

Reconocimiento de Información

Caso práctico

Gerard Díaz Hoyos

KeepCoding
Bootcamp de Ciberseguridad
5a edición

En el presente documento se va a realizar un pequeño informe de inteligencia de la conocida cadena hotelera **Hilton**.



Observando los *Bug Bounties* de la web [hackerone](https://www.hackerone.com), vemos que la compañía **Hilton** se postula como posible plataforma online para ser analizada y “atacada” dentro de los límites que ellos mismos establecen, con ánimo de mejorar la ciberseguridad de sus servicios web.

El *scope* mostrado y, por tanto, los dominios con los que iniciaremos la investigación son los siguientes:

hilton.com Authentication functionality when a user creates a Hilton Honors account (https://www.hilton.com/en/hilton-honors/join/). To create a Hilton Honors account, finders should complete the free sign-up process. The string "Test-Hackerone" must be prepended to the First and Last name fields for all Honors accounts created for the purposes of security testing.	Domain	In scope	Critical	Eligible
hilton.com.tr	Domain	In scope	Critical	Eligible
hilton.io	Domain	In scope	Critical	Eligible
hiltonbusinessonline.com	Domain	In scope	Critical	Eligible
hiltonhawaiianvillage.jp	Domain	In scope	Critical	Eligible
hiltonjapan.co.jp	Domain	In scope	Critical	Eligible
hiltonlocalbiz.com	Domain	In scope	Critical	Eligible
hiltonmanage.com	Domain	In scope	Critical	Eligible

Nos centraremos en los siguientes dominios raíz:

- 1) **hilton.com**
- 2) **hilton.io**
- 3) **hiltonmanage.com**

(Se había empezado a hacer el análisis con 2 dominios más, pero ha sido suficiente hacerlo con los 3 indicados por la gran cantidad de resultados obtenidos mediante las primeras herramientas reportadas en las siguientes páginas).

Entorno de investigación

Para la realización del análisis de la compañía **Hilton**, se va a usar un entorno virtualizado de **Kali Linux**, que vendrá ya con determinadas herramientas preinstaladas que se irán usando para encontrar información de interés.

También se usará una máquina virtual de **Greenbone** para realizar un escaneo automatizado de vulnerabilidades posibles.

Por último, y debido a la naturaleza de este tipo de investigaciones, se usarán también herramientas externas (**Cero, Gotator, Maltego, Spiderfoot**, etc.) y consultas a Redes Sociales conocidas como pueden ser **Linkedin, GitHub, Facebook, Instagram**, etc.

Footprinting

Por Footprinting entendemos el conjunto de técnicas utilizadas para recopilar información de un sistema. Sería una primera fase de reconocimiento, en la que se pueden descubrir posibles vectores hacia él. Las distintas técnicas dentro de esta etapa de investigación se clasifican en técnicas de reconocimiento horizontal o vertical.

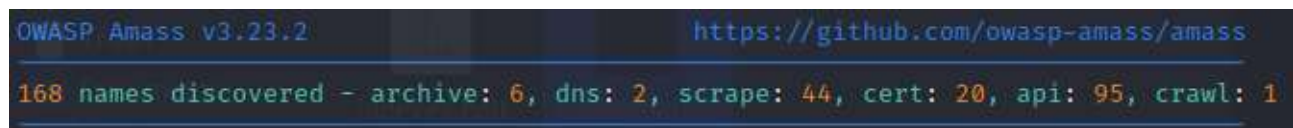
Iniciamos el análisis realizando un reconocimiento vertical mediante la herramienta **Amass**, que realiza técnicas de reconocimiento pasivo y activo, de OSINT, etc.

Antes de comenzar a usarla, se debe configurar el archivo **config.ini** con todas las variables y parámetros que se quieran aplicar en el momento de lanzar la herramienta (el archivo se adjuntará dentro de la carpeta que contendrá esta práctica). Indicaremos, por tanto, los dominios que queremos analizar para encontrar todos los subdominios posibles, desactivaremos la aplicación de fuerza bruta (que ya se realizará posteriormente), no haremos permutaciones, se añade alguna *API key* de aquellos servicios de los cuales disponemos de cuenta (aunque este paso no es estrictamente necesario), etc.

Tras este paso, ya estamos listos para lanzar **Amass** con el siguiente comando, desde la terminal de Linux:

```
amass enum -src -v -config config_practica.ini -dir hilton-amass
```

En este caso obtenemos **168 subdominios**:



```
OWASP Amass v3.23.2 https://github.com/owasp-amass/amass
168 names discovered - archive: 6, dns: 2, scrape: 44, cert: 20, api: 95, crawl: 1
```

Generamos, así, el archivo **amass_original.txt**

A continuación se realizará fuerza bruta para seguir intentando sacar el máximo de subdominios posibles. Para ello, haremos uso de diccionarios publicados en Internet (en este caso se ha utilizado [SecLists](#)).

Aunque, primeramente, utilizaremos la herramienta **DNSValidator**, con la cual obtendremos un listado de servidores DNS confiables para resolver los subdominios.

```
dnsvalidator -tL https://public-dns.info/nameservers.txt -threads 50 -o resolvers.txt
```

Obtenemos el archivo **resolvers.txt** con más de 5000 registros validados; de manera secundaria, si se observa que con tantos registros la aplicación de fuerza bruta se ralentiza en exceso, usaremos el archivo de **dns-resolvers.txt** incluido en las propias *SecLists* descargadas anteriormente, que tiene exactamente 986 registros

validados y sería totalmente usable.

Comenzamos a lanzar ataques de fuerza bruta con la herramienta **Puredns**, con los distintos dominios raíz y con un par de diccionarios de palabras en cada uno de ellos para descubrir más subdominios.

(1er diccionario: *namelist.txt* con el 1er dominio: **hilton.com**)

```
puredns bruteforce /root/Desktop/SecLists-master/Discovery/DNS/namelist.txt hilton.com -r  
resolvers.txt -w hilton10.txt
```

Obtenemos 385 registros en el archivo *hilton10.txt*

(2o diccionario: *shubs-subdomains.txt* para el 1er dominio también)

```
puredns bruteforce /root/Desktop/SecLists-master/Discovery/DNS/shubs-subdomains.txt hilton.com -r  
resolvers.txt -w hilton11.txt
```

Obtenemos 583 dominios válidos en el archivo *hilton11.txt*

Repetiremos 4 veces más este mismo comando combinando estos 2 mismos diccionarios con los 2 restantes dominios raíz del *scope* de Hilton. Por alguna razón, sólo se obtienen 5 subdominios más, generando así el archivo *hilton21.txt*.

Juntamos todos los resultados, filtrando para que no se repitan con el siguiente script:

```
sort -u amass_original.txt hilton10.txt hilton11.txt hilton21.txt > subdominios-hilton.txt
```

A continuación, se procede a realizar las permutaciones correspondientes con la herramienta **Gotator**, utilizando uno de los diccionarios de prefijos que aparecen en las *SecLists* (*deepmagic.com-prefixes-top500.txt*):

```
gotator -sub subdominios-hilton.txt -perm /root/Desktop/SecLists-  
master/Discovery/DNS/deepmagic.com-prefixes-top500.txt -depth 1 -numbers 10 -adv -md -mindup >  
gotator.txt
```

Se obtiene una gran cantidad de registros (mas de 10 millones). Con ánimo de “resolver” esta ingente cantidad de subdominios obtenidos con las permutaciones, utilizaremos **Puredns resolve**:

```
puredns resolve gotator.txt -r resolvers.txt -w sub-hilton.txt
```

Obtenemos 46 registros validados en el archivo *sub-hilton.txt*

Ahora, con ánimo de seguir filtrando y obteniendo más subdominios, vamos a analizar los certificados mediante la herramienta **Cero**. Lanzaremos los siguientes comandos, teniendo en cuenta los 3 dominios raíz escogidos al inicio.

```
cero < subdominios-hilton.txt | grep hilton.com > sub-cero1.txt
```

```
cero < subdominios-hilton.txt | grep hilton.io > sub-cero2.txt
```

```
cero < subdominios-hilton.txt | grep hiltonmanage.com > sub-cero3.txt
```

Obtenemos 201, 34 y 0 resultados, respectivamente.

Y volvemos a descartar los resultados repetidos, juntándolos en el archivo *sub-cero-total.txt* (106 registros)

```
sort -u sub-cero1.txt sub-cero2.txt sub-cero3.txt > sub-cero-total.txt
```

Y por último juntamos todos los subdominios que hemos ido obteniendo a lo largo de las acciones anteriores, generando el archivo *subdominios-hilton-total* con 803 subdominios:

```
sort -u sub-cero-total.txt subdominios-hilton.txt sub-hilton.txt > subdominios-hilton-total
```

A partir de aquí ya podemos considerar que se han reunido suficientes subdominios con la aplicación de las técnicas anteriores.

Vamos a utilizar ahora la herramienta **DNSx** para resolver estos subdominios y obtener el máximo número de Ips válidas:

```
dnsx -a -resp-only -l subdominios-hilton-total -o ips.txt
```

Que tras filtrar el resultado, para descartar las ips repetidas, obtenemos 215 direcciones IP.

Archivo: *ips-final.txt*

Y para preparar la fase de análisis de vulnerabilidades, se utiliza una vez más **DNSx** para encontrar aquellos subdominios que son nombres canónicos – **CNAME** –, es decir, aquellos que están apuntando a otros subdominios en vez de a una IP concreta. Esta información es relevante porque estos subdominios son susceptibles de recibir el ataque conocido como *Subdomain Takeover*, que permite a los atacantes hacerse con el control total del mismo, subir archivos, etc.

```
dnsx -cname -resp-only -l subdominios-hilton-total -o cname-final.txt
```

```
sort -u cname-final.txt > cname-total.txt
```

Localizamos 102 subdominios CNAME y generamos el archivo *cname-total.txt*

Tras todos estos pasos, se han obtenido:

- **803 subdominios → subdominios-hilton-total**
- **215 direcciones IP → ips-final.txt**
- **102 registros CNAME → cname-total.txt**

Fingerprinting

Fingerprinting normalmente se asocia a las técnicas de identificación y rastreamiento de un objetivo: tecnologías que utiliza, servidor y versión, puertos abiertos, sistema operativo, etc.

Identificación de puertos:

Para comenzar esta etapa de identificación, se deberían escanear los puertos de las direcciones IP's que se han encontrado en los pasos anteriores (en concreto, 65.535 puertos para cada IP).

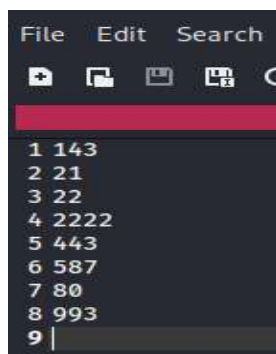
Debido a la gran cantidad de puertos, se suele utilizar para dar una primera pasada, la herramienta **Masscan**, que nos otorgará de mucha velocidad en el escaneo.

Utilizaremos el siguiente comando:

```
masscan -p0- -iL ips-final.txt --rate 5000 -oG masscan1.txt
```

Como se puede observar, obtenemos el fichero **masscan1.txt**.

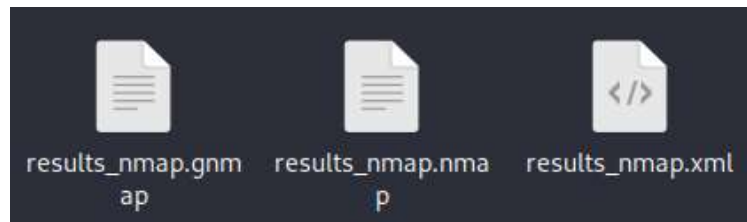
El parámetro rate indica la velocidad con la que hará el escaneo de puertos. Pese a que se ha intentado, no se ha podido poner una velocidad menor (que hubiera ofrecido un nivel de escaneo superior y, posiblemente, la localización de más puertos abiertos). El tiempo necesario para realizar el escaneo con una velocidad de 5000 ha sido de casi 6 horas y media, por ello se decide respetar el resultado obtenido (será el siguiente, tras aplicar un filtrado de los resultados: **puertos_masscan.txt**):



Con este listado de puertos abiertos, ahora usaremos la herramienta **Nmap** contra las mismas Ips que han sido escaneadas con Masscan; de este modo, se nos permitirá conocer los servicios y sus versiones correspondientes que corren a través de ellos. Se usará con el comando siguiente:

```
nmap -sS -n -Pn -sV -sC -O -vv --open --reason -p 21,22,80,143,443,587,993,2222 -oA results_nmap -iL ips-final.txt
```

La mayoría de resultados apuntan a los servicios http y https de los puertos 80 y 443, respectivamente.



Identificación web:

Para la identificación web, usaremos la herramienta **Httpx**, que nos permitirá escanear aquellos subdominios que tengan puertos HTTP abiertos, centrándonos en los puertos que comúnmente despliegan este tipo de servicios. La usaremos con el comando:

```
httpx -p 80,443,8080,8000,8001,8443,8008 -list subdominios-hilton-total -silent -o webs2.txt
```

Obtenemos 766 direcciones web o subdominios., en el archivo *webs2.txt*.

Ahora sería conveniente filtrar estas webs obtenidas para ver cuales de ellas no están protegidas por un WAF (*Web Application Firewall*). La herramienta que nos permitirá descubrir esta información será **Waf00f**, que usaremos del siguiente modo, a través de la consola de comandos también:

```
wafw00f -i http_apps.txt -o wafwebs.txt -v
```

686 registros en el archivo *wafwebs.txt*

Filtramos el resultado para que sólo tengamos las urls, creando así el archivo *nowafwebs.txt*.

El siguiente paso será utilizar la herramienta **EyeWitness**, con la que realizaremos capturas de pantalla para todos los servicios web descubiertos. Obtendremos la carpeta *hilton.webs*.

```
eyewitness --web -f webs2.txt -d hilton-webs
```

El resultado no ha sido óptimo. La mayoría de capturas apuntan a errores desconocidos, errores por acceso denegado, etc.

Table of Contents

- Uncategorized (Page 1)
- 401/403 Unauthorized (Page 1)
- 404 Not Found (Page 1)

Uncategorized	2
401/403 Unauthorized	4
404 Not Found	2
Errors	753
Total	761

Web Request Info	Web Screenshot
http://SiteManager.hilton.com Resolved to: 167.187.100.51 Page Title: 403 - Forbidden: Access is denied. Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Sat, 24 Jun 2023 08:11:10 GMT Connection: close Content-Length: 1233 Response Code: 403 Source Code	<div> <div>Server Error</div> <div> <div>403 - Forbidden: Access is denied.</div> <div>You do not have permission to view this directory or page using the credentials that you supplied.</div> </div> </div>

http://af.hilton.com Resolved to: 184.24.14.92 Page Title: Access Denied Server: AkamaiGHost Mime-Version: 1.0 Content-Type: text/html Content-Length: 263 Expires: Sat, 24 Jun 2023 08:11:56 GMT Date: Sat, 24 Jun 2023 08:11:56 GMT Connection: close Response Code: 403 Source Code	Access Denied You don't have permission to access "http://af.hilton.com/" on this server. Reference #18.11551060.1687594315.26a93def
--	---

Web Request Info	Web Screenshot
http://a1.hilton.com Resolved to: 52.25.5.50 Page Title: 404 Date: Sat, 24 Jun 2023 08:11:14 GMT Content-Type: text/html Content-Length: 217 Connection: close Server: Apache Last-Modified: Thu, 01 Oct 2020 11:02:38 GMT ETag: "d9-5b099f44a600b" Accept-Ranges: bytes Response Code: 404 Source Code	404, not found.

Errors

Web Request Info	Web Screenshot
http://aloha-1.hilton.com Resolved to: 167.187.103.215	Unknown error while attempting to screenshot
https://aloha-1.hilton.com Resolved to: 167.187.103.215	Unknown error while attempting to screenshot
http://albuquerque.hilton.com Resolved to: 167.187.200.18	Unknown error while attempting to screenshot
http://aloha.hilton.com Resolved to: 167.187.103.217	Unknown error while attempting to screenshot
http://albany.hilton.com Resolved to: 167.187.200.18	Unknown error while attempting to screenshot
https://alumni.hilton.com:8443 https://alumni.hilton.com Resolved to: 44.208.138.79	Unknown error while attempting to screenshot

Y también un par de página web de *login* para algún servicio desconocido:

Web Request Info	Web Screenshot
https://acrl.hilton.com Resolved to: 167.187.101.96 Page Title: the Lobby Login X-Frame-Options: SAMEORIGIN Referrer-Policy: origin Content-Type: text/html; charset=utf-8 Content-Length: 9158 X-EdgeConnect-MidMile-RTT: 105 X-EdgeConnect-Origin-MEX-Latency: 38 Expires: Sat, 24 Jun 2023 08:11:28 GMT Cache-Control: max-age=0, no-cache, no-store Pragma: no-cache Date: Sat, 24 Jun 2023 08:11:28 GMT Connection: close Set-Cookie: PF=hKBKmCBKMJNdodqv03fBvT; Path=/; Secure; HttpOnly; SameSite=None Response Code: 200 Source Code	

Posteriormente, se puede utilizar la herramienta **whatweb**, que nos ofrecerá información adicional de las distintas Ips que hemos obtenido.

```
whatweb -a 3 -i nowafwebs.txt --color=never > whatwebs.txt
```

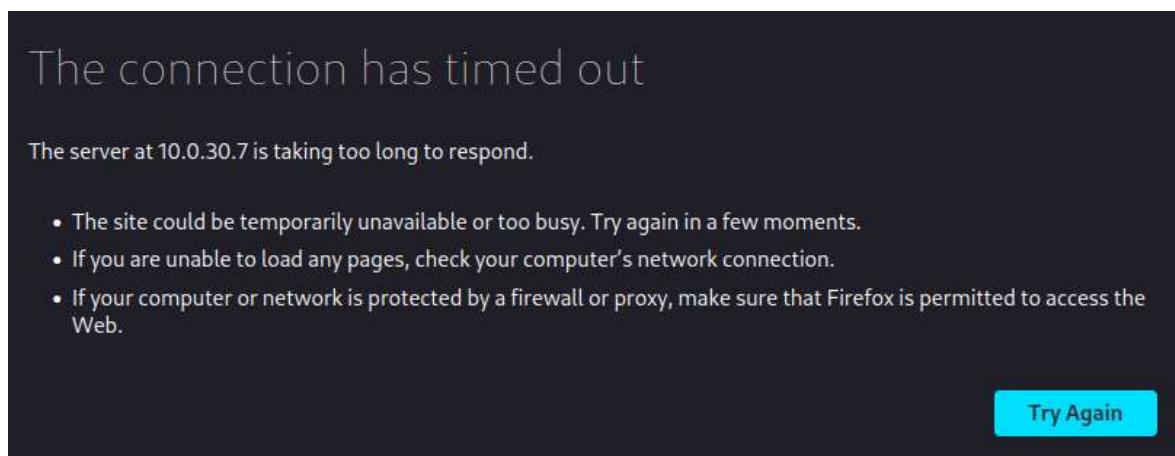
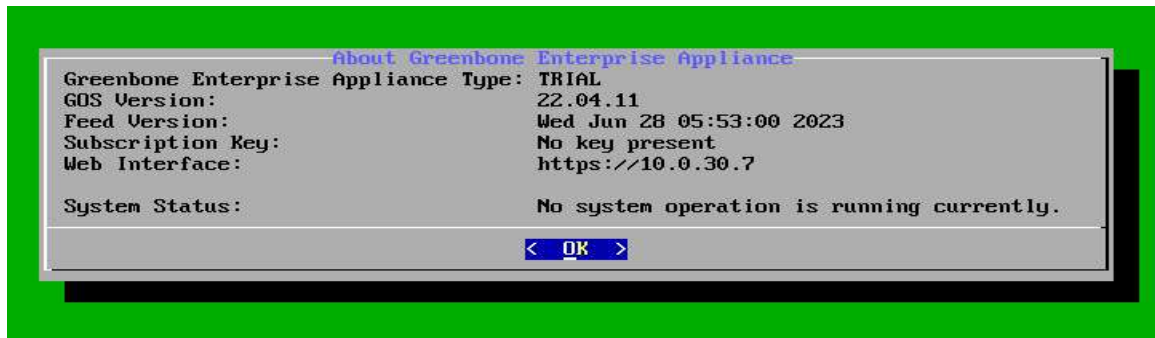
A modo de ejemplo:

```
1034 https://apac.hilton.com/amexkrisflyer [200 OK] Bootstrap[4.6.1],  
Cookies[XSRF-TOKEN,amex_kfa_hilton_redemption_session], Country[UNITED  
STATES][US], Frame, HTML5, HTTPServer[Ubuntu Linux][nginx/1.14.0  
(Ubuntu)], HttpOnly[XSRF-TOKEN,amex_kfa_hilton_redemption_session],  
IP[167.71.197.30], JQuery[1.11.2,3.6.0], Script[text/javascript], Strict-  
Transport-Security[max-age=31536000; includeSubDomains; preload],  
Title[Amex KFA Hilton Redemption], UncommonHeaders[x-content-type-  
options], probably WordPress, X-Frame-Options[SAMEORIGIN], X-UA-  
Compatible[IE=EmulateIE7,IE=edge], nginx[1.14.0]  
1035 https://www.managementservices.hilton.com/ [301 Moved Permanently] Apache,  
Country[UNITED STATES][US], HTTPServer[Apache], IP[198.61.165.107],  
RedirectLocation[https://managementservices.hilton.com//], Strict-  
Transport-Security[max-age=31536000; includeSubDomains; preload],  
Title[301 Moved Permanently]  
1036 https://www.hilton.com/en/hotels/ISTHITW [403 Forbidden] Country[EUROPEAN  
UNION][EU], HTML5, HTTPServer[AkamaiNetStorage], IP[92.123.32.164],  
Script[text/javascript], Title[Hilton Page Reference Code], X-UA-  
Compatible[ie=edge]
```

Por último, se intenta hacer descubrimiento de contenido usando la herramienta **Dirsearch**, pero no se ha conseguido que se ejecutara correctamente.

Análisis de vulnerabilidades

Un buen punto de inicio sería realizar un análisis de software a varias máquinas con puertos abiertos mediante alguna herramienta que automatice esta tarea; se ha intentado usar **Greenbone Community Edition**, pero por algún tipo de error (creo que proveniente de VirtualBox) no ha acabado de funcionar. Error: no se puede abrir la interfaz web de ningún modo, pese a comprobar conectividad, IP correspondiente, configuración de Greenbone, etc.



Realizaremos un análisis de vulnerabilidades web con la herramienta **Nuclei**, aprovechando el documento en el que hemos guardado todas las IP's anteriormente. Lo usaremos con el comando:

```
nuclei -l ips-final.txt -o nuclei-results.txt
```

Se encuentran las siguientes vulnerabilidades:

```
[revoked-ssl-certificate] [ssl] [low] 104.239.192.125:443
[untrusted-root-certificate] [ssl] [low] 142.0.173.134:443
[weak-cipher-suites] [ssl] [medium] 162.242.170.33:443 [[tls10 TLS_ECDHE_RSA_
WITH_AES_128_CBC_SHA]]
```

Y algún servicio o aplicación que no está actualizado a la última versión o alguna mala configuración de las cabeceras HTTP, pero no lo considera como una vulnerabilidad como tal.

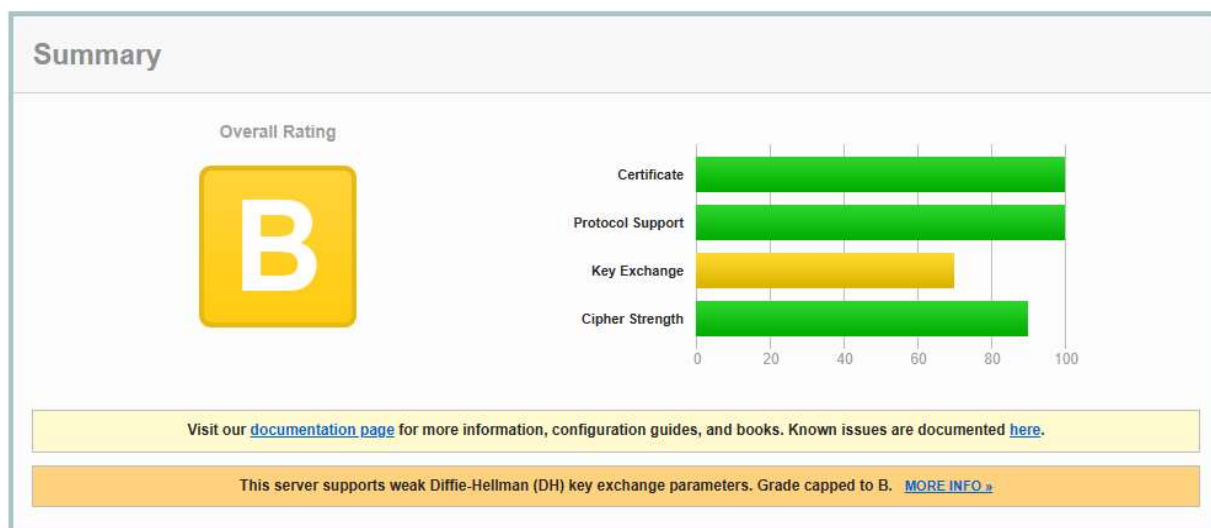
Con la herramienta **Subzy** podemos comprobar que los subdominios que aparecían en los registros **CNAME** (obtenidos anteriormente, en la primera fase de reconocimiento) no presenten vulnerabilidades relacionadas con, el indicado anteriormente también, *Subdomain Takeover*.

```
subzy run --targets cname-total.txt
```

Pero no se encuentra ninguna vulnerabilidad al respecto.

```
(root@kali) - [~/Desktop/Footprinting]
# subzy run --targets cname-total.txt
[ * ] Fingerprints not found; saving them to "/root/subzy/fingerprints.json"
[ * ] Loaded 102 targets
[ * ] Loaded 44 fingerprints
[ No ] HTTPS by default (--https)
[ 10 ] Concurrent requests (--concurrency)
[ No ] Check target only if SSL is valid (--verify_ssl)
[ 10 ] HTTP request timeout (in seconds) (--timeout)
[ No ] Show only potentially vulnerable subdomains (--hide_fails)
[ NOT VULNERABLE ] - apic-s.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apip.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apip-prv.hilton.io.edgekey.net
[ NOT VULNERABLE ] - api.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apic.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apic-prv.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apic-t.hilton.io.edgekey.net
[ NOT VULNERABLE ] - api-prv.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apip-t.hilton.io.edgekey.net
[ NOT VULNERABLE ] - apip-s.hilton.io.edgekey.net
```

Utilizamos el servicio web [SSL Labs](https://www.ssllabs.com/) para analizar el TLS/SSL del dominio raíz principal (**hilton.com**). Se obtiene el siguiente resultado:



Parecido al resultado de aplicar la herramienta Nuclei, se nos informa de que hay claves o logaritmos de cifrado débiles.

Ahora se hace un análisis de los mecanismos de cifrado de las aplicaciones con la herramienta **Testssl** cogiendo las webs obtenidas en los pasos anteriores:

```
testssl -iL webs2.txt -log
```

(Se agrupa el contenido de todos los *logs* en el archivo *ssl-total.log*)

Se encuentran exclusivamente 2 tipos de vulnerabilidades en varias webs analizadas:

```
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
BREACH (CVE-2013-3587) potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
```

CVE-2013-3587 : el protocolo HTTPS, como es usado en aplicaciones web no especificadas, puede cifrar datos comprimidos sin ofuscar apropiadamente la longitud de los datos no cifrados, facilitando a atacantes de tipo “*man-in-the-middle*” obtener valores secretos en texto plano al observar las diferencias de longitud durante una serie de adivinaciones en las que una cadena en una URL de peticiones HTTP coincide potencialmente con una cadena desconocida en un cuerpo de respuesta HTTP.

Impacto

Vector 3.x CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Puntuación base 3.x 5.90

Severidad 3.x MEDIA

Vector 2.0 AV:N/AC:M/Au:N/C:P/I:N/A:N

Puntuación base 2.0 4.30

Severidad 2.0 Pendiente de análisis

CVE-2013-0169: permite a atacantes remotos llevar a cabo ataques de distinción y de recuperación de texto plano mediante el análisis estadístico de datos de temporización para paquetes manipulados, también conocido como el problema de “*Lucky Thirteen*”.

- CVSS Scores & Vulnerability Types	
CVSS Score	2.6
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	310

Para la comprobación de servicios de correos, se ha usado el servicio web *dmarc analyzer* contra el dominio raíz **hilton.com**.

Pero en este caso no se ha encontrado nada relevante.

hilton.com

DNS Record Total look ups: 8 Look ups: 4

No problems were detected with this record

v=spf1 include:spf.protection.outlook.com include:_spf-a.hilton.com include:_spf-b.hilton.com include:_spf-c.hilton.com -all

spf.protection.outlook.com

DNS Record Look ups: 0

No problems were detected with this record

v=spf1 ip4:40.92.0.0/15 ip4:40.107.0.0/16 ip4:52.100.0.0/14 ip4:104.47.0.0/17 ip6:2a01:111:f400::/48 ip6:2a01:111:f403::/49 ip6:2a01:111:f403:8000::/50 ip6:2a01:111:f403:c000::/51 ip6:2a01:111:f403:f000::/52 -all

IP Records

40.92.0.0/15
40.107.0.0/16
52.100.0.0/14
104.47.0.0/17
2a01:111:f400::/48
2a01:111:f403::/49
2a01:111:f403:8000::/50
2a01:111:f403:c000::/51
2a01:111:f403:f000::/52

_spf-a.hilton.com

DNS Record Look ups: 1

No problems were detected with this record

```
v=spf1 a:mail.hiltonres.com ip4:192.251.124.90 ip4:167.187.200.23 ip4:167.187.100.149 ip4:167.187.100.14 ip4:167.187.100.163 ip4:167.187.100.164 -all
```

A/AAAA Records

mail.hiltonres.com

- A - 204.0.9.10

IP Records

```
192.251.124.90
167.187.200.23
167.187.100.149
167.187.100.14
167.187.100.163
167.187.100.164
```

_spf-b.hilton.com

DNS Record Look ups: 2

No problems were detected with this record

```
v=spf1 a:mail2.hiltonres.com include:_spf.salesforce.com ip4:167.187.100.153 ip4:167.187.100.152 -all
```

A/AAAA Records

mail2.hiltonres.com

- A - 63.127.180.66

IP Records

```
167.187.100.153
167.187.100.152
```

_spf.salesforce.com

DNS Record Look ups: 1

No problems were detected with this record

```
v=spf1 exists:%{_spf.mta.salesforce.com} -all
```

%{_spf.mta.salesforce.com}

Example: 192.0.2.3._spf.mta.salesforce.com

%{_}

The IP address of the sender (Example: 192.0.2.3)

_spf-c.hilton.com


DNS Record Look ups: 0

```
v=spf1 ip4:184.73.165.130 ip4:54.75.242.97 ip4:54.251.34.9 ip4:50.16.214.104 ip4:54.228.189.137 ip4:54.254.102.43 ip4:174.129.192.189 ip4:167.187.9.82 ip4:167.187.9.83 -all
```

IP Records

```
184.73.165.130
54.75.242.97
54.251.34.9
50.16.214.104
54.228.189.137
54.254.102.43
174.129.192.189
167.187.9.82
167.187.9.83
```


Y con el servicio web de [dmarcian](#), hallamos que **hilton.com** es susceptible de recibir ataques de *phishing*:




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

v=DMARC1;p=quarantine;fo=1;rua=mailto:dmarc_rua@hilton.com;ruf=mailto:dmarc_ruf@hilton.com

For more insight into your DMARC record we recommend our [DMARC Inspector](#).




SPF

Your domain has a valid SPF record and the policy is sufficiently strict.

— Details

v=spf1
include:spf.protection.outlook.com
include:_spf-a.hilton.com include:_spf-b.hilton.com include:_spf-c.hilton.com
-all

For more insight into your SPF record we recommend our [SPF Surveyor](#).



DKIM

Your DKIM record is valid.

— Details

v=DKIM1; k=rsa;
p=MlIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBcGKCAQEAvIR5SLtVvsU2c46scwrUfpW25/h9ZiOMs3ctvwnniLXYM2lvx0Zpzb6W6tAhNhZKPQREILRJEar80iH7P00FZCwofoTJgkJe6RpKfeUFZj85NF5yO8BRd3jo0kM9bbgIf80C+yjc4lrzhL9D8FxeFodEail0Uvr00m+bPTpZlcVyyhv3WdrwrdiK00U+IZlp0F9lghUOSnfrSiFPGxeuCnCclHR3ziUsqrBuMlfeMe8X36tX6G3+1+WkQ+SRM5jSBaYdBe+FrBbjenPUzEhteZa36OwesES2Z9tMO6dxbXfvJSQDxtgBo4FvIOPC+R65j9ZGEb7uXNe3tcM4ehyprwQIDAQAB;

For more insight into your DKIM record we recommend our [DKIM Inspector](#).

OSINT

Open Source Intelligent: conjunto de herramientas y técnicas utilizadas para la recopilación de información pública.

Se puede empezar esta etapa de la investigación haciendo un rastreo simple en Internet para ver si podemos conseguir datos básicos del objetivo, tales como la empresa matriz (**Hilton Worldwide Holdings Inc.**) , la web principal, datos históricos, director general de la compañía, fundador, etc.

Hilton Hotels & Resorts	
	
Hilton	
HOTELS & RESORTS	
Tipo	Hotel
ISIN	US43300A1043
Industria	hostelería
Forma legal	empresa privada
Fundación	1919
Fundador	Conrad Hilton
Sede central	Cisco, Texas, Estados Unidos
Productos	Residencia temporal
Servicios	Hoteles Turismo
Empleados	15000
Empresa matriz	Hilton Worldwide
Sitio web	hilton.com
[editar datos en Wikidata]	

Así mismo, siempre deberíamos observar la página web principal (www.hilton.com) e intentar ver qué información podría sernos de utilidad: marcas de la compañía, sección de “prensa”, organigrama, información sobre los ejecutivos con la que luego localizarles en redes sociales, etc.

NUESTRAS MARCAS



Executive Bios

Shaping Global Business

Collectively, our Executive Committee brings in over 200 years of experience to the company. With diverse backgrounds and proven track records of success, they're well positioned to keep Hilton at the forefront of the hospitality industry.



Christopher J. Nassetta

President & Chief Executive Officer



Kristin Campbell

General Counsel



Laura Fuentes

Executive Vice President & Chief Human Resources Officer



Danny Hughes

Executive Vice President & President, Americas



Kevin Jacobs

Chief Financial Officer & President, Global Development



Katherine Lugar

Executive Vice President, Corporate Affairs



Matthew W. Schuyler

Chief Brand Officer



Chris Silcock

Executive Vice President & Chief Commercial Officer



Simon Vincent

Executive Vice President & President, Europe, Middle East & Africa



Alan Watts

President, Asia Pacific

Christopher J. Nassetta

President & Chief Executive Officer



También se puede realizar una búsqueda de documentos públicos y reguladores. Por ejemplo, registros regulatorios, informes financieros, presentaciones públicas, etc...

**UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION**

**SECURITIES EXCHANGE ACT OF 1934
Release No. 90052 / September 30, 2020**

**ACCOUNTING AND AUDITING ENFORCEMENT
Release No. 4182 / September 30, 2020**

**ADMINISTRATIVE PROCEEDING
File No. 3-20109**

In the Matter of

**HILTON WORLDWIDE
HOLDINGS INC.,**

Respondent.

**ORDER INSTITUTING CEASE-AND-
DESIST PROCEEDINGS PURSUANT TO
SECTION 21C OF THE SECURITIES
EXCHANGE ACT OF 1934, MAKING
FINDINGS, AND IMPOSING A CEASE-
AND-DESIST ORDER**

Se pueden usar búsqueda en Google con palabras clave, para encontrar noticias relativas a incidentes de ciberseguridad, que nos den pistas sobre por donde abordar un posible ataque.

HOTELES HILTON



ROBAN DATOS DE TARJETAS DE CRÉDITO USADAS EN HOTELES HILTON

ON: SEPTEMBER 29, 2015 / IN: MALWARE - VIRUS

Los clientes que hayan usado sus tarjetas de crédito en hoteles Hilton o en locales dentro de ellos podrían ser víctimas del robo de datos bancarios: entidades financieras están investigando

[LEER MÁS](#)

Un paso importante sería intentar localizar direcciones de correo electrónico pertenecientes a trabajadores de la compañía (práctica muy común cuando se quieren lanzar campañas de *phishing*). El servicio web hunter.io puede ser muy útil para ello y para conocer el formato general que tienen los emails corporativos:

Domain Search [®]

hilton.com

hilton.com 8,394 results x

Filters ^

Q

Type v

Department v

Show only results with v

8,394 results for your search

Export

Find by name v

Christine Conner

christine.conner@hilton.com

94%

Save as lead

2 sources v

Karla Spotts

karla.spotts@hilton.com

94%

Save as lead

3 sources v

Praveen Kumar

praveen.kumar@hilton.com

Company ^

Hilton

Explore Hilton's portfolio of hotels and distinct brands across the globe. Book directly for the best rates during your next st... more

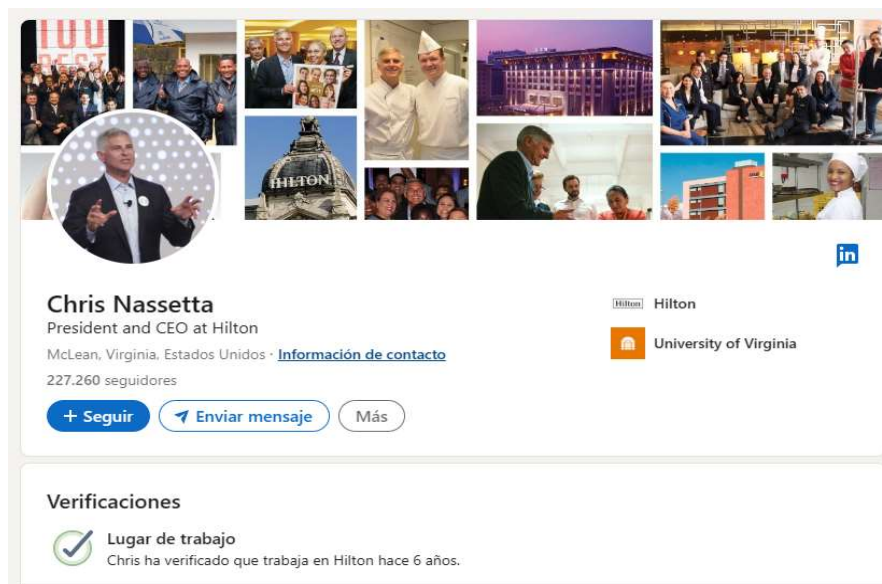
Email pattern: {first}.{last}@hilton.com

Accept all: YES [®]

Industry: Travel

Address: 1 Monarch Beach, 92629, Dana Point, California, United States

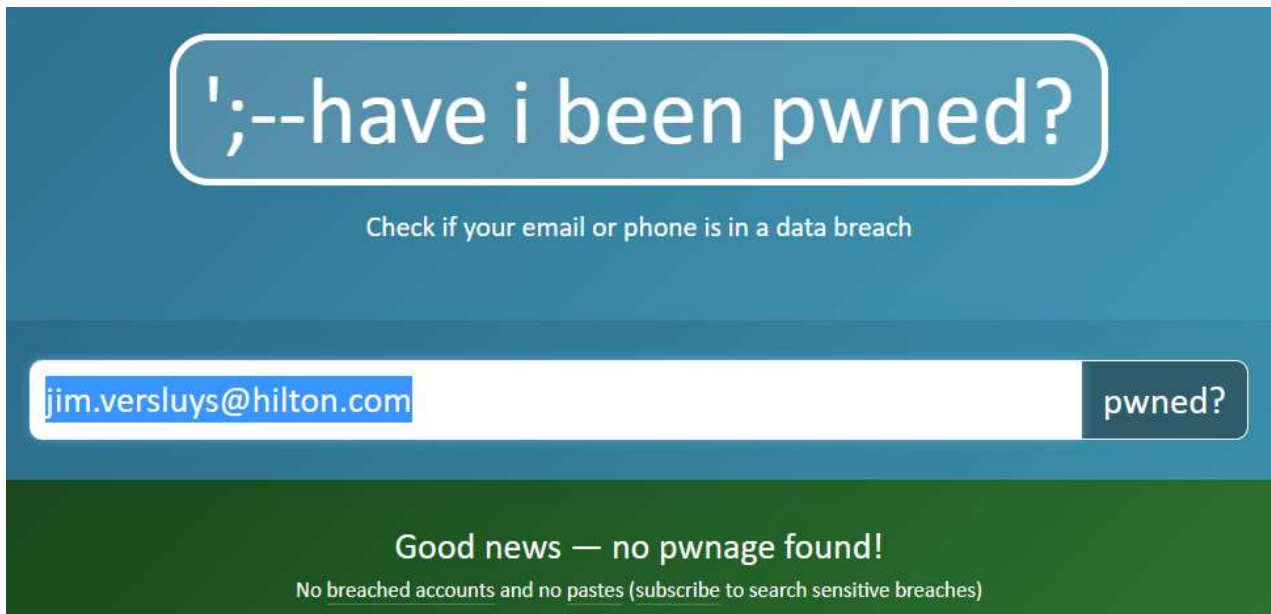
También es interesante entrar en redes sociales, especialmente para localizar información y perfiles del equipo directivo de la compañía. En este caso, la tarea es muy fácil, ya que como se ha mostrado en una captura de pantalla anterior, en la propia página web oficial de Hilton, se ofrecen *links* de acceso directo a las redes sociales de los principales ejecutivos de la compañía (conocer datos de aquellos actores que más privilegios tienen dentro de la compañía, puede facilitar la tarea de atacar con éxito la compañía).



En **Github** (que puede ser una buena fuente de información a través de repositorios, usuarios de la plataforma y que pertenecen a la compañía, etc.) no se ha encontrado nada relevante. Así mismo, con la herramienta **Github-search** tampoco se ha hallado ninguna pista relevante.

Y con la web haveibeenpwned.com podríamos realizar una búsqueda de alguno de los mails localizados para ver si ha sido comprometido por alguna brecha de seguridad.

En este caso en concreto, y tras realizar varias búsquedas, no se ha encontrado nada relevante.



';--have i been pwned?

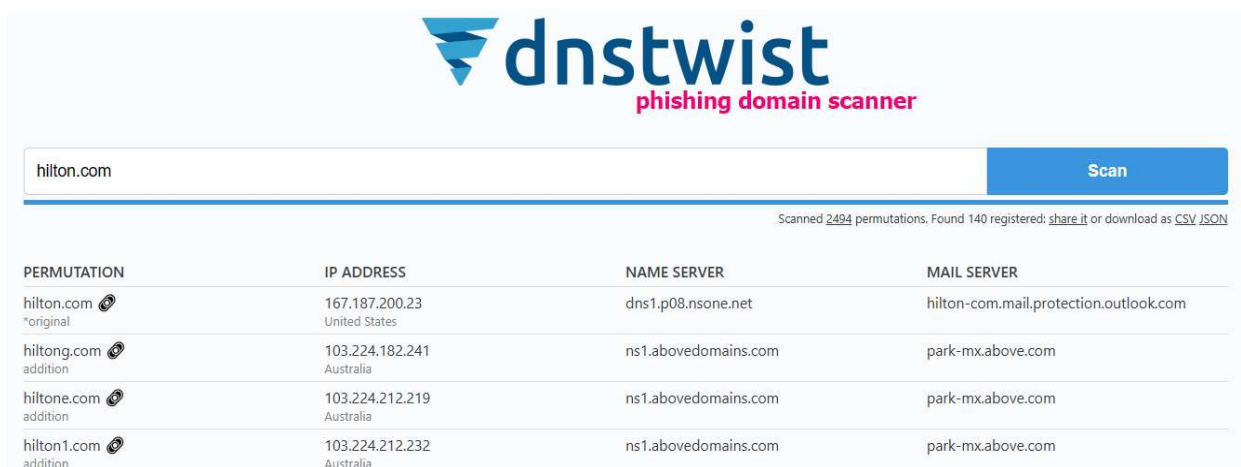
Check if your email or phone is in a data breach






jim.versluys@hilton.com pwned?

Good news — no pwnage found!

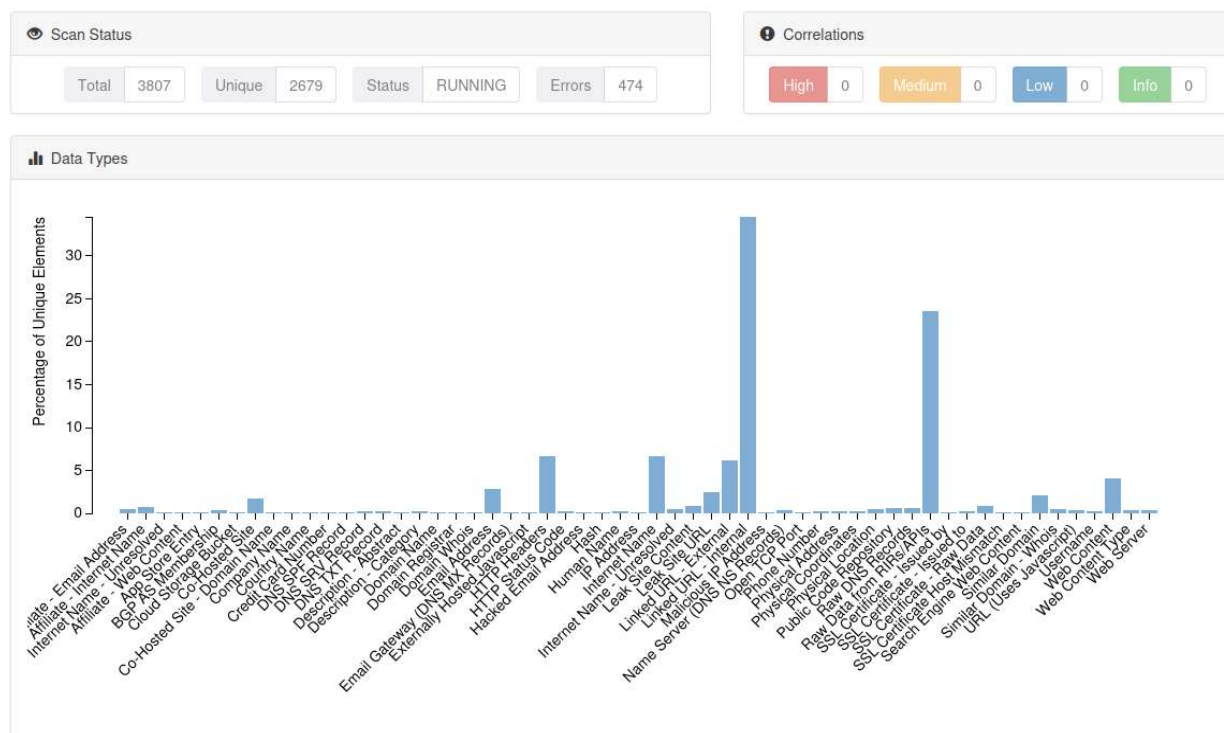
No breached accounts and no pastes (subscribe to search sensitive breaches)

La web dnstwist.it nos puede brindar información sobre las dominios más parecidos al original y central de la compañía, que también puede facilitar ataques de *phishing*.



 dnstwist phishing domain scanner			
hilton.com			Scan
Scanned 2494 permutations. Found 140 registered: share it or download as CSV JSON			
PERMUTATION	IP ADDRESS	NAME SERVER	MAIL SERVER
hilton.com  *original	167.187.200.23 United States	dns1.p08.nsone.net	hilton-com.mail.protection.outlook.com
hiltong.com  addition	103.224.182.241 Australia	ns1.abovedomains.com	park-mx.above.com
hiltone.com  addition	103.224.212.219 Australia	ns1.abovedomains.com	park-mx.above.com
hilton1.com  addition	103.224.212.232 Australia	ns1.abovedomains.com	park-mx.above.com

Y siempre nos podremos ayudar de software que automatice estas búsquedas, tales como **Maltego**, **Spiderfoot**, etc. (que tienen versiones gratuitas limitadas y de pago con más funcionalidades). En este caso se ha hecho una rápida búsqueda con **SpiderFoot** a través de la máquina virtual de Kali Linux, y esta es la información que se ha encontrado tras poner como objetivo el dominio raíz **hilton.com**.



Destacan especialmente los *flags*: Linked URL – internal, RAW data from RIRs/APIs, HTTP Headers, Internet Name, Linked URL – external.

Por lo general, este tipo de búsquedas requieren de paciencia y minuciosidad con tal de acabar encontrando información que pueda comprometer la seguridad de la compañía. Por ejemplo, en LinkedIn se podían encontrar casi 3000 contactos referenciados con la compañía **Hilton** y, si se dispusiera de una cuenta Pro de LinkedIn, se podría hacer una búsqueda de cada uno de los trabajadores o ex-trabajadores que aparecieran, para intentar ir desgranando fugas de información, otros *mails* corporativos, contactos varios, etc.

Por lo general, pareciera que la securización de la compañía **Hilton** es buena, puesto que haciendo análisis generales de las redes sociales de algunos de sus integrantes, especialmente la cúpula directiva, no es fácil encontrar datos personales de los mismos (como perfiles personales de otras RRSS, correos electrónicos personales, etc.)