AUTOR DEL LIBRO

Luis Herrero Pérez es Oficial de Transmisiones del Cuerpo General del Ejército de Tierra. Es Diplomado en Informática Militar, ha cursado el "Máster en Sistemas de la Información y las Comunicaciones para la Defensa por la Universidad Rey Juan Carlos y el "Máster Universitario de Ciberseguridad" por la Universidad Carlos III de Madrid, en el que obtuvo el premio extraordinario de fin de Máster. Ha cursado diversos cursos de Ciberseguridad, tanto nacionales como internacionales, ha participado en numerosos ejercicios internacionales de ciberseguridad, organizados por la OTAN y por sus centros asociados. Dispone de las certificaciones GPEN de SANS y OSCP de Offensive Security.

Es profesor en el "Máster en Búsqueda Avanzada de Evidencias Digitales y Lucha contra el Cibercrimen" y en el "Máster en Ciberseguridad. *Red Team Blue Team*", ambos de la UAM.

GLOSARIO DE TÉRMINOS

- **AD:** *Active Directory*
- **AES:** *Advanced Encryption Standard*
- **AP:** *Access Point*
- **CMS:** *Content Management System*
- **CVE:** *Common Vulnerabilities and Exposures*
- **CVSS:** *Common Vulnerability Scoring System*
- **DMZ:** *Demilitarized Zone*
- **DNS:** *Domain Name System*
- **DoS:** *Denial of Service* (denegación de servicio)
- **FQDN:** *Fully Qualified Domain Name*
- **ICANN:** *Internet Corporation for Assigned Names and Numbers*
- **IoT:** *Internet of Things*
- **LDAP:** *Lightweight Directory Access Protocol*
- **NDA:** *Non-Disclosure Agreement*
- **OSINT:** *Open Source Intelligence*
- **OWASP:** *Open Web Application Security Project*
- **pth:** *pass-the-hash*
- **ptt:** *pass-the ticket*
- **RGPD:** Reglamento General de Protección de Datos

- **ROE:** *Rules Of Engagement* (Reglas de enfrentamiento)
- **SAM:** Security Account Manager
- **SGBD:** Sistema Gestor de Bases de Datos
- **SQL:** Structured Query Language
- **TLD:** Top Level Domain
- **TTL:** Time To Live
- **TTP:** Tácticas, Técnicas y Procedimientos
- **VM:** *Virtual Machine*
- **WMI:** *Windows Management Instrumentation*

1

INTRODUCCIÓN

Cuando una persona se quiere introducir en el mundo de la ciberseguridad desde el punto de vista ofensivo, uno de los principales problemas que suele tener es encontrar la información necesaria para empezar, no por la falta de la misma, sino más bien justo por lo opuesto: existe un exceso de información que puede provocar frustración por empezar con aspectos demasiado complejos o por no estar estructurada.

Este libro tiene como objetivo que todas aquellas personas que se quieren iniciar en el "*hacking*" comprendan los conceptos básicos necesarios y conozcan la metodología que se debe seguir durante el proceso, además de trabajar con una batería inicial de herramientas necesarias para las distintas fases. Dada la naturaleza y el propósito del libro, hay técnicas más avanzadas o muy específicas que se mencionan pero en las que no se entra en profundidad, sin embargo, una vez que el lector asimile los conceptos del libro, le resultará mucho más sencillo buscar información para profundizar en dichos aspectos.

A pesar de que los conceptos que se comienzan manejando son básicos en cuanto a seguridad, se da por hecho que el lector dispone de conocimientos previos de informática y redes, que resultan muy necesarios para este mundo. Por ello, en este libro se parte del supuesto de que el lector sabe manejar con soltura Sistemas Operativos **Linux** y **Windows** y posee unos conocimientos básicos de protocolos de red, aunque esto no quiere decir que sea imprescindible conocer hasta el mínimo detalle todos los protocolos ni ser un experto administrador de sistemas. Se sobreentiende que la propia inquietud del lector interesado en la ciberseguridad le animará a profundizar en aquellos aspectos en los que detecte que deberá tener mayores conocimientos.

El libro pretende dar la información teórica necesaria para comenzar en el hacking, que está acompañada de numerosos ejemplos prácticos realizados sobre un laboratorio que el propio lector puede crear. Para ello se estructura de la siguiente forma:

En el segundo capítulo se encontrarán las definiciones y conceptos básicos, incluida la explicación de los diferentes tipos de análisis de seguridad que se pueden encontrar y las diferencias entre los mismos. A continuación, se indican diferentes metodologías que se pueden seguir a la hora de realizar un test de penetración.

El tercer capítulo comienza con la explicación de la primera fase que se realiza en un test de penetración, a semejanza de lo que haría un atacante. Se explican diferentes técnicas de realizar un reconocimiento para obtener información, así como algunas herramientas útiles para el mismo.

El cuarto capítulo sigue el flujo de la fase de enumeración y se explican algunas técnicas para obtener información a partir de los puertos y los servicios expuestos por un equipo en Internet. El capítulo concluye con una introducción a la enumeración web.

El quinto capítulo está dedicado a la explotación de sistemas, consistente en la obtención de acceso utilizando la información obtenida en la fase de enumeración. Se explican algunas de las herramientas más comunes que se pueden utilizar, así como diferentes técnicas de explotación, con ejemplos sobre servicios concretos identificados anteriormente.

El sexto capítulo se enfoca en las acciones a realizar una vez que se logra acceso a un equipo. Se verá la forma de obtener información del equipo y de la red interna, así como la forma de utilizar esta información para moverse lateralmente a otros equipos o para escalar privilegios para tomar control total del sistema. De igual forma, se muestran algunas técnicas sencillas de permanecer en el sistema, aunque se pierda el primer acceso y se incidirá en la importancia del borrado de huellas y de limpiar las acciones realizadas en el equipo.

El séptimo capítulo se dedica a la comprobación de la seguridad de las redes WiFi, tan extendidas en los hogares, empresas y establecimientos públicos. A nivel teórico, se citan los diferentes protocolos de seguridad existentes y se enumeran los tipos de ataques que se pueden realizar en función del elemento atacado. Asimismo, se proporcionan las bases para poder seleccionar el adaptador más adecuado para esto y se realiza un ejemplo práctico en el que se obtiene la contraseña de una red WiFi.

Para concluir, se incluye un apéndice con los pasos necesarios para crear un entorno virtual que permita seguir los ejemplos indicados en todos los capítulos.

2

DEFINICIONES Y CONCEPTOS BÁSICOS

"*Los males, cuando se los descubre a tiempo, se los cura pronto; pero ya no tienen remedio cuando, por no haberlos advertido, se los deja crecer hasta el punto de que todo el mundo los ve.*"

Nicolás Maquiavelo

Diariamente se producen numerosos ciberataques; cuando alguno de ellos es detectado surgen varias preguntas: *quién* ha sido, *cuando* entró en los sistemas, *qué* ha hecho y qué se ha llevado, *cuanto* tiempo ha estado dentro y *cómo* consiguió acceder. Es probable que nunca se pueda identificar al atacante, y averiguar lo que ha hecho en el sistema puede requerir un proceso largo y costoso, pero lo que es aún más preocupante para muchas organizaciones es si podrá recuperarse de los daños y recuperar la información perdida. Sin embargo, si la organización hubiera identificado previamente el *cómo* y el *qué*, habría podido protegerse de una manera más adecuada y evitar el ataque o, al menos, aprender de sus vulnerabilidades para minimizar los daños.

El objetivo de la ciberseguridad es minimizar los riesgos, reduciendo las vulnerabilidades y bloqueando las amenazas, en un proceso continuo que va desde la detección de las vulnerabilidades hasta el análisis de los ataques recibidos, pasando por la monitorización en tiempo real de lo que sucede en los sistemas.

2.1 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Cuando hablamos de la seguridad de la información nos referimos a las medidas para proteger la información sensible de una organización o persona. Aunque abarca también la información procesada o almacenada en sistemas no

informático, es un concepto íntimamente relacionado con la ciberseguridad, puesto que, hoy en día, la mayor parte de la información se procesa o almacena en sistemas informáticos.

Independientemente del propósito final del atacante, todos los ataques buscarán afectar al menos a una de las dimensiones básicas de la seguridad de la información o de los sistemas. Una correcta seguridad de la información consiste adoptar las medidas adecuadas para proteger estas dimensiones, lo que se traduce en un proceso continuo de actualización y mejora de las medidas de seguridad, basado en nuevas vulnerabilidades y amenazas.

- **Confidencialidad**: el principio de confidencialidad se basa en proteger la información del acceso por parte de personas o sistemas no autorizados. Por extensión, se deben proteger también los sistemas y redes que transmiten, procesan o almacenan dicha información. Un atacante puede comprometer la información de formas sencillas sin necesitar grandes conocimientos: por ejemplo, haciendo *shoulder surfing* (es decir, mirar de manera disimulada) cuando un administrador introduce su contraseña, o a través de lo que se ha dado en denominar *dumpster diving* (una manera fina de referirse a buscar en la basura) para buscar papeles con información sensible.

- **Integridad**: este principio se basa en evitar que se produzcan cambios no autorizados en la información ni en los sistemas. Un ataque que modifique la integridad de la información puede tener consecuencias de todo tipo para una organización o persona, por poner unos pocos ejemplos, se pueden hacer fraudes económicos modificando números de cuenta bancaria, dar accesos a personas no autorizadas modificar mensajes transmitidos, entre otros muchos.

- **Disponibilidad**: la disponibilidad permite que la información y los sistemas sean accesibles por las personas o sistemas que deben acceder a los mismos, en el momento que sea requerido. Ejemplos típicos de ataques contra la disponibilidad son los de Denegación de Servicio (DoS).

- **Autenticidad**: que consiste en que una entidad es quien dice ser, de modo que se garantice la fuente de la que procede la información. Es decir, que no se ha producido una suplantación de identidad.

- **Trazabilidad**: de modo que se puedan identificar las acciones realizadas sobre la información y los sistemas, de modo que se pueda determinar quién y cuándo ha accedido y ha realizado las modificaciones. Este principio también se puede denominar **auditoría**.

2.2 DEFINICIONES BÁSICAS

Anteriormente se han introducido los conceptos de riesgo, vulnerabilidad y amenaza que están relacionados pero que conviene diferenciar:

Una **amenaza** es un agente que puede causar un daño. Algunas amenazas son "naturales", como inundaciones, incendios o terremotos; frente a ellas hay que tener una adecuada redundancia de los sistemas y una buena política de backup. Otras tienen un origen más humano y pueden ser intencionadas o no intencionadas; entre estas amenazas se pueden encontrar Estados, organizaciones criminales, compañías rivales, empleados descontentos, o usuarios poco concienciados o descuidados. De manera resumida, la amenaza será el "atacante".

Una **vulnerabilidad** es una debilidad o un fallo que se puede utilizar para causar un daño de manera voluntaria o involuntaria. Algunos tipos de vulnerabilidades son fallos en el desarrollo del *Software* o en el diseño del *Hardware*, un mal diseño de la arquitectura de los sistemas o malas configuraciones.

El **riesgo** es la posibilidad de que una amenaza explote una vulnerabilidad. Una amenaza intentará materializar el riesgo mediante un ataque, para lo que utilizará un **vector de ataque**, que es el camino que sigue una amenaza para lograr sus fines.

De estos tres conceptos se pueden encontrar múltiples definiciones diferentes, pero conviene diferenciarlas adecuadamente y acudir a fuentes fiables, puesto que es bastante común leer definiciones que mezclan los términos. Por ejemplo, es común leer que entre las amenazas se encuentran el "espionaje", el "beneficio económico" o el "*phishing*", pero los dos primeros casos serían el propósito y el último sería el vector de ataque.

Cuando se realiza un análisis de seguridad surgen los conceptos de **caja negra, gris** o **blanca**, referidos al grado de conocimiento que se tendrá previamente a la realización del mismo. Este conocimiento puede variar desde ser nulo (caja negra) hasta conocer toda la información de los sistemas (blanca), lo que incluye el esquema de red y, tal vez, disponer de un usuario interno con privilegios elevados. Entre medias está la caja gris, que es un conocimiento parcial que puede irse ampliando por parte de la organización según se haya acordado previamente.

2.3 VULNERABILIDADES

Antes de proseguir con los diferentes análisis de seguridad es conveniente profundizar más en el conocimiento de las vulnerabilidades, dado que el propósito de los análisis de seguridad es identificar estas con el fin de corregirlas.

Resulta complicado hacer una clasificación de tipos de vulnerabilidades, dado que estas se pueden agrupar de distintas maneras, según el propósito de la persona u organización que establezca la clasificación. Posiblemente, la primera clasificación general que se puede hacer consiste en clasificar las vulnerabilidades según cual sea la fuente de la misma, de modo que se podrían identificar vulnerabilidades en el *Hardware*, vulnerabilidades introducidas en el diseño e implementación de las arquitecturas, vulnerabilidades en el desarrollo del *Software*, vulnerabilidades producidas en la implementación del *Software* y vulnerabilidades en la operación del usuario. No conviene menospreciar estas últimas, pues un usuario poco concienciado con la seguridad será el eslabón más débil en la seguridad de una organización.

2.3.1 Tipos de vulnerabilidades según su severidad

El *Common Vulnerability Scoring System* (CVSS) es un estándar abierto de evaluación de la gravedad de vulnerabilidades conocidas, para lo que se utilizan unas métricas para asignar una puntuación final y, a partir de ella, establecer la severidad de la vulnerabilidad correspondiente. Los aspectos que se son: el vector de acceso, la complejidad de la explotación, el nivel de autenticación que tiene que tener el atacante en el sistema, el impacto sobre la confidencialidad, la integridad y la disponibilidad.

Una vez evaluados todos esos aspectos y asignada la puntuación correspondiente a cada uno, estas puntuaciones se suman para dar lugar a un número entre 0 y 10, que sirve para reflejar los siguientes grados de severidad:

- Nula: recibe una puntuación de 0.
- Baja: de 0,1 a 3,9.
- Media: de 4,0 a 6,9.
- Alta: de 7,0 a 8,9.
- Crítica: de 9 a 10.

2.3.2 Tipos de vulnerabilidades según el tiempo transcurrido desde su descubrimiento

Vulnerabilidades de día cero (*zero-day*)

Se trata de vulnerabilidades en los sistemas para las que no existen parches que las puedan solucionar. Desde que un atacante descubre la existencia de este tipo de vulnerabilidades hasta que el fabricante publica el parche puede transcurrir mucho tiempo, años incluso, en el que el sistema está comprometido. Es posible,

incluso, que la vulnerabilidad se haga pública pero el fabricante no haya podido desarrollar aún el parche correspondiente, de modo que el número de potenciales atacantes se incrementa exponencialmente.

Vulnerabilidades de día uno (one-day)

Este caso se da cuando la vulnerabilidad es pública y ha sido reconocida por el desarrollador, que ha publicado los parches correspondientes. Normalmente, en ciertos entornos los parches no se aplican instantáneamente, puesto que requieren de un proceso de pruebas acorde con las políticas de la organización. Este periodo de tiempo desde que estos parches se publican hasta que se aplican en todos los sistemas puede ser utilizado por potenciales atacantes, que conocerán la existencia de la vulnerabilidad, podrán estudiar los parches para ver la forma de explotarla, y tendrán tiempo de buscar sistemas que no estén parcheados.

Vulnerabilidades antiguas

Se trata de vulnerabilidades que se conocen desde hace más tiempo, para las que suelen existir parches o nuevas versiones y también existen *exploits* públicos para aprovechar las mismas. Aun así, en ocasiones los sistemas estarán sin parchear por diversos motivos, por lo que un atacante podría utilizar las mismas para comprometer los sistemas.

2.4 TIPOS DE AMENAZAS

Dejando a un lado las amenazas naturales, contra las que poco se puede hacer aparte de tener redundancia de los sistemas y unas buenas políticas de *backup*, las amenazas se pueden clasificar según su nivel de organización.

2.4.1 Poco estructuradas

Son personas que actúan de manera individual o grupos pequeños, que no pertenecen a ninguna organización ni tienen financiación externa. Normalmente, la explotación se basará en vulnerabilidades conocidas y documentadas y usarán técnicas poco sofisticadas.

Sus propósitos pueden ser por simple curiosidad, para demostrar sus capacidades, realizar acciones de hacktivismo o intentar obtener beneficios económicos, si bien estos últimos propósitos son más propios de amenazas estructuradas.

Los objetivos de estas amenazas serán objetivos de oportunidad, que se puedan descubrir durante el reconocimiento al utilizar alguna técnica o herramienta de las que se hablará en el capítulo dedicado al reconocimiento.

2.4.2 Estructuradas

Un peldaño por encima están las amenazas estructuradas. Estas son grupos organizados, que tienen tiempo y conocimientos para planificar adecuadamente sus ataques y que pueden tener algún mecanismo de financiación.

Estas amenazas generalmente realizarán ataques específicos contra objetivos concretos y establecidos previamente. Dedicarán más tiempo para obtener toda la información posible del objetivo y normalmente utilizarán vulnerabilidades no documentadas para realizar la explotación.

Normalmente, una amenaza que quiera llevar a cabo un ataque de *ramsomware* contra una empresa entrará dentro de esta categoría, al igual que grupos hacktivistas.

2.4.3 Muy estructuradas

Se trata de organizaciones grandes profesionalizadas, con financiación y con recursos humanos, materiales y de tiempo para poder llevar a cabo sus ataques

Los objetivos son muy específicos, generalmente empresas estratégicas, objetivos gubernamentales o personas pertenecientes a ciertos colectivos no afines.

Los propósitos de estas amenazas excederán normalmente a los económicos, estando más bien encaminadas a buscar a una superioridad estratégica u operacional.

2.5 TIPOS DE ATAQUES

La categorización de los ataques no es una tarea sencilla, puesto que dependerá de los criterios utilizados por cada fuente. Algunos de los criterios más habituales para clasificar los ciberataques son el propósito o el vector de ataque utilizado. Otra posible clasificación sería según el principio atacado (Confidencialidad, Integridad, Disponibilidad o Autenticidad), pero también podrían dividirse en activos o pasivos, o clasificarse según el objetivo atacado (red, WiFi, cliente, persona…). En resumen, se pueden haber tantas clasificaciones como se desee y en cada una de ellas se podrán encontrar numerosos matices.

2.5.1 Tipos de ataques según su propósito

Ciberespionaje

Estos ataques consisten en realizar acciones de espionajes en el ciberespacio, o utilizando el ciberespacio como medio, de modo que se obtenga información perteneciente a empresas, organizaciones gubernamentales o personas pertenecientes a organizaciones no alineadas con el atacante.

Este tipo de ataques normalmente se llevará a cabo por Estados o por empresas que tienen el fin de obtener información sobre empresas rivales.

Cibercrimen / ciberdelito

Este término abarca aquellas acciones delictivas que emplean el ciberespacio como herramienta o como objetivo. Este concepto abarca tanto actividades delictivas tradicionales, pero ejecutadas a través del ciberespacio (como pueden ser timos, suplantaciones de identidad, venta de drogas o de armas), como delitos específicos de los sistemas de información (por ejemplo, denegaciones de servicio, degradación o destrucción de sistema). Generalmente el propósito de estos ataques será económico.

Este tipo de ataques se dirigen contra empresas, personas individuales o contra organismos públicos, y normalmente se llevará a cabo por organizaciones criminales o por individuos a sueldo.

Hacktivismo

Son ataques que buscan controlar o dañar equipos y sistemas con el fin de dar visibilidad a una causa, política o no. Las motivaciones pueden ser políticas, ideológicas, búsqueda de venganza o ganas de atraer la atención.

Ejemplos de ataques que entran en esta categoría son las acciones en las que los atacantes publican bases de datos tras atacar a una empresa, o los *defacement* de sitios web para mostrar un mensaje contrario a la empresa propietaria del mismo.

Este tipo de ataques normalmente se llevará a cabo por grupos activistas contra empresas y gobiernos.

Ciberterrorismo

Tiene el propósito final de crear miedo generalizado en la población e influir en la misma y en el gobierno. Como consecuencia de la ejecución de acciones en el ciberespacio para destruir o interrumpir servicios esenciales.

Ejemplos de ataques que entran en esta categoría son las acciones en las que los atacantes publican bases de datos tras atacar a una empresa, o los *defacement* de sitios web para mostrar un mensaje contrario a la empresa propietaria del mismo.

Este tipo de ataques normalmente se llevará a cabo por grupos terroristas, bien sea de manera independiente o como pantalla de gobiernos.

Ciberguerra

Es la utilización del ciberespacio para alcanzar una superioridad militar, debilitando o destruyendo objetivos estratégicos u operacionales de una nación enemiga en el marco de un conflicto armado.

Dentro de la definición anterior se incluyen diferentes acciones que abarcan un amplio espectro: desde acciones de propaganda y espionaje hasta ataques contra infraestructuras críticas. En cualquier caso, para que una acción pueda ser considerada como acción de guerra debe enmarcarse dentro de las normas que regulan los conflictos armados y respetar lo establecido.

Si bien es bastante complicado que se dé una situación de guerra formal únicamente en el ciberespacio, puesto que muchas de las acciones podrían afectar a población civil, es cierto que se ha usado en ocasiones como complemento a acciones bélicas. Un ejemplo de esto se produjo en la guerra de Osetia del Sur, donde el movimiento de las fuerzas rusas iba acompañado de acciones en el ciberespacio contra objetivos de Georgia.

Por la propia definición de guerra, estos ataques sólo se pueden llevar a cabo por organizaciones militares en el marco de un conflicto bélico, e irán dirigidos contra objetivos conforme a lo regulado en los tratados internacionales.

2.5.2 Tipos de ataques según el vector de ataque

El concepto “vector de ataque”, que se introdujo anteriormente al hablar del riesgo, proviene del ámbito militar y es el método que utiliza la amenaza para aprovechar una vulnerabilidad y atacar el sistema.

Una vez que un atacante ha obtenido suficiente información del objetivo, incluidos sistemas y datos personales de los empleados de la organización, estará en condiciones de elegir la mejor forma de atacarlo con garantías de éxito.

La clasificación de los ataques según el vector utilizado es un poco complicada, dado que en muchos casos la línea es difusa y, en muchas ocasiones, se usa una combinación de varios para materializar un ataque. Sin ánimo de ser exhaustivos, algunos ataques según el vector utilizado son los siguientes:

- *Malware*. Son aquellos programas que ejecutan acciones maliciosas en un equipo. El término malware abarca numerosos tipos de programas, como virus, gusanos, troyanos, *keyloggers*, *ramsomware*, *adware* o *spyware*.
- *E-mail*. Se puede utilizar para enviar spam, para realizar *phishing* o para enviar *malware*. En muchas ocasiones, el correo electrónico sirve como vector de ataque inicial para que la persona descargue y ejecute el *malware* en el sistema.
- Navegación por Internet. En muchas ocasiones asociado a los dos anteriores, Internet se pude utilizar para robar información o para descargar *malware* en la víctima.
- Aplicaciones y páginas web. Las páginas web de las empresas son, en muchas ocasiones, aplicaciones. Un atacante las puede utilizar para llevar a cabo ataques a las aplicaciones con el fin de lograr acceso o extraer información de las mismas y de sus bases de datos relacionadas. Algunos tipos de ataques Web conocidos son las inyecciones SQL o los ataques de Cross Site Scripting (XSS), entre otros muchos.

2.6 TIPOS DE ANÁLISIS DE SEGURIDAD

Una vez vistos los conceptos básicos anteriores es necesario conocer la terminología relacionada con los distintos análisis de seguridad, para diferenciarlos adecuadamente.

En primer lugar, es necesario comprender adecuadamente el término ***hacking***. El término *hacker* se utilizó desde su origen para definir a aquella persona que estudiaba en profundidad una tecnología, con el fin de conocerla de modo que pudiera modificarla y realizar tareas para las que no estaba pensada originalmente. Esta definición se adoptó en el ámbito informático, pero su significado ha ido variando, de tal manera que, actualmente, se suele utilizar el término *hacking* para definir el acceso no autorizado a sistemas ajenos con el propósito de ocasionar

daños. La RAE reconoce el término *hacker* (aunque lo redirige a "jáquer") en sus dos acepciones: "pirata informático" y "persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora".

2.6.1 Ethical Hacking

Para evitar la anterior connotación negativa se inventó este término para definir aquel *hacking* que no tiene propósitos dañinos, también denominado *white hat hacking* o *hacking* ético (afortunadamente, el término "jáquing" no se encuentra en el diccionario de la RAE). Estos términos se utilizan para definir la utilización de técnicas ofensivas para acceder a sistemas con la finalidad de detectar vulnerabilidades y reportarlas para que puedan ser solucionadas.ee

2.6.2 Penetration Testing

Se suele denominar por su forma abreviada *pentesting* o *pentest*, aunque también se pueden encontrar en español como "test de penetración". A lo largo de esta obra se emplearán estos términos indistintamente.

Se trata de un subconjunto del *Ethical Hacking*, en el que se utilizan las mismas tácticas, técnicas y procedimientos (TTP) empleadas por atacantes reales para encontrar vulnerabilidades y explotarlas para acceder y tomar control de los sistemas, siempre según lo que se haya acordado al definir el alcance de las pruebas y conforme a las reglas de enfrentamiento (ROE). Un test de penetración servirá para identificar las amenazas y los riesgos, así como para determinar el impacto que tendrían sobre los sistemas.

2.6.3 Red Teaming

Se trata del proceso de realizar una simulación de ataque en la que se aplican TTP ofensivos, con el fin de valorar y mejorar los procedimientos de una organización, así como sus tecnologías y las capacidades de detección y respuesta ante incidentes. Por ello, cuando se realizan acciones de *Red Team* existe un *Blue Team* defensivo y, posiblemente, equipos denominados con otros colores que tienen distintos cometidos, como el *Purple Team*, que existe para integrar las medidas defensivas del *Blue Team* con las vulnerabilidades detectadas y los ataques realizados por el *Red Team*. En un escenario ideal el *Purple Team* debería ser, más que un equipo, una dinámica de cooperación entre el *Red Team* y el *Blue Team*.

Aunque las técnicas y las herramientas que se emplean un *Red Team* puedan ser exactamente las mismas que se emplean durante un *pentesting*, se diferencian en aspectos fundamentales como el propósito y la duración.

2.6.4 Análisis de vulnerabilidades

Los análisis de vulnerabilidades tienen el propósito de identificar todas las vulnerabilidades existentes en los sistemas, pero sin llegar a explotarlas. Un análisis de vulnerabilidades también debería comprender aspectos que no se realizan en un test de penetración, como la revisión de las políticas de seguridad de la organización y de la documentación de seguridad. Existen, por tanto, notables diferencias entre un análisis de vulnerabilidades y un test de penetración.

2.6.5 Auditoría de seguridad

Las auditorías de seguridad implican comprobar el estado de la seguridad de una organización conforme a unos estándares de seguridad determinados, para lo que se suelen emplear *checklists* en los que el auditor refleja múltiples aspectos.

2.7 TIPOS DE *HACKERS*

Es común identificar los distintos tipos de hackers según colores de sombreros. Al hablar del *Ethical Hacking* se introdujo el término *white hat hacking*. Como se puede deducir, un ***white hack hacker*** es aquel que lleva a cabo acciones de hacking debidamente autorizadas con el propósito de identificar vulnerabilidades.

Por el contrario, un ***black hat hacker*** es aquel que tiene propósitos maliciosos, cuyos fines consisten en obtener un beneficio personal o económico, o causar daños a una organización o persona.

Entre medias se encontrarían los denominados ***grey hat hackers***. Como corresponde al color, hay muchos tonos de gris y bajo esta denominación caben unos cuantos tipos de personas. Por ejemplo, aquí entrarían aquellos que atacan a una organización para, a continuación, ponerse en contacto con ella y ofrecer sus servicios. También podrían entrar en este tipo aquellos que trabajan para un gobierno con el fin de obtener información sobre otros países.

2.8 ASPECTOS ÉTICOS Y LEGALES

A lo largo del capítulo se ha utilizado la palabra ético para referirse a ciertas acciones realizadas con un buen propósito, y se ha identificado a los hackers por colores según sus intenciones. Se podría pensar que, si las acciones están autorizadas y el *hacker* ético se ciñe a lo acordado y no revela la información que pueda obtener a lo largo de sus acciones, se está cumpliendo la legalidad.

Sin embargo, en muchas ocasiones la línea de separación entre lo legal y lo ilegal puede ser muy fina. Pensemos en una acción de ingeniería social en la que el *hacker* ético engaña a un empleado para que le proporcione sus credenciales y luego las utiliza para acceder al sistema y a la información manejada por el mismo, como haría un atacante real. Si se piensa bien, en este caso se está produciendo una suplantación de identidad y podría tener consecuencias legales tanto para el *hacker* ético como para la empresa.

Para intentar minimizar los problemas legales, es fundamental definir muy bien los aspectos que se indicarán posteriormente al hablar de la preparación de un *test* de penetración. La organización que encarga una acción de hacking ético o la hace con su propio personal, debe haber establecido de manera clara a todos sus empleados la política que seguirá en cuanto al empleo de sus sistemas de información. Por supuesto, en el informe final, se deberán omitir los datos personales de aquellos empleados sobre los que se hayan realizado acciones o de los que se haya podido obtener información.

Ahora bien, qué sucedería si, durante una acción de *hacking* ético, como podría ser un test de penetración, se encuentran elementos que revelen que la organización ha recibido o está recibiendo un ataque real. Obviamente, el *pentester* pararía las acciones e informaría inmediatamente al personal de contacto en la organización. A partir de ahí se abren dos vías: denunciar o ir por libre e intentar averiguar qué ha pasado. Una investigación del incidente podría llevar a obtener información del potencial atacante, así como direcciones IP de equipos implicados en el ataque. Puede surgir la tentación de acceder a esas direcciones IP e, incluso, hacer acciones ofensivas sobre las mismas, como podrían ser denegaciones de servicio o hacer todo el proceso de hacking para intentar acceder a los sistemas. Dejando al margen que esos sistemas pueden ser sistemas legítimos que han sido previamente vulnerados por el atacante para utilizarlos como salto intermedio, si nos trasladamos al mundo "físico" sería el equivalente de agredir a un carterista al que hemos pillado in fraganti: puede parecer justo y resultar satisfactorio, pero a efectos legales resultará de difícil justificación.

2.9 TIPOS DE PENTESTING

Existen múltiples aspectos que se pueden comprobar durante la realización de un *pentesting*, en función de las necesidades de la organización, el tiempo y el presupuesto. Para poder determinar adecuadamente las acciones que se llevarán a cabo es necesario conocer, al menos someramente, los tipos de *pentesting* más comunes.

- ***Network***. Consiste en localizar sistemas y servicios en una red y buscar vulnerabilidades en los sistemas operativos y aplicaciones de servidor, malas configuraciones o cualquier cosa que pudiera permitir a un atacante explotarlos de manera remota.
- **Client-Side**. Tiene como propósito encontrar vulnerabilidades en *software* instalado en equipos de usuario.
- **Web.** Su finalidad es encontrar vulnerabilidades en las aplicaciones web de una organización.
- **Wireless.** Consiste en comprobar la seguridad de las redes *wireless* (generalmente Wi-Fi) existentes en las instalaciones de una organización.
- **Ingeniería social**. Consiste en atacar a los usuarios para logar que revelen información, ejecuten alguna aplicación maliciosa, accedan a sitios web controlados por el atacante, o realicen otras acciones que pudieran permitir a un atacante obtener ventaja de sus acciones.
- **Físico**. Durante un *pentest* físico se intentará acceder a las instalaciones del cliente con el fin de acceder a sus equipos, encontrar documentación, robar dispositivos de almacenamiento, desplegar dispositivos para realizar posteriores acciones remotas, y cualquier otra acción que pudiera realizar un atacante. Este tipo de test puede resultar peligroso para el *pentester*, de modo que deberá portar un permiso de ejecución y disponer de un punto de contacto en la organización que le avale en caso de que sea detectado por la seguridad.

Generalmente un *pentest* no será de un único tipo, sino que se utilizará una combinación de varios de ellos. Por ejemplo, un *pentest client-side* suele llevar aparejado, al menos, la realización de acciones de ingeniería social.

2.10 METODOLOGÍAS

Para llevar a cabo un test de penetración se debe seguir una metodología. Aunque un pentester experimentado habrá desarrollado la suya propia, siempre resulta conveniente conocer algunas metodologías y seguirlas, sin perjuicio de realizar las adaptaciones necesarias para adecuarlas a las necesidades y gustos personales. Entre las más conocidas se encuentran las siguientes:

- **Penetration Testing Framework.** Se enfoca principalmente en el *Network pentesting*. Proporciona una guía paso a paso de cada aspecto a evaluar e indica las herramientas y comandos a utilizar. Incluye secciones dedicadas a VoIP, Bluetooth y *Wireless*, entre otras secciones. Está disponible en *http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html*.

- **Penetration Testing Execution Standard (PTES)**. Define las actividades que se deben contemplar en un *pentest,* con el propósito de que las organizaciones a las que se les realiza reciban un producto que puedan entender y que proporcione valor para el negocio. Este estándar proporciona datos para las distintas fases de un *pentest*: interacciones previas, como la definición del ámbito y las ROE; actividades de reconocimiento; modelado de la amenaza; análisis de vulnerabilidades; explotación; post explotación, y elaboración del informe. Se encuentra disponible en *http://www.pentest-standard.org/index.php/Main_Page*.

- ***Open Web Application Security Project (OWASP) Testing Guide***. A diferencia de las anteriores, esta metodología se centra exclusivamente en la seguridad de aplicaciones web y en describir en detalle las diferentes comprobaciones que se deben llevar a cabo, además de indicar las herramientas que se pueden usar a lo largo del proceso. Se encuentra disponible en *https://owasp.org/www-project-web-security-testing-guide/*.

2.11 FASES DE UN PENTEST

El proceso de un test de penetración comprende varias fases que se pueden agrupar en tres bloques principales: preparación, ejecución y presentación de resultados. De la primera y la última se hablará en este capítulo, la fase de ejecución es la parte técnica, y es a la que se dedicará el resto del libro.

2.11.1 Fase de preparación

Preparación con el cliente

En esta fase participan el responsable del equipo de *pentesting* y el responsable designado por la organización, para definir varios aspectos del *pentesting*, entre los cuales se incluye en qué consistirá, las responsabilidades de ambas partes y la duración del mismo.

Dado que, generalmente, existe bastante desconocimiento por parte de las organizaciones, es muy probable que sus responsables no tengan claras sus necesidades o no las sepan expresar más que de una manera muy genérica, por lo que esta fase comenzará con una reunión inicial para plantear cuestiones que sirvan para guiarle. Se pueden utilizar cuestionarios basados en los incluidos en el PTES, que sirvan para delimitar el test, la duración, qué tipo de *pentesting* realizar y el alcance. Durante esta reunión se pueden tratar los aspectos más relevantes para la organización, entre los que pueden estar sus sistemas más sensibles, sus principales preocupaciones y las amenazas identificadas.

La fase de preparación finalizará con los siguientes documentos:

- **Acuerdo de confidencialidad**. También conocido como **NDA** (*Non-Disclosure Agreement*), cuyo propósito es proteger la información de la organización que se pueda conocer durante el *pentesting*. Obliga a proteger las comunicaciones, equipos utilizados, soportes de almacenamiento y los resultados del *pentesting*.

- **ROE**. Describen las prácticas que se seguirán. Esto incluye aspectos como la duración del *pentesting* y el horario, si será de caja blanca, negra o gris, la periodicidad de las reuniones entre el personal responsable de la organización y el equipo de *pentesting*, así como información de contacto en ambos sentidos, para imprevistos o comunicaciones urgentes, entre otros aspectos.

- **Alcance del** test. El alcance determina qué rangos de IP, nombres de dominio, equipos o aplicaciones deben comprobarse y cuales deben excluirse expresamente. También determina la profundidad, lo que condicionará la posibilidad de realizar la explotación y post-explotación (términos de los que se hablará posteriormente). Asimismo, el alcance también debe contemplar los tipos de test que se llevarán a cabo (*network*, *client-side*, web, etc.).

El alcance y las ROE son conceptos que se suelen confundir, para evitar mezclar los conceptos se puede decir que el alcance determina *qué* se puede hacer, mientras que las ROE determinan el *cómo* hacerlo.

- **Permiso de ejecución**. Se trata de una autorización firmada por el responsable de la organización para llevar a cabo el *pentest*. Es un documento fundamental, sin el cual jamás se debería iniciar ninguna acción, y que deberá llevar encima todo el personal que participe en el test, sobre todo en el caso de realizar un *pentest* físico.

Preparación de la infraestructura de ataque

Antes de iniciar cualquier tipo de test de penetración es necesario configurar la infraestructura, lo que implica una planificación no sólo del *software* y *hardware* necesarios, sino también de la infraestructura de red necesaria.

Al igual que un atacante real, un equipo de *pentesting* necesitará ordenadores desde lo que lanzar sus ataques, así como máquinas de apoyo y, probablemente, una infraestructura en Internet que permita ocultar el origen de los ataques. Es importante tener en cuenta que la misma infraestructura no servirá para todos los *pentest* que se realicen, será necesario adaptarla o crear una infraestructura nueva cada vez.

Todos los equipos que se utilicen durante un test de penetración deben estar actualizados completamente (tanto el S.O. como las aplicaciones) y no tener aplicaciones ni servicios innecesarios.

Equipos ofensivos

Aunque para las acciones ofensivas es bastante habitual utilizar equipos con Sistema Operativo **Linux**, no hay que descartar la utilización de **Windows**. Es más, resulta conveniente disponer de distintos equipos con distintos sistemas operativos, dado que es posible realizar acciones y encontrar herramientas específicas para uno de ellos, o que simplemente funcionen mejor en un sistema que en otro.

Los equipos que se utilicen para las acciones ofensivas deben ser totalmente diferentes de los de uso personal y de los empleados en el trabajo diario. Los motivos para ello son tanto de seguridad, ya que en ocasiones se trabaja con malware, como de privacidad, puesto que se puede comprometer tanto la información de la organización como la del propio equipo atacante, al exponerlo a la red interna. En muchas ocasiones será necesario modificar las configuraciones del equipo atacante e instalar aplicaciones que no se empleen habitualmente, por lo que, además de utilizar

un equipo específico, es conveniente crear una imagen del equipo antes de iniciar el análisis y restaurarla al finalizar el mismo.

Cuando se vayan a configurar los equipos ofensivos se deben determinar dos aspectos: el primero es si se utilizarán equipos físicos o máquinas virtuales, y el segundo es si se instalará una distribución existente o si se va a utilizar un sistema propio en el que se hayan instalado herramientas. La mayor parte de las distribuciones están basadas en **Linux**, algunas de las más populares son **Kali Linux** (*https://www.kali.org/*) o **Parrot OS** (*https://www.parrotsec.org/*), pero también existen algunas basadas en **Windows**, como **PentestBox** (*https://pentestbox.org/*) o **Commando VM** (*https://github.com/fireeye/commando-vm*), que consisten en paquetes que se instalan en un equipo que ya dispongan previamente de **Windows**. En el apéndice dedicado a la configuración del laboratorio se indicará cómo configurar una Máquina Virtual (VM) a partir de una distribución.

2.11.2 Fase de ejecución

Se trata de la parte técnica del *pentest* que se puede dividir en: reconocimiento, enumeración explotación y post-explotación. Durante esta fase se deben documentar todas las acciones realizadas y los resultados de las mismas, lo que resulta esencial tanto de cara al informe final como para deshacer las modificaciones realizadas en los sistemas a lo largo del proceso.

2.11.3 Fase de presentación de resultados

Esta fase resulta fundamental en un test de penetración, dado que sirve para exponer a la organización las acciones realizadas, las vulnerabilidades y riesgos de sus sistemas y unas recomendaciones para mejorar la seguridad. Sin entrar en excesivos detalles del informe final, este debe contemplar como mínimo los siguientes apartados:

1. **Resumen ejecutivo**. Breve y dirigido al personal de la dirección con escasos o nulos conocimientos técnicos y que no tendrá tiempo para leer el informe completo.

2. **Introducción**. Descripción a alto nivel, indicación de la duración, participantes y resumen de los principales riesgos.

3. **Metodología seguida**. Descripción técnica de las acciones realizadas y los resultados obtenidos. No debe ser un copia-pega de los resultados

de las herramientas ni de la salida de la ejecución de los comandos, que deberán ir en los anexos, si se quieren incluir.

4. **Vulnerabilidades encontradas**. Descripción detallada e individualizada de las vulnerabilidades detectadas, indicando el riesgo, sistemas afectados, cómo se podría explotar y recomendaciones para corregirlas.

5. **Conclusiones**. Un resumen general del estado de la seguridad y de las vulnerabilidades, así como unas recomendaciones para el futuro.

6. **Anexos**.

3

RECONOCIMIENTO

La fase de reconocimiento comenzará una vez que se finalice la definición del alcance, se firmen los documentos necesarios y se elabore un plan para el test de penetración. De esta forma, aunque el test a realizar sea de caja negra, se tendrá al menos un mínimo de información que servirá como punto de partida a partir del cual obtener más información relacionada con la organización objetivo. Este punto de partida inicial puede ser simplemente el nombre de la organización, que será generalmente el punto de partida de un atacante, o bien se puede comenzar con más información, como: nombre del dominio; rango de direcciones IP, o nombres de algunas personas pertenecientes a la organización, por poner tres ejemplos comunes.

Esta fase es muy importante, ya que permitirá conocer la organización lo suficiente como para llevar a cabo las fases posteriores. Por ello, aunque en el punto de partida se disponga de información sobre la organización, antes de comenzar el ataque es necesario hacer un estudio profundo sobre la misma para conocerla lo mejor posible y estudiarla en búsqueda de posibles vulnerabilidades e información que permita llevar a cabo el ataque.

Como resultado del reconocimiento, uno de los productos que se obtendrá es una relación de posibles objetivos, que deberá ser cuidadosamente verificada antes de proseguir con las siguientes fases para confirmar que dichos objetivos entran dentro del alcance. Es incluso posible que algunos de los objetivos encontrados no sean ni siquiera conocidos por personal de la organización, por lo que en el caso de un test de penetración es conveniente verificar los mismos con el representante de ésta, así como relacionarlos en el informe final.

Durante el reconocimiento se evitará en la medida de lo posible interactuar con el objetivo, o se interactuará con el de una manera "normal", por ejemplo

navegando normalmente en sus sitios web, pero desde direcciones IP que no comprometan al pentester.

En este capítulo se verá cómo obtener información de la organización a partir de fuentes abiertas, lo que denomina "reconocimiento pasivo" u OSINT (del inglés *Open Source Intelligence*).

3.1 OSINT / RECONOCIMIENTO PASIVO

Con el reconocimiento pasivo se buscará toda la información posible sobre la red y los sistemas del objetivo sin establecer conexión directa con el mismo. Internet proporciona una gran ayuda a la hora de buscar información en fuentes abiertas, por lo que será la base para realizar este reconocimiento.

Durante el reconocimiento pasivo se buscará información relativa, entre otras cosas a: nombres de dominio; direcciones IP; organizaciones con las que se relaciona; tecnologías empleadas; infraestructura de red; direcciones de correo; nombres de empleados, sus cargos e información personal de los mismos. Asimismo, es necesario obtener cuanta información sea posible de cómo funciona la organización, sus ubicaciones físicas (sobre todo en el caso de que el test de penetración incluya una parte física), su estructura jerárquica, el área de negocio de la organización, la terminología empleada por personal de la organización. Para ello, las herramientas que se utilizarán serán comunes y al alcance de cualquiera:

- Buscadores web.
- Redes sociales.
- Foros.
- Ofertas de empleo.
- Bases de datos online.
- Búsqueda de metadatos en archivos.

Estos aspectos se tratarán en los siguientes apartados, pero antes de entrar en ellos es necesario mencionar una técnica que aunque parezca antigua, hoy en día puede seguir proporcionando información interesante. Se dice que "la basura de uno es el tesoro de otro" y esto es especialmente cierto en el mundo de la ciberseguridad, donde se ha adoptado el término "*Dumpster diving*" para definir algo que se ha realizado toda la vida: buscar en la basura para obtener información útil sobre la organización o sobre el personal de la misma o sus clientes.

3.1.1 Redes sociales

Las redes sociales tienen el inconveniente de que generalmente requieren un registro previo para poder ver información. En muchas ocasiones también será necesario interactuar de alguna forma con las cuentas sobre las que se está obteniendo información. A pesar de lo anterior, pueden proporcionar información valiosa sobre personal de una organización y sobre la organización misma, por lo que puede merecer la pena utilizarlas para obtener información.

Obviamente, independientemente de que nos situemos desde el punto de vista de un atacante como de un *pentester*, no parece adecuado utilizar las cuentas personales ni profesionales, por lo que la utilización de redes sociales implica un trabajo previo de creación de perfiles en diversas redes sociales y darles vida, de modo que parezcan cuentas legítimas. Es necesario tener en cuenta que, aparte de que estaremos contraviniendo los términos de uso de las redes sociales, la interacción con usuarios de las mismas en muchos casos supone una acción de ingeniería social, por lo que se deberá llevar a cabo con total precaución y protegiendo la información obtenida. Para un atacante real esto es más sencillo, dado que no tiene miramientos a la hora de crear cuentas falsas ni vulnerar la legislación relativa a la protección de datos personal.

3.1.2 Foros

Existen numerosos foros donde se tratan temas técnicos donde los administradores de los sistemas suelen hacer preguntas acerca de configuraciones o problemas que se encuentran en su trabajo diario y es posible que revelen el nombre de su organización de manera inadvertida o intencionadamente, o que se les pueda relacionar de alguna manera con la misma. En este caso, a través de los foros se puede obtener información acerca de las tecnologías empleadas por una organización, e identificar alguna vulnerabilidad o mala configuración.

3.1.3 Ofertas de empleo

En las ofertas de empleo para personal informático las organizaciones suelen relacionar las tecnologías que deben conocer los futuros empleados, por lo que son una buena fuente de información para un atacante, que únicamente tiene que leerlas para hacer una relación inicial de posibles tecnologías y herramientas, aunque deberá confirmarla y ampliarla posteriormente.

3.1.4 Búsquedas en Internet

Las personas y las organizaciones tienden a revelar información de manera inadvertida o intencionada, por ejemplo en redes sociales o a través de campañas de publicidad en Internet. Se puede obtener mucha información interesante y útil a través de diferentes buscadores realizando una serie de búsquedas con una sintaxis adecuada.

Aunque los buscadores ya proporcionan información únicamente escribiendo una palabra o una frase, también proporcionan una serie de operadores de búsqueda (también denominados directivas) que se pueden utilizar para ayudar a centrar las búsquedas en detalles específicos. Esto ha permitido acuñar el término "*Google Hacking*" y, derivado del anterior, "*Bing Hacking*". Aunque ambos son bastante parecidos es interesante conocer la existencia de ambos dado que, en ocasiones, no proporcionan los mismos resultados, además de que en Bing se puede encontrar algún operador que no existe en Google.

3.1.5 Google Hacking

El termino se atribuye a Johny Long, conferenciante habitual en los congresos DEF CON, en los que ha tratado en varias ocasiones la utilización de buscadores para buscar información de interés para un atacante, denominando "*Google Hacking for Penetration Testers*" a la impartida en la DEF CON 13 (año 2.002), que se toma como origen del término y a la que siguió la publicación de un libro con el mismo nombre.

Se trata de una técnica de búsqueda basada en la combinación de diferentes operadores de búsqueda para obtener resultados sensibles que afecten a un objetivo y que puedan ser utilizados por un atacante. Se trata de un tema muy amplio, por lo que en este apartado se verán únicamente los conceptos básicos de cómo utilizar algunos operadores.

Los operadores de Google permiten hacer búsquedas sobre sitios y dominios específicos, así como páginas que contengan contenido relacionado, también permiten buscar en función de texto que se pueda encontrar en el título de las páginas, de las URL o en el contenido de la página.

- "**site:**". Este operador permite indicar el nombre de un sitio o un dominio sobre el que se limitarán las búsquedas. Por ejemplo:

  site:sitioejemplo.es

Se pueden combinar diferentes operadores para acotar más la búsqueda. Los resultados de las búsqueda también cambiarán según se utilicen o no comillas, por lo que puede resultar interesante probar distintas formas de buscar. Por ejemplo:

site:"sitioejemplo.es" intext:"windows"

- "**related:**". Este operador se utiliza para buscar páginas con un contenido similar a la página que se indica el nombre de un sitio o un dominio sobre el que se harán las búsquedas. En muchas ocasiones no devolverá nada de interés, pero puede servir para encontrar alguna relación entre organizaciones en función del contenido de sus sitios web o los hipervínculos existentes. Por ejemplo, si se buscan los sitios relacionados con un banco cualquiera, se encontrarán páginas de otras entidades:

related:bancoejemplo.es

- "**link:**". Busca únicamente en páginas que tienen un enlace a un sitio web:

link:sitioejemplo.es.

- "**intitle:**". Con este operador se restringen las búsquedas a palabras en el título de la página. Este operador resulta muy útil para localizar sitios web que muestren el índice de archivos y carpetas ubicados en un directorio, lo que permitirá a un atacante acceder a información sensible.

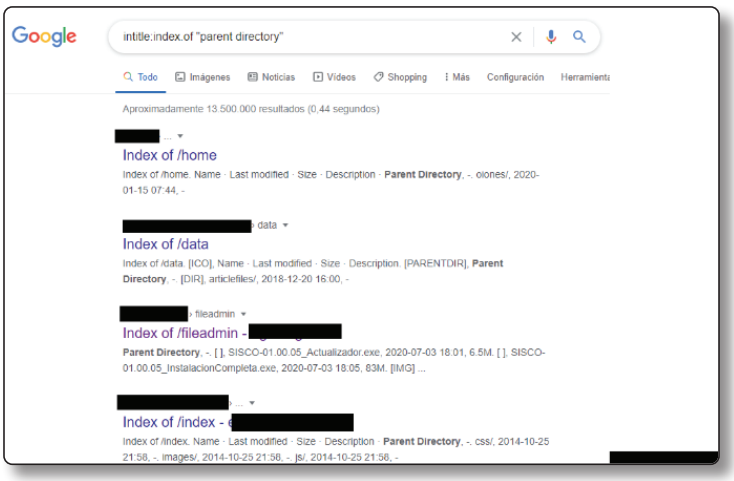

Fig. 3.1-1. Búsqueda utilizando el operador "intitle:"

- "**inurl:**". Este operador busca de manera específica direcciones URL que contengan un texto determinado. Se puede utilizar para buscar *scripts* correspondientes a implementaciones de sitios web con vulnerabilidades conocidas. En el siguiente ejemplo se busca una extensión concreta de **WordPress** con vulnerabilidades conocidas y se refina la búsqueda para encontrar archivos que permitan identificar la versión:

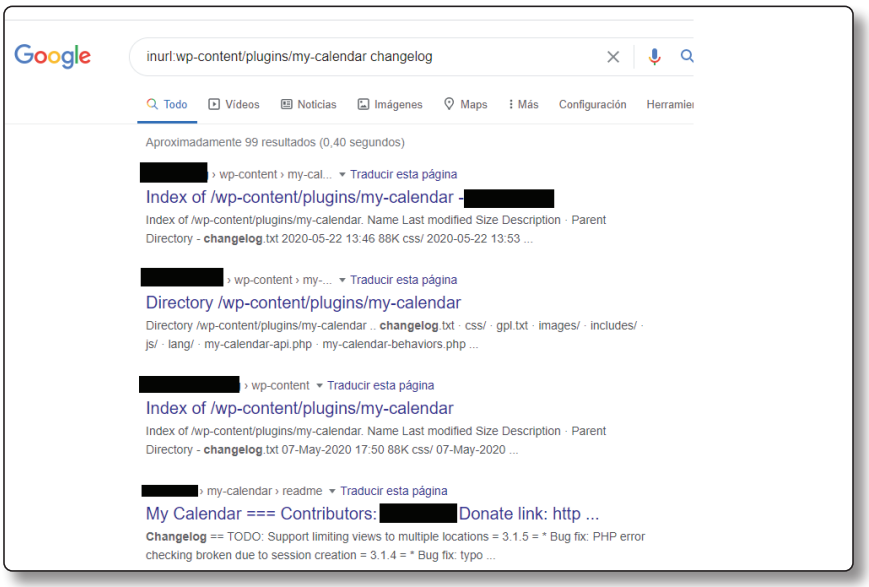

Fig. 3.1-2. Búsqueda utilizando el operador "inurl:"

- "**intext:**". Este operador busca exclusivamente en el texto de la página.

intext:windows

Uno de los elementos más interesantes a buscar durante la fase de reconocimiento son archivos (ofimáticos o de otro tipo), no solamente por su contenido, sino por los metadatos que puedan contener. Sobre los metadatos se hablará más adelante en este capítulo, pero para poder analizar los metadatos es necesario disponer previamente de los archivos y los buscadores web facilitan la búsqueda, dado que identifican distintos tipos de archivos en función de su extensión.

- "**filetype:**". En Google este operador se comporta igual que el operador "**ext:**", lo que permite buscar archivos si Google los ha identificado por su extensión. Si este operador se utiliza sin aplicar un mayor filtrado, en muchas ocasiones Google no devolverá resultados. El operador "***site:***"

visto anteriormente es uno de los operadores que se suelen combinar con este, puesto que permite buscar archivos concretos en un sitio específico.

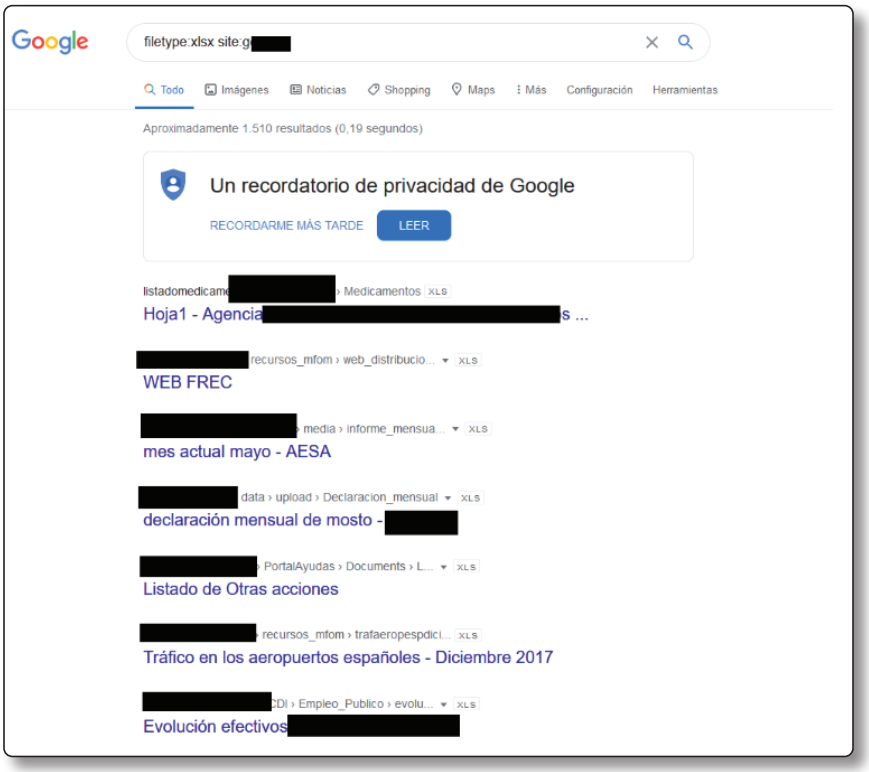

Fig. 3.1-3. Búsqueda de archivos Excel en un sitio concreto.

Además de combinar varios operadores en la barra de búsquedas, estos se pueden modificar para excluir elementos de búsquedas concretas. Para ello se antepondrá un guion delante. Por ejemplo, la siguiente búsqueda se limitará al sitio *sitioejemplo.es* y mostrará todas las páginas indexadas que no contengan en su texto la palabra *Windows*:

site:sitioejemplo.es -intext:windows

Existen multitud de operadores aparte de los que ya se han mencionado, que se pueden combinar prácticamente de manera ilimitada para realizar búsquedas de vulnerabilidades o sitios y páginas de interés. En internet se pueden encontrar numerosos ejemplos, entre los que es de destacar la *Google Hacking Database* (*https://www.exploit-db.com/google-hacking-database*), que es un sitio web mantenido

por **Offensive Security** donde se recopilan términos de búsqueda específicos, denominados *Dorks*, categorizados en función de los objetivos perseguidos con los mismos.

3.1.6 Otros motores de búsqueda

Además de las búsquedas de que se pueden hacer con buscadores como Google o Bing, existen motores de búsqueda que permiten encontrar dispositivos conectados, lo que puede resultar de interés a la hora de localizar direcciones IP correspondientes a *routers* o identificar e incluso controlar cámaras de vigilancia, entre muchas otras posibilidades. Los dos más conocidos son **Shodan** y **Zoomeye**, pero existen otros que pueden resultar interesantes, como **Greynoise**, **Censys, Onyphe** o **Bynaryedge**.

Shodan

A diferencia de los buscadores tradicionales, **Shodan** se centra en encontrar todo tipo de dispositivos conectados a Internet, que pueden ser *routers*, servidores web, cámaras de vigilancia, objetos de la "Internet de las cosas" (IoT) o cualquier otro elemento que se pueda conectar. **Shodan** se puede utilizar de forma gratuita, si bien para utilizar todo su potencial es necesario registrarse y suscribirse pagando la cuota correspondiente.

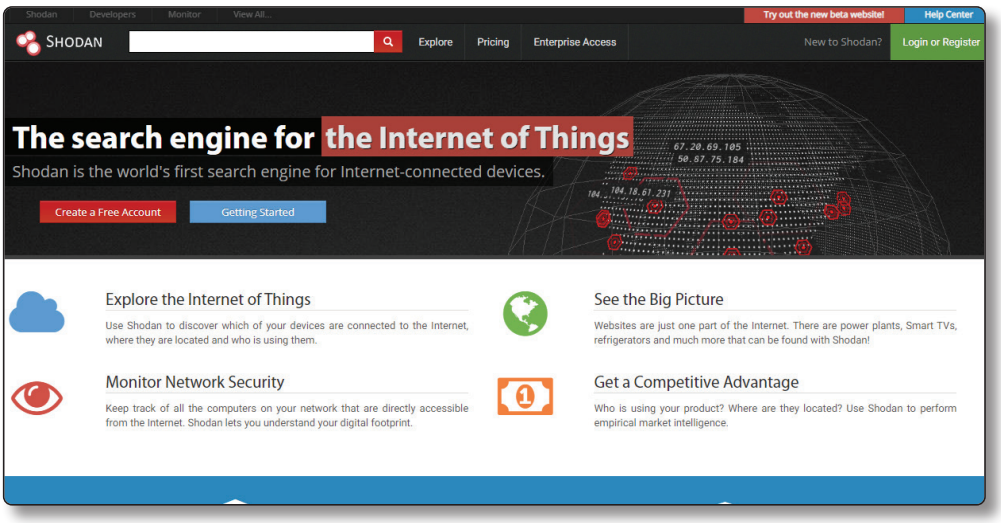

Fig. 3.1-4. Página principal del buscador Shodan.

Además de las búsquedas propias, **Shodan** ofrece una serie de búsquedas predefinidas, categorizadas y agrupadas en función de su popularidad.

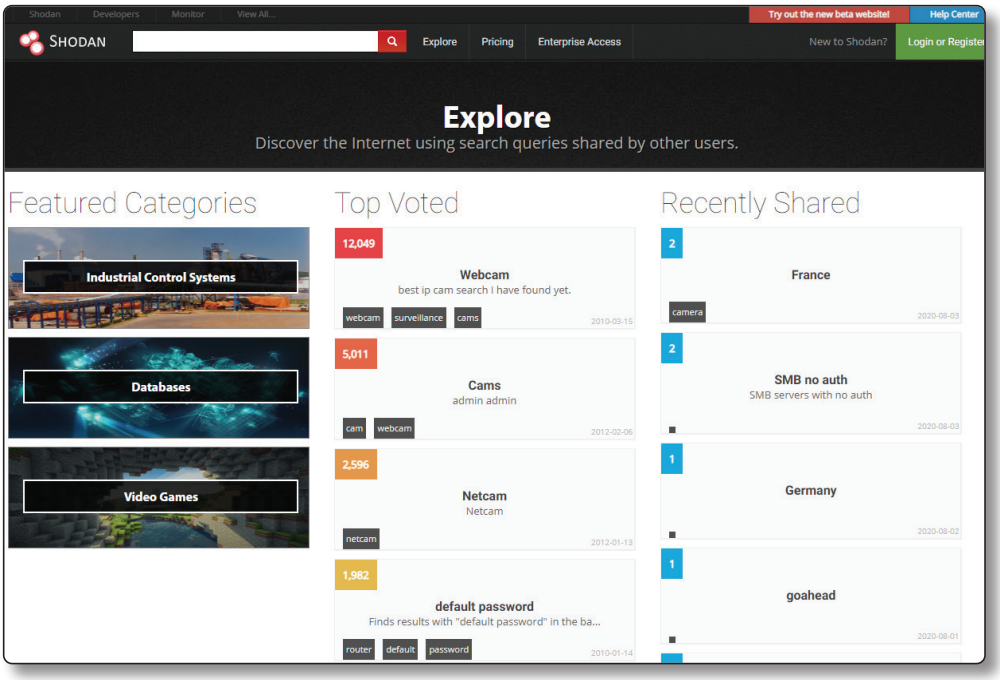

Fig. 3.1-5. Búsquedas predefinidas en Shodan.

Si se selecciona alguna de las categorías se mostrarán las direcciones IP y más información de los elementos correspondientes, que a su vez se podrán seleccionar para obtener más información, como su ubicación, tecnologías utilizadas, vulnerabilidades conocidas o puertos abiertos, entre otras cosas.

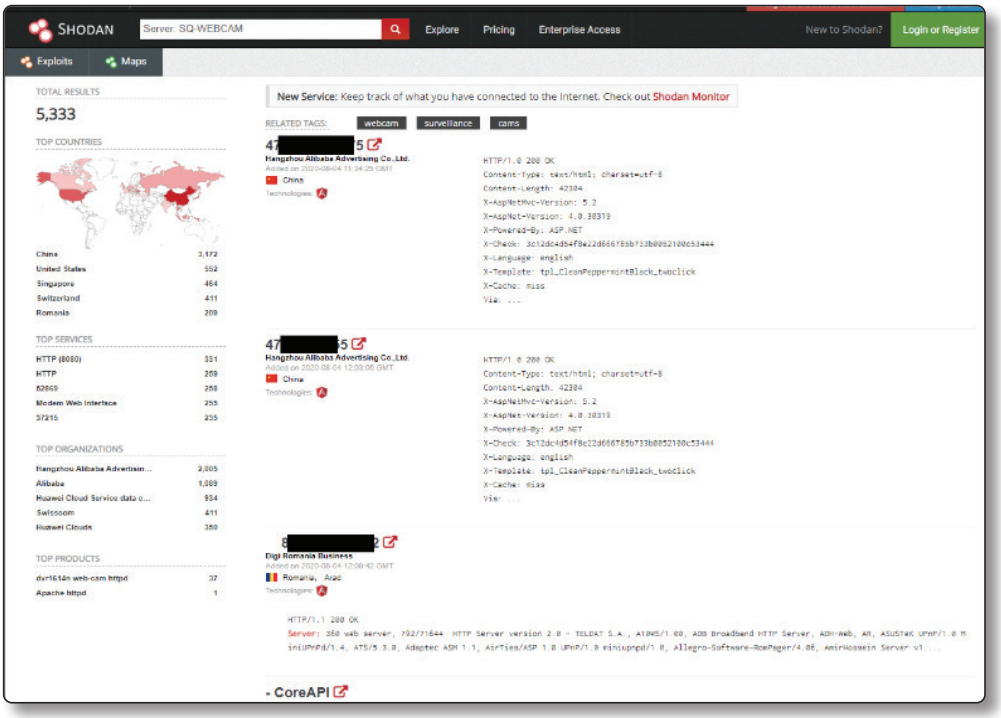

Fig. 3.1-6. Búsqueda realizada con Shodan.

Zoomeye

Este motor de búsqueda, de origen chino, ofrece una funcionalidad similar a la de **Shodan** y, al igual que este, permite realizar una serie de búsquedas gratuitas y ofrece más posibilidades en caso de estar registrados y suscritos.

Al igual que en **Shodan**, se pueden realizar búsquedas propias o utilizar las opciones que proporciona la herramienta a través de búsquedas predefinidas. Por ejemplo, en este caso muestra una lista de tipos de elementos en el panel izquierdo, que se pueden ir seleccionando para encontrar información de elementos concretos conectados.

3.1.7 Bases de datos Whois

Cualquier dispositivo conectado a Internet puede ser localizado a través de su dirección IP pública, bien sea IPv4 de 32 bits o IPv6, de 128 bits. A una persona no le suele resultar sencillo recordar estas direcciones y, además, estas direcciones pueden cambiar. Para solucionar estos problemas se usan los nombres de dominio,

que son elementos fundamentales en la infraestructura de Internet puesto que permiten acceder a servidores y recursos disponibles en la red utilizando direcciones comprensibles y fáciles de recordar.

Un nombre de dominio permite asociar direcciones IP con recursos en Internet, lo que permite que las organizaciones ofrezcan servicios o información y que su acceso sea más sencillo por parte del público general. El nombre de dominio de una organización tiene una estructura formada por varias partes, generalmente se compondrá del nombre del dominio raíz, separado por un punto del dominio de nivel superior (TLD), que es el que figura al final del nombre del dominio (los habituales **.com**, **.es**, **.org** u otros). A su vez, un dominio puede tener varios subdominios que se pueden emplear para identificar diferentes servicios. Estos subdominios se anteponen al nombre del dominio, también separados por un punto. Por ejemplo, los nombres **www.google.com**; **mail.google.com**; **drive.google.com** son subdominios del dominio **google.com**.

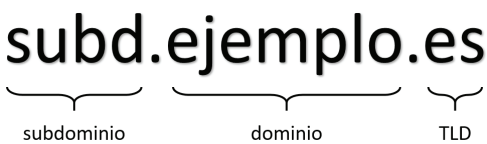

Fig. 3.1-7. Estructura de un nombre de dominio.

En función de si el test de penetración es de caja blanca, gris o negra, estos nombres de dominio se podrán haber proporcionado por la organización o será necesario obtenerlos durante el reconocimiento, por ejemplo a través de búsquedas más o menos complejas en navegadores.

En cualquier caso, una vez que ya se dispone de algunos nombres de dominio es necesario buscar más información correspondiente a los mismos, como direcciones IP, servidores DNS, obtener nombres de las personas relacionadas con esos dominios, números de teléfono, direcciones de correo electrónico.

Cuando una organización registra un nombre de dominio tiene que proporcionar cierta información de la empresa, así como del propietario y del personal técnico responsable del dominio. Esta información se registra a través de entidades denominadas "registradores", que la almacenan en bases de datos y permiten el acceso generalmente público a la información de los registros de nombres.

Esta información pública era totalmente accesible a través del protocolo **whois**, y se podía consultar a través del navegador o a través de líneas de comandos, salvo que el propietario del dominio pagara una cuota para ocultar ciertos datos, lo que no

era lo habitual. Lamentablemente para los intereses de un *pentester* y de un atacante, esto ha cambiado con la entrada en vigor del Reglamento General de Protección de Datos (RGPD) en 2018, con lo que la ICANN (que es la organización que coordina los nombres de dominio a nivel mundial y es la responsable de whois) se vio obligada a realizar ciertas modificaciones. Actualmente, cuando se registra un dominio, se pide consentimiento para mostrar los datos personales en las búsquedas, y en caso de darse el consentimiento, estos datos no se mostrarán en búsquedas Whois.

Consultas Whois a través del navegador

Dado que existen múltiples registradores y no es posible conocer a priori el registrador utilizado por la organización, para realizar las consultas se puede acudir a diversas páginas web:

- *https://lookup.icann.org/*. Se puede utilizar para búsquedas sobre distintos dominios, sin embargo si se intenta buscar algún dominio .es no devolverá resultados.
- *https://www.dominios.es/dominios/*. Para dominios **.es**.
- *https://whois.domaintools.com/*. Permite buscar diferentes dominios, incluidos aquellos en que los TLD son **.es**.

En función de la página que se utilice se obtendrán unos resultados más o menos detallados, por lo que resultará interesante utilizar las diferentes alternativas. Como se puede ver, en este caso la organización tiene información oculta, pero aun así ofrece cierta información que puede ser útil, como los servidores de nombres.

Consultas Whois a través de línea de comandos

Existen aplicaciones de líneas de comandos que permiten realizar consultas whois. Esta herramienta se encuentra por defecto en las distribuciones **Linux** y la mayor parte de sistemas Unix-like, pero para **Windows** es necesario descargar alguna herramienta, por ejemplo la herramienta **whois** de la suite de **sysinternals**, que proporciona Microsoft de manera gratuita (*https://docs.microsoft.com/en-us/sysinternals/downloads/whois*), o la herramienta **WhoisCL** de Nirsoft. En cualquier caso, la sintaxis básica es sencilla, basta con ejecutar el comando seguido del nombre del dominio.

Sin embargo, con la ejecución básica a través de línea de comandos no se obtendrá información de los dominios **.es**, como se puede ver en la siguiente captura de la salida de **whois** en **Linux**:

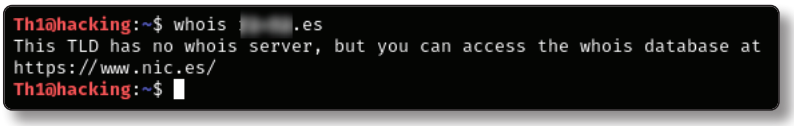

Fig. 3.1-8. Búsqueda whois desde la consola de Linux.

En **Linux** se puede utilizar el parámetro **-I**, que en primer lugar consultará a *whois.iana.org* y a continuación consultará al servidor whois que se indique como autoritativo para esa petición.

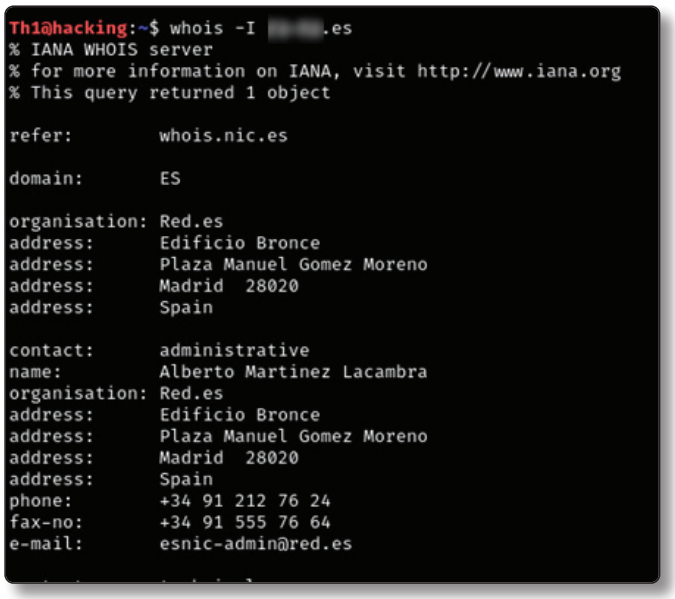

Fig. 3.1-9. Búsqueda whois especificando el servidor de búsqueda.

En ocasiones, como en el ejemplo anterior, la información que se obtendrá será genérica y no proporcionará información relacionada con la organización que tiene registrado el dominio.

3.2 RECONOCIMIENTO ACTIVO

Con las técnicas anteriores no se interactúa con el objetivo, pero existen otras técnicas y herramientas de reconocimiento activo, que ya implican un contacto más directo con el objetivo.

3.2.1 DNS

Explicado brevemente, el sistema de nombres de dominio (DNS) es un protocolo que se utiliza para asociar nombres de dominio con las direcciones IP correspondientes. Esta información se almacena en una base de datos jerárquica distribuida, en la que en cada nivel se encuentran diferentes servidores, que resuelven los nombres y responden a las peticiones que les formulan los clientes, dentro de su espacio de nombres.

En el caso de encontrar algún servidor DNS durante las búsquedas whois, se pueden hacer consultas a los mismos para intentar encontrar equipos relacionados con la organización. En este punto en necesario tener en cuenta que es posible que alguno de los equipos que se identifiquen en este punto no pertenezca a la organización objetivo o quede fuera del alcance, por lo que resultará necesario verificarlo convenientemente antes de utilizarlo en posteriores fases.

Para que un servidor DNS proporcione información acerca de un dominio es necesario hacer las consultas adecuadas para los distintos tipos de registros. Aunque existen numerosos tipos de registros, los siguientes pueden proporcionar información muy valiosa:

- **NS** (NameServer). Contiene el nombre de los servidores de nombres asociados a un dominio concreto.
- **A** (Address / host). Relaciona la dirección IPv4 de un dominio. El equivalente para IPv6 es el **AAAA** (quad-A).
- **MX** (Mail Exchange). Identifica los servidores de correo de un dominio.
- **TXT** (Text). Permite incluir cualquier cadena de texto, que se puede utilizar para distintos propósitos, como almacenar información del propietario.
- **CNAME** (Canonical name). Permite indicar nombres alternativos (alias) para un host.
- **SOA** (Start Of Authority). Indica que un servidor es autoritativo para una zona. Estos registros contienen información administrativa sobre la zona y tienen una gran importancia para las transferencias de zona, sobre las que se hablará posteriormente.
- **PTR** (Pointer / reverse). Se usan para búsquedas inversas, lo que permite encontrar los registros correspondientes a una dirección IP.

- **SPF** (Sender Policy Framework). Es un registro TXT que indica los nombres de servidores o direcciones IP autorizadas para enviar correos electrónicos en nombre del dominio.
- **RP** (Responsible Person). Este es un registro meramente informativo que no se usa habitualmente, pero en caso de usarse contendrá información de la persona responsable de un dominio.
- **SRV** (Service location). Aunque tampoco se usa habitualmente, sirve para indicar qué servicios están disponibles en el dominio, el nombre del equipo y el puerto en el que se encuentra cada servicio.

Herramientas para obtener información de un servidor DNS

Para obtener información de un servidor DNS se pueden utilizar diferentes herramientas e instrucciones de línea de comandos. Algunas de ellas están disponibles por defecto en prácticamente cualquier sistema operativo o, al menos, en casi todas las distribuciones **Linux**, mientras que otras es preciso descargarlas en el equipo en el que se van a ejecutar.

Nslookup

Esta instrucción está disponible por defecto en **Windows** y en casi cualquier distribución de **Linux** y Unix-like. La ejecución básica es sencilla: basta con ejecutar el comando e indicar el dominio o un nombre de host como parámetro.

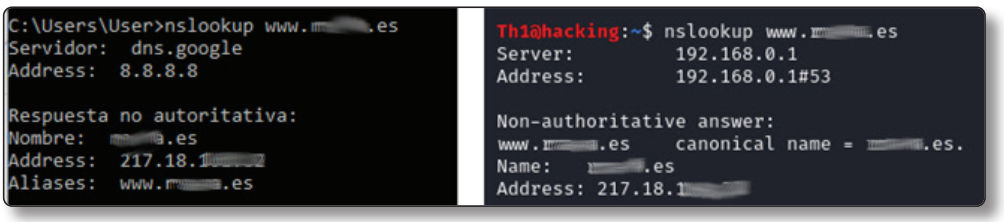

Fig. 3.2-1. Ejecución de nslookup en Windows (izqda.) y Linux (dcha.).

Nslookup también permite especificar diferentes parámetros para ejecutar consultas más complejas, pero una de las características que la hacen interesante es que permite trabajar de manera interactiva. Para ello se ejecutará el comando **nslookup** sin indicar ningún parámetro ni el dominio, de esta forma se abrirá un prompt desde el que se podrán realizar consultas más complejas.

Nslookup permite indicar qué servidor DNS se quiere utilizar la resolución de nombres, lo que permite utilizar los servidores que se hayan podido obtener al hacer las búsquedas **whois**. En caso de que no se disponga de ningún servidor DNS pero se conozca el dominio de la organización, se puede utilizar nslookup para obtener información de los servidores DNS.

Para indicar un servidor DNS diferente se utiliza la instrucción "**server**", seguida de la dirección IP o del nombre del servidor.

```
server servidor_DNS
```

Por defecto, nslookup buscará los registros "**A**", pero se querrá obtener información de otros registros, por lo que se puede indicar el tipo de registro sobre el que se quiere preguntar con la instrucción "**set type=**", seguida del tipo de registro deseado (por ejemplo, **set type=MX**) o de "**any**", en caso de que se quiera obtener información de todos los registros. Por ejemplo, si se quieren conocer los servidores DNS asociados a un dominio, será necesario especificar los registros **ns**, o consultar todos.

```
set type=any
```

Una vez que ya se haya configurado nslookup para hacer las búsquedas sobre el servidor y los registros deseados, se indicará el dominio directamente en el prompt. En este ejemplo, se usa uno de los servidores que se encontraron durante la búsqueda whois.

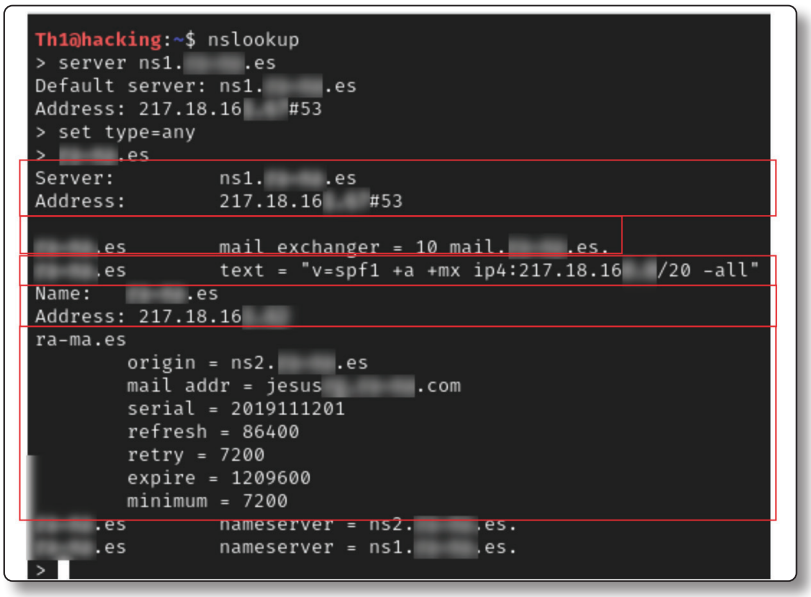

Fig. 3.2-2. Consulta de nslookup en Linux indicando el servidor DNS.