

SAD

UNIDAD 2 TAREA 0

***RECOPIACIÓN PASIVA DE INFORMACIÓN
UTILIZANDO GOOGLE HACKING Y SHODAN***



ÍNDICE

PARTE 1: GOOGLE HACKING.....	3
1.1. BÚSQUEDA EN GOOGLE.....	3
1.2. CONSULTA CON GOOGLE DORKS.....	7
PARTE 2: SHODAN.....	11
2.1 EXPLORACIÓN DE SHODAN.....	11
PARTE 3: RELFEXIÓN ÉTICA.....	17

PARTE 1: GOOGLE HACKING

1.1. BÚSQUEDA EN GOOGLE:

En esta parte, vamos a usar 5 búsquedas avanzadas al dominio de una empresa, con la intención de recopilar información de dicha empresa de forma pasiva, así como documentar y comentar los resultados obtenidos.

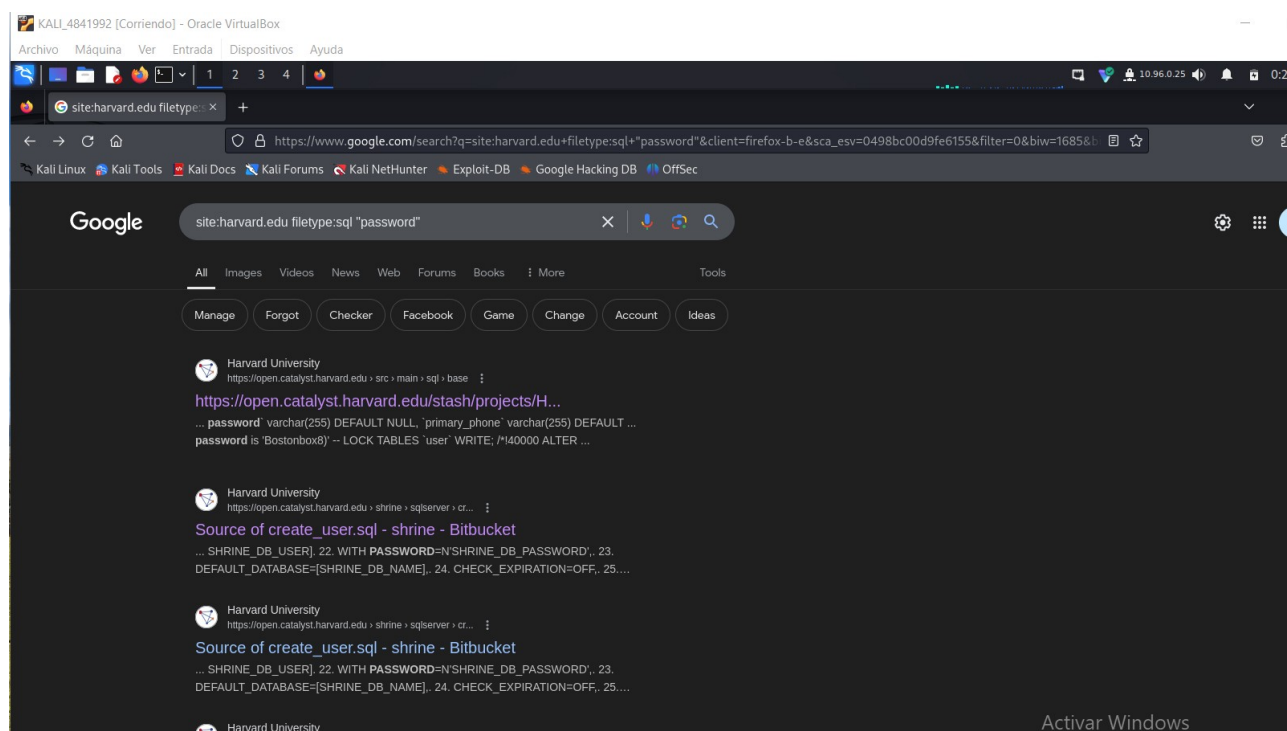
Yo voy a probar con Harvard, es una prestigiosa universidad americana. Es una universidad privada, por tanto técnicamente cuenta como empresa.

Toda esta práctica la estoy haciendo en una máquina virtual kali y usando Proton VPN.

Mi primer dork, es **site:harvard.edu** para buscar en el dominio de la universidad, **filetype:sql** para buscar bases de datos y **"password"** para que solo busque bases de datos sql con la palabra password (contraseña) a ver si encontramos alguna base de datos expuesta. El dork completo sería:

site:harvard.edu filetype:sql "password"

Este es el resultado:



El resto de enlaces no contienen nada interesante pero el primero nos lleva a lo que parece ser un backup de una base de datos:

Ver la Configuración para activar Wi-Fi

La contraseña sin encriptar es "Bostonbox8" a saber de qué porque no queda muy claro aquí. De todos modos esto es de 2015 obviamente estará obsoleto casi una década después.

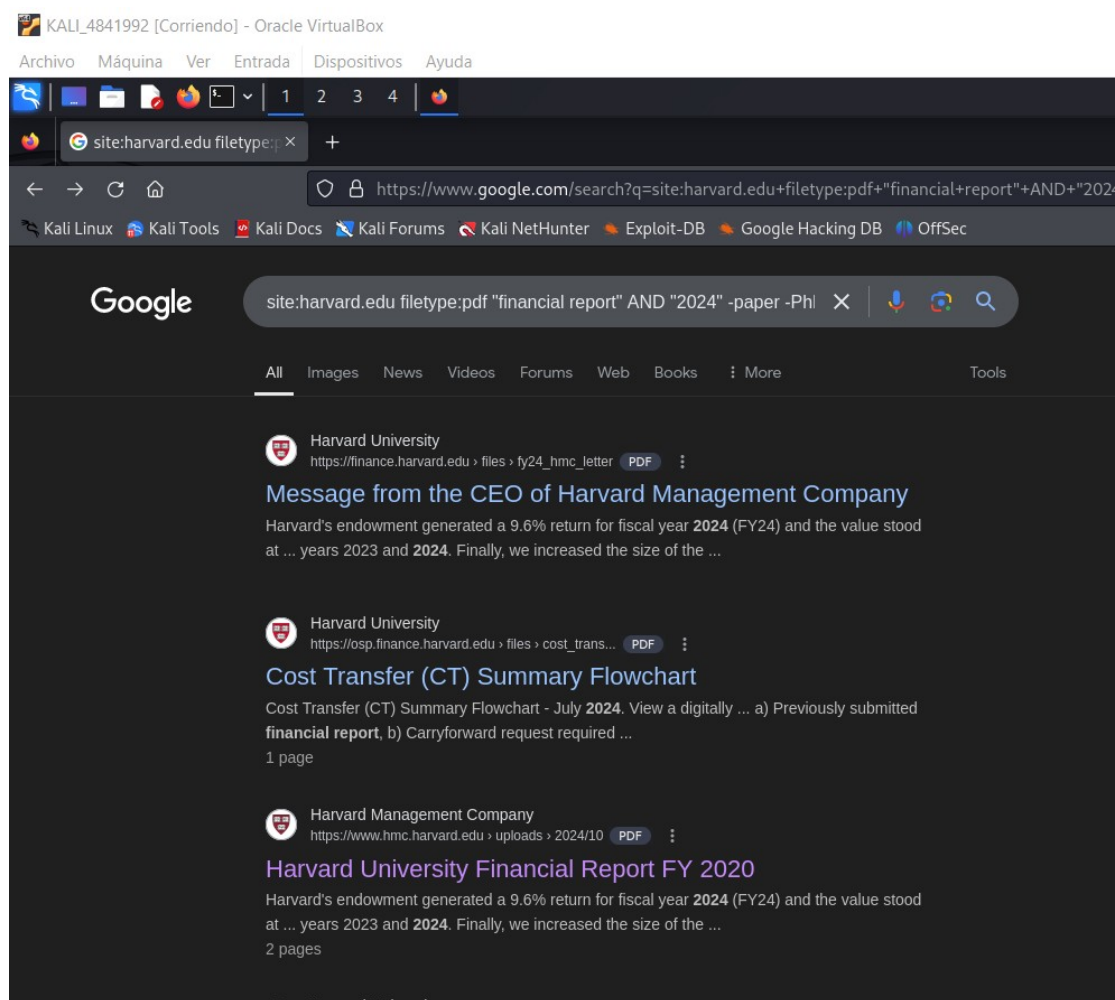
A continuación he usado **site:harvard.edu filetype:txt "user"**

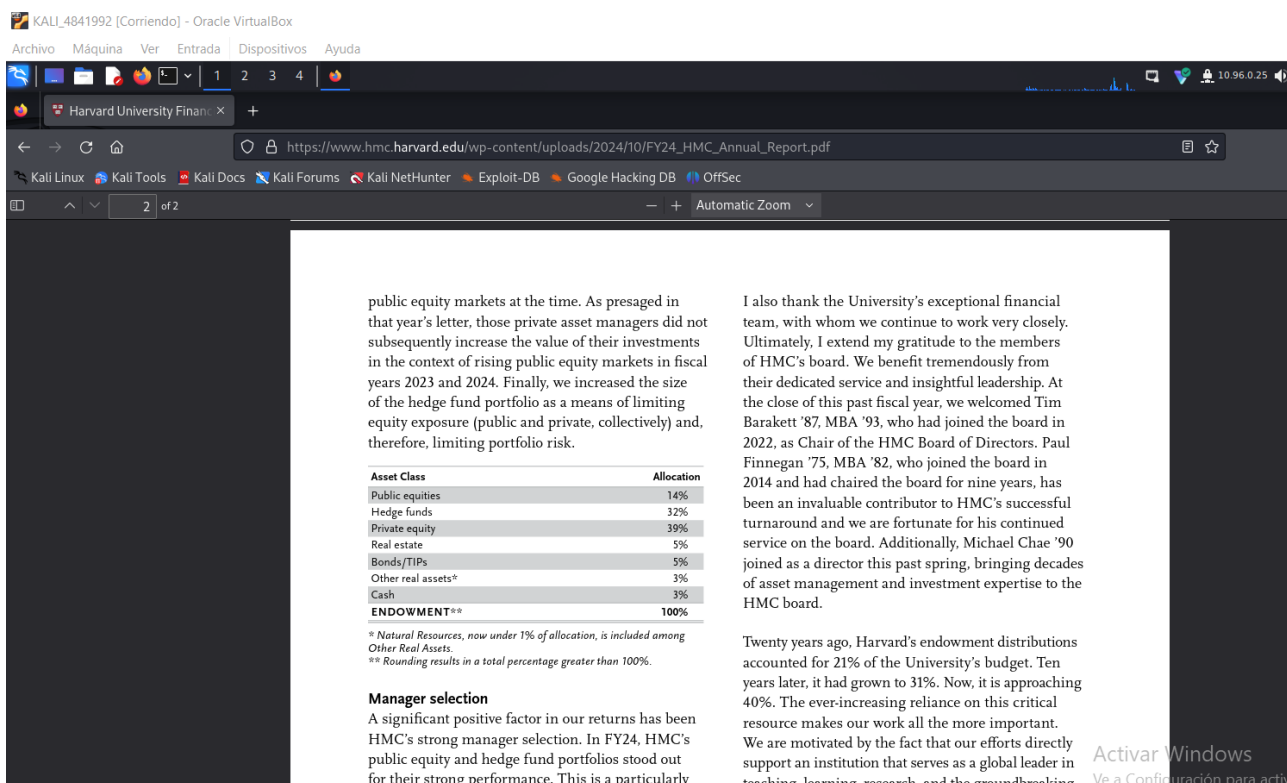
La idea era buscar algún tipo de información de usuarios indexada en un txt, pero no conseguí nada relevante, a lo más que llegué fue a un read.txt sobre tweets borrados que solicitó un investigador por alguna razón, pero no pude acceder a los tweets buscando en los directorios porque estaban todos protegidos y me salía forbidden excepto el readme.

El tercer dork usado es **site:harvard.edu filetype:pdf "financial report" AND "2024" -paper -PhD -academic**

La idea es buscar informes financieros de la universidad. Usando el operador AND para que busque ficheros que contienen tanto "financial report" como "2024" porque la idea es buscar informes financieros actuales, y también el operador - para filtrar resultados académicos tales como papers, doctorados (PhD) etcétera.

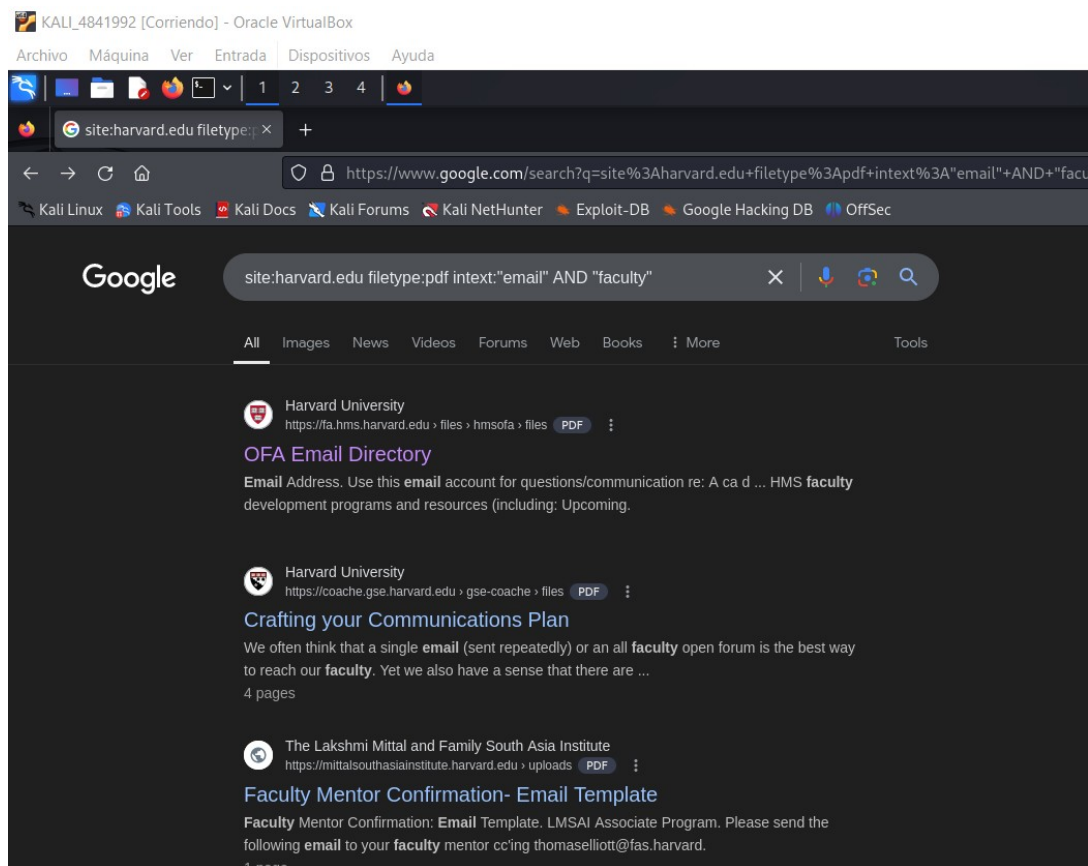
Con esto llegué a encontrar la información sobre el portfolio de inversiones de la Universidad:

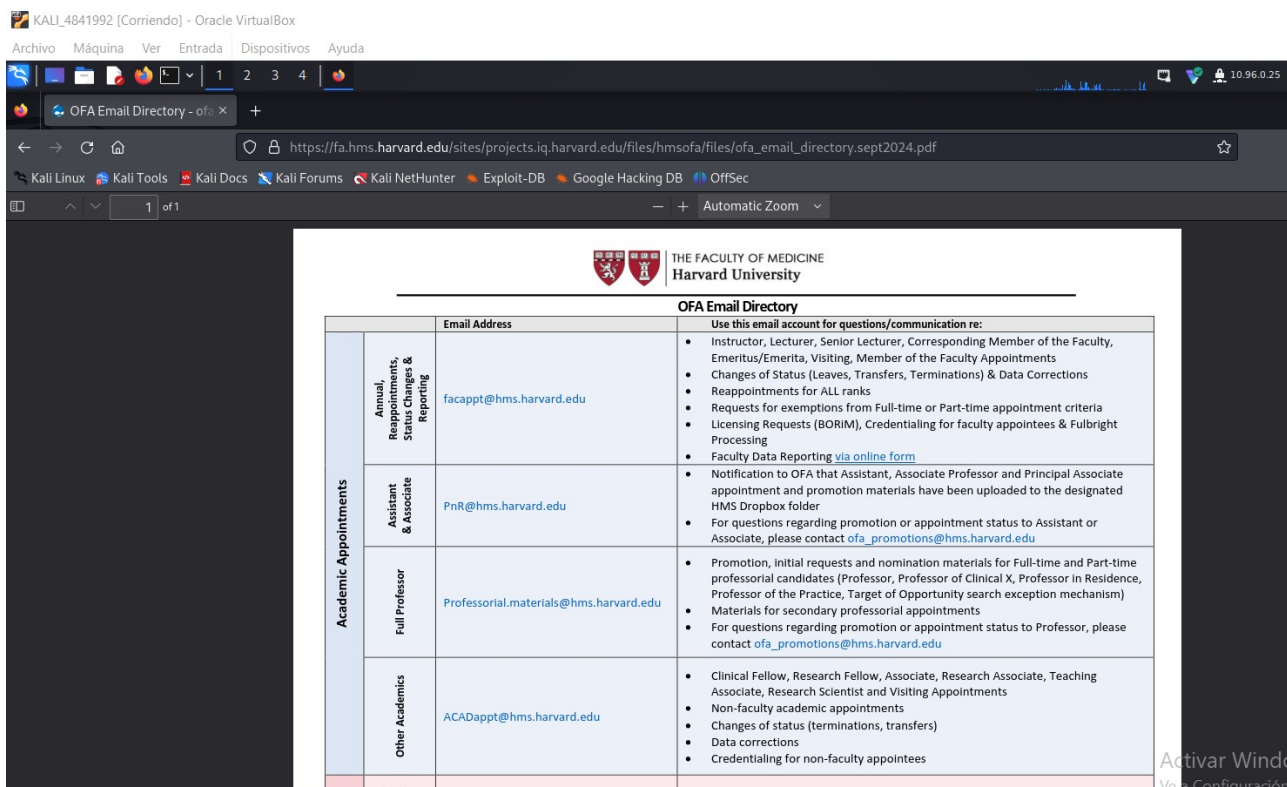




El cuarto dork es ***site:hardvard.edu filetype:pdf intext:"email" AND "faculty"***

La idea aquí es buscar los correos electrónicos de los profesores de las distintas facultades, algo que podría buscar un atacante para realizar por ejemplo un ataque de phishing. Con esto encontré los email de la facultad de medicina de este curso:





El último dork usado es: **site:harvard.edu filetype:log "error"**

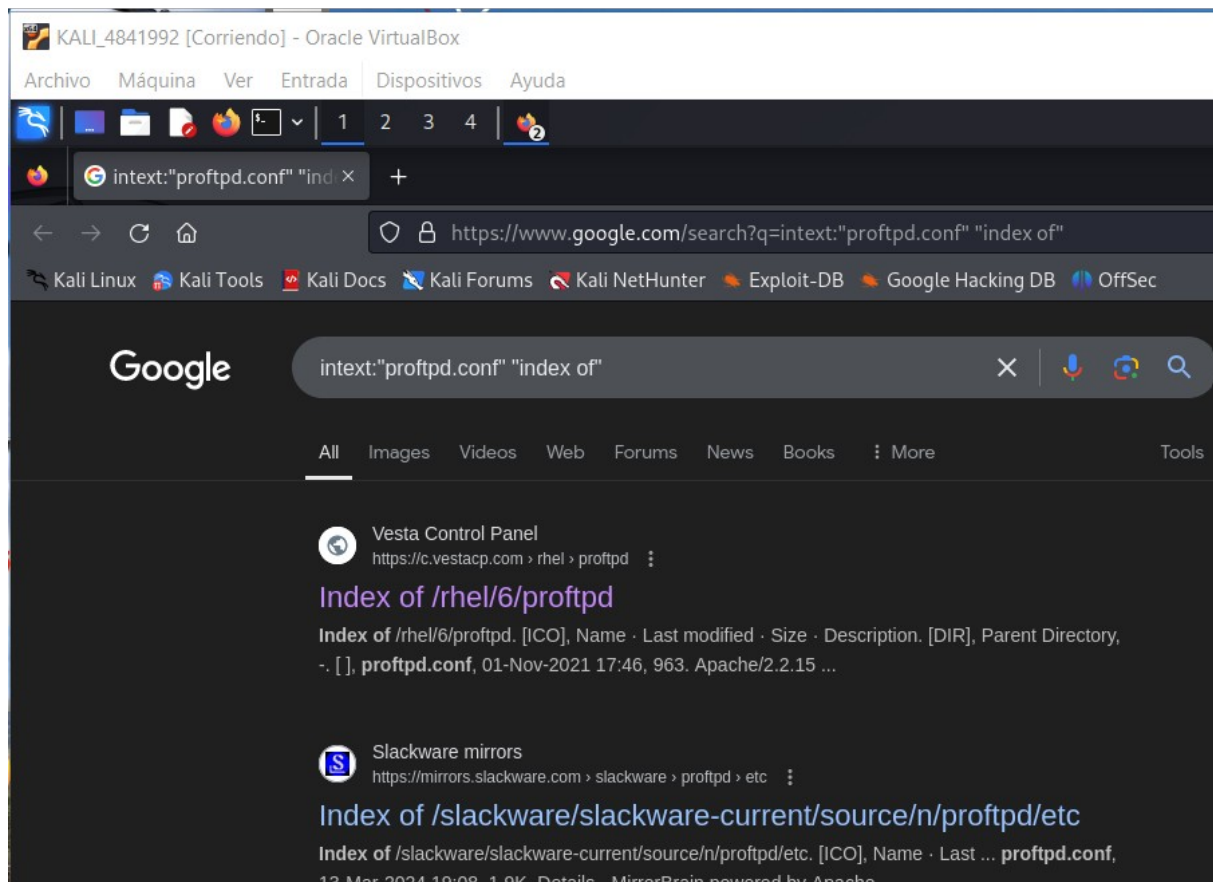
La idea aquí es buscar logs del sistema con errores, en busca de encontrar vulnerabilidades de seguridad. Yo no he encontrado nada, pero tampoco los he mirado todos, puede que con paciencia y analizando todos los logs con error se encuentre un agujero de seguridad.

Con esto termina este apartado.

1.2. CONSULTA CON GOOGLE DORKS:

El primer dork de exploithub que he usado es: **intext:"proftpd.conf" "index of"**

Este nos permite acceder al fichero de configuración de un montón de servidores ftp. Aquí un ejemplo:



Index of /rhel/6/proftpd

Name	Last modified	Size	Description
Parent Directory	-		
proftpd.conf	01-Nov-2021 17:46	963	

Apache/2.2.15 (CentOS) Server at c.vestacp.com Port 443

c.vestacp.com/rhel/6/proftpd × +

← → ↻ 🏠 🔒 https://c.vestacp.com/rhel/6/proftpd/proftp

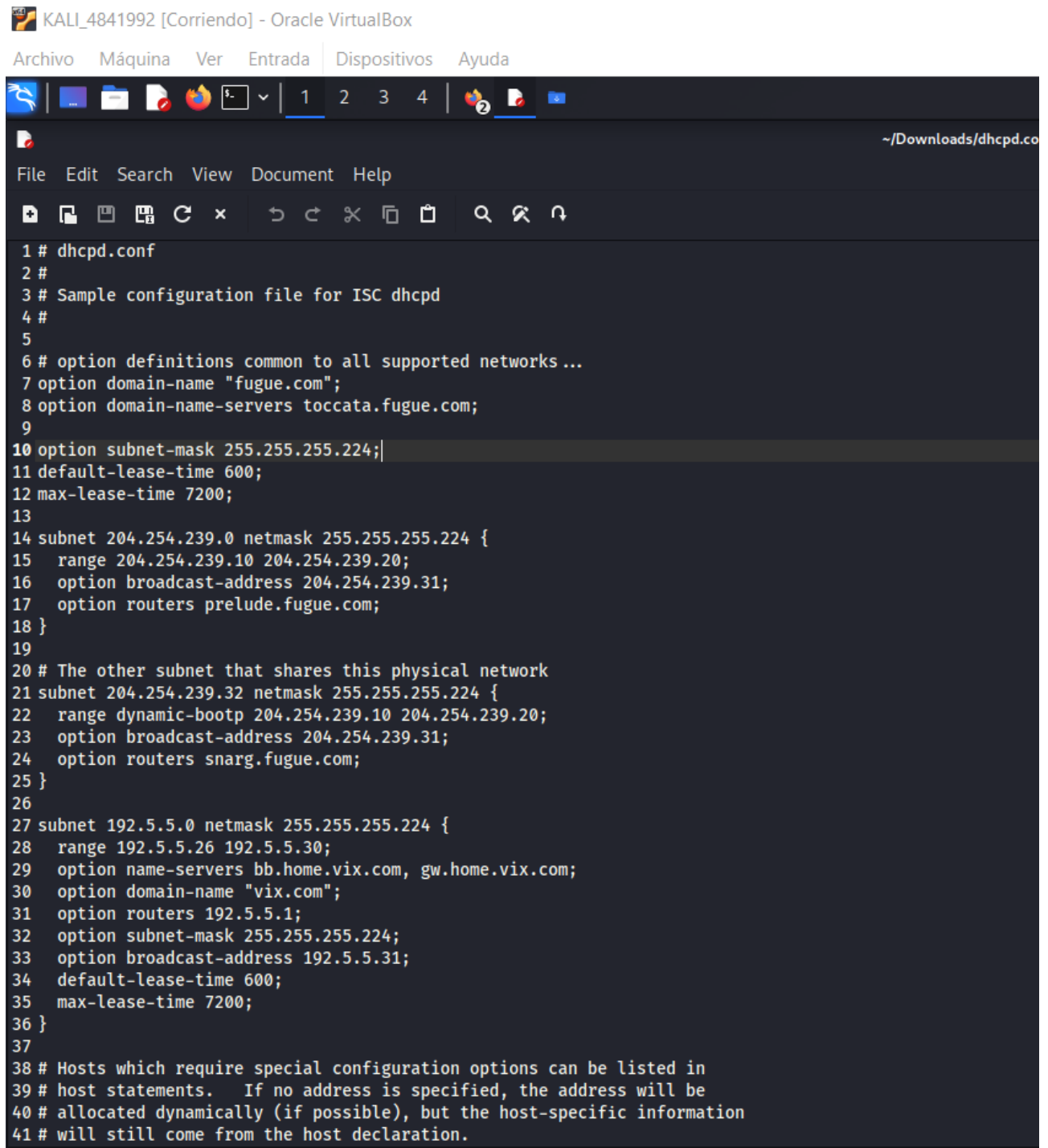
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

```
ServerName                "FTP"
ServerIdent               on "FTP Server ready."
ServerAdmin               root@localhost
DefaultServer             on
VRootEngine               on
DefaultRoot               ~ !adm
AuthPAMConfig             proftpd
AuthOrder                 mod_auth_pam.c* mod_auth_unix.c
UseReverseDNS             off
User                     nobody
Group                    nobody
MaxInstances              20
UseSendfile               off
LogFormat                 default "%h %l %u %t \"%r\" %s %b"
LogFormat                 auth      "%v [%P] %h %t \"%r\" %s"
ListOptions               -a
RequireValidShell         off
PassivePorts              12000 12100

<Global>
  Umask                   002
  IdentLookups            off
  AllowOverwrite          yes
  <Limit ALL SITE_CHMOD>
    AllowAll
  </Limit>
</Global>
```

El siguiente dork usado es: ***intext:"dhcp.conf" "index of"***

Nos permite al fichero de configuración de un servidor dhcp. En esta captura se puede ver cómo obtenemos el nombre del dominio, la ip del broadcast, los routers y la subred:

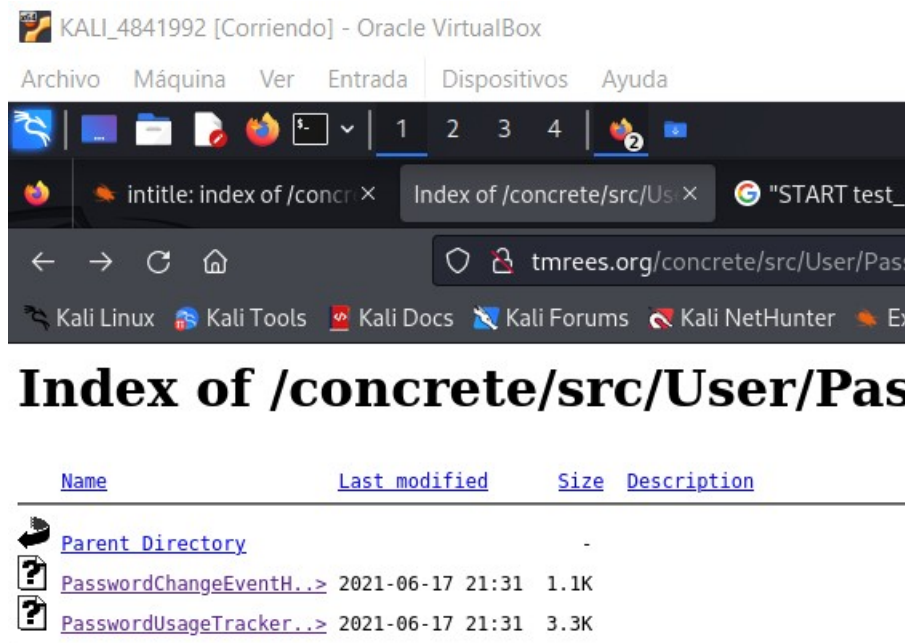


The screenshot shows a Kali Linux virtual machine window titled "KALI_4841992 [Corriendo] - Oracle VirtualBox". The interface includes a menu bar (Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda) and a toolbar. A file editor is open, displaying the contents of a file named "dhcpd.conf" located at "~Downloads/dhcpd.co". The file content is as follows:

```
1 # dhcpd.conf
2 #
3 # Sample configuration file for ISC dhcpd
4 #
5
6 # option definitions common to all supported networks...
7 option domain-name "fugue.com";
8 option domain-name-servers toccata.fugue.com;
9
10 option subnet-mask 255.255.255.224;
11 default-lease-time 600;
12 max-lease-time 7200;
13
14 subnet 204.254.239.0 netmask 255.255.255.224 {
15     range 204.254.239.10 204.254.239.20;
16     option broadcast-address 204.254.239.31;
17     option routers prelude.fugue.com;
18 }
19
20 # The other subnet that shares this physical network
21 subnet 204.254.239.32 netmask 255.255.255.224 {
22     range dynamic-bootp 204.254.239.10 204.254.239.20;
23     option broadcast-address 204.254.239.31;
24     option routers snarg.fugue.com;
25 }
26
27 subnet 192.5.5.0 netmask 255.255.255.224 {
28     range 192.5.5.26 192.5.5.30;
29     option name-servers bb.home.vix.com, gw.home.vix.com;
30     option domain-name "vix.com";
31     option routers 192.5.5.1;
32     option subnet-mask 255.255.255.224;
33     option broadcast-address 192.5.5.31;
34     default-lease-time 600;
35     max-lease-time 7200;
36 }
37
38 # Hosts which require special configuration options can be listed in
39 # host statements.  If no address is specified, the address will be
40 # allocated dynamically (if possible), but the host-specific information
41 # will still come from the host declaration.
```

El último dork es ***intitle: index of /concrete/Password***

Este nos permite acceder a ficheros PHP que registran contraseñas:



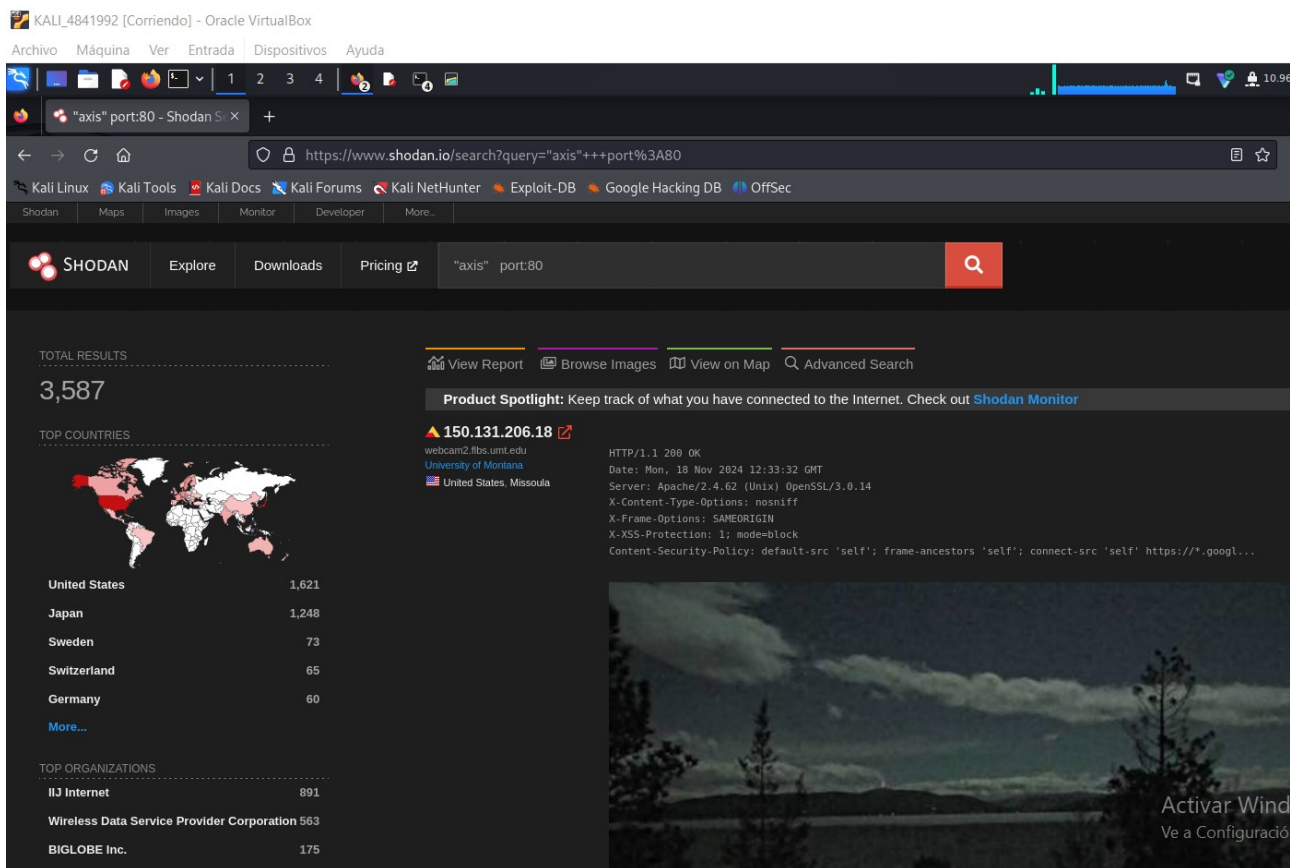
Pasamos a Shodan:

PARTE 2: SHODAN

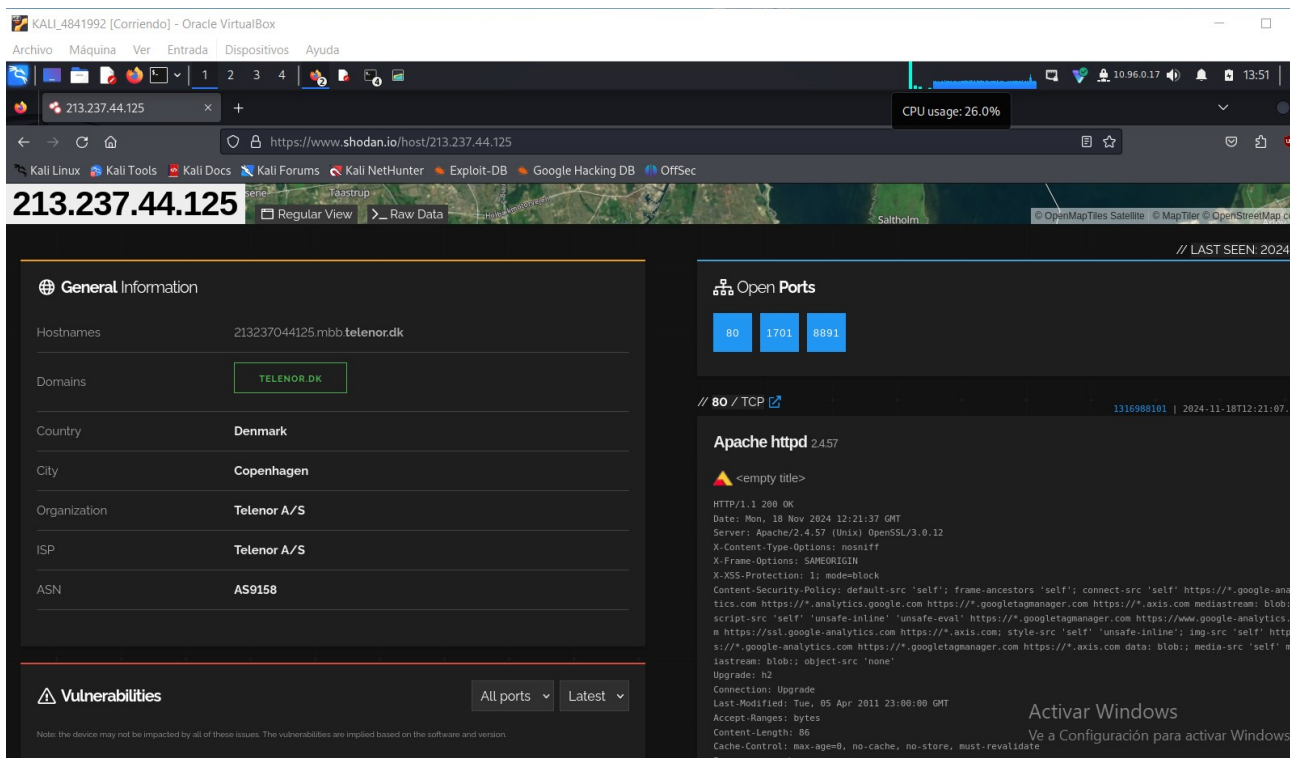
2.1. EXPLORACIÓN DE SHODAN:

Mi primera búsqueda es **“axis” port:80**

Explicación: Axis es una marca de cámaras de red, y el puerto 80 es un puerto típico de servicio HTTP. Por tanto una axis con ese puerto vulnerable significa que es posible acceder a la cámara desde su ip.



Como se ve en la captura, la búsqueda devuelve más de 3500 resultados de varias partes del mundo. Vamos a documentar una:



La ip es 213.237.44.125 Es una cámara de un servidor apache HTTP corriendo Linux. Es de Dinamarca, Copenhage, el proveedor de Internet es Telenor A/S con host telenor.dk

¿No sé que contiene la cámara ni si está protegida con contraseña y no voy a comprobarlo porque no voy a interactuar. No obstante, muchas cámaras y routers protegidos con contraseña probablemente tengan algo del tipo user user, admin admin, etc, es sorprendente lo común que es que la gente deje esa contraseña por defecto en algo tan sensible como un router o una cámara web.

La siguiente búsqueda es “**default password**” La idea es buscar dispositivos con la contraseña por defecto, lo que sería una vulnerabilidad obvia. Al buscarlo me he encontrado con esto tan curioso:

KALI_4841992 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

"default password" - Shodan X Has anyone who uses the X Over 20,000 Ubiquiti Cam X +


← → ↻ 🏠 <https://www.shodan.io/search?query=default+password>

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

403

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Grav](#)

TOP COUNTRIES



United States	194
Taiwan	36
Argentina	17
Ukraine	17
Canada	16
More...	

TOP PORTS

10001	107
8081	37
8001	33
5900	17
5901	11
More...	

TOP ORGANIZATIONS

Jaguar Communications	88
-----------------------	----

64.130.160.118

64.130.160-118.pool.dsl.srtc.com
[South Central Rural Telecommunications Cooperative Inc.](#)
United States, Horse Cave
[compromised](#)

Ubiquiti Networks Device:
IP Address: 64.130.160.118
MAC Address: 24:A4:3C:97:63:E1
Alternate IP Address: 169.254.99.225
Alternate MAC Address: 24:A4:3C:96:63:E1
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**
Product: LAP
Version: XM.ar7240.v5.5.6.17762.130528.1755

64.72.116.143

64-72-116-143.ip.jagcom.net
[Jaguar Communications](#)
United States, Owatonna

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 18 Nov 2024 12:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: DENY
X-Content-Type-Options: nosniff

c7b
<!DOCTYPE html>
<html><head>
<meta charset="utf-8"/>
<link rel="shortcut icon" type="ima...

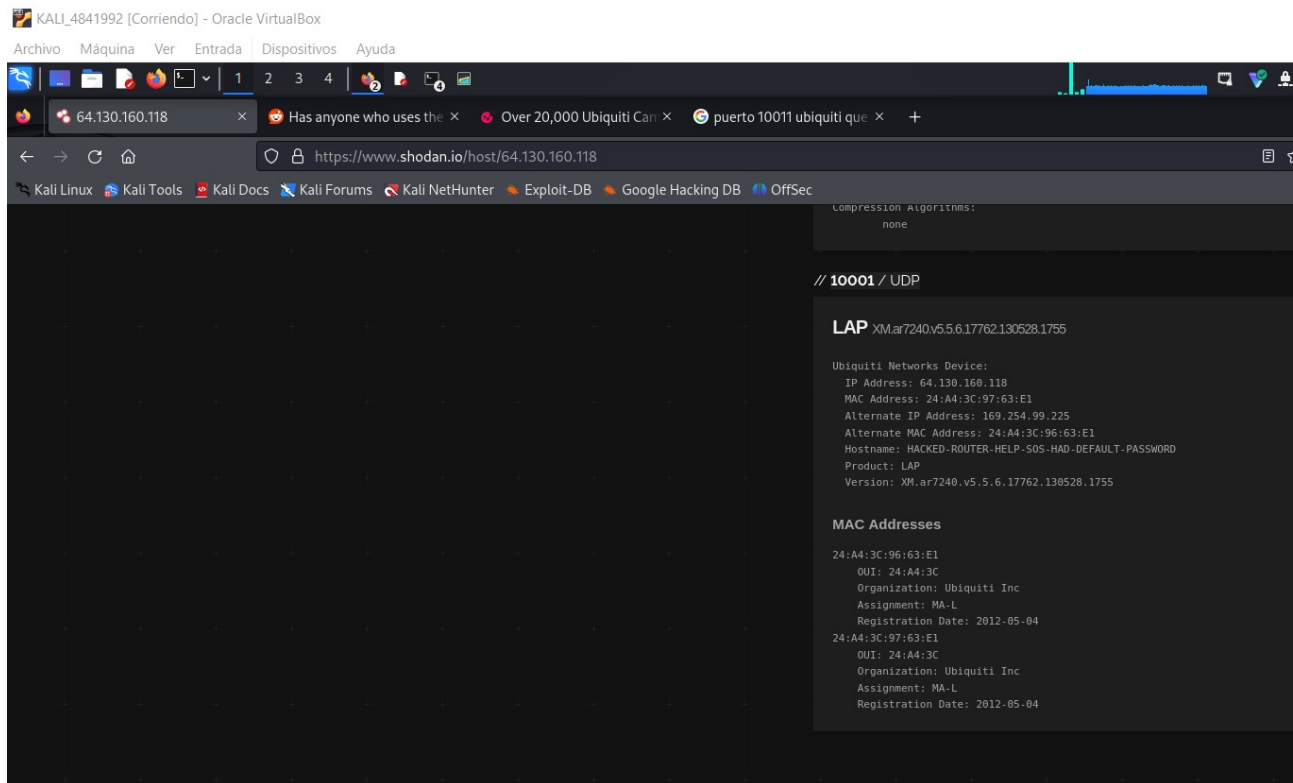
50.198.63.38

50-198-63-38-static.hfc.comcastbusiness.net
[Comcast Cable Communications, LLC](#)
United States, Chicago

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 18 Nov 2024 10:11:47 GMT
Content-Type: text/html
Transfer-Encoding: chunked

El primero, el host es **HACKED-ROUTER-HELP-SOS-HAD-DEFAULT-PASSWORD**

Tiene expuestas la ip y la MAC. Me pregunto si esto es un honeypot como la copa de un pino, o es que el hacker estaba chistoso.



Se trata de un router Ubiquiti que tiene vulnerable el puerto 10001, este puerto se usa para protocolos de comunicaciones entre dispositivos. Lo que significa que el dispositivo está completamente comprometido.

Buscando parece ser que esto proviene de una serie de pruebas de penetración en las que se vulneraron más de 20.000 routers y cámaras Ubiquiti y este es uno de esos routers. Desde luego no seré yo quién entre en la ip para comprobarlo, ni siquiera con máquina virtual y VPN.

[Enlace](#)

La última búsqueda es **“Apache/2.4.39” port:80**

La idea aquí es buscar una versión específica del servidor Apache que es la 2.4.39 que tiene exploits que permiten realizar una escalada de privilegios, está obsoleta pero aún hay dispositivos que la usan, un dispositivo que sigue usando esta versión es claramente vulnerable. El puerto 80 es uno de los puertos típicos de los servidores Apache, el otro es el 443.

KALI_4841992 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

"Apache/2.4.39" port:80 × +

← → ↻ 🏠 🔒 https://www.shodan.io/search?query="Apache%2F2.4.39"+port%3A80


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

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing "Apache/2.4.39" port:80 🔍

TOTAL RESULTS
46,348

TOP COUNTRIES



Country	Count
United States	25,751
China	9,276
Japan	2,457
Hong Kong	1,702
Singapore	889

[More...](#)

TOP ORGANIZATIONS

Organization	Count
Root Networks, LLC	17,530
Aliyun Computing Co., LTD	3,975
Amazon Technologies Inc.	2,716

View Report Browse Images View on Map Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

AXIS

166.252.168.147
147.sub-166-252-168.myvzw.com
Wireless Data Service Provider Corporation
United States, Gaithersburg

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2024 13:45:04 GMT
Server: **Apache/2.4.39** (Unix) OpenSSL/1.1.1c
Last-Modified: Fri, 06 Sep 2019 09:37:49 GMT
Accept-Ranges: bytes
Content-Length: 1316
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html

403 Forbidden

38.35.100.216
connect.rcp.net
Root Networks, LLC
United States, Los Angeles

HTTP/1.1 403 Forbidden
Date: Mon, 18 Nov 2024 13:44:50 GMT
Server: **Apache/2.4.39** (Win64) PHP/7.2.18
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1

403 Forbidden

38.35.81.25
connect.rcp.net
Root Networks, LLC
United States, Los Angeles

HTTP/1.1 403 Forbidden
Date: Mon, 18 Nov 2024 13:44:49 GMT
Server: **Apache/2.4.39** (Win64) OpenSSL/1.1.1b PHP/7.2.18 mod_fcgid/2.3.10-dev
Content-Length: 332

Hay unos cuantos resultados, por ejemplo otra cámara Axis.

KALI_4841992 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

166.252.168.147

https://www.shodan.io/host/166.252.168.147

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

Purcellville Harrison Island Gaithersburg Denwood Leisure World Cloverly Burtonsville Darnestown North Potomac

166.252.168.147

Regular View Raw Data

// TAGS: self-signed

General Information

Hostnames	147.sub-166-252-168.myvzw.com
Domains	MYVZW.COM
Country	United States
City	Gaithersburg
Organization	Wireless Data Service Provider Corporation
ISP	Verizon Business
ASN	AS6167

Open Ports

80	443	554	9191	9443	49152
----	-----	-----	------	------	-------

// 80 / TCP

Apache httpd 2.4.39

AXIS

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2024 13:45:04 GMT
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1c
Last-Modified: Fri, 06 Sep 2019 09:37:49 GMT
Accept-Ranges: bytes
Content-Length: 1316
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html

CVE-2022-2068 CVE-2022-1292 CVE-2022-1293

Web Technologies

KALI_4841992 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

166.252.168.147

https://www.shodan.io/host/166.252.168.147

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

Purcellville Harrison Island Gaithersburg Denwood Leisure World Cloverly Burtonsville Darnestown North Potomac

166.252.168.147

Regular View Raw Data

// TAGS: self-signed

General Information

Hostnames	147.sub-166-252-168.myvzw.com
Domains	MYVZW.COM
Country	United States
City	Gaithersburg
Organization	Wireless Data Service Provider Corporation
ISP	Verizon Business
ASN	AS6167

Open Ports

80	443	554	9191	9443	49152
----	-----	-----	------	------	-------

// 80 / TCP

Apache httpd 2.4.39

AXIS

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2024 13:45:04 GMT
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1c
Last-Modified: Fri, 06 Sep 2019 09:37:49 GMT
Accept-Ranges: bytes
Content-Length: 1316
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html

CVE-2022-2068 CVE-2022-1292 CVE-2022-1293

Web Technologies

Vemos la ip, que es la 166.252.168.147 el hostname es de Estados Unidos y el proveedor es Verizon Business. Y efectivamente Apache escucha por el puerto 80 y es vulnerable a un atacante.

Terminamos esta parte y pasamos a la reflexión ética.

PARTE 3: REFLEXIÓN ÉTICA

Yo he hecho un uso ético y de práctica de estas herramientas. No obstante podría haber entrado en varias cámaras de seguridad, hacerme con el control de servidores apache y routers. Es lo que haría un atacante malicioso. Esto también es ilegal y si te pillas puedes enfrentar consecuencias penales tales como ir a la cárcel.

Incluso si lo haces solo con fines de aprendizaje, sin intención maliciosa, sigue siendo ilegal y puedes enfrentar problemas legales. Por tanto, el hacker ético debe hacer su trabajo en un entorno real con permiso explícito de los sistemas que ataca para descubrir sus vulnerabilidades.

Dicho esto, en sí usar Google Dorking no es ilegal, solo estás consultando información pública, ahora bien, si tú utilizas esa información para loguearte en sistemas sobre los que no tienes permiso vulnerando la contraseña, o haces algún tipo de ataque, eso es un delito. El escaneo de puertos está en un área gris, técnicamente no es un ataque, pero según el país puede ser ilegal.

En resumen, un hacker ético debe actuar con inteligencia y respetando la ley de su país, recurriendo quizás a herramientas de entrenamiento en red local o en sistemas en red suyos o para los que tiene permiso para actuar