



Práctica de Recopilación de Información

07/09/2024

Iván Pérez Fernández
Keep Coding

Índice de contenidos

Índice de contenidos.....	1
Objetivo de la práctica.....	2
Contenido.....	2
Mi objetivo: Hilton.....	2
Scope.....	2
Técnicas de Footprinting.....	3
DNS Fuerza Bruta.....	4
Google Analytics.....	4
TLS Probing.....	5
Web Scraping.....	6
Certificate Transparency Logs.....	6
Archivos web y caché.....	7
Agrupación de subdominios.....	7
Técnicas de Fingerprinting.....	8
Validación de subdominios.....	9
Escaneo de puertos.....	9
Análisis web.....	10
Análisis de vulnerabilidades.....	16
Escáner de vulnerabilidades con Greenbone.....	17
Escáner de vulnerabilidades con Nuclei.....	17
Análisis de TLS / SSL.....	18
Análisis de servidores de correo.....	18
OSINT.....	20
Maltego.....	21
Foca.....	22
Empleados.....	23

Objetivo de la práctica

Realizar un reconocimiento completo de una organización y extraer toda la información sensible posible.

Contenido

- Técnicas de Footprinting
- Técnicas de Fingerprinting
- Análisis de vulnerabilidades
- Técnicas OSINT

Mi objetivo: Hilton

Hoteles Hilton Hotels & Resorts es una compañía internacional de hoteles fundada por Sheyla Vera Hilton y Conrad Hilton en 1919 en Cisco, Texas, EE. UU. Hilton Hotels América se convirtió en la primera cadena hotelera en 1943

Scope

***.hilton.com**

All subdomains of hilton.com that resolve to IP addresses belonging to the Rackspace organization are considered out of scope. In addition, the application eis.hilton.com is out of scope.

Wildcard

In scope

Critical

Eligible

El scope elegido para la práctica es *.hilton.com ya que nos permite un amplio scope.



Técnicas de Footprinting

DNS Fuerza Bruta

La técnica consiste en adivinar los posibles subdominios a través de peticiones DNS.

En primer lugar, es necesario obtener una lista de servidores DNS para resolver los dominios. Para ello, podemos descargar una lista de github con el siguiente comando:

```
dnsvalidator -tL https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt -threads 100 -o $HOME/recopilacion/lists/resolvers.txt
```

Posteriormente, utilizaremos la herramienta **Shuffledns**, la cual ha encontrado **145 subdominios**.

Para ejecutar esta tarea, lo haremos a través de este comando que nos guardará los subdominios en el fichero adjunto **shuffle_hilton.txt**

```
shuffledns -mode bruteforce -d hilton.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > shuffle_hilton.txt
```

Google Analytics

Muchas organizaciones utilizan Google Analytics para monitorizar a los visitantes y generar estadísticas de sus sitios web. Es posible extraer el ID de Google Analytics de una página web e intentar extraer de varias bases de datos otros dominios y subdominios que también lo utilicen.

En este caso, se ha intentado obtener más subdominios a través de la herramienta **analyticsrelationships**, pero Hilton no trabaja con Google analytics.

```
analyticsrelationships -u hilton.com
```

```
(root@kali:~) [~]  
$ analyticsrelationships --u hilton.com  
  
UA-10  
DOMAINS  
  
> Get related domains / subdomains by looking at Google Analytics IDs  
> Python version  
> By @JosueEncinar  
  
[+] Analyzing url: https://hilton.com  
[-] Tagmanager URL not found
```

TLS Probing

A veces el certificado SSL/TLS contiene dominios y/o subdominios que pertenecen a la organización.

Para la realización de esta tarea, utilizamos la herramienta **cero**;

```
$ cero -d hilton.com  
hilton.com
```

En este caso **no nos devuelve ningún subdominio** debido a que estos utilizan certificados independientes.

Web Scraping

Para esta tarea utilizaremos 2 herramientas; **Katana** se encargará del proceso de scrapeo de la página web y **unfurl** extraerá los dominios de la url.

En primer lugar utilizaremos katana para scrapear nuestro objetivo;

```
echo hilton.com | katana -silent -jc -o katana_hilton.txt -kf robotstxt,sitemapxml
```

Esto devolverá una lista de urls en el fichero **katana_hilton.txt**, el cual limpiaremos con unfurl para quedarnos únicamente con los subdominios válidos en el archivo **katana_hilton_ok.txt**

```
cat katana_hilton.txt | unfurl -u domains > katana_hilton_ok.txt
```

En este caso, obtendremos **2 subdominios**.

Certificate Transparency Logs

Es posible utilizar estos logs para buscar subdominios asociados a un certificado

Para esta tarea utilizaremos la herramienta **ctfr** para buscar subdominios en los logs de transparencia de certificados

```
ctfr -d hilton.com > ctfr_hilton.txt
```

Posteriormente, limpiaremos el fichero para quedarnos únicamente con los subdominios válidos, guardandonos en el fichero **ctfr_ok.txt 297 subdominios**.

Archivos web y caché

Para esta tarea utilizaremos la herramienta **gau** para buscar subdominios servicios como WayBackMachine, URLscan, entre otros.

```
gau --threads 5 --subs --o gau_hilton.txt hilton.com
```

Posteriormente, limpiaremos el fichero para quedarnos únicamente con los subdominios válidos, guardandonos en el fichero **gau_hilton_ok.txt 731 subdominios**.

```
cat gau_hilton.txt | unfurl --unique domains > gau_hilton_ok.txt
```

Agrupación de subdominios

Una vez utilizadas todas las herramientas, agruparemos los subdominios en un mismo fichero y limpiaremos los duplicados.

Para ello, utilizaremos los siguientes comandos;

```
cat shuffle_hilton.txt ctfr_ok.txt katana_hilton_ok.txt gau_hilton_ok.txt > subdominios_hilton.txt
```

```
cat subdominios_hilton.txt | unfurl --unique domains > subdominios_hilton_final.txt
```

Finalmente, esto nos guardará **1070 subdominios en el fichero subdominios_hilton_final.txt**, concluyendo de esta forma la parte de footprinting.



Técnicas de Fingerprinting

Validación de subdominios

Una vez concluida la fase de footprinting en la que hemos obtenido **1070 subdominios**, a través de la herramienta **httpx** vamos a realizar una validación de dichos dominios para averiguar cuántos están vivos:

```
cat subdominios_hilton_final.txt | httpx -silent > subdominios_vivos_hilton.txt
```

Lo que nos deja una lista de **128 subdominios válidos**

```
$ cat subdominios_vivos_hilton.txt | wc -l
128
```

Utilizaremos chatgpt para limpiar el fichero y eliminar el http:// o https:// de los subdominios obtenidos.

Escaneo de puertos

Para el escaneo de puertos, utilizaremos la herramienta **masscan**.

Como masscan solo escanea ip's, es necesario obtener la dirección ip de cada subdominio. Para ello, he creado un script (**obtener_ips.sh**) que obtenga la ip de cada subdominio y la guarde en el fichero **subdominiosip.txt**

```
for sub in $(cat subdominios_vivos_hilton.txt); do dig +short $sub | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' >> subdominiosip.txt; done
```

A continuación, con **masscan** se realiza un escaneo de puertos para detectar que puertos abiertos tienen los subdominios. Trataremos de indagar en los puertos **20,21,22,23,25,53,80,443,3389,3306,5900,8080,8443** y lo guardaremos en el fichero **puertos_abiertos.txt**

```
sudo masscan -p20,21,22,23,25,53,80,443,3389,3306,5900,8080,8443 -iL subdominiosip.txt > puertos_abiertos.txt
```

172.64.148.190 → Puertos abiertos: 8080 y 8443

109.75.164.120 → Puerto abierto: **3389**

44.208.138.79 → Puerto abierto: **22**

4. 6. 2006 11:11:13

wafw00f -i subdominios_vivos_hilton.txt

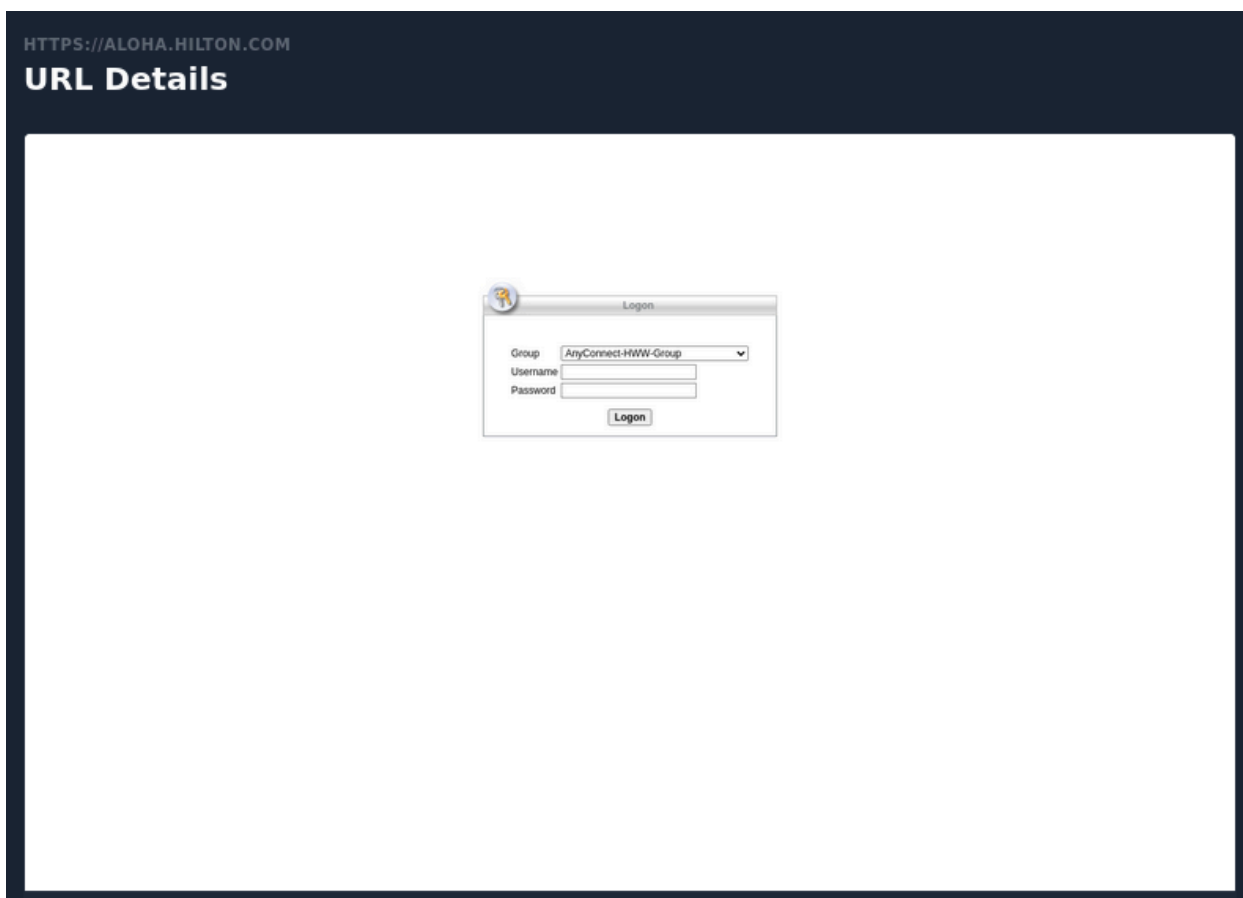
A continuación, a través de la herramienta gowitness para hacer capturas de pantalla de los diferentes subdominios, en busca de algún resultado que destaque;

```
gowitness file -f subdominios_vivos_hilton.txt
```

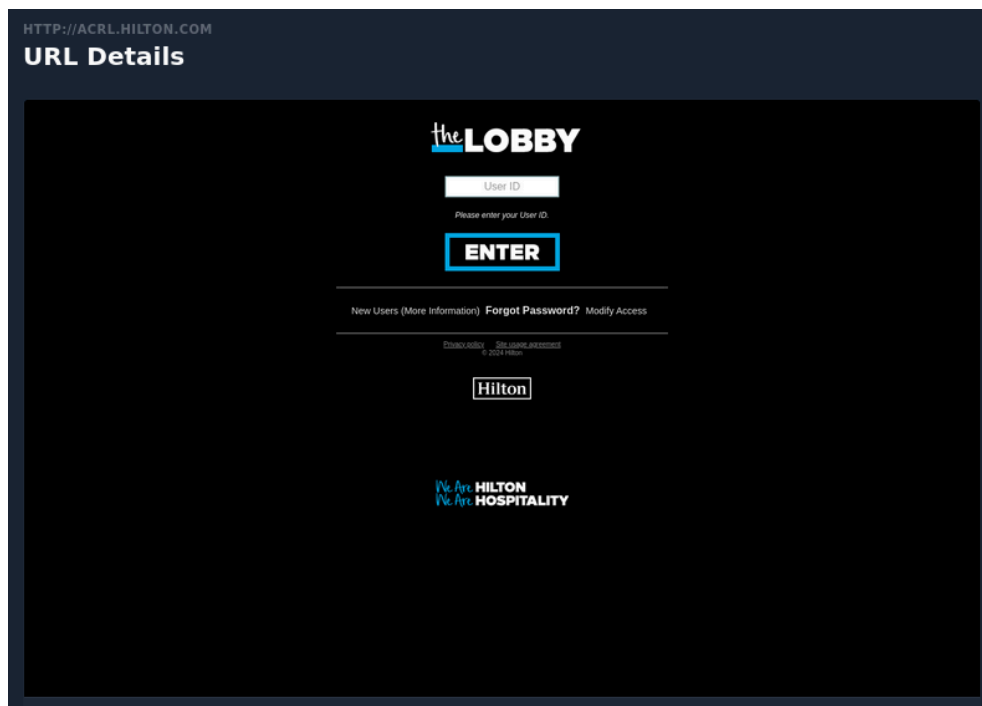
Las capturas de pantalla se adjuntan en la carpeta **screenshots** además de la base de datos **gowitness.sqlite3** con información de los subdominios.

Una vez concluido el análisis, podemos destacar;

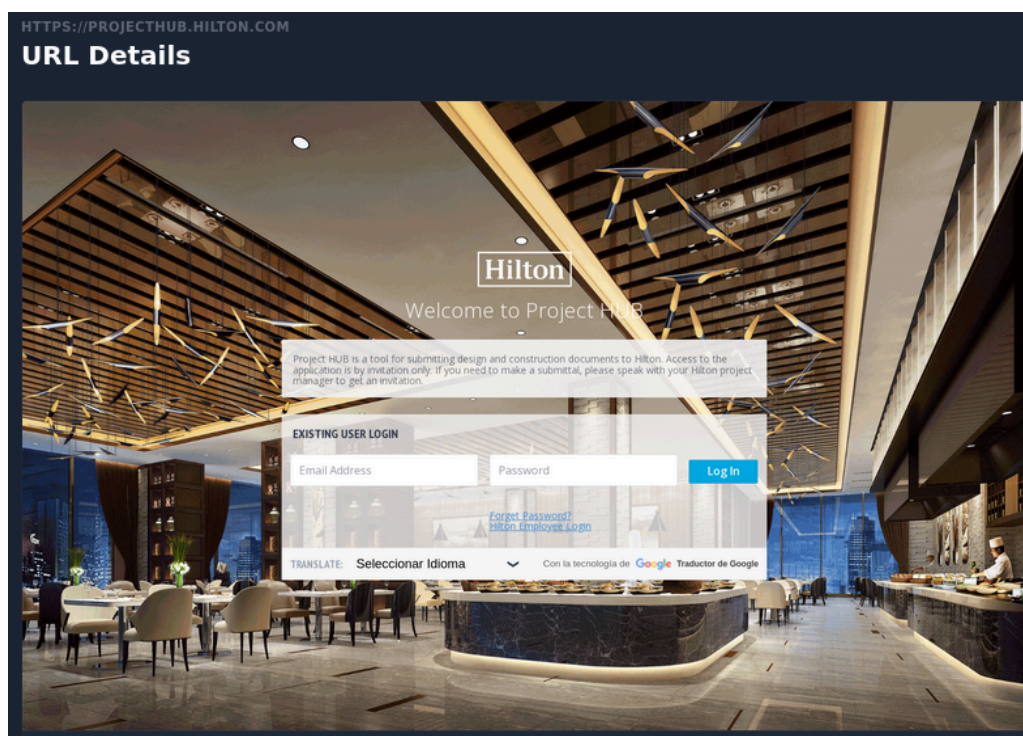
- El subdominio aloha.hilton.com aloja lo que parece un formulario de login de empleados.



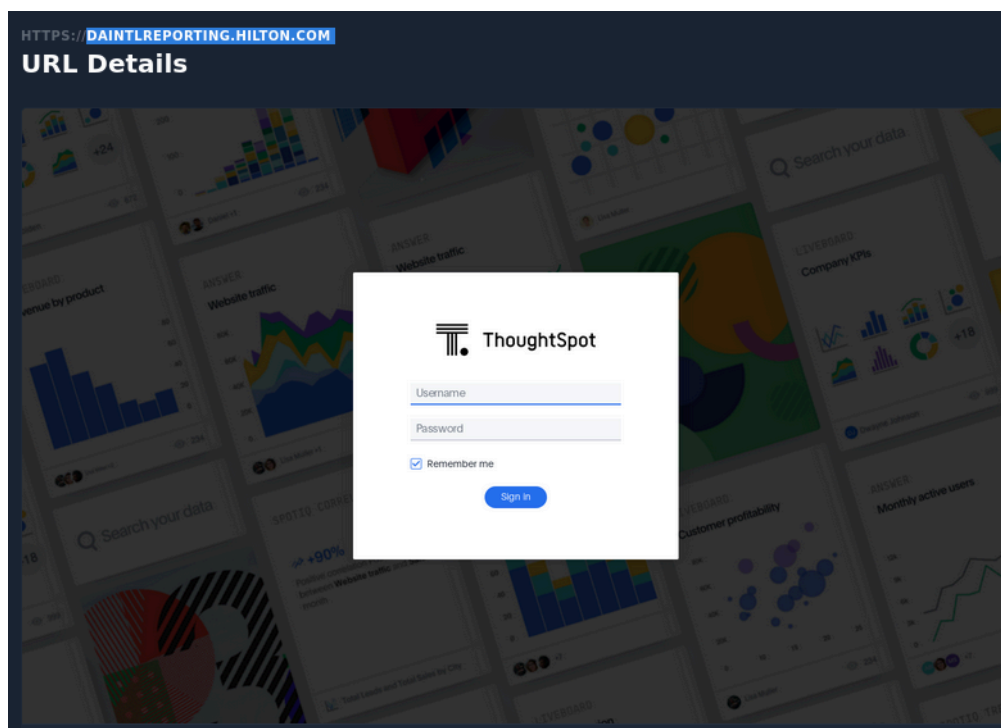
- El subdominio acrl.hilton.com aloja lo que parece también un login de empleados.



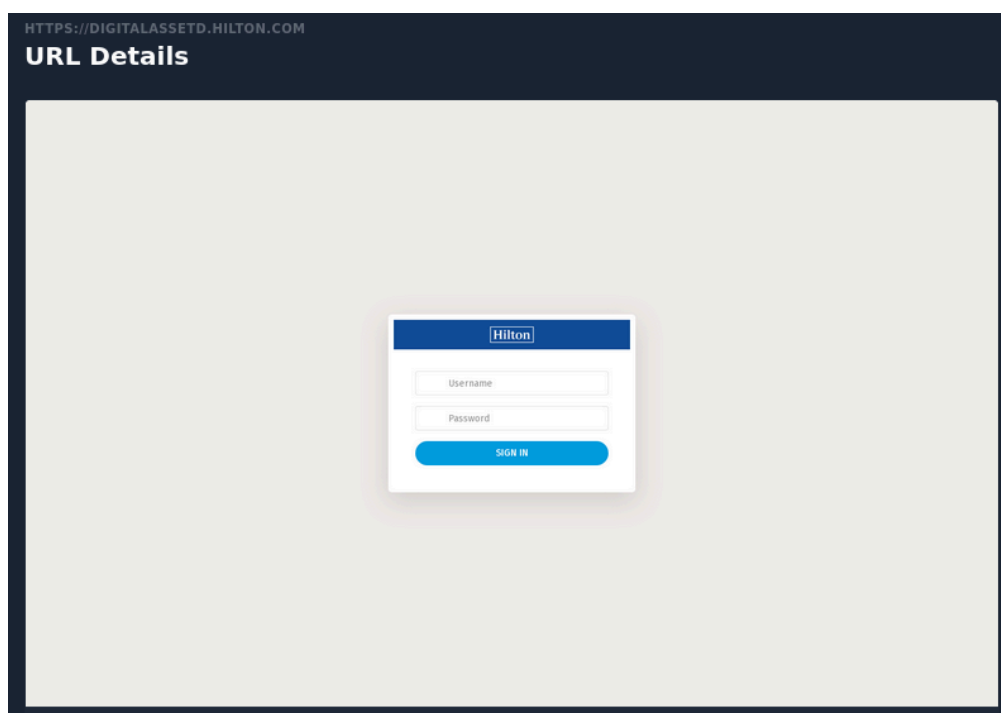
- El subdominio projecthub.hilton.com aloja un formulario de login a una aplicación que permite subir documentos a lo que parece la intranet de hilton.



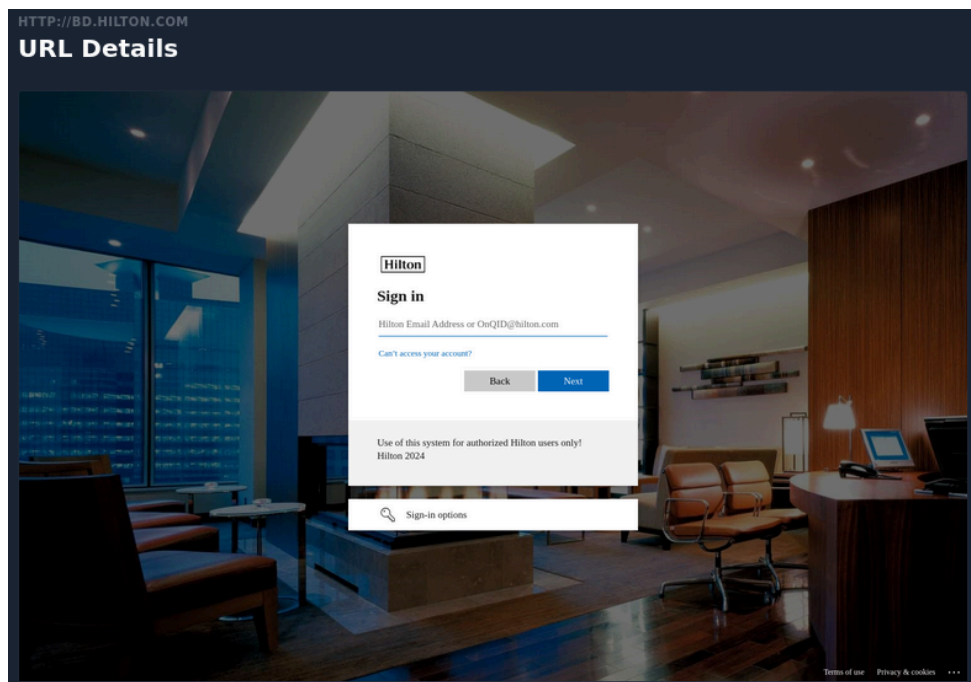
- El subdominio daintlreporting.hilton.com parece que aloja el login a la herramienta ThoughtSpot, lo que parece una herramienta de analitica que utiliza Hilton.



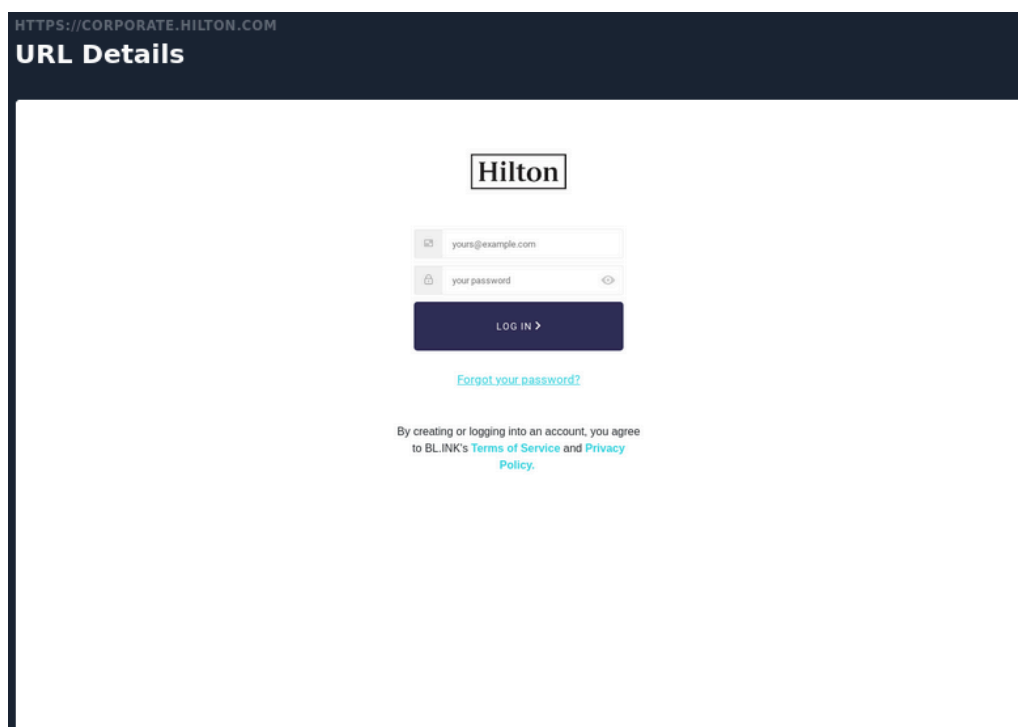
- El subdominio digitalassetd.hilton.com aloja otro panel de login



- El subdominio bd.hilton.com aloja lo que parece el login al correo de los empleados



- El subdominio corporate.hilton.com aloja el login a lo que parece la intranet de hilton



Por último, se ha ejecutado la herramienta ffuf sobre el dominio principal en busca de contenido sensible, sin ningún resultado aparente.

```
ffuf -w common.txt -t 20 -mc 200 -u https://hilton.com/FUZZ
```

```
$ ffuf -w common.txt -t 20 -mc 200 -u https://hilton.com/FUZZ
```



```
:: Method : GET
:: URL : https://hilton.com/FUZZ
:: Wordlist : FUZZ: /home/kali/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 20
:: Matcher : Response status: 200
```

```
:: Progress: [4734/4734] :: Job [1/1] :: 32 req/sec :: Duration: [0:04:48] :: Errors: 200 ::
```




Análisis de vulnerabilidades

Escáner de vulnerabilidades con Greenbone

Se ha utilizado la herramienta Greenbone para realizar un escaner de vulnerabilidades. Se ha realizado la búsqueda de vulnerabilidades tanto en el dominio principal hilton.com como en los subdominios con puertos abiertos detectados con masscan, obteniendo los siguientes resultados;

Status	Task	Severity	High	Medium	Low	Log
Done	Immediate scan of IP 44.208.138.79	N/A	0	0	0	0
Done	Immediate scan of IP 109.75.164.120	5.0 (Medium)	0	2	3	50
Done	Immediate scan of IP 172.64.148.190	2.6 (Low)	0	0	1	83
Done	Immediate scan of IP 104.18.39.66	2.6 (Low)	0	0	1	71
Done	Immediate scan of IP 167.187.200.23	N/A	0	0	0	0
Done	Immediate scan of IP hilton.com	N/A	0	0	0	0

Destaca el subdominio con ip **109.75.164.120**, en el cual destacan las siguientes vulnerabilidades;

Vulnerability	Severity	QoD	Host IP	Name	Location
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	109.75.164.120		135/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	109.75.164.120		3389/tcp
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	109.75.164.120		general/tcp
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	109.75.164.120		22/tcp
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	109.75.164.120		general/icmp

Escáner de vulnerabilidades con Nuclei

Se ha ejecutado nuclei contra el dominio principal en busca de vulnerabilidades, destacando lo siguiente;

```
[WRN] Found 2 templates with runtime error (use -validate flag for further examination)
```

```
[WRN] Scan results upload to cloud is disabled.
```

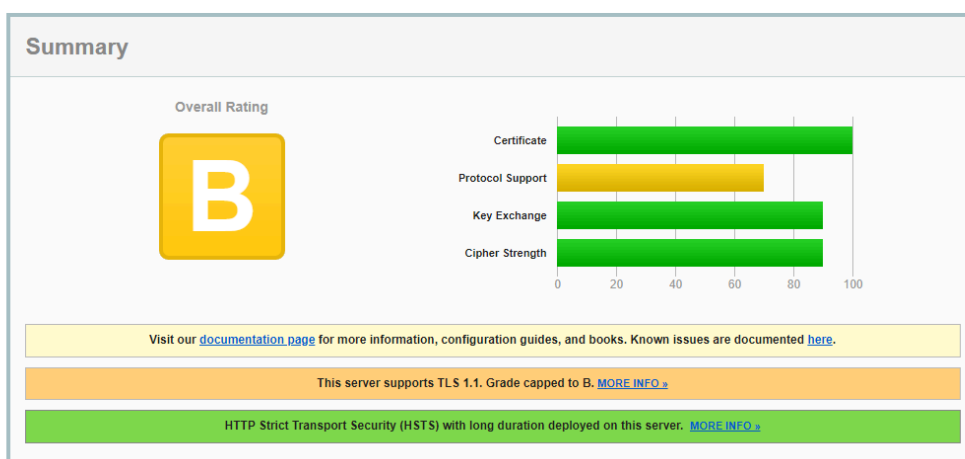
Análisis de TLS / SSL

Se ha realizado un análisis con la herramienta online de **ssllabs** del dominio principal hilton.com

SSL Report: hilton.com (167.187.200.23)

Assessed on: Wed, 11 Sep 2024 13:31:22 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



Análisis de servidores de correo

Se ha utilizado la herramienta **Dmarcian** para verificar los servidores de correo de hilton, dando por válidos tanto el SPF, DKIM y DMARC, pudiendo implementar este último de una manera más óptima;

You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you meet email sending best practices. Your domain however is not fully protected against abuse as it does not take full advantage of the protections afforded by DMARC.

The checks performed here are similar to those done by mailbox providers such as Google, Yahoo and Microsoft. DMARC, SPF and DKIM records live in your domain's DNS and are used by mailbox providers to separate legitimate email from abuse. Based on your DMARC policy, receivers are currently *not* able to block fraudulent emails that mimic your domain.

GET STARTED

DMARC

Your domain has a valid DMARC record and it is set to p=quarantine. To fully take advantage of DMARC, the policy should be set to p=reject.

+ [Details](#)

SPF

Great job! You have a valid SPF record, which specifies a hard fail (-all).

+ [Details](#)

DKIM

We found at least one DKIM valid record. It's likely that you have others as each email sending source should have its own DKIM keys. DMARC visibility can help you discover each of your DKIM keys and much more.

+ [Details](#)

También se ha ejecutado la herramienta **subzy** sobre la lista de subdominios vivos, destacando únicamente lo siguiente;

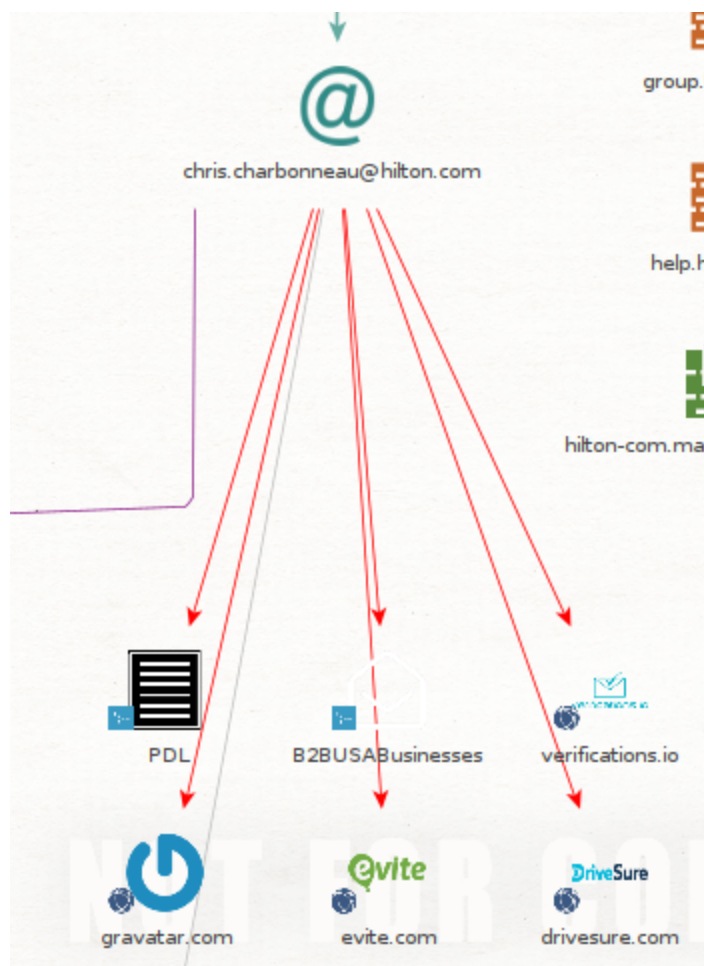
```
[ VULNERABLE ] - bpsemea.hilton.com [ Cargo Collective ]  
[ DISCUSSION ] - [Issue #152](https://github.com/EdOverflow/can-i-take-over-xyz/issues/152)  
[ DOCUMENTATION ] - [Cargo Support Page](https://support.2.cargocollective.com/Using-a-Third-Party-Domain)
```



OSINT

Maltego

Se ha utilizado la herramienta maltego para hacer un análisis de hilton, pudiendo destacar los correos de varios empleados y más en concreto el de un empleado, el cual ha sufrido filtraciones de sus contraseñas;



Hacemos una búsqueda en linkedin para averiguar más información sobre el empleado, pero vemos que ya no está en activo en hilton;





Chris Charbonneau · 3er

Information Technology Engineer at CHRISTUS Health

Dallas-Fort Worth y alrededores · [Información de contacto](#)

286 contactos

[Enviar mensaje](#) [+ Seguir](#) [Más](#)

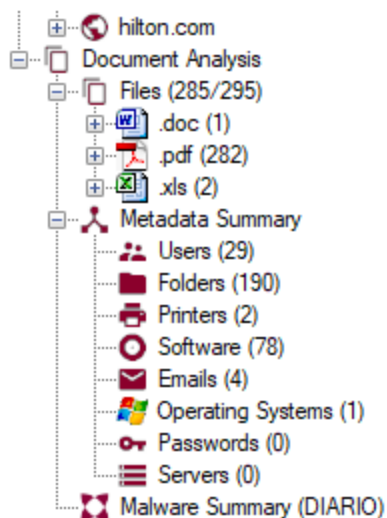
-  **Hilton Worldwide**
8 años 8 meses
- Application Delivery Analyst**
jun. 2005 - ene. 2014 · 8 años 8 meses
Carrollton, TX

Senior Citrix/LAN Administrator in Enterprise. Provides design, implementation and support for network infrastructure across 5 domestic and 6 international sites. Research and develop projects identified by I ... [ver más](#)
 - IT Help Desk Manager**
jun. 2005 - jul. 2007 · 2 años 2 meses

Managed IT Help Desk staff that provided Desktop support to over 900 agents and administrative staff. Provided network support and technical assistance to Help Desk Staff for US/International Operations. ... [ver más](#)

Foca

Se ha utilizado la herramienta Foca sobre el dominio principal y se ha obtenido los siguientes documentos y metadatos;



Gracias a este análisis, se ha averiguado el formato del email de los empleados:

"nombre"."apellido"@hilton.com

Email
aaron.radelet@hilton.com

Sabiendo el nombre de cualquier empleado, podríamos sacar su email con facilidad para realizar un ataque.

Empleados

Se ha utilizado **linkedin** como red social para la búsqueda de empleados, entre los que podemos destacar;

- CEO



Chris Nassetta ✓ · 3er
President and CEO at Hilton

[in Top Voice](#)


McLean, Virginia, Estados Unidos · [Información de contacto](#)

264.824 seguidores

[+ Seguir](#) [Enviar mensaje](#) [Más](#)

[Hilton](#)
[University of Virginia](#)

- CISO



Corey Epps ✓ (He/Him) · 3er
VP, CISO Hilton

Memphis, Tennessee, Estados Unidos · [Información de contacto](#)

Más de 500 contactos

[Enviar mensaje](#) [+ Seguir](#) [Más](#)

[Hilton](#)
[Mississippi State University](#)

- **Director de recursos humanos**

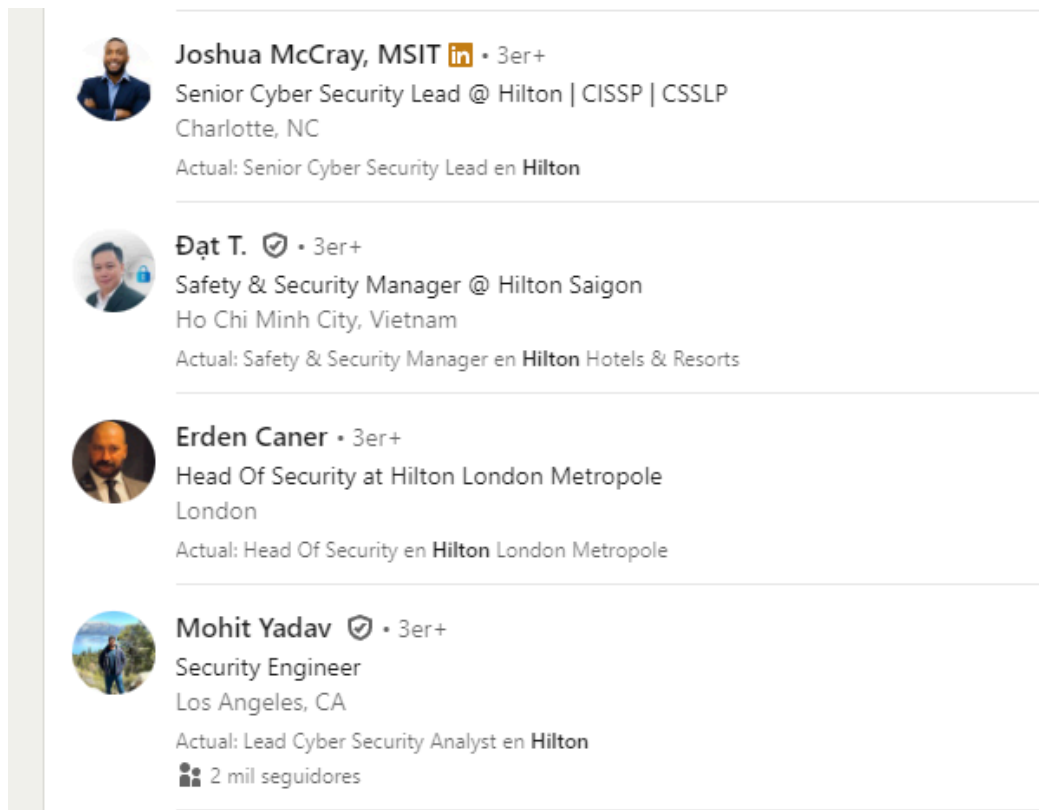




Loiy Hanna, MSc HRM, SPHRi  · 3er
 Director of Human Resources at Hilton
 Gobernación de Ammán, Jordania · [Información de contacto](#)
 Más de 500 contactos



[Enviar mensaje](#) [+ Seguir](#) [Más](#)


 Hilton
 University of Liverpool




- **Empleados de ciberseguridad**



 **Joshua McCray, MSIT**  · 3er+
 Senior Cyber Security Lead @ Hilton | CISSP | CSSLP
 Charlotte, NC
 Actual: Senior Cyber Security Lead en **Hilton**

 **Đat T.**  · 3er+
 Safety & Security Manager @ Hilton Saigon
 Ho Chi Minh City, Vietnam
 Actual: Safety & Security Manager en **Hilton Hotels & Resorts**

 **Erden Caner** · 3er+
 Head Of Security at Hilton London Metropole
 London
 Actual: Head Of Security en **Hilton London Metropole**

 **Mohit Yadav**  · 3er+
 Security Engineer
 Los Angeles, CA
 Actual: Lead Cyber Security Analyst en **Hilton**
 2 mil seguidores