Recopilacion de Informacion

De

Daniel Shved

Nuestro objetivos es *BlackRock.com e *ishares.com

•Dominios relacionados

• Información de cada dominio.

• Análisis de vulnerabilidades.

• Correos corporativos.

HERRAMIENTAS USADAS:

Aclarar que algunas las use únicamente para aprender, y otras no pude lanzarlas y no tuve tiempo para arreglarlo. No todas tienen una utilidad practica pues la información se solapa entre unas y otras.

- https://bgp.he.net/
- nslookup: mira los dns records para ip.
- Puredns bruteforce : fuerza bruta dns de blackrock.com
- gotator: permutaciones dns.
- Puredns resolve : para ver los validos.
- dig: para ver si se puede sacar ip o es servidor de carga o intermediario.
- https://viewdns.info/dnsreport/?domain=blackrock.com
- Dnsnum: ips de servidores principales, ¿6 servidores de carga? y 2 mail. Intento de trasnferencia de zona.
- Robot.txt mas subdominios
- Google Dorks para buscar documentos.
- Ctfr
- Amass: Mucha información y modo activo.
- Nmap, puertos y modo agresivo
- Greenbone / Open Vas: Escaner Vulnerabiliades.

ASN:

Lista de rangos de servidores de Black Rock

NSLOOKUP:

Intento de sacar información genérica de los servidores principales:

```
┌──(kali㉿kali)-[~/Herramientas/BlackRock]
└─$ nslookup https://www.blackrock.com/
Server:         8.8.8.8
Address:        8.8.8.8#53

** server can't find https://www.blackrock.com/: NXDOMAIN


┌──(kali㉿kali)-[~/Herramientas/BlackRock]
└─$
```

PUREDNS

Utilizamos fuerza bruta con puredns para sacar dominios

```
┌──(kali㊍kali)-[~/Herramientas/dnsresolvers]
└─$ puredns bruteforce /home/kali/Herramientas/SecLists/Discovery/DNS/namelist.txt  b
w output.txt


    _
   | |
   | |___   __  _  __  ___    __  _ __   ___
   |  _  | |  ||  ||  |/ _ \  /  || '_ \ / __|
   | |_) | |_||_||__|\  __/  \  || | | |\__ \
   |_.__/\__,_||   \___|  \_||_| |_||___/
   | |
   |_|               puredns v2.0.1

Fast and accurate DNS resolving and bruteforcing


Crafted with <3 by @d3mondev
https://github.com/sponsors/d3mondev


   ─────────────────────────────────────────────
   [+] Mode                  : bruteforce
   [+] Domain                : blackrock.com
   [+] Wordlist              : /home/kali/Herramientas/SecLists/Discovery/DNS/namelist.tx
   [+] Resolvers             : resolvers.txt
   [+] Rate Limit            : unlimited
   [+] Rate Limit (Trusted)  : 500 qps
   [+] Wildcard Threads      : 100
   [+] Wildcard Tests        : 3
   [+] Write Domains         : output.txt
   ─────────────────────────────────────────────


Resolving domains with public resolvers
[ETA 00:00:00] |███████████████████████████████| 151265/151265 rate: 3370 qps

Detecting wildcard root subdomains
[ETA 00:00:00] |███████████████████████████████| 126/126 queries: 100 (time: 0

Validating domains against trusted resolvers
[ETA 00:00:00] |███████████████████████████████| 126/126 rate: 126 qps (time:

Found 126 valid domains:
alumni.blackrock.com
tms.blackrock.com
www.blackrock.com
emea.blackrock.com
it.blackrock.com
remote.blackrock.com
mybenefits.blackrock.com
pru.blackrock.com
legacy.blackrock.com
vcs.blackrock.com
csg.blackrock.com
apps.blackrock.com
```

GOTATOR

Utilizamos gotator para hacer permutaciones de dominios.

```
[1] working in progress

┌──(kali㉿kali)-[~]
└─$ gotator -sub /home/kali/Herramientas/Texto/blackrockgot.txt -perm /home/kali/Herramien
tas/SecLists/Discovery/DNS/deepmagic.com-prefixes-top500.txt -depth 1 -numbers 10 -mindup
-adv -md > gotator1.txt
```

```
┌──(kali㉿kali)-[~]
└─$ cat gotator1.txt
blackrock.com
ishares.com
reserved-multicast-range-not-delegated.ishares.com
reserved.ishares.com
multicast.ishares.com
range.ishares.com
not.ishares.com
delegated.ishares.com
nothing.ishares.com
dynamic.ishares.com
static.ishares.com
dip.ishares.com
pools.ishares.com
rev.ishares.com
dsl.ishares.com
cable.ishares.com
ip.ishares.com
ipt.ishares.com
res.ishares.com
163data.ishares.com
164data.ishares.com
162data.ishares.com
165data.ishares.com
161data.ishares.com
166data.ishares.com
160data.ishares.com
```

UTILIZAMOS PUREDNS PARA VALIDAR

Puredns resolve para validar. Resultado en archivo adjunto listadominios.txt

```
kali@kali: ~/Herramientas/SecLists/Discovery/DNS ×   kali@kali: ~ ×
└─$ puredns resolve gotator1.txt -r /home/kali/Herramientas/dnsresolvers/resolvers.txt

puredns

        puredns v2.0.1
Fast and accurate DNS resolving and bruteforcing

Crafted with ♥ by @d3mondev
https://github.com/sponsors/d3mondev

[*] Mode                   : resolve
[*] File                   : gotator1.txt
[*] Resolvers              : /home/kali/Herramientas/dnsresolvers/resolvers.txt
[*] Rate Limit             : unlimited
[*] Rate Limit (Trusted)   : 500 qps
[*] Wildcard Threads       : 100
[*] Wildcard Tests         : 3

Resolving domains with public resolvers
[ETA 00:00:00] |                          | 3310/3310 rate: 3310 qps (time: 00
[ETA 00:00:00] |                          | 3310/3310 rate: 3310 qps (time: 00
[ETA 00:00:00] |                          | 3310/3310 rate: 3310 qps (time: 00
[ETA 00:00:00] |                          | 3310/3310 rate: 3310 qps (time: 00
[ETA 00:00:00] |                          | 3310/3310 rate: 3310 qps (time: 00
:00)

Detecting wildcard root subdomains
[ETA 00:00:00] |                          | 34/34 queries: 32 (time: 00:00:00)

Validating domains against trusted resolvers
[ETA 00:00:00] |                          | 34/34 rate: 34 qps (time: 00:00:00
[ETA 00:00:00] |                          | 34/34 rate: 34 qps (time: 00:00:00
[ETA 00:00:00] |                          | 34/34 rate: 34 qps (time: 00:00:00
)

Found 34 valid domains:
ns4.blackrock.com
ns.blackrock.com
www.blackrock.com
uk.ishares.com
blackrock.com
ns1.blackrock.com
us.ishares.com
jp.blackrock.com
de.ishares.com
ca.ishares.com
```

Intente sacar mas dominios con favicon https://www.blackrock.com/blk-corp-assets/favicon.ico
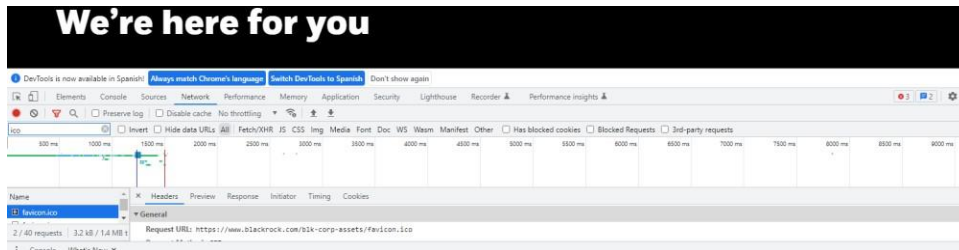
Resultado murmurnash 416443431

Pero me daba error en shodan.

VIEWDNS

View dns nos da la ip de los 6 servidores principales

https://viewdns.info/dnsreport/?domain=blackrock.com
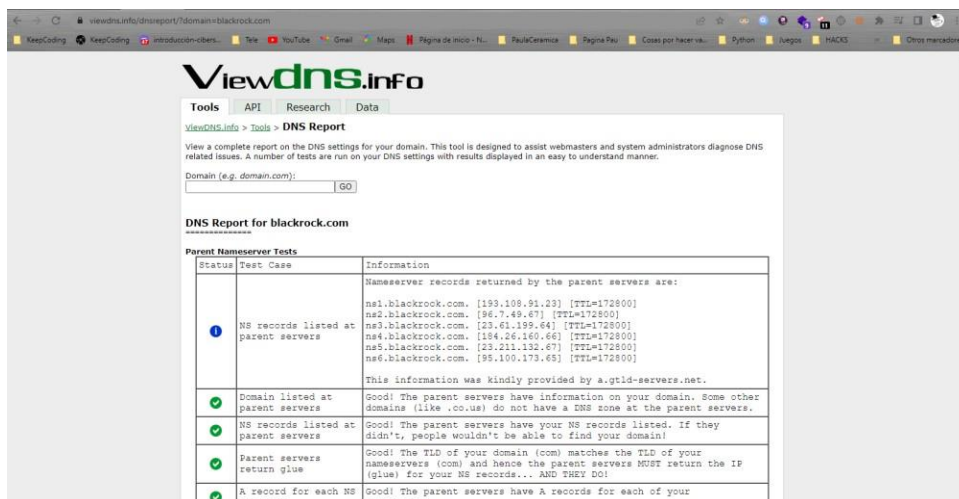
ns1.blackrock.com. [193.108.91.23] [TTL=172800]
ns2.blackrock.com. [96.7.49.67] [TTL=172800]
ns3.blackrock.com. [23.61.199.64] [TTL=172800]
ns4.blackrock.com. [184.26.160.66] [TTL=172800]
ns5.blackrock.com. [23.211.132.67] [TTL=172800]
ns6.blackrock.com. [95.100.173.65] [TTL=172800]

Intento transferencia de zona:

```
└─$ dnsenum --enum --noreverse blackrock.com
dnsenum VERSION:1.2.6

  ─────     blackrock.com     ─────

Host's addresses:
_____

blackrock.com.                        300      IN    A      69.52.13.199
blackrock.com.                        300      IN    A      69.52.2.199


Name Servers:
_____

ns1.blackrock.com.                    300      IN    A      193.108.91.23
ns5.blackrock.com.                    300      IN    A      23.211.132.67
ns6.blackrock.com.                    300      IN    A      95.100.173.65
ns3.blackrock.com.                    300      IN    A      23.61.199.64
ns2.blackrock.com.                    300      IN    A      96.7.49.67
ns4.blackrock.com.                    300      IN    A      184.26.160.66


Mail (MX) Servers:
_____

mxb-00162b01.gslb.pphosted.com.       30       IN    A      67.231.156.56
mxa-00162b01.gslb.pphosted.com.       30       IN    A      67.231.148.58


Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for blackrock.com on ns1.blackrock.com ...

AXFR record query failed: REFUSED
Trying Zone Transfer for blackrock.com on ns6.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns5.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns2.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns3.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns4.blackrock.com ...
AXFR record query failed: REFUSED
```

```
└$ dnsenum --enum --noreverse blackrock.com
dnsenum VERSION:1.2.6

  ——    blackrock.com    ——

Host's addresses:
_____

blackrock.com.                      300     IN    A     69.52.13.199
blackrock.com.                      300     IN    A     69.52.2.199


Name Servers:
_____

ns1.blackrock.com.                  300     IN    A     193.108.91.23
ns5.blackrock.com.                  300     IN    A     23.211.132.67
ns6.blackrock.com.                  300     IN    A     95.100.173.65
ns3.blackrock.com.                  300     IN    A     23.61.199.64
ns2.blackrock.com.                  300     IN    A     96.7.49.67
ns4.blackrock.com.                  300     IN    A     184.26.160.66


Mail (MX) Servers:
_____

mxb-00162b01.gslb.pphosted.com.     30      IN    A     67.231.156.56
mxa-00162b01.gslb.pphosted.com.     30      IN    A     67.231.148.58


Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for blackrock.com on ns1.blackrock.com ...

AXFR record query failed: REFUSED
Trying Zone Transfer for blackrock.com on ns6.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns5.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns2.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns3.blackrock.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for blackrock.com on ns4.blackrock.com ...
AXFR record query failed: REFUSED
```

Resultado en archivo: dnsenum blackrock.txt y dnsnum ishares.txt

MAS DOMINIOS

Google analytics

```
┌──(kali㉿kali)-[~]
└$ analyticsrelationships --url blackrock.com

UA-ID
DOMAINS

> Get related domains / subdomains by looking at Google Analytics IDs
> GO Version
> By @JosueEncinar

[-] Analyzing url: https://blackrock.com
[-] Found UA directly
[-] Obtaining information from builtwith and hackertarget

>> UA-11733486
|__ blackrock.com
|__ snekane.com
|__ ishares401k.com
|__ blackrockinternational.com
|__ ishares.com
|__ blackrock.co.uk
|__ blackrock.co.jp
|__ ishares.co.jp
```

Robot.txt

```
User-agent: *

Disallow: /au-institutional-iframe*
Disallow: /pensions-planning-iframe*
Disallow: /capstone*

Disallow: /*.dl$

Disallow: /*sign-on.oauth
Disallow: /*sign-on.saml
Disallow: /*sign-on-popup.saml
Disallow: /user-platform/
Disallow: /userplatform/
Disallow: /search/
Disallow: /*?truepdf*
Disallow: /*?norepdf*

Disallow: /X/
Disallow: /compliance/

Disallow: /ref/docs

Disallow: /api-tester/

SITEMAP: https://www.blackrock.com/ae/sitemap.xml
SITEMAP: https://www.blackrock.com/ae/product-sitemap.xml
SITEMAP: https://www.blackrock.com/aladdin/sitemap.xml
SITEMAP: https://www.blackrock.com/americas-offshore/sitemap.xml
SITEMAP: https://www.blackrock.com/americas-offshore/product-sitemap.xml
SITEMAP: https://www.blackrock.com/at/sitemap.xml
SITEMAP: https://www.blackrock.com/at/product-sitemap.xml
```

Amass modo activo

```
┌──(kali㉿kali)-[~/Herramientas]
└─$ sudo amass enum -active -d blackrock.com -brute -w /home/kali/Herramientas/SecLists/Di
scovery/DNS/deepmagic.com-prefixes-top500.txt -src -ip -dir amass4owasp -config /home/kali
/Herramientas/recopilacion-de-informacion-main/amass/config.ini -o amass_results_owasp.txt

■
```

```
OWASP Amass v3.19.3                          https://github.com/OWASP/Amass

634 names discovered - scrape: 325, dns: 49, brute: 5, cert: 122, crawl: 7, archive: 18, api: 108

ASN: 702 - UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
        193.128.6.0/24        1    Subdomain Name(s)
ASN: 2856 - BT-UK-AS BTnet UK Regional network, GB
        217.32.0.0/12         2    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        3.80.0.0/12           1    Subdomain Name(s)
        52.70.0.0/15          1    Subdomain Name(s)
        35.168.0.0/13         1    Subdomain Name(s)
        34.224.0.0/12         1    Subdomain Name(s)
        44.192.0.0/11         2    Subdomain Name(s)
ASN: 11336 - BGLOBAL - Barclays Global Investors
        69.52.34.0/24         6    Subdomain Name(s)
        69.52.42.0/23         124  Subdomain Name(s)
        69.52.32.0/24         35   Subdomain Name(s)
ASN: 31747 - BLACKROCK-FINANCIAL-MANAGEMENT-2
        69.52.2.0/24          31   Subdomain Name(s)
        69.52.66.0/24         17   Subdomain Name(s)
        69.52.12.0/23         125  Subdomain Name(s)
        69.52.147.0/24        2    Subdomain Name(s)
        69.52.69.0/24         11   Subdomain Name(s)
        199.242.4.0/23        20   Subdomain Name(s)
        69.52.0.0/24          8    Subdomain Name(s)
        199.242.6.0/24        36   Subdomain Name(s)
        69.52.129.0/24        1    Subdomain Name(s)
        69.52.134.0/23        4    Subdomain Name(s)
        199.242.0.0/23        7    Subdomain Name(s)
        69.52.33.0/24         1    Subdomain Name(s)
ASN: 12154 - INFOUSA - InfoUSA
        206.165.240.0/21      4    Subdomain Name(s)
ASN: 2516 - KDDI KDDI CORPORATION
        125.28.0.0/15         1    Subdomain Name(s)
        111.87.0.0/17         2    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        34.208.0.0/12         1    Subdomain Name(s)
        108.157.104.0/21      4    Subdomain Name(s)
        108.157.224.0/21      4    Subdomain Name(s)
        54.193.0.0/17         1    Subdomain Name(s)
        44.224.0.0/11         4    Subdomain Name(s)
ASN: 27552 - TWDX - TowardEX Technologies International, Inc.
        216.93.240.0/20       2    Subdomain Name(s)
ASN: 22843 - PROOFPOINT-NET-NORTH-AMERICA - Proofpoint, Inc.
        67.231.156.0/24       1    Subdomain Name(s)
ASN: 10223 - UECOMM-AU Uecomm Ltd
        203.94.128.0/18       3    Subdomain Name(s)
ASN: 8220 - COLT COLT Technology Services Group Limited, GB
        80.169.0.0/16         1    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
```

|	
	p_webanalytics,sfp_webframework,sfp_webserver,sfp_whatcms,sfp_whois,sfp_whoisolo gy,sfp_whoxy,sfp_wigle,sfp_wikileaks,sfp_wikipediaedits,sfp_xforce,sfp_yandexdns,sfp_z etalytics,sfp_zoneh
SOCKS Server Type. Can be '4', '5', 'HTTP' or 'TOR'	TOR
SOCKS Server IP Address.	127.0.0.1
SOCKS Server TCP Port. Usually 1080 for 4/5, 8080 for HTTP and 9050 for TOR.	9050
SOCKS Username. Valid only for SOCKS4 and SOCKS5 servers.	
SOCKS Password. Valid only for SOCKS5 servers.	
User-Agent string to use for HTTP requests. Prefix with an '@' to randomly select the User Agent from a file containing user agent strings for each request, e.g. @C:\useragents.txt or @/home/bob/useragents.txt. Or supply a URL to load the list from there.	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0

Module Settings
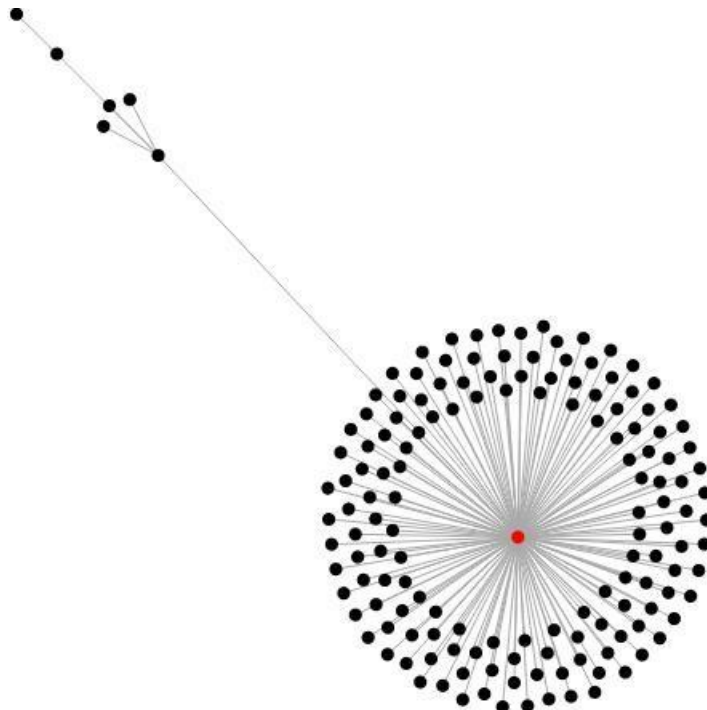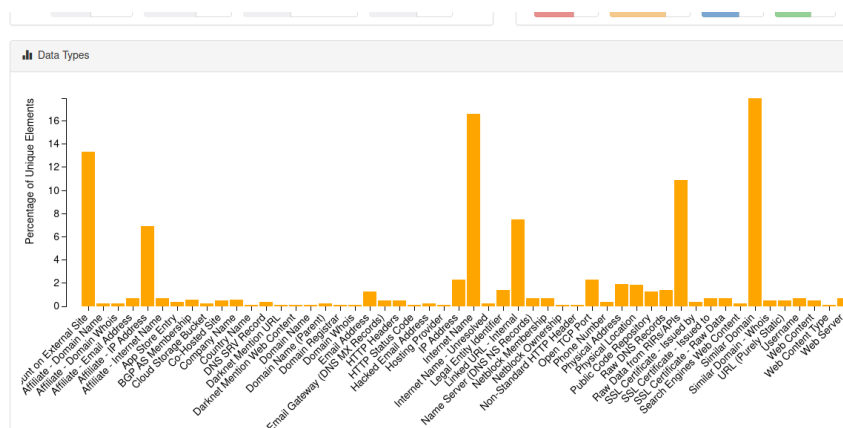
```
piderfoot -s blackrock.com -t EMAILADDR -f -x -q
Source                    Type                           Data
sfp_skymem                Email Address                  hazel.pitchers@blackrock.com
sfp_skymem                Email Address                  vijay.battu@blackrock.com
sfp_skymem                Email Address                  jennifer.oneil@blackrock.com
sfp_skymem                Email Address                  pat.todd@blackrock.com
sfp_skymem                Email Address                  ishares_marketing@blackrock.com
sfp_emailformat           Email Address                  john.moran@blackrock.com
sfp_emailformat           Email Address                  dmcintyr@blackrock.com
sfp_emailformat           Email Address                  julie.stewart@blackrock.com
sfp_emailformat           Email Address                  amy.lassers@blackrock.com
sfp_emailformat           Email Address                  rui.zhao@blackrock.com
sfp_emailformat           Email Address                  35a51b16.305f9c9c@blackrock.com
sfp_emailformat           Email Address                  emeawebmaster@blackrock.com
sfp_emailformat           Email Address                  david.helson@blackrock.com
sfp_emailformat           Email Address                  debbie.marks@blackrock.com
```

Archivo: spider email.txt

CON EYEWITNESS Y MANUALMENTE

Hago una lista de dominios de interés, principalmente paginas que tengan usuario y contraseña:
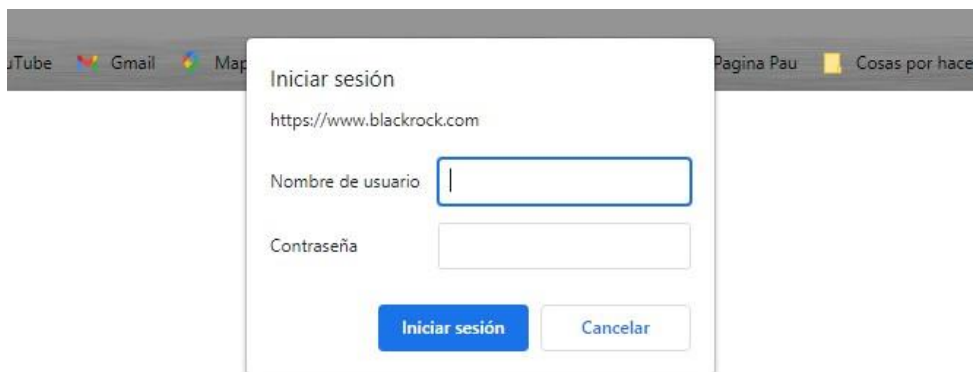
Archivo: lista dominios interesantes.txt

Saco ips de las que puedo con dig: Otras no me da, o me da un servidor de akamai.

Archivo: listado de ips.txt

NMAP

Nmap sobre lista de ips.


```
  ┌──(kali㉿kali)-[~/Herramientas/BlackRock]
  └─$ sudo nmap -Pn -F -iL brip.txt -oN nmapoutput.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-16 18:19 EDT
Nmap scan report for 69.52.2.199
Host is up (0.11s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 69.52.13.199
Host is up (0.12s latency).
Not shown: 85 filtered tcp ports (no-response), 13 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 69.52.13.253
Host is up (0.12s latency).
Not shown: 89 filtered tcp ports (no-response), 9 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 69.52.42.253
Host is up (0.18s latency).
Not shown: 81 filtered tcp ports (no-response), 17 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 69.52.12.107
Host is up (0.12s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for a104-83-38-230.deploy.static.akamaitechnologies.com (104.83.38.230)
Host is up (0.010s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

Archivo nmapoutput.txt

Intente agresivo pero se quedo pillado:

```
┌──(kali㉿kali)-[~/Herramientas/BlackRock]
└─$ sudo proxychains nmap -Pn -A -sC -sU 69.52.2.199 -oN nmapagresivo.txt
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-16 19:01 EDT
```

OPEN VAS

Open Vas, me pelee mucho con este, decidí poner configuración estándar para evitar problemas. Tambien reduje la lista de dominios por el tiempo.

Dio un resultado potencialmente interesante:

Archivo: report-open vas .txt

CONCLUSION

Esta empresa tiene una cantidad inmensa de sus activos expuestos a internet, muy posiblemente tenga varios vectores de ataque entre sus portales de login.