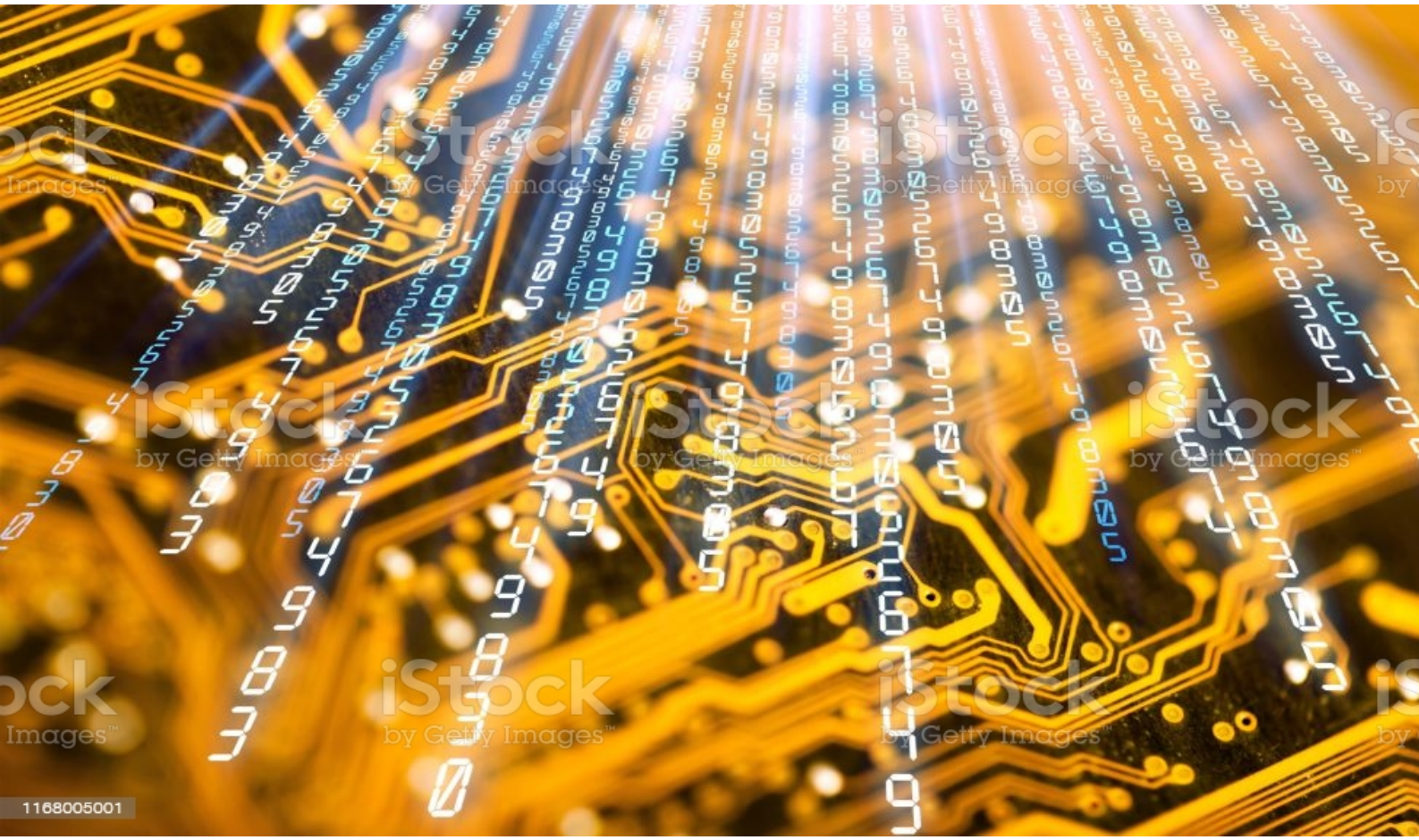
III Bootcamp Full Stack Ciberseguridad

Modulo 3 - Information Gathering

Caso práctico: Reconocimiento de una organización



Marcos Alonso González
30 enero 2022
alonsogonzalezmarcos@gmail.com

Objetivo:

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

Contenido:

- Técnicas de Footprinting
- Técnicas de Fingerprinting
- Técnicas OSINT

Detalles:

En esta práctica el alumno aplicará las técnicas y utilizará las diferentes herramientas vistas durante el módulo.

Preparación

El alumno deberá elegir una organización que esté dentro del programa de hackerone.

- Crear una cuenta en https://hackerone.com/
- Elegir una organización con varios dominios en el scope.
- Elegir una organización con subdominios en el scope.
- Comprobar detalladamente que está permitido atacar dichos dominios.

Desarrollo

El objetivo es obtener la máxima información posible de la organización elegida. Esto incluye, pero no limita:

- Dominios relacionados (dentro del scope).
- Información de cada dominio.
- Análisis de vulnerabilidades.
- Correos corporativos.

Índice

1. Organización

El primer paso es elegir una organización entre todas las disponibles como objetivo en hacekerone.com, teniendo en cuenta que cumpla con los requisitos del ejercicio.

La organización de hackerone.com elegida para este ejercicio práctico ha sido:

Se trata de una plataforma de seguridad basada en datos para la nube.

1.1. Scope del objetivo

Encontramos dentro del scope del objetivo 2 dominios, ambos cuentan con subdominios.

www.lacework.com

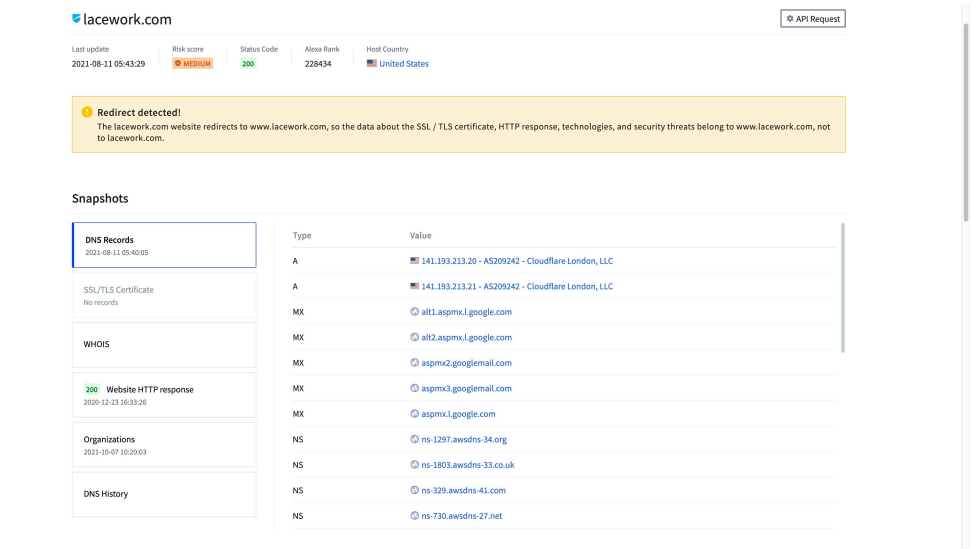
***.lacework.net**

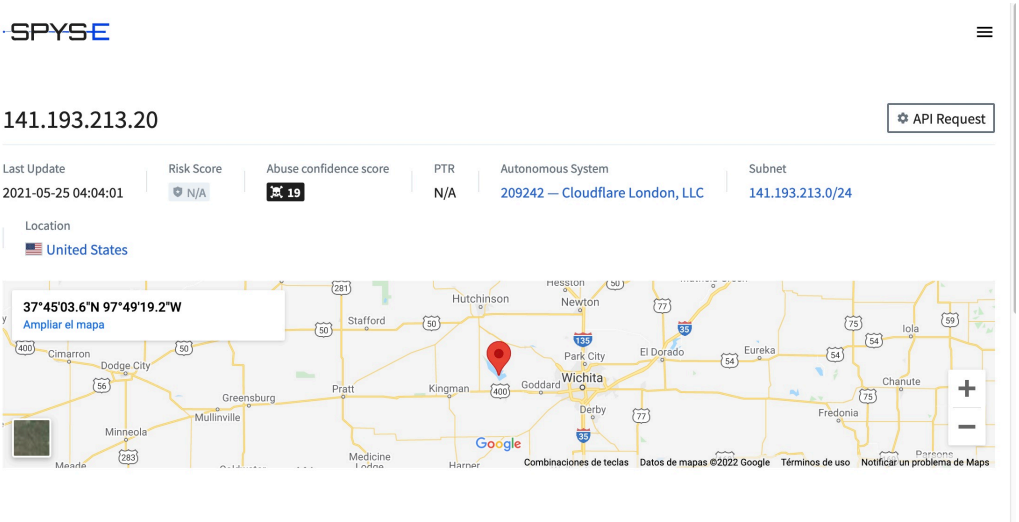
2. Footprinting

Es una técnica utilizada para recopilar información de un sistema. Es una primera fase de reconocimiento donde podemos descubrir posibles vectores de ataque del sistema objetivo. Es por tanto el paso previo a descubrir posibles puntos de explotación.

2.1. Reconocimiento general

En primer lugar podemos hacer un reconocimiento general de los activos de la organización, utilizando herramientas online como **spyse**, que ofrece algunos detalles generales de la compañía y el dominio, así como de las IPs en las que se encuentra, que en este caso están dentro del un sistema autónomo ASN que asegurado por **Cloudflare**





Mediante **crunchbase.com** encontramos que Lacework, Inc. ha adquirido recientemente (11.11.2021) la compañía Soluble, también de servicios de seguridad en la nube. En una noticia relacionada encontramos otra dirección de correo electrónico no corporativa que habrá que investigar más adelante (Lacework@inkhouse.com).

Utilizando la herramienta online de **https://bgp.he.net/** podemos descubrir más información genérica de la organización:

```
descr:          Lacework, Inc
                6201 America Center Drive, Suite 200
                San Jose CA 95002
                United States

OrgTechHandle: LACEW2-ARIN
OrgTechName:   Lacework Security
OrgTechPhone:  +1-888-292-5027
OrgTechEmail:  security@lacework.net
OrgTechRef:    https://rdap.arin.net/registry/entity/
LACEW2-ARIN

OrgAbuseHandle: LACEW2-ARIN
OrgAbuseName:   Lacework Security
OrgAbusePhone:  +1-888-292-5027
OrgAbuseEmail:  security@lacework.net
OrgAbuseRef:    https://rdap.arin.net/registry/entity/
LACEW2-ARIN
```

2.2. Reconocimiento horizontal

Scope del objetivo

Encontramos dentro del scope del objetivo 2 dominios, uno de ellos permite subdominios:

www.lacework.com
***.lacework.net**

2.2.1. Descubrimiento e investigación sobre IPs y DNS

Para descubrir las IPs de lacework.com y lacework.net utilizamos **nslookup** en Kali, obteniendo el siguiente resultado:

```
(kali㉿kali)-[~]
└─$ nslookup lacework.com

Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   lacework.com
Address: 141.193.213.21
Name:   lacework.com
Address: 141.193.213.20


(kali㉿kali)-[~]
└─$ nslookup lacework.net

Server:         10.1.0.1
Address:        10.1.0.1#53

Non-authoritative answer:
Name:   lacework.net
Address: 52.218.179.43
```

Utilizando el protocolo WHOIS mediante la herramienta online de https://bgp.he.net/ podemos descubrir que lacework.com está hosteados con Cloudflare.

```
origin:          AS209242
IP range: 168.100.6.0/24
```

Si lanzamos **whois** en Kali vemos que **ambas direcciones asociadas a lacework.com** (141.193.213.21 y 141.193.213.20) se encuentran alojadas en WPEngine, Inc. Con esto confirmamos que, como indica el "In Scope" de hackerone, este website esta construido en WordPress, ya que este host solo aloja ese tipo de webs.

```
whois 141.193.213.20

NetRange:       141.193.213.0 - 141.193.213.255
OrgName:        WPEngine, Inc.
```

La direccion IP **asociada a lacework.net** se nos muestra como perteneciente a Amazon:

```
whois 52.218.179.43

NetRange:       52.192.0.0 - 52.223.191.255
OrgName:        Amazon Technologies Inc.
```

Esta dirección IP es dinámica y cambiará con el paso de los días, al estar alojada en un servicio en la nube como es AWS.

Por tanto, esto no confirma que estas direcciones pertenezcan a lacework.com, por lo que tenderemos que utilizar otras técnicas para validar el resultado.

Con el comando

```
whois -h whois.radb.net  -- '-i origin AS209242' | grep -Eo
"([0-9.]+){4}/[0-9]+" | uniq
```

podemos comprobar que el rango de IPS de Lacework, Inc. están dentro del ASN (AS209242) que nos indicaba https://bgp.he.net/.

Utilizando la herramienta online **Domain Research Suite** también podemos reportar que dominios tiene asociados Lacework, Inc., obteniendo todos los que se relacionan en el punto 1 del Anexo 1.

Con **viewdns.info** y alguno de estos dominios, encontramos más información de la que proporciona la búsqueda de lacework.com en esta misma herramienta online, por ejemplo, un correo electrónico del administrador del dominio y la dirección y teléfono de la organización:

```
Domain Name.....: lacework.com.kz

Organization Using Domain Name
Name.....: Hostmaster
Organization Name.....: LACEWORK, INC.
Street Address.....: 6201 America Center Dr Suite 200
City.....: San Jose, CA
State.....: -
Postal Code.....: 95002
Country.....: US

Administrative Contact/Agent
NIC Handle.....: HOSTERKZ-436041
Name.....: LACEWORK INC.
Phone Number.....: +1.8882925027
Fax Number.....: +1.8882925027
Email Address.....: domain-admin@lacework.com
```

También otras direcciones de IP asociadas a un gestor de dominios (MarkMonitor Inc.):

```
Nameserver in listed order

Primary server.........: ns1.markmonitor.com
Primary ip address.....: 64.124.69.50

Secondary server.......: ns2.markmonitor.com
Secondary ip address...: 64.124.69.52
```

Incluso haciendo la búsqueda de otras direcciones de anexo, encontramos hasta el nombre del administrador del dominio:

```
Domain Name: lacework.us
Registry Domain ID: DE75A6D42B29D44A8A6555839B035102D-NSR
Registrant Name: Matthew Zeier
Registrant Organization: LACEWORK, INC.
Admin Name: Matthew Zeier
```

Hacemos para finalizar una búsqueda más exhaustiva de la organización con **Maltego**.

Usamos para ello la maquina Footprinting L3. Lo que hacen estas maquinas de la aplicación es una búsquedas de los subdominios, IPS, hosts, DNS, ASN, etc.

Hay que tener en cuenta que lacework.net cuenta con IP dinámica, por lo que los resultados son para este dominio son válidos temporalmente y habría que hacer de nuevo la búsqueda en días posteriores para actualizarla.

Los resultados los muestra en forma de gráfico, con lo que se hace muy visual y nos sirve para comparar rápidamente con los resultados de otras herramientas que hemos utilizado anteriormente.

Se pueden comprobar los gráficos obtenidos en la búsqueda en el **archivo comprimido *"18.MaltegoLacework".***

2.2.2. DNS reverse

Automatizamos la búsqueda de dns reverse para el rango de direcciones IP obtenidas para lacework.com , con la técnica **dnsreverse sweeping** (barrido) utilizando las herramientas dnsx y mapcidr, lanzando los siguientes comandos:

```
echo 17.253.20.0/23 | mapcidr -silent | dnsx -ptr -resp-only

whois -h whois.radb.net  -- '-i origin AS209242' | grep -Eo
"([0-9.]+){4}/[0-9]+" | uniq
| mapcidr -silent | dnsx -ptr -resp-only
```

Los resultados son dominios que podrían pertenecer a la compañía y serían susceptibles de atacar, si bien quedan fuera del scope de esta investigación.

Se guardan los resultados en el **archivo *"1. DominiosDNSreverseLacework".***

2.2.3. IP history

Utilizando esta opción en **viewdns.info** podemos observar las IPs que ha tenido históricamente el dominio lacework.com.

Los resultados se adjuntan en el **archivo *"2. IpHistoryLacework"***

2.2.4. Favicon hashing

Por último, dentro del reconocimiento horizontal, vamos a utilizar la técnica de **favicon hashing.**

Los pasos a seguir han sido:

1. Hemos hallado la dirección donde se almacena el favicon de lacework.com inspeccionando las herramientas de desarrollador del navegador, en la sección red:

https://www.lacework.com/wp-content/uploads/2019/03/cropped-lacework-favicon-32x32.png

2. Utilizaremos la herramienta de **MurMurHash** para hallar el hash de la imagen y buscar otros dominios donde también se utilice. Lanzamos el comando

```
python3 MurMurHash.py
```

3. Y pegamos seguidamente la url del favicon, obteniendo el hash 1656871411

4. Luego en **shodan.io** lanzamos la búsqueda http.favicon.hash:1656871411.

En este caso no encuentra resultados utilizando este hash, pero en teoría gracias a esta técnica se pueden obtener otros dominios o subdominios que pueden pertenecer o no a la compañía y podemos obtener información sensible.

Si se obtienen resultados en shodan.io con el favicon de la url https://app.soluble.cloud/favicon.ico , perteneciente a la organización adquirida por Lacework, Inc. como se ha señalado antes.

En este caso el hash obtenido es -9625865032.3 y usando Shodan obtenemos 110 resultados, la mayoría alojados en Amazon y con servidor Nginx, a excepción de 7 alojadas en Google y 6 en A100 ROW GmbH. Solo uno de los resultados muestra un dominio con servidor Werkzeug httpd.

2.3. Reconocimiento vertical

Vamos ahora a utilizar técnicas de reconocimiento vertical, algunas son técnicas activas y otras pasivas.

2.3.1. Dns Brute-Force

Esta técnica sirve para adivinar subdominios mediante peticiones DNS.

Utilizaremos la herramienta **puredns**. Para hacer fuerza bruta y averiguar posibles subdominios utilizamos diccionarios.

Es importante recordar utilizar tambien un listado de servidores DNS confiables para resolver los subdominios.

Lanzamos el comando

```
puredns bruteforce /home/kali/Tools/SecLists/Discovery/DNS/
dns-Jhaddix.txt lacework.net -r resolvers.txt
```

Dentro de resolvers.txt hemos añadido todos los servidores DNS listados en la url https://public-dns.info/nameservers.txt

Con este diccionario no hemos obtenido subdominios a pesar de realizarse una búsqueda larga. Aunque si hayamos una nueva wildcard root:

*.fra.lacework.net

Probamos con otro diccionario menor utilizando el mismo comando y sustituyendo el diccionario utilizado

```
puredns bruteforce /home/kali/Tools/SecLists/Discovery/DNS/
deepmagic.com-prefixes-top50000.txt lacework.net -r
resolvers.txt
```

Obtenemos una lista de **2237 subdominios**, que aparecen detallados en el **archivo *"3.SubdomainsPurednsLaceworknet.txt"***

Probando manualmente algunos de ellos en navegador, todos redirigen a: https://login.lacework.net/ui/

Sobre esa lista de 2237 subdominios vamos a probar ahora cuantos resuelven a una IP utilizando el comando

```
puredns resolve subdomains_lacework.txt -r resolvers.txt
```

Obtenemos **77 valid domains**, es decir 77 subdominios que resuelven con una IP.

Pueden verse los resultados en el archivo
"4.ResolveSubdomainsPurednsLacework"

2.3.2. Web scraping

Se utiliza para obtener información de manera recursiva de una web.

De toda la información que se puede obtener (código fuente, código JS, subdominios, etc.) lo que interesa es quedarse con los subdominios y comprobar posteriormente que son válidos y que pertenecen a la organización objetivo.
Para esta técnica utilizamos las herramientas **gospider** y **unfurl**

Se pueden filtrar los resultados para obtener dominios únicos de los resultados, lanzando el siguiente comando, utilizando al mismo tiempo gospider y unfurl:

```
cat gospiderlaceworknet.txt | grep -Eo '(http|https)://[^/"]+'
| unfurl --unique domains
```

Se obtienen los siguientes resultados, entre los que figuran algunos subdominios de *.lacework.com

www.lacework.com
gmpg.org
static.addtoany.com
ajax.googleapis.com
cdnjs.cloudflare.com
s.w.org
www.lacework.net
fr.lacework.com
de.lacework.com
info.lacework.com
login.lacework.net
support.lacework.com
academy.lacework.com
twitter.com
www.linkedin.com
www.facebook.com
www.youtube.com
script.crazyegg.com
code.jquery.com
view.ceros.com
www.googleoptimize.com
cdn.popt.in

2.3.3. Certificate transparency logs

Mediante los certificados HTTPS de los dominios se puede obtener información valiosa sobre una web, pudiendo comprobar si el propietario del certificado es el mismo que el que dice serlo de la web.

También pueden hallarse otros dominios similares o subdominios asociados.

Hay una herramienta llamada **ctfr** que es útil para automatizar la búsqueda de certificados de un dominio.

Esta herramienta lo que hace es llamar a la página https://crt.sh/ utilizando un %. al inicio de la búsqueda para encontrar subdominios.

Probamos diferentes búsquedas lanzando los comandos:

```
python3 ctfr.py -d lacework.net
python3 ctfr.py -d lacework.com
python3 ctfr.py -d lacework.%
```

Los resultados pueden verse en el archivo ***"5. ResultadosCtfrLacework.txt"***

La última búsqueda no encuentra otros dominios que no sean .com o .net. Pero si encuentra subdominios como

`es.lacework.com`

La página principal de lacework.com no tiene opción para navegar a web en idioma español, pero en ese dominio se puede encontrar la web con algunos títulos de sección traducidos a español.

Esta herramienta permite hacer búsqueda de forma recursiva, por ejemplo con dominios o subdominios que encontremos que tienen asterisco, por ejemplo

```
*.hack3rs.corp.lacework.net
```

Esto puede ayudar a encontrar otros dominios que no aparezcan en la búsqueda principal. Probamos en este caso lanzando el comando

```
python3 ctfr.py -d hack3rs.corp.lacework.net
```

Pero no obtenemos más resultados de los aparecidos anteriormente para este dominio:

```
[!] ---- TARGET: hack3rs.corp.lacework.net ---- [!]
```

```
[-]  *.hack3rs.corp.lacework.net
hack3rs.corp.lacework.net

[!]  Done. Have a nice day! ;).
```

Para comprobar la validez de los resultados obtenidos para “lacework” como organización buscamos en la url

https://crt.sh/?O=lacework&output=json

obteniendo el json archivado en ***“6.Crtshlacework.txt***" y encontrando que todos los certificados obtenidos pertenecen a Lacework, Inc.

Lo mismo ocurre si modificamos el script de ctfr.py con vim, cambiando la q de la búsqueda por O y lanzando el comando

```
python3 ctfr.py -d lacework
```

Obteniendo el siguiente resultado y comprobando que los certificados corresponden a Lacework, Inc.:

```
[!] ---- TARGET: lacework ---- [!]
[-]  Lacework, Inc
[!]  Done. Have a nice day! ;).
```

2.3.4. Fuentes pasivas

shodan.io

Hay algunas herramientas online como **shodan.io** o **censys.io** que se pueden utilizar para hacer footprinting de dominios de la organización objetivo.

Utilizamos el cliente **shodan domain** de Kali, previa inicialización de API key valida, con los comandos

```
shodan domain --save lacework.net
shodan domain --save lacework.com
```

Los resultados obtenidos figuran en formato .json el archivo
"***7.ShodanLacework.json***"

crobat

Podemos utilizar también la herramienta **crobat** para hacer búsqueda de subdominios con el comando

```
crobat -s lacework.net | sort | uniq
crobat -s lacework.com | sort | uniq
```

Los resultados obtenidos figuran en el archivo ***"8. CrobatLacework.txt".***

wayback

Una herramienta para hallar enlaces a archivos web históricos es **wayback.**
Utilizamos el listado de subdominios obtenidos con crobat para hacer la búsqueda lanzando el comando

```
cat crobatlaceworkcom.txt | waybackurls > waybacklacework.txt
```

Los resultados obtenidos figuran en el archivo ***"9. WaybackLacework.txt".***

GitHub search

Otra fuente pasiva que podemos utilizar para hallar mas subdominios es GitHub y la herramienta **github search** para automatizar la búsqueda. Busca entre todos los repositorios existentes en GitHub el dominio objetivo.

Generamos un token desde nuestro perfil de GitHub (developer settings) y lanzamos el comando

```
python3 github-subdomains.py -t <personal token> -d
lacework.net
python3 github-subdomains.py -t <personal token> -d
lacework.com
```

En este caso no conseguimos nuevos subdominios con ninguna de las dos búsquedas, solo algunos ya obtenidos con otras herramientas:

```
docs.lacework.com
support.lacework.com
www.lacework.com
packages.lacework.com
```

2.3.5. Amass

Amass es una herramienta muy completa de OWASP que permite footprinting activo y pasivo, además de reconocimiento vertical y horizontal. Mapea la superficie de ataque lo que permite descubrir activos de la organización objetivo.

Comenzamos con **reconocimiento vertical:**

```
amass enum -src -d lacework.com
```

Resultado:

```
---------------------------------------------------------------
1 names discovered - api: 1
---------------------------------------------------------------
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.

  104.16.0.0/14           5    Subdomain Name(s)
```

Hemos hallado 5 subdominios en el rango de IPs 104.16.0.0/14, pero ninguno pertenece a servidor propio de la organización, sino a Cloudflare.

Hacemos lo mismo para lacework.net, con más resultados:

```
amass enum -src -d lacework.net

---------------------------------------------------------------
85 names discovered - archive: 8, scrape: 2, dns: 1, alt: 7,
api: 1, crawl: 3, cert: 63
---------------------------------------------------------------
ASN: 16509 - AMAZO-ZPDX9 - Amazon.com, Inc.

ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.

ASN: 0 - Reserved Network Address Blocks
        10.0.0.0/8              1    Subdomain Name(s)
ASN: 209242 - AS209242
        141.193.213.0/24        2    Subdomain Name(s)
        199.60.103.0/24         2    Subdomain Name(s)
        2606:2c40::/48          2    Subdomain Name(s)
```

Observamos que de los 85 subdominios de lacework.net obtenidos, algunos utilizan IPs de Amazon, otros de Cloudflare, pero también tiene 6 subdominios en ASN AS209242 que ya sacamos con la herramienta online de https://bgp.he.net/.

Probamos ahora con la **flag —active** que hace un reconocimiento más exhaustivo. Tira de técnicas también activas: saca información con fuerza bruta de los DNS, escanea puertos, intenta transferencia de zona, escanea protocolos TLS y SSL, etc.

Primero probamos para lacework.com:

```
amass enum -src -active -ip -v -d lacework.com
```

Los resultados se diferencia a los obtenidos sin —active en cuanto a número y tipos de subdominios obtenidos y todos los mostrados son del ASN propio de Lacework:

```
-------------------------------------------------------------
4 names discovered - dns: 1, crawl: 1, cert: 2
-------------------------------------------------------------

ASN: 209242 - AS209242
        141.193.213.0/24        8   Subdomain Name(s)
```

Lanzamos el mismo comando para lacework.net:

```
amass enum -src -active -ip -v -d lacework.net
```

Los resultados se diferencia a los obtenidos sin —active en cuanto a tipos de subdominios obtenidos, no tanto en cuanto a número.

```
-------------------------------------------------------------
82 names discovered - archive: 2, scrape: 4, dns: 2, alt: 6,
api: 5, crawl: 21, cert: 42
-------------------------------------------------------------
```

También se pude configurar la búsqueda incluyendo APIs de servicios como shodan o censys, además de incluir diccionarios personalizados. Para ello se edita el archivo config.ini.

```
amass enum -src -active -ip -v --config config.ini -d
lacework.net
```

De esta manera se obtienen mayor número de resultados:

```
------------------------------------------------------------
101 names discovered - archive: 6, scrape: 6, dns: 2, brute:
4, api: 16, crawl: 39, cert: 28
------------------------------------------------------------
```

Incluso hayamos subdominios en un nuevo ASN:

```
ASN: 6939 - HURRICANE - Hurricane Electric LLC
        2602:fd3f::/46          1    Subdomain Name(s)
        64.71.128.0/18          1    Subdomain Name(s)
```

La lista de subdominios completos obtenida con estas configuraciones están almacenadas en el **archivo *"10. AmassLacework.txt"***

2.3.6. Reconftw

Esta es otra herramienta que sirve para hacer un reconocimiento completo a través de diferentes técnicas: pasivas, fuerza bruta, permutaciones, certificados de transparencia, DNS, etc.

El comando básico para un reconocimiento completo sería:

```
./reconftw.sh -d lacework.com -r
```

Entre la información más interesante encontramos:

Total subdomains:

- 24 alive
- 24 new web probed

1 new possible DNS takeover

Resolved IP addresses (No WAF)

13.224.111.91
141.193.213.20
141.193.213.21
209.170.205.127
35.198.112.85
52.6.19.39
54.145.67.249
54.156.233.42
54.205.199.210
64.71.144.202

333 new urls with params

Lo más importante es que encontramos una **posible vulnerabilidad** con el modulo nuclei:

```
[2022-01-27 06:36:11] [CVE-2017-5487] [http] [medium] https://es.lacework.com/wp-json/wp/v2/users/
```

Buscamos referencia a la vulnerabilidad en:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5487

Se trata de una vulnerabilidad de la **versión Wordpress 4.7.0.**

Una función desconocida del archivo *wp-includes/rest-api/endpoints/class-wp-rest-users-controller.php* del componente *REST API* es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase divulgación de información. Esto tiene repercusión sobre la confidencialidad. La explotación se considera fácil.

Encontramos **exploit** para esta vulnerabilidad:

https://www.exploit-db.com/exploits/41497

Además, se encuentran:

- listado de IPs,

- puertos de las IPs propias de Lacework (141.193.213.20, 141.193.213.21) que podrían utilizar versiones deprecadas de SSL(2.0 y 3.0) y TLS (1.0 y 1.1.)
- gran cantidad de urls de archivos,
- endpoints,
- una larga lista de dominios obtenidos por fuzzing,
- de dominios con contenido js,
- CMS de varios dominios con autores y versiones de plugin y themes de Wordpress sobre los que podríamos comprobar si haya alguna vulnerabilidad,
- etc.

Los resultados que hemos obtenido se adjuntan en el archivo *"**11. ReconwftLacework.com***"

2.3.7. Spiderfoot

La última herramienta que vamos a utilizar para footprinting es spiderfoot, muy util para la recopilación de información.

Con el comando

```
spiderfoot -T
```

tenemos acceso a ver todo el tipo de información que podemos obtener, que es muchísima.

Podemos conseguir correos electrónicos de la organización con el comando

```
spiderfoot -s lacework.com -t EMAIL_ADDR -f -x -q
```

Obtener que servidores utiliza con

```
spiderfoot -s lacework.com -t WEBSERVER_BANNER -f -x -q
```

Si tiene algún certificado SSL expirado con

```
spiderfoot -s lacework.com -t SSL_CERTIFICATE_EXPIRED -f -x -q
```

Y toda la información completa del dominio objetivo con el comando

```
spiderfoot -s lacework.com -q
```

Y más de 100 tipos diferentes de información, en resumen, una herramienta que auna la información relativa a Footprinting que hemos estado descubriendo a través de diferentes herramientas con anterioridad

Se adjunta en el **archivo *"19.SpiderfootLacework.txt"*** alguna de la información obtenida.

3. Fingerprinting

Consiste en extraer información concreta de un objetivo: tecnologías que utiliza, servidor y versión, puertos abiertos, sistema operativo, etc..

3.1. Escaneo de puertos

El concepto más básico del fingerprinting. Nos sirve para averiguar que puertos de un sistema están abiertos y a la escucha. Si encontramos un puerto abierto, dispondrá al otro lado de un servicio susceptible de atacar.

La herramienta más utilizada en el escaneo de puertos es nmap

3.1.1. Nmap

Lo primero que se puede hacer con nmap es descubrir hosts, es decir, descubrir si una máquina está o no funcionando.

Escaneo básico

Un primer mapeo básico para descubrir hosts de los subdominios de lacework.com y lacework.net es utilizando el comando

```
nmap -sn -iL subdomains_lacework.txt
```

donde incluimos un archivo con la lista de subdominios obtenidos mediante técnicas de footprinitng.

Obtenemos como resultado que hay 2313 hosts activos de 2616 direcciones IP escaneadas:

```
Nmap done: 2316 IP addresses (2313 hosts up) scanned in 150.19 seconds
```

Escaneo inicial sencillo

Lanzamos el comando

```
sudo nmap -Pn -sS -iL subdomains_lacework.txt
```

Esta técnica es capaz de evitar los bloqueos de los firewall, al contrario de lo que puede ocurrír con el escaneo básico inicial.

La **flag -sS** simula un paquete real que pide conectarse al puerto. Al ser protocolo TCP SYN, donde interrumpe la conexión cuando ha recibido la primera respuesta, por lo que ya sabe que está abierto. Si recibe un reset de la máquina, es que está cerrrada.

Escaneo complejo

Vamos a hacer más complejo el escaneo tratando de sacar las versiones de los servicios que se encuentran tras los puertos.
Esto lo hacemos añadiendo la **flag -sV**

```
sudo nmap -Pn -sS -sV -p0- lacework.com
```

Escaneo completo

Por último hacemos un escaneo más completo y preciso.
Usamos nuevas flags no usadas anteriormente:

—open: para que solo muestre puertos abiertos
-O: para que averigue el sistema operativo
-sC: lanza scripts que tiene por defecto para sacar más información. Primero hace escaneo de puertos y luego lanza los scripts a los que están abiertos.
—reason: da información sobre porque ha encontrado los puertos que están abiertos
-p0-: escanea todos los puertos
-T4: aumenta la velocidad de búsqueda, por defecto está la -T3.

```
sudo nmap -Pn -sS -sV --open -O -sC --reason -p0- -T4 -oA
nmaplaceworkcom -iL subdomains_lacework.txt
```

Escaneo individualizado

Ya que no hemos obtenido resultados en cuanto a averiguar las versiones d los servicios de los puertos abiertos de la lista de subdominios, probamos ahora escaneaos individuales a los 37 subdominios que resolvimos con IP con puredns anteriormente, con el comando:

```
sudo nmap -Pn -sS -sV -T4 <subdominio>
```

De esta manera obtenemos como información interesante para algunos subdominios como:

deploy.lacework.net
net174.lacework.net
sub-97-249-119.lacework.net

```
PORT      STATE    SERVICE         VERSION

80/tcp     open     http         nginx 1.15.10
```

Se comprueba con CVE si hay alguna vulnerabilidad para esa versión de nginx, peo no existe al menos que se conozca:

https://www.cvedetails.com/vulnerability-list.php?vendor_id=10048&product_id=17956&version_id=176499&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=0&sha=b5757b4d4b5af043ee6a84da4af8773cecb19b82

3.2. Análisis web

Para hacer este análisis web hemos utilizado las siguientes herramientas: **httpx, EyeWitness, dirsearch, gobuster, wappalyzer**

3.2.1. httpx

Esta herramienta ayuda a saber que urls tienen https y cuales http. Ademas con el comando

```
httpx -list subdomains_lacework.txt -silent -probe
```

comprobamos cuales responden con FAILED, es decir los que la herramienta no puede abrir y cuales con SUCCESS.

Se adjunta una lista de subdominios en el **archivo *"11. httpx_urls_lacework.txt"*** que han respondido con SUCCESS. Esta lista puede servirnos para tirarla con otras herramientas como nmap o EyeWitness.

3.2.2. EyeWitness

Esta herramienta nos da la posibilidad a través de la realización de capturas de pantalla de las urls ver con que status responden y como se muestran (200, 403, 404, etc.).

Asi podemos comprobar cuales podemos visitar, cuales están prohibidas, cuales no existen, etc.

Lanzamos el comando

```
./EyeWitness.py --web -f subdomains_lacework.txt
```

Obtenemos un **report** que podemos visualizar en el navegador, el resultado puede verse en el **archivo*"12. EyeWitnesslaceworkhtml.zip"***

3.2.3. dirsearch

Esta herramienta prueba fuerza bruta para hallar directorios de las url que tengamos como objetivo.

Se puede lanzar con el comando

```
dirsearch -i 200 -t10 --format=csv -u <url>
```

Lo hemos lanzado sobre varias urls:

https://academy.lacework.com
https://blog.lacework.com
https://careers.lacework.com
https://community.lacework.com
https://de.lacework.com
https://docs.lacework.com
https://es.lacework.com
https://fr.lacework.com
https://get.lacework.com
https://info.lacework.com
https://it.lacework.com
https://jp.lacework.com
https://lacework.com
https://nht.lacework.com
https://nl.lacework.com
https://partners.lacework.com
https://www.lacework.com

3.2.4. Wappalyzer

Wappalyzer se puede instalar como plugin en Firefox. Proporciona información sobre la arquitectura de la web, con que componentes está construida. Probamos sobre algunas url objetivo, encontrando entre otras cosas que:

https://blog.lacework.com , https://careers.lacework.com

Utiliza una versión beta de Bootstrap (Bootstrap@4.0.0-beta.3). Según snyk.io esta versión pude ser susceptible a ataques Cross-site Scripting (XSS):

https://snyk.io/test/npm/bootstrap/4.0.0-beta

https://docs.lacework.com

Utiliza una versión beta de Docusaurus (Docusaurus 2.0.0-beta.13) Según snyk.io la versión beta.15 pude ser susceptible a ataques graves de denegación de servicio (DoS), por lo que podrá probarse a atacar esta versión 13:

https://snyk.io/test/npm/@docusaurus/core

4. Escáneres de vulnerabilidades

En un análisis de vulnerabilidades podemos utilizar métodos pasivos y activos.

4.1. WPScan

Aprovechando los dominios que hemos sacado con reconftw que cuentan con Wordpress como CMS, lanzamos **wpscan** con el comando sobre los mismos

```
wpscan --url –ignore-main-redirect
```

4.1.1. XML-RPC

Obtenemos una posible vulnerabilidad muy conocida con estos dominios:

```
https://nl.lacework.com, https://jp.lacework.com, https://
it.lacework.com, https://fr.lacework.com, https://
es.lacework.com, https://de.lacework.com
```

```
XML-RPC seems to be enabled: https://nl.lacework.com/
xmlrpc.php
```

Una vulnerabilidad **xmlrpc.php** permite entre otras cosas realizar ataques de denegación de servicio, así como ataques de fuerza bruta para la obtención de users y passwords de Wordpress.

Para tratar de explotar esta vulnerabilidad, probamos primero la respuesta que da el enlace descubierto en un navegador y observamos que es la que debería dar para tratar de realizar el ataque:

```
XML-RPC server accepts POST requests only.
```

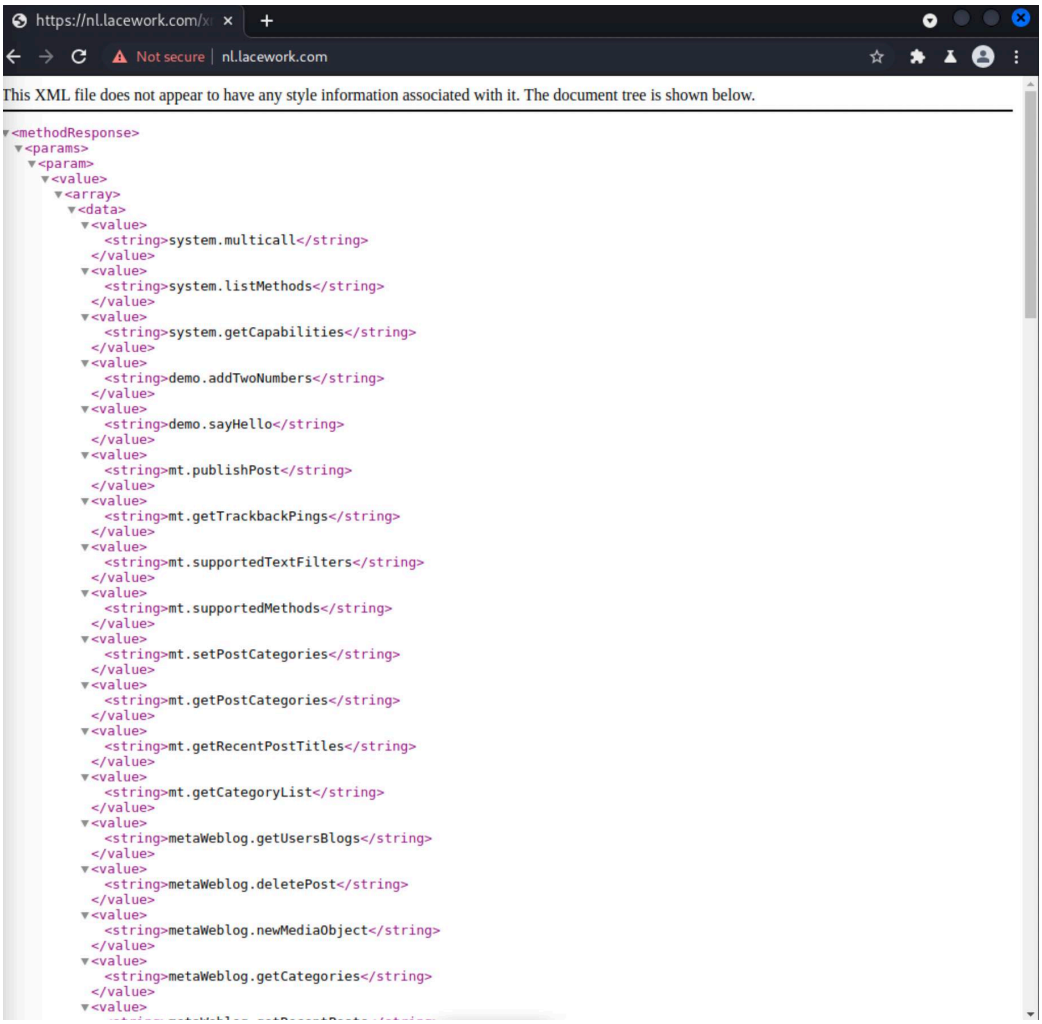
Vamos a utilizar ahora **Burp Suite.** Abrimos el navegador chromium dentro de la aplicación y vamos a https://nl.lacework.com/xmlrpc.php.

Previamente habremos habilitado la opción **"Intercept is on"** dentro de la sección Intercept en Burp Suite. Interceptamos la petición GET y la sustituimos por esta petición POST:

```
POST /xmlrpc.php HTTP/1.1
Host: nl.lacework.com
Content-Length: 135

<?xml version="1.0" encoding="utf-8"?>
<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```

La respuesta en el navegador es la que se espera:

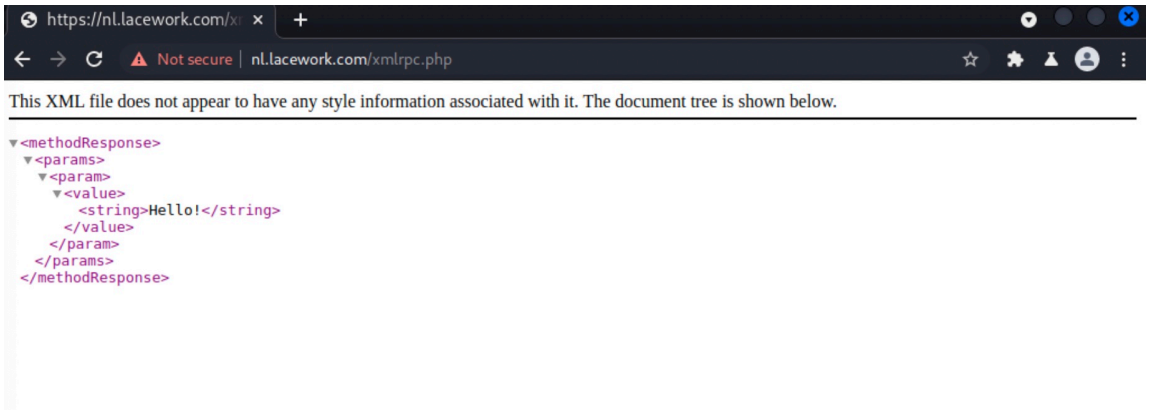


Seguidamente enviamos otra petición POST para probar a interactuar con el servidor:

```
POST /xmlrpc.php HTTP/1.1
Host:nl.lacework.com
Content-Length: 130

<?xml version="1.0" encoding="utf-8"?>
<methodCall>
<methodName>demo.sayHello</methodName>
<params></params>
</methodCall>
```

La respuesta obtenida en el navegador sigue siendo la esperada:



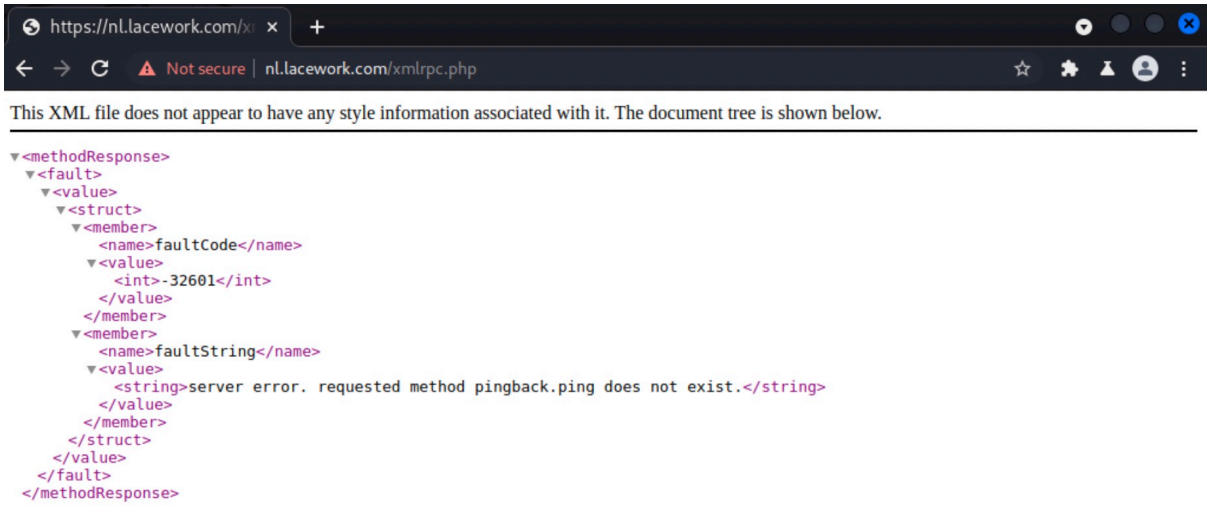
Sin embargo, cuando probamos a enviarle una petición POST que contenga un pingback para ver si el servidor responde,

```
POST /xmlrpc.php HTTP/1.1
Host: nl.lacework.com
Content-Length: 303

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>pingback.ping</methodName>
```

```
<params>
<param>
<value><string>https://postb.in/1562017983221-4377199190203</
string></value>
</param>
<param>
<value><string>https://nl.lacework.com/</string></value>
</param>
</params>
</methodCall>
```

Nos devuelve desde el navegador lo siguiente:



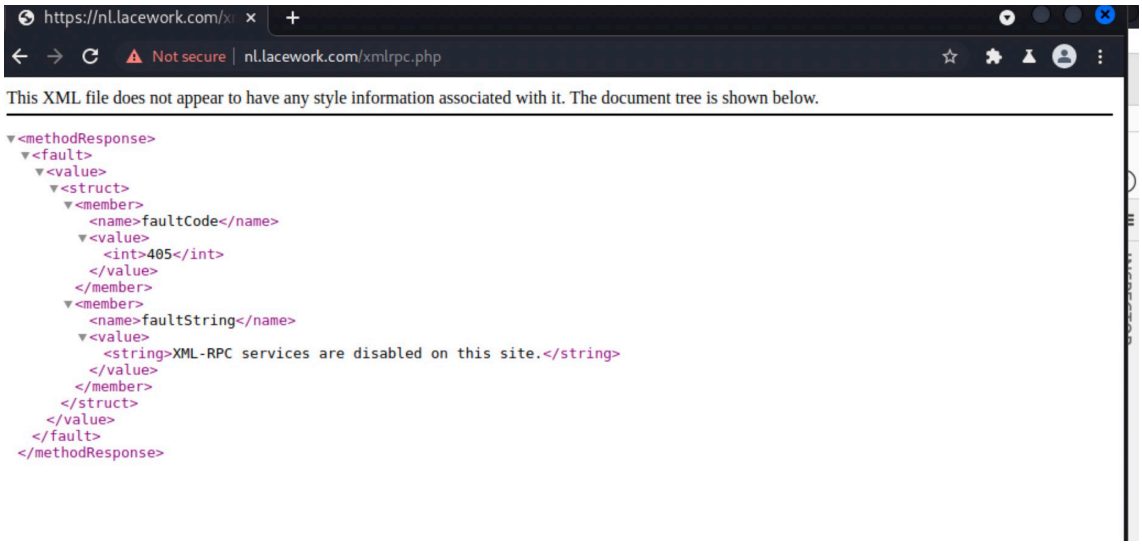
También probamos a lanzar la petición de ataque de fuerza bruta de users y passwords:

```
POST /xmlrpc.php HTTP/1.1
Host: nl.lacework.com
Content-Length: 235

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
```

```
<param><value>\{\{your username\}\}</value></param>
<param><value>\{\{your password\}\}</value></param>
</params>
</methodCall>
```

Y el servidor devuelve la siguiente respuesta



Por tanto, podemos concluir que **los dominios XPL-RPC.php hallados no son susceptibles a la vulnerabilidad esperada.**

4.1.2. Versiones plugins y themes

Por otro lado wpscan nos permite encontrar las versiones de Wordpress utilizada, de los temes y de los plugins que contiene el dominio, por lo que a partir de ahí podemos investigar más posibles vulnerabilidades.

En este caso se ha encontrado que la version de Wordpress en la 5.8.3 que no cuenta con vulnerabilidades conocidas y que ademas sirvió como actualización de seguridad para anteriores versiones vulnerables.

Se adjuntan todos los resultados de los dominios escaneados en el **archivo *“13.WPscanlacework.txt”***

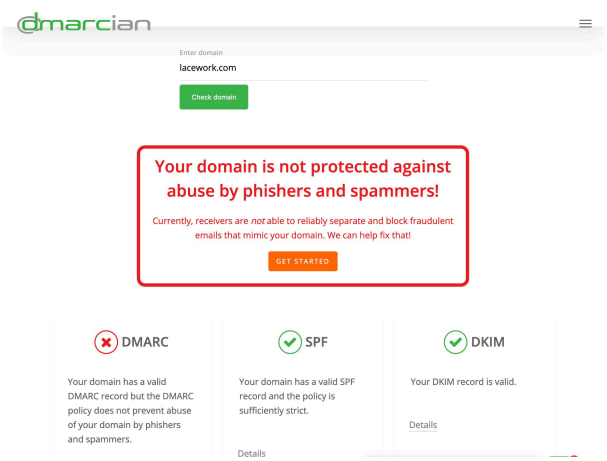
4.2. Análisis de servidores de correo

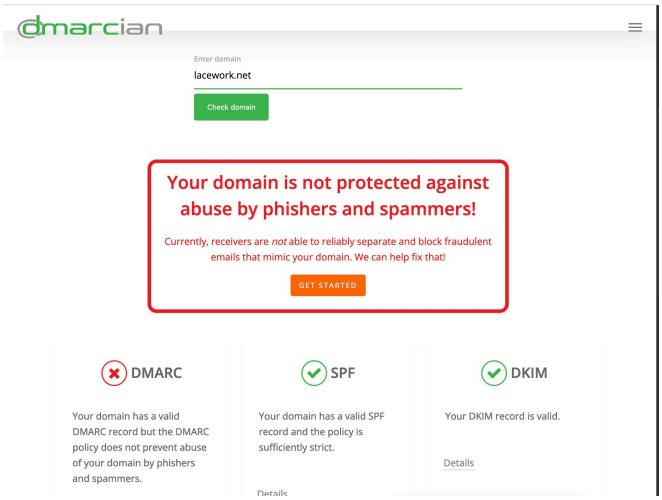
Hay tres protocolos que otorgan seguridad a los servidores de correos:

-SPF: Valida a los remitentes
-DKIM: Sirve para cifrar los correos
-DMARC: Comprueba, utilizando DNS que los registros de SPF y DKIM son correctos, y aplica las reglas necesarias para permitir o bloquear el correo electrónico.

Se puede comprobar si un servidor de correo cuenta con los tres sistemas de seguridad utilizando algunas herramientas online como **dmarcian**:

Comprobamos tanto el servidor de lacework.com como de lacework.net y vemos que la politica de DMARC no está correctamente configurada para saber si el correo que reciben es malicioso o no.





También se puede automatizar esta búsqueda utilizando la herramienta **spoofcheck**

Lanzamos el comando

```
python3 spoofcheck.py lacework.com
```

y

```
python3 spoofcheck.py lacework.net
```

Y nos saca como resultado:

```
+] lacework.com has no SPF record!
[*] No DMARC record found. Looking for organizational record
[+] No organizational DMARC record
[+] Spoofing possible for lacework.com!
```

Se adjuntan los resultados en el archivo ***"14.Spoofcheck_lacework.txt"***

4.3. Subdomain takeover

A través de la herramienta **subzy** podemos conseguir hallar si algún subdominio a los que apunta un subdominio objetivo no está registrado por la organización que estamos investigando.

En primer lugar utilizamos **nslookup** para averiguar el **canonical name** de un dominio, es decir si está apuntando a otra dirección. Lo hacemos con el comando

```
nslookup es.lacework.com
```

Nos muestra como canonical name

```
lacework.sl.smartling.com
```

Le pasamos subzy con el comando

```
subzy -target lacework.sl.smartling.com
```

Y nos encuentra que ese subdominio puede ser vulnerable:

```
[ * ] Loaded 1 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)

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

[  VULNERABLE  ]  -  lacework.sl.smartling.com
[  Smartling  ]

[  DISCUSSION  ]  -  https://github.com/EdOverflow/can-i-
take-over-xyz/issues/67

[  DOCUMENTATION  ]  -  Not available

-----------------
```

Esto significa que no está registrado ese dominio (lacework.sl.smartling.com) y que alguien que acceda al mismo puede registrar ese dominio y atacar a la organización.

Smartling es un servicio de traducción de webs

Sin embargo, esto ocurre en la teoría, ya que si vamos al grupo de discusión de GitHub (https://github.com/EdOverflow/can-i-take-over-xyz/issues/67) vemos que el caso se ha terminado declarando **EDGE CASE,** no se puede concretar si es no vulnerable.

5. OSINT

Osint (Open Source Intelligent) es el conjunto de herramientas y técnicas utilizado para la recopilación de información pública, su posterior análisis y correlación para convertirlo en información útil sobre un objetivo.

5.1. Sobre la empresa

He encontrado una noticia interesante sobre el crecimiento económico de la empresa en el último año:

https://www.newswire.ca/news-releases/lacework-raises-1-3-billion-at-8-3-billion-valuation-820445968.html

Además, en esta misma web se recogen otras **noticias de interés** sobre Lacework:

https://www.newswire.ca/news/lacework/?page=1&pagesize=100

Existe un **perfil en Vimeo** de la empresa que no está enlazado desde la web principal lacework.com. Contiene videos sobre algunos empleados y la organización y productos de Lacework:

https://vimeo.com/user138237655

Perfiles en GitHub:

Con la herramienta **github-search** podemos conseguir perfiles en GitHub de la empresa o de empleados de la misma.

Lanzando el comando

```
python3 github-users.py -t <token de Github> -k lacework
```

conseguimos hacernos con un listado de posibles perfiles de la compañía y empleados, algunos de ellos con correo electrónico incluido.

También podemos ver si encontramos expresiones regulares dentro de los repositorios, para ver si incluyen algun password o información más sensible, con el comando

```
python3 github-secrets.py -t <token de Github> -s lacework
```

En este caso si hemos encontrado algunos username y passwords en repositorios. Se adjuntan los resultados de las búsquedas en el **archivo *"15. GitHubSearchLacework"***

Emails corporativos:

Se pueden utilizar varias herramientas para obtener correos electrónicos. En esta investigación hemos utilizado **Spiderfoot, Infoga** y **Maltego**, obteniendo resultados con todas las herramientas.

Posteriormente es importante verificar que los correos electrónicos son válidos, lo que puede hacerse con la propia herramienta de Maltego o con otras herramientas online como **Intelligence X** o **Aware online**

Se adjunta un listado de los correos electrónicos corporativos obtenidos en el archivo ***"16.EmailsLacework.txt".***

Como último paso, se pueden comprobar también si alguno de esos correos ha sido comprometidos utilizando el **transform "Have I been pwned?"** en **Maltego.** Se adjuntan también los archivos de Maltego con las verificaciones de correos electrónicos realizadas en el archivo comprimido ***"17.MaltegoLacework".***

Información corporativa y board members

Podemos utilizar crunchbase.com para hallar información sobre la empresa: información genérica, aspectos financieros, inversores, perfiles de empleados, etc. Por ejemplo:

https://www.crunchbase.com/organization/lacework

https://www.crunchbase.com/organization/lacework/company_financials
https://www.crunchbase.com/organization/lacework/people
https://www.crunchbase.com/organization/lacework/signals_and_news

Dominios libres:

Utilizando **dnstwist.it** podemos ver que dominios similares a lacework.com y lacework.net están a la venta, lo que podría ser utilizado como un vector de ataque por phishing web.

Se pueden consultar los resultados en ***"18.DnstwistLacework.csv".***

5.2. Sobre los empleados

Visitando la página https://www.lacework.com/about-us/ podemos encontrar el perfil de algunos de los directivos de la organización con enlaces a sus perfiles de Linkedin, y algunos de ellos, aunque pocos, también de Twitter.

Con los datos obtenidos de **Maltego** y **Spiderfoot** disponemos de algunos correos electrónicos corporativos de empleados de la empresa y los nombres de usuario obtenidos de Twitter, utilizamos la herramienta **lampyre.io** para conseguir más información de alguno de ellos, en concreto se pueden obtener posibles cuentas de Skype:

amy.vosters@lacework.net

skype_profile_uid. amy.vosters@lacework.net
skype_profile_deep_link skype://amy.vosters@lacework.net?chat

Para esta investigación vamos a centrarnos en 2 empleados de la organización que servirán de ejemplo de como hemos obtenido la información sobre ellos:

Amy Vosters

Encontramos por primera vex su nombre cuando descubrimos la vulnerabilidad CVE-2017-5487 con **reconftw.**

A través de la web https://es.lacework.com/wp-json/wp/v2/users/ encontramos varios empleados y/o colaboradores del blog de lacework.com que no se encuentran en la sección "About us" de la web.

En esta web Amy Vosters aparece como una de las autoras de artículos blog en la canonnical name web https://www.lacework.com/author/amy-vosterslacework-net/

Haciendo búsqueda en internet encontramos a una Amy Vosters que tiene este dominio:

https://amyvosters.com/

La primera pista para relacionarle con la compañía cuando veo que reside en San Jose (California), el mismo sitio donde está ubicada Lacework, Inc.

Después, con el correo amy.vosters@lacework.net encontrado con **spiderfoot,** hago búsqueda en lampyre.io y la foto que aparece, parece ser la misma persona que aparece en las fotos de la web amyvosters.com

Foto en lampyre.io

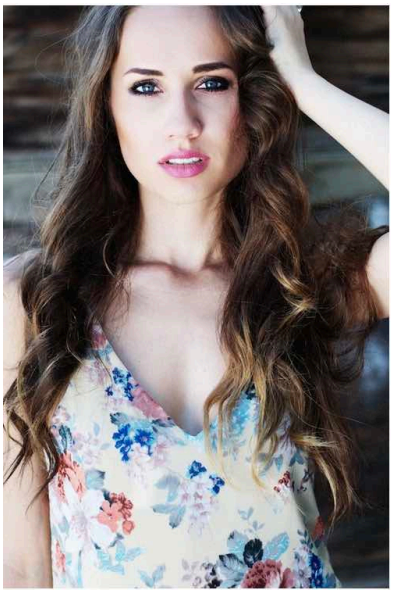
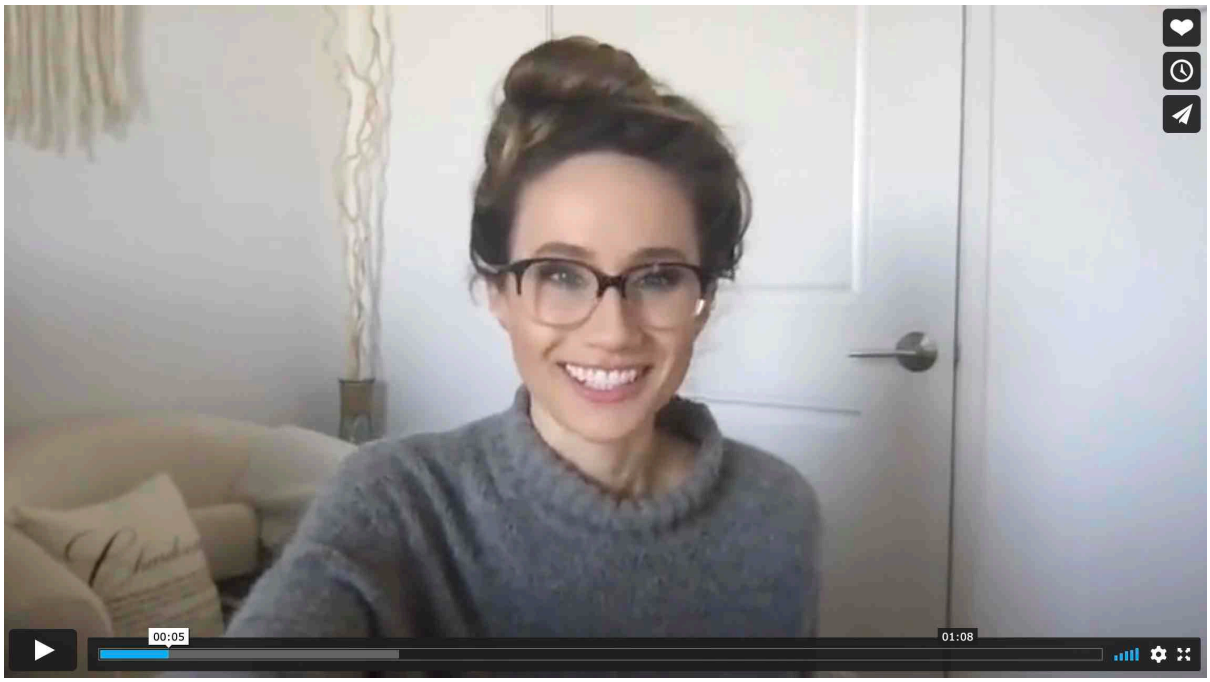


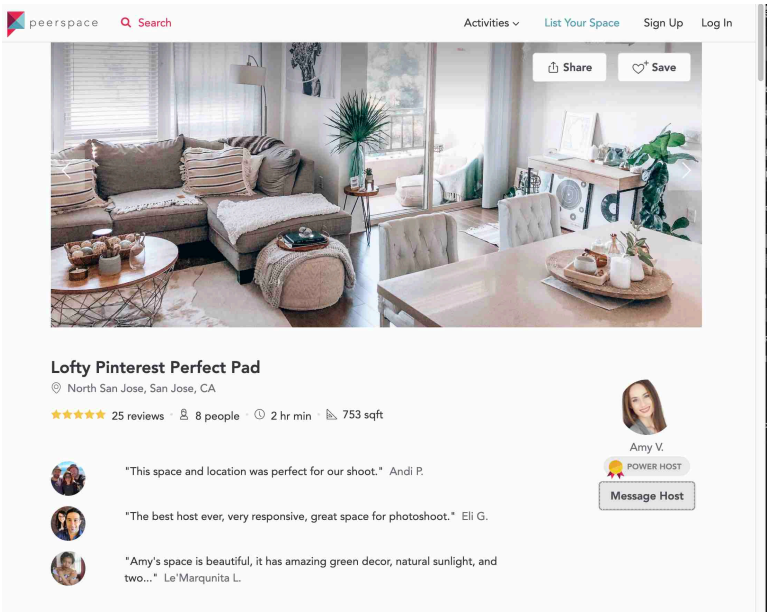
Foto en amyvosters.com

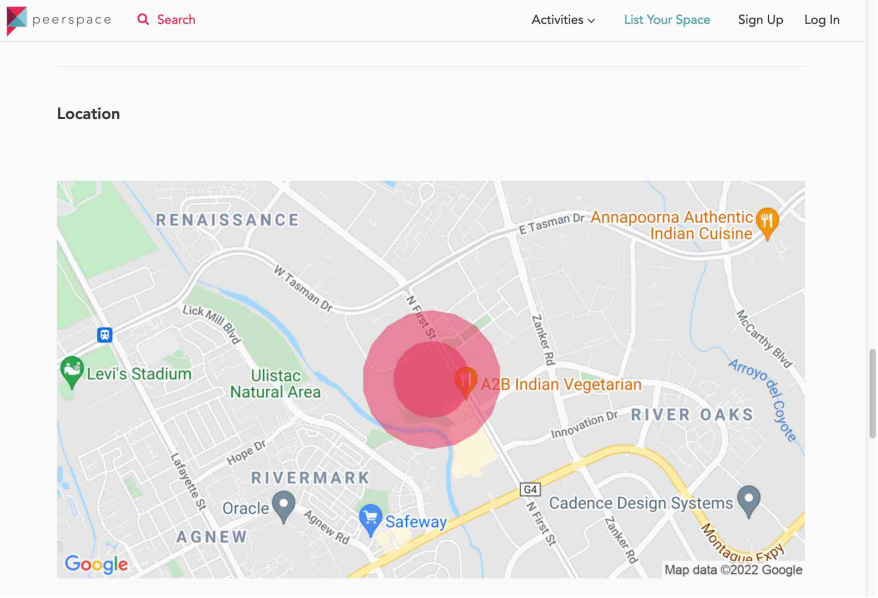
Finalmente, cuando encuentro el canal de la organización en Vimeo, parece que no quedan dudas de que se trata de la misma persona



Al principio del video parece que menciona que es “Campaign (otra palabra que no entiendo) Manager” en Lacework.

Incluso en su web amyvosters.com tiene enlace a otra web https://www.peerspace.com/pages/listings/5f58215cfd540e000cb54c40 donde parece que alquila un espacio por horas y se puede encontrar la localización exacta del sitio y contactar con ella directamente.





https://www.google.es/maps/place/A2B+Indian+Vegetarian+Restaurant/@37.3989388,-121.948242,15.82z/data=!4m5!3m4!1s0x808fc94b5e84c3c3:0x10ef46a7a694ef34!8m2!3d37.4026853!4d-121.940452

Cuenta además con un enlace a otra web donde tiene un perfil con más datos personales y acceso al perfil de 888 friends: https://www.modelmayhem.com/amyvosters

También se pueden utilizar la gran cantidad de fotos con las que cuenta Amy Vosters en estas webs para analizar los metadatos de las mismas con la herramienta **exiftool.**

Analizo alguna como esta y consigo ver, en los metadatos, entre otros datos, la fecha en que fue tomada, pero no la localización:

```
Image Size: 800x1355
Megapixels: 1.1
Date/Time Created: 2018:06:28 21:39:56
```

Chris Pedigo

Los pasos que he seguido en la investigación de Chris Pedigo son:

1. También localizo su nombre al igual que el de Amy Vosters a partir del enlace https://es.lacework.com/wp-json/wp/v2/users/. Aparece en uno de las lineas de esta web “"Chris Pedigo, Global Field CTO, Author at Lacework"

2. A través de una primera búsqueda en DuckDuckGo, con “Chris Pedigo, Global Field CTO Lacework” encuentro su repositorio en GitHub:

https://github.com/Pedigo-Lacework

3. Utilizo la técnica de .patch al final de la dirección URL de los commits pero aparece otro correo de otro empleado de lacework, no el suyo (scott.ford@lacework.net)

4, Reduzco la búsqueda a “Chris Pedigo Lacework” en Google y la segunda entrada me muestra el enlace https://twitter.com/pedigo36.

5. Utilizo lampyre.io para hacer búsqueda por el **username pedigo36**

Entre otra información encontramos:

Facebook

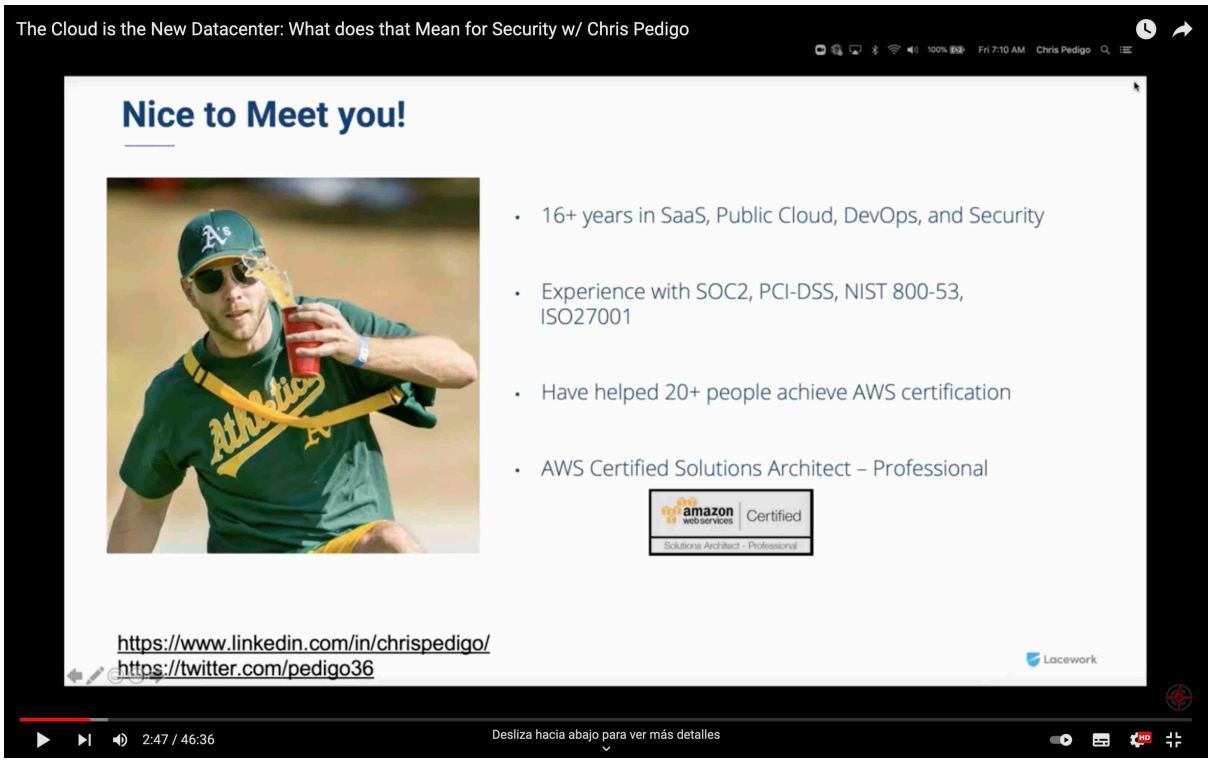
fullname
Chris Pedigo
email_part p******6@gmail.com

6. A partir de aquí es fácil deducir que su correo personal puede ser pedigo36@gmail.com

7. Hacemos nueva búsqueda en **lampyre.io** con ese correo y obtenemos confirmación al aparecer la misma imagen que con pedigo36.

8. A través de un video de Youtube localizado, el nombre de usuario pedigo36 vuelve a aparecer asociado a Chris Pedigo:

https://www.youtube.com/watch?v=37BfcvocCHs



5.3. Perfiles en redes sociales

Con la herramienta **sherlock** podemos extraer posibles perfiles de redes sociales si disponemos de username.

Hacemos esta búsqueda con el comando

```
python3 sherlock <username>
```

Hay que comprobar posteriormente los resultados obtenidos, ya que aparecen perfiles en algunas redes sociales que no existen.

También puede utilizarse de nuevo para esta tarea **Spiderfoot** con el comando

```
spiderfoot -m sfp_accounts -s <"username"> -q -n
```

Y por último, hemos utilizado tambien **OSRFramework**

```
usufy --list usernames.txt -p all
```

En el **archivo *"20.PerfilesLacework.txt"*** se incluyen los perfiles obtenidos de Amy Vosters, Chris Pedigo y otros empleados de Lacework de los que se ha hallado username con anterioridad.

En los casos de Amy Vosters Chris Pedigo podemos encontrar que sus perfiles de Facebook son abiertos, por lo que podemos encontrar mucha más información e ambas personas utilizando las búsquedas avanzadas o a través de los metadatos de las fotografías que tienen colgadas.

https://www.facebook.com/amy.vosters.9
https://www.facebook.com/Pedigo36/