120  Dell Inc.
192.168.1.109   5c:60:ba:5b:0d:7a     22    1320  HP Inc.
192.168.1.111   08:00:27:d1:f7:db    279   16740  PCS Systemtechnik GmbH
192.168.1.113   f0:1f:af:5f:cb:50      2     120  Dell Inc.
192.168.1.114   18:fd:74:67:68:45      5     300  Routerboard.com
192.168.1.115   08:00:27:bd:09:da      8     480  PCS Systemtechnik GmbH
192.168.217.125 4c:d7:17:12:d5:ce      1      60  Unknown vendor
192.168.250.96  08:00:27:89:5a:7d      1      60  PCS Systemtechnik GmbH
172.17.0.1      4c:d7:17:12:d5:ce      1      60  Unknown vendor
172.17.0.1      00:68:eb:d9:94:a2      1      60  HP Inc.
172.17.0.1      08:00:27:89:5a:7d      1      60  PCS Systemtechnik GmbH
0.0.0.0         08:00:27:d1:f7:db      4     240  PCS Systemtechnik GmbH
192.168.65.132  08:00:27:d5:50:7b      9     540  PCS Systemtechnik GmbH
0.0.0.0         fc:34:97:02:24:0e      4     240  ASUSTek COMPUTER INC.
192.168.1.116   fc:34:97:02:24:0e      6     360  ASUSTek COMPUTER INC.
10.0.2.15       08:00:27:89:5a:7d      1      60  PCS Systemtechnik GmbH
Currently scanning: 10.74.122.0/8   |   Screen View: Unique Hosts
```

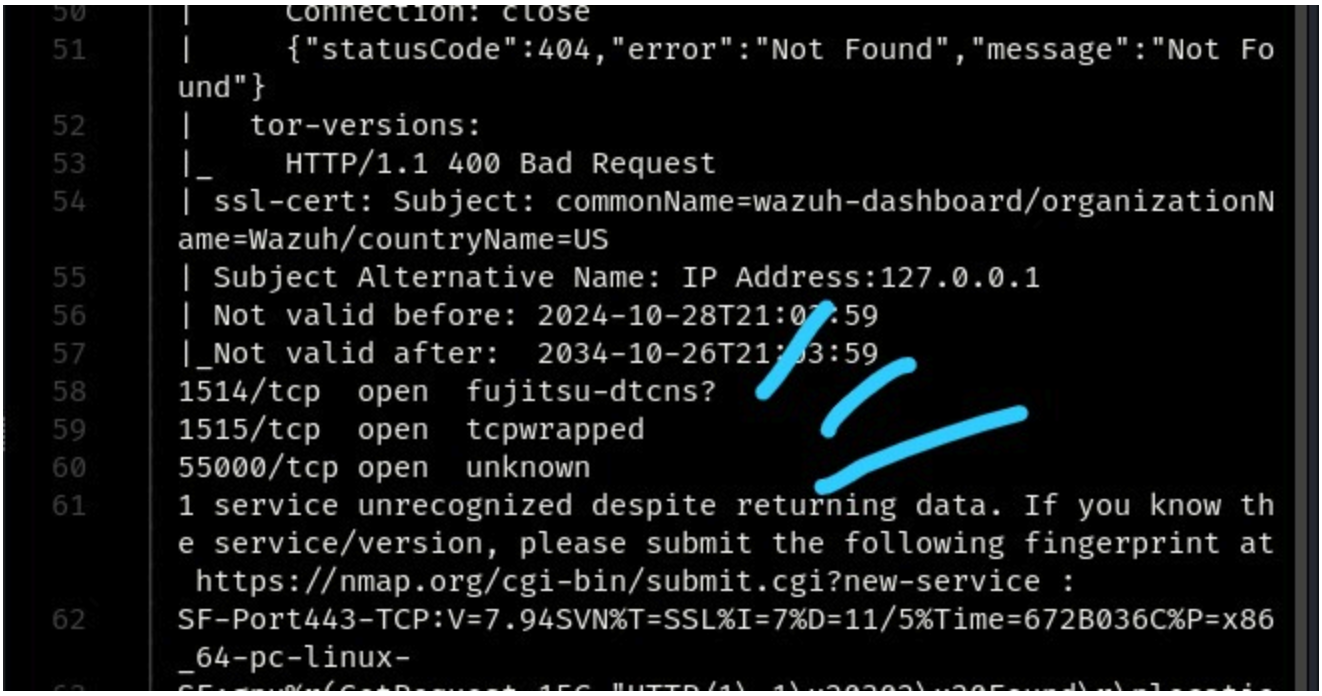
Fase 2 Enumeracion de Servicios

Como objetivo principal antes de enuemerar los servicios fue la deteccion del IDS wazuh los servicios y los puertos que usa wazuh son:
ssh 22
111 tcp

443 tcp

```
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 e9:a2:c9:c5:14:64:b7:d4:80:05:d7:07:a5:9a:8e:5a (RSA)
|_  256 86:3d:5d:26:eb:9b:05:9a:21:92:d4:01:ad:14:0d:05 (ECDSA)
111/tcp   open  rpcbind        2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
443/tcp   open  ssl/https
| http-title: Wazuh
|_Requested resource was /app/login?
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=wazuh-dashboard/organizationName=Wazuh/countryNa
| Subject Alternative Name: IP Address:127.0.0.1
| Not valid before: 2024-09-06T23:50:03
|_Not valid after:  2034-09-04T23:50:03
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, TL
|     HTTP/1.1 400 Bad Request
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     osd-name: wazuh-server
|     x-frame-options: sameorigin
|     content-type: application/json; charset=utf-8
|     cache-control: private, no-cache, no-store, must-revalidate
|     set-cookie: security_authentication=; Max-Age=0; Expires=Thu, 01 Jan 1970
|     content-length: 77
```

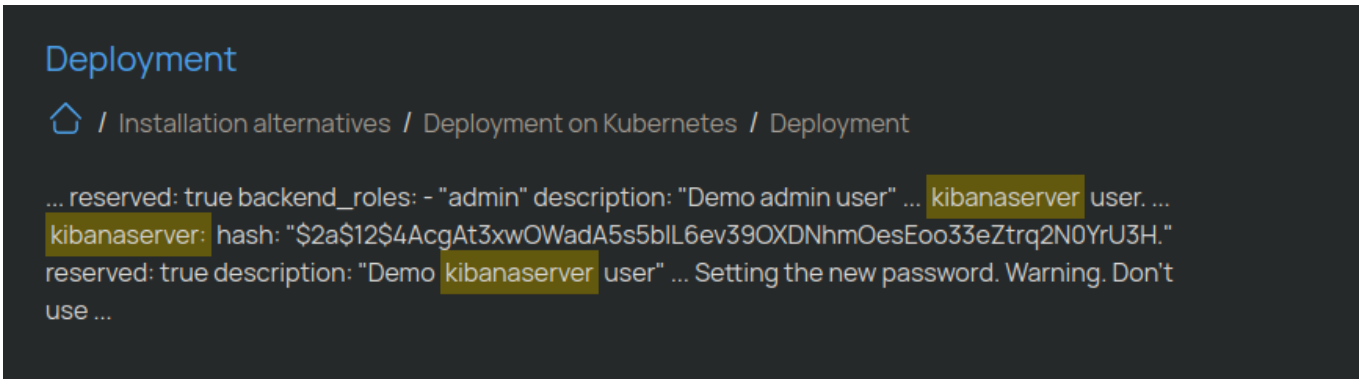
aparte wazuh tiene estos tres puertos, los agentes solo cuentan con solo uno puerto



Fase POC

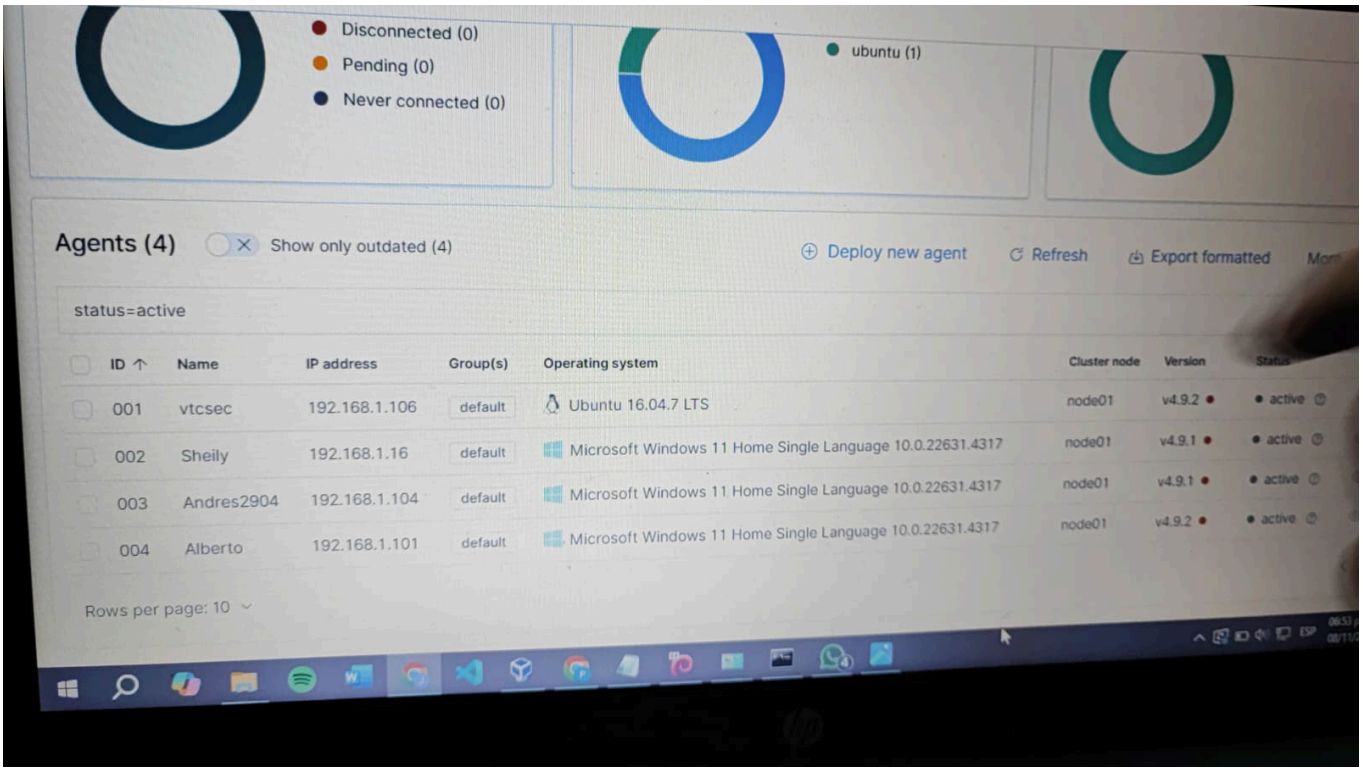
El servidor wazuh era la ip 192.168.1.111

otra desventaja que tuvieron el otro equipo que no conocian el IDS como tal existia de un segundo usuario.



Esta claro en la documentacion el usario kiabanaserver y wazuh-user>
https://documentation.wazuh.com/current/search.html?q=kibanaserver&check_keywords=yes&area=default

Es por eso que no era necesario hacer un ataque de fuerza bruta

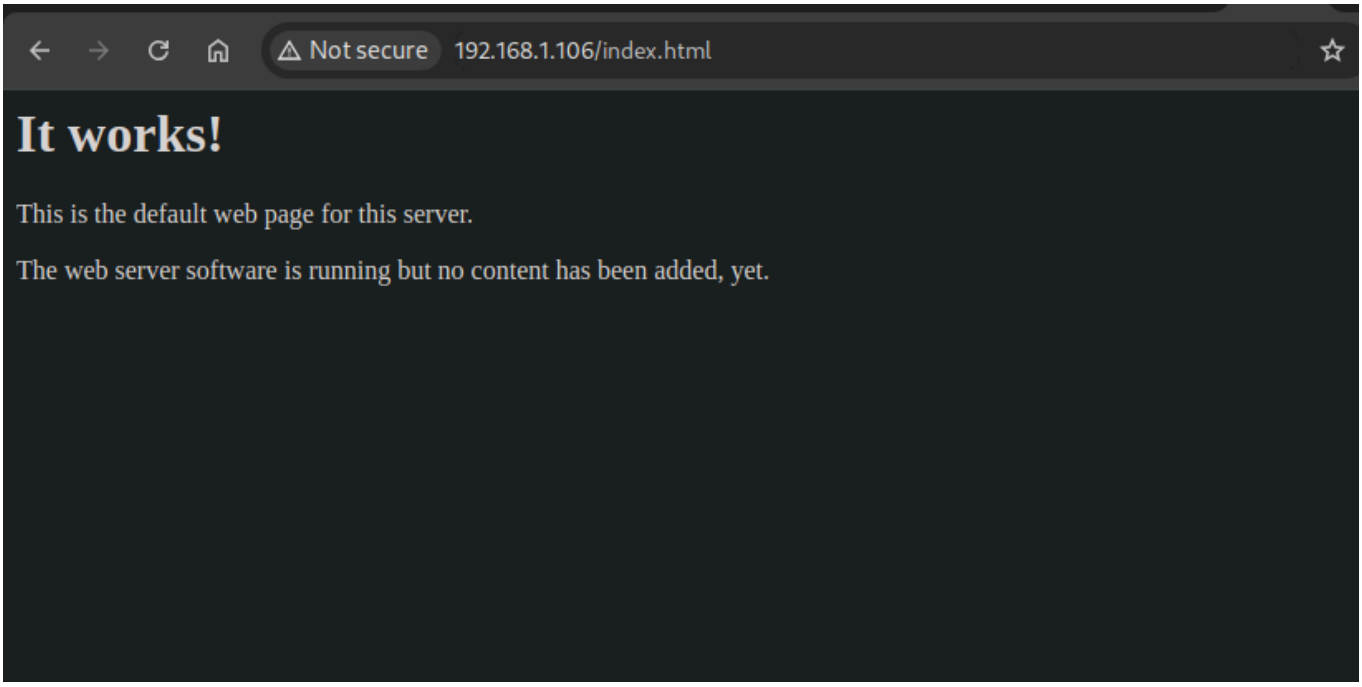


Con esta informacion ya no era necesario las demas ips que tambian habian maquinas virtuales.

El objetivo se estaba siendo bien claro que la maquina que estaban protegiendo era la linux ubuntu con la version 16

Se Escaneo de puertos al victima ubuntu y tenia los puertos
80,22,443, 21

Lo primero que se hizo es ver que tenia ese puerto 80 en el navegador



Despues toco enumeros recursos compartidos

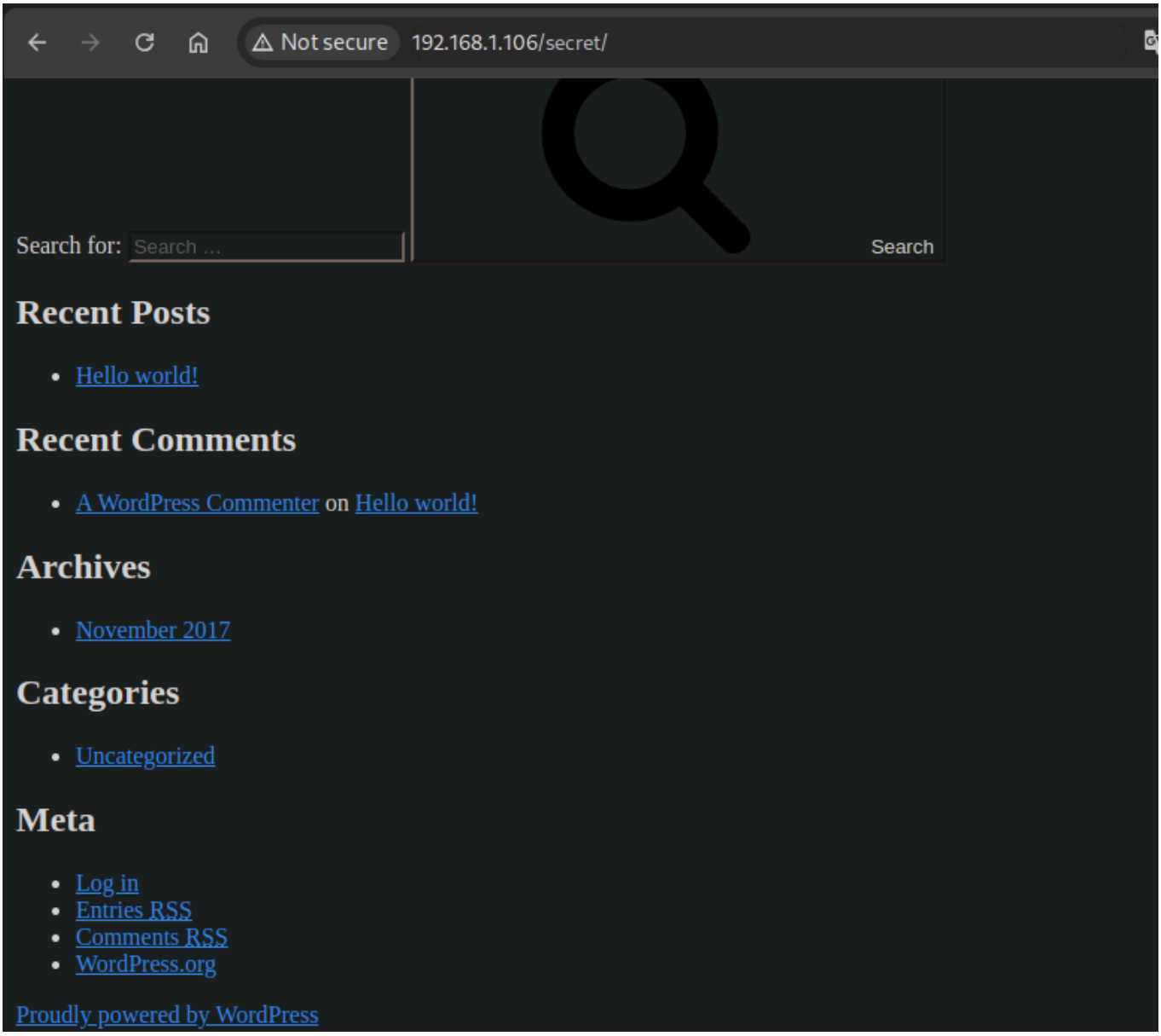
```
└─# wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt --hc 404 http://192.168.1.106/FUZZ

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.106/FUZZ
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        4 L      25 W       177 Ch      "http://192.168.1.106/"
000000013:   403        9 L      28 W       278 Ch      ".htpasswd"
000000012:   403        9 L      28 W       278 Ch      ".htaccess"
000000011:   403        9 L      28 W       278 Ch      ".hta"
000002020:   200        4 L      25 W       177 Ch      "index.html"
000003537:   301        9 L      28 W       315 Ch      "secret"
000003588:   403        9 L      28 W       278 Ch      "server-status"

Total time: 5.860579
Processed Requests: 4614
Filtered Requests: 4607
Requests/sec.: 787.2942
```

```
┌──(root㉿kali)-[/home/romeo188/tools]
└─# wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt -z list,.php,.html,.txt,.env --hc 404 http://192.168.1.106/FUZZFUZ2Z

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.106/FUZZFUZ2Z
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   403        9 L      28 W       278 Ch      ".php"
000000013:   403        9 L      28 W       278 Ch      ".htpasswd - .php"
000000012:   403        9 L      28 W       278 Ch      ".htaccess - .php"
000000011:   403        9 L      28 W       278 Ch      ".hta - .php"

Total time: 6.076519
Processed Requests: 4614
Filtered Requests: 4610
Requests/sec.: 759.3162
```

se uso otra herrienta para ver mas de los recursos

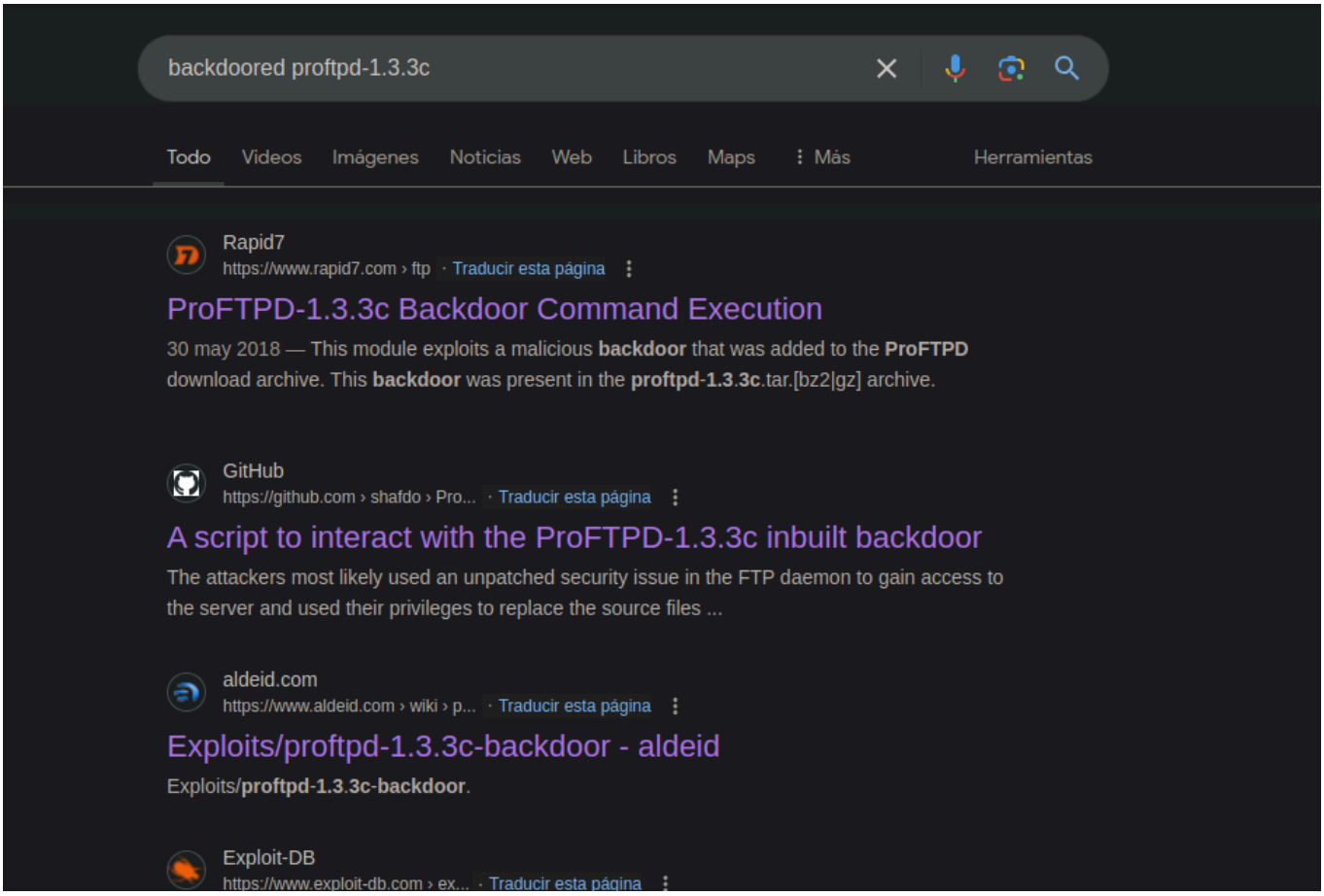
```
┌──(root㉿kali)-[/home/romeo188/tools]
└─# gobuster dir -u http://192.168.1.106 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.106
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/secret               (Status: 301) [Size: 315] [--> http://192.168.1.106/secret/]
/server-status        (Status: 403) [Size: 278]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

vemos que existe la ruta secret



Examinado la url el camino no era alli para la intrucion

El puerto 21 tenia una version deprecada que tenia una version de 1.3.3, toco investigar sobre ese servicio.



Descripcion de la vulneravilidad

El domingo 28 de noviembre de 2010, alrededor de las 20:00 UTC, el servidor de distribución principal del proyecto ProFTPD se vio comprometido. Los atacantes probablemente utilizaron un problema de seguridad no corregido en el demonio FTP para obtener acceso al servidor y utilizaron sus privilegios para reemplazar los archivos fuente de ProFTPD 1.3.3c con una versión que contenía una puerta trasera. La modificación no autorizada del código fuente fue detectada por Daniel Austin y transmitida al proyecto ProFTPD por Jeroen Geilman el miércoles 1 de diciembre, y corregida poco después.

Cualquiera que haya descargado ProFTPD 1.3.3c desde uno de los servidores de réplica oficiales entre el 28 de noviembre de 2010 y el 2 de diciembre de 2010 probablemente se verá afectado por el problema. La puerta trasera introducida por los atacantes permite a los usuarios no autenticados acceder remotamente como root a los sistemas que ejecutan la versión modificada maliciosamente del demonio ProFTPD.

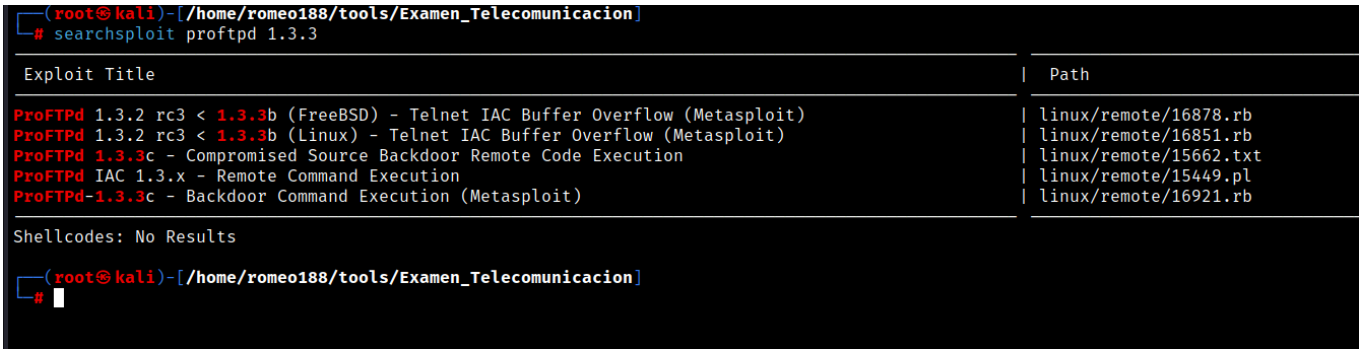
```
https://github.com/shafdo/ProFTPD-1.3.3c-
Backdoor_Command_Execution_Automated_Script.git
```

```
https://www.aldeid.com/wiki/Exploits/proftpd-1.3.3c-backdoor
```

Fase de LPE

La escalada de privilegios locales, cuando ya tienen acceso al sistema y estan intentando elevar permisos dentro del mismo.

para explotar la vulnerabilidad se uso searchsploit

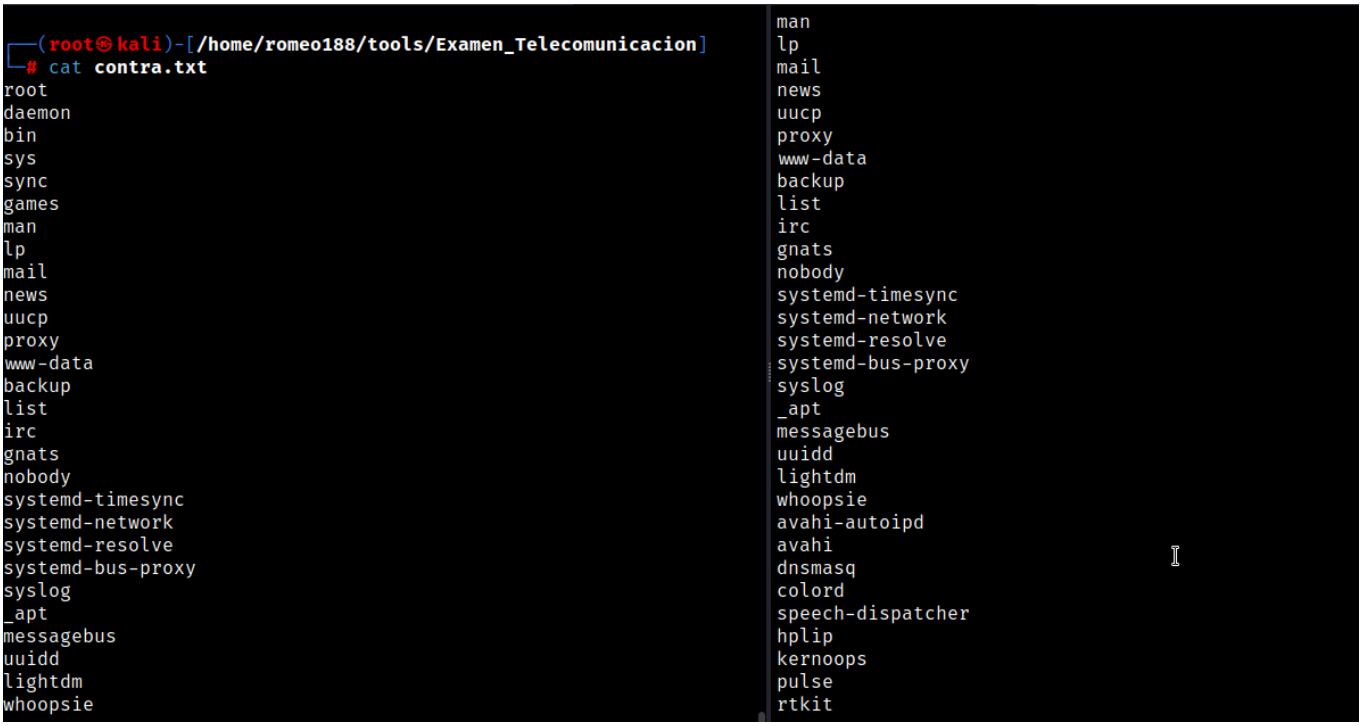


```
┌──(root㉿kali)-[/home/romeo188/tools/Examen_Telecomunicacion]
└─# searchsploit -m linux/remote/16921.rb
  Exploit: ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
      URL: https://www.exploit-db.com/exploits/16921
     Path: /usr/share/exploitdb/exploits/linux/remote/16921.rb
    Codes: OSVDB-69562
 Verified: True
File Type: Ruby script, ASCII text
Copied to: /home/romeo188/tools/Examen_Telecomunicacion/16921.rb


┌──(root㉿kali)-[/home/romeo188/tools/Examen_Telecomunicacion]
└─#
```

Con ese exploit uno ya podia ingresar como Root al servidor
se enumero las posibles contraseñas

```
# cat /etc/passwd
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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
```

en las ruta podemos listar las posibles contrañas y usuarios que se guardaron en dos archivos uno para los usuarios y el otro para las contraseñas , tambien se lista los grupos
cat /etc/passwd



para finalizar se escaneo los servidores de la ip 192.168.1.104 y 192.168.1.101 la 1.101 tenia estos servicios y puertos abiertos.

```
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5432/tcp  open  postgresql?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49683/tcp open  unknown
49684/tcp open  unknown
49685/tcp open  unknown
49686/tcp open  unknown
49687/tcp open  unknown
49688/tcp open  unknown
49791/tcp open  msrpc         Microsoft Windows RPC
6 services unrecognized despite returning data. If you know the service/versi
nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF:\0\t\0\r\xc8\r\0\x0f\0\x11\0\x13\0\x15\0\x17\0\x19\0\x1b\0\x1d\0\x1f\0
SF:);
MAC Address: 68:E4:3B:30:AE:38 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: ALBERTO, NetBIOS user: <unknown>, NetBIOS MAC: 68:e4:3b:30:ae:38 (unknown)
|_clock-skew: 1s
| smb2-time:
|   date: 2024-11-09T01:05:31
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov  8 19:05:46 2024 -- 1 IP address (1 host up) scanned in 174.54 seconds

        [*] Dirección IP: 192.168.1.101
        [*] Puertos abiertos: 135,139,445,5040,5357,5432,49664,49665,49668,49669,49670,49675,49683,49684,49685,49686,49687,49688,4979
1
```

La otra ip 1.104

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.0.30)
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.1.104/dashboard/
443/tcp  open  ssl/http      Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.0.30)
|_ssl-date: TLS randomness does not represent time
| http-title: Welcome to XAMPP
|_Requested resource was https://192.168.1.104/dashboard/
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| tls-alpn:
|_  http/1.1
3306/tcp open  mysql         MariaDB (unauthorized)
7680/tcp open  pando-pub?
9012/tcp open  ssl/websocket WebSocket++ 0.8.2
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=Peter Thorson/organizationName=Zaphoyd Studios/stateOrProvinceName
| Not valid before: 2011-11-15T21:20:06
|_Not valid after:  2012-11-14T21:20:06
9013/tcp open  websocket     WebSocket++ 0.8.2
9014/tcp open  websocket     WebSocket++ 0.8.1
MAC Address: 08:BF:B8:D9:32:2E (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov  8 18:56:29 2024 -- 1 IP address (1 host up) scanned in 48.34 seconds
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov  8 18:56:29 2024 -- 1 IP address (1 host up) scanned in 48.34 seconds

        [*] Dirección IP: 192.168.1.104
        [*] Puertos abiertos: 80,443,3306,7680,9012,9013,9014
```

Continuará . . . !