Hacking Ético

3ª Edición

¡Cómo convertirse en hacker ético
en 21 días o menos!

Hacking Ético

3ª Edición

¡Cómo convertirse en hacker ético
en 21 días o menos!

Karina Astudillo B.

Ra-Ma®

La ley prohíbe
fotocopiar este libro

Hacking Etico. 3ª Edición. ¡Cómo convertirse en hacker ético en 21 días o menos!

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-9964-767-8
Depósito legal: M-31990-2018
Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé
Filmación e impresión: Safekat
Impreso en España en noviembre de 2018

A Dios y al Universo por conspirar
para que se cumplan mis metas.

A mis padres, Laura y Pancho,
por su cariño y apoyo constante.

A mis hijos lanudos, Niko y Kira
por alegrar mis días
con sus travesuras y juegos.

ÍNDICE

ACERCA DE LA AUTORA **11**
COMUNÍQUESE CON KARINA ASTUDILLO B. 12

PREFACIO **13**
AUDIENCIA OBJETIVO 14
¿Cuáles son los requisitos? 14
¿POR QUÉ CONVERTIRME EN PENTESTER? 14
¿CÓMO ESTÁ DIVIDIDO EL LIBRO? 16
REGALO PARA EL LECTOR 17
CAMBIOS EN LA 3ª EDICIÓN 17

CAPÍTULO 1. INTRODUCCIÓN AL HACKING ÉTICO **19**
1.1 EL CÍRCULO DEL HACKING 19
1.2 TIPOS DE HACKING 20
1.3 MODALIDADES DEL HACKING 21
1.4 SERVICIOS DE HACKING ADICIONALES 23
1.5 ELABORACIÓN DE LA PROPUESTA E INICIO DE LA AUDITORÍA 25
1.6 CREANDO NUESTRO LABORATORIO DE HACKING 25
1.7 RECURSOS ÚTILES 27

CAPÍTULO 2. RECONOCIMIENTO O FOOTPRINTING **29**
2.1 RECONOCIMIENTO PASIVO 30
2.2 RECONOCIMIENTO ACTIVO 31
2.3 HERRAMIENTAS DE RECONOCIMIENTO 31
2.4 FOOTPRINTING CON GOOGLE 32
2.5 LAB: CLONANDO WEBSITES 34
2.6 LAB: DNS FOOTPRINTING CON NSLOOKUP 38

2.7 OBTENIENDO INFORMACIÓN DE DIRECTORIOS WHO-IS 42
2.8 REPOSITORIOS DE IPV4INFO Y HURRICANE ELECTRIC 45
2.9 LAB: FOOTPRINTING CON MALTEGO 47
2.10 HERRAMIENTAS DE TRACEROUTE VISUAL 55
2.11 HERRAMIENTAS DE RASTREO DE CORREOS 57
2.12 MEDIDAS DEFENSIVAS 59
2.13 RECURSOS ÚTILES 60

CAPÍTULO 3. ESCANEO 63
3.1 PING SWEEPERS 64
3.2 HERRAMIENTAS DE TCP-PING 66
3.3 ESTADOS DE PUERTOS 67
3.4 TÉCNICAS DE ESCANEO 68
3.5 ESCÁNER DE PUERTOS: NMAP 70
3.5.1 Lab: Escaneo de puertos con NMAP 73
3.6 ANALIZADORES DE VULNERABILIDADES 74
3.6.1 Lab: Análisis de vulnerabilidades con OpenVAS 76
3.6.2 Lab: Análisis de vulnerabilidades con Nessus 82
3.7 MEDIDAS DEFENSIVAS 92
3.8 RECURSOS ÚTILES 93

CAPÍTULO 4. ENUMERACIÓN 95
4.1 PROTOCOLOS NETBIOS Y CIFS/SMB 96
4.2 ENUMERACIÓN DE WINDOWS CON COMANDOS Y HERRAMIENTAS DE SOFTWARE 100
4.2.1 Lab: Enumeración de Windows desde el CLI 110
4.2.2 Otras herramientas para enumerar Windows 111
4.3 LAB: ENUMERANDO DIVERSOS PROTOCOLOS CON NETCAT 114
4.4 MEDIDAS DEFENSIVAS 117
4.5 RECURSOS ÚTILES 117

CAPÍTULO 5. EXPLOTACIÓN O HACKING 119
5.1 MECANISMOS DE HACKING 119
5.2 FRAMEWORKS DE EXPLOTACIÓN 120
5.2.1 Metasploit Framework 121
5.3 ATAQUES DE CLAVES 178
5.3.1 Ataques de fuerza bruta 179
5.3.2 Ataques basados en diccionario 181
5.3.3 Lab: Obteniendo claves con Medusa 183
5.3.4 Lab: Crackeando claves con John The Ripper 186

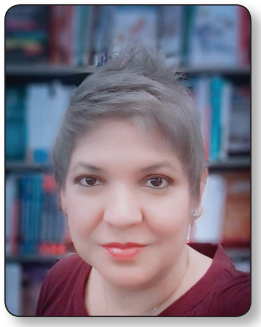
5.3.5 Lab: Crackeando claves con Ophcrack 191
5.3.6 Creando nuestros propios diccionarios 196
5.3.7 Captura de claves usando sniffers de red 200
5.4 ATAQUES DE INGENIERÍA SOCIAL 212
5.4.1 Ataques con software malicioso 213
5.5 ATAQUES DE DENEGACIÓN DE SERVICIO (DOS) 225
5.6 BURLANDO LA AUTENTICACIÓN DE WINDOWS CON KALI LINUX 228
5.7 HACKING WIFI 233
5.7.1 Wifi hacking con Aircrack 233
5.7.2 Lab: Ataque basado en diccionario al protocolo WPA/WPA2 234
5.7.3 Lab: Ataque al protocolo WEP 238
5.8 HACKING WEB 242
5.8.1 El OWASP Top 10 245
5.8.2 Analizadores de vulnerabilidades web 248
5.8.3 OWASP Mutillidae 249
5.8.4 Lab: Escaneando Metasploitable2 con ZAP 251
5.9 MEDIDAS DEFENSIVAS 256
5.10 RECURSOS ÚTILES 258

CAPÍTULO 6. POST EXPLOTACIÓN 259
6.1 ESCALAMIENTO DE PRIVILEGIOS 261
6.1.1 Lab: Escalando privilegios con GetSystem en Meterpreter 261
6.2 BÚSQUEDA DE INFORMACIÓN RELEVANTE 265
6.3 ROOTKITS Y BACKDOORS 267
6.3.1 Lab: Levantando backdoors 268
6.4 PIVOTEO Y RECONOCIMIENTO INTERNO 271
6.4.1 Lab: Pivoteando con Meterpreter 271
6.5 LIMPIEZA DE RASTROS 277
6.5.1 Lab: Borrando logs en Windows 277
6.5.2 Lab: Borrando logs en Unix/Linux 279
6.6 MEDIDAS DEFENSIVAS 280
6.7 RECURSOS ÚTILES 282

CAPÍTULO 7. ESCRIBIENDO EL INFORME DE AUDITORÍA SIN SUFRIR UN COLAPSO MENTAL 283
7.1 PASOS PARA FACILITAR LA DOCUMENTACIÓN DE UNA AUDITORÍA 284
7.2 RECURSOS ÚTILES 293

CAPÍTULO 8. CERTIFICACIONES INTERNACIONALES RELEVANTES.....295
8.1 CERTIFIED ETHICAL HACKER (CEH) 296
8.2 OPEN PROFESSIONAL SECURITY TESTER (OPST) 299
8.3 OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP).....299
8.4 CERTIFIED PENETRATION TESTER (CPT).....300
8.5 PENETRATION TESTER (GPEN).....301
8.6 ¿QUÉ EXAMEN DEBO TOMAR? 301
8.7 RECURSOS ÚTILES 302
RECOMENDACIONES FINALES 303
GLOSARIO DE TÉRMINOS TÉCNICOS.....305

ACERCA DE LA AUTORA



Karina Astudillo B. es una consultora de sistemas especializada en seguridad informática, redes y sistemas *UNIX/Linux*. Es Ingeniera en Computación, MBA, y cuenta con certificaciones internacionales como: *Certified Ethical* Hacker *(CEH), Computer Forensics US, CCNA R&SW, CCNA Security, CCNA Wireless, Hillstone Certified Security Professional (HCSP), Cisco Certified Academy Instructor (CCAI), Sun Certified Solaris System Administrator* (SCSA) y *VmWare VSP*.

Karina inició su carrera en el mundo de las redes en el año 1995, gracias a una oportunidad de trabajo en un proyecto con *IBM* en su alma máter, la *Escuela Superior Politécnica del Litoral (ESPOL)*. Desde entonces el mundo de las redes, los sistemas operativos y la seguridad, la fascinaron al punto de convertirse en su pasión.

Años más tarde, luego de adquirir experiencia trabajando en el área de servicio al cliente de la corporación transnacional *ComWare*, se convirtió - primero en consultora de sistemas independiente en el año 2002 a través de *Consulting Systems* - para cofundar en el 2007 *Elixircorp S.A.*, empresa de seguridad informática de la que formaría parte hasta junio de 2018.

Paralelamente a la consultoría, Karina siempre ha tenido una pasión innata por enseñar, gracias a lo cual surgió la oportunidad de vincularse con la docencia como profesora de la *Facultad de Ingeniería en Electricidad y Computación (FIEC)* allá por el año 1996.

En la actualidad es instructora del programa *Cisco Networking Academy* y de los programas de *Maestría en Sistemas de Información (MSIG) y Maestría en Seguridad Informática Aplicada (MSIA)* de *FIEC-ESPOL*.

Debido a esta experiencia docente consideró incluir como parte de la oferta de su empresa, programas de preparación en seguridad informática, entre ellos talleres de Hacking Ético. Al publicar el éxito de estos talleres en su blog personal, empezó a recibir solicitudes de estudiantes que se encontraban en ciudades y países diferentes que preguntaban por los cursos, sólo para desilusionarse cuando se les contestaba que sólo se dictaban de forma presencial en Ecuador.

Fue entonces cuando nació la idea de crear la serie "Cómo Hackear" para poder transmitir – sin límites geográficos - los conocimientos sobre el taller de Introducción al Hacking Ético, el primero en la Serie.

En sus momentos de esparcimiento Karina disfruta leer sobre ciencia ficción, viajar, compartir con su familia y amigos y escribir sobre ella en tercera persona ;-D

COMUNÍQUESE CON KARINA ASTUDILLO B.

Siéntase libre de consultar a la autora o realizar comentarios sobre el libro en:

- ✓ **Email:** *karina@karinaastudillo.com*
- ✓ **Website personal (libros, cursos y blog):** *https://www.KarinaAstudillo.com/*
- ✓ **Website empresarial:** *https://www.Consulting-Systems.tech/*
- ✓ **Facebook:** *https://facebook.com/KarinaAstudilloBooks/*
- ✓ **YouTube Channel (Academia Hacker):** *https://www.youtube.com/c/karinaastudillo/*

PREFACIO

La seguridad informática ha ganado popularidad en los últimos años y ha pasado de ser considerada un gasto, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial.

En algunos países esto ha sucedido de forma acelerada, en otros el paso ha sido más lento; pero en última instancia hemos convergido todos en un mundo digital en el que la información es el activo intangible más valioso con el que contamos.

Y al ser un activo, debemos protegerlo de posibles pérdidas, robos, mal uso, etc. Es aquí en donde juega un papel preponderante un actor antes desconocido: el ***hacker ético***.

El rol del hacker ético es efectuar - desde el punto de vista de un cracker - un ataque controlado hacia la infraestructura informática de un cliente, detectando vulnerabilidades potenciales y explotando aquellas que le permitan penetrar las defensas de la red objetivo, pero sin poner en riesgo los servicios y sistemas auditados. Y todo esto con el solo propósito de alertar a la organización contratante de los riesgos de seguridad informática presentes y cómo remediarlos.

Este individuo debe tener la capacidad de saber cuándo es mejor no explotar un hueco de seguridad y solamente reportarlo al cliente versus cuándo es preciso ejecutar un exploit para demostrar la gravedad de la vulnerabilidad. Es una mezcla entre la mente criminal de Hannibal, las acciones de la Madre Teresa y el background profesional de un verdadero nerd.

¿Pero dónde encontramos a estos héroes? La respuesta a esta pregunta se torna cada vez más difícil si creemos en los estudios realizados por importantes

empresas consultoras, que indican que año a año se ensancha la brecha entre la oferta y la demanda de profesionales certificados en seguridad informática.

Y es por este motivo que se vuelve esencial contar con profesionales de tecnología entusiastas, pero sobre todo con altos valores éticos y morales, que estén dispuestos a aceptar el desafío de convertirse en **hackers éticos** o también denominados **pentesters**.

Este libro es para ellos.

AUDIENCIA OBJETIVO

Si es usted un estudiante, profesional o entusiasta de la informática, curioso, perseverante y con un ferviente deseo de aprender cómo penetrar en los sistemas informáticos, entonces este libro es para usted.

No se requieren conocimientos previos de hacking ético, el nivel del libro es introductorio y por ende parte de cero en dicha área. No obstante, es imprescindible tener una formación base en sistemas computacionales o tecnologías de la información.

¿Cuáles son los requisitos?

- ✓ Conocer el modelo OSI y sus diferentes capas.
- ✓ Poseer nociones sobre la arquitectura TCP/IP (direccionamiento IP, subnetting, enrutamiento, funcionamiento de protocolos como ARP, DNS, HTTP, SMTP, DHCP, etc.).
- ✓ Saber usar y administrar sistemas Windows y Linux.

¿POR QUÉ CONVERTIRME EN PENTESTER?

El deseo de convertirse en hacker ético o pentester proviene de una aspiración personal, así que no tengo forma de influir en ello, pero sí puedo darle algunas razones prácticas de por qué se necesitan hackers éticos a nivel mundial y por qué sería buena idea convertirse en uno:

1. **La brecha entre la oferta y la demanda de profesionales en ciberseguridad continúa creciendo:** de acuerdo a un estudio efectuado por Cybersecurity Ventures[1] faltarán alrededor de 3.5 millones de profesionales en ciberseguridad para cubrir la demanda tan sólo en Estados Unidos para el 2021. Por lo tanto, existe amplia cabida en el mercado para la profesión de hacker ético.

2. **Ser pentester es lucrativo:** los especialistas en hacking ético están entre los profesionales de tecnología mejores pagados de acuerdo con PayScale[2], recibiendo hasta alrededor de $130K anuales quienes trabajan en relación de dependencia. El estudio no aclara si incluye contratistas independientes, pero mi propia experiencia me dice que la consultoría independiente puede generar mayores ingresos anuales.

3. **La profesión de hacker ético es interesante y divertida:** si siente usted pasión por su profesión, cualquiera que esta sea, no la verá como trabajo porque se sentirá motivado y feliz al realizar sus tareas. Pero, ser pentester es especialmente divertido porque cada proyecto es diferente y entraña enfrentar distintos desafíos para lograr la meta de vencer las defensas y penetrar los sistemas del cliente.

4. **Ser hacker ético es legal:** a diferencia de los crackers (hackers maliciosos) que penetran los sistemas de terceros sin permiso con el ánimo de lucrar a partir de robar secretos o pedir rescates por la información ajena, con el riesgo de pasar muchos años en la cárcel si son descubiertos, al pentester le pagan por incursionar en los sistemas de las empresas con la debida autorización. Traducción: buena paga por divertirse explotando vulnerabilidades y reportar cómo remediarlas.

5. **Ser hacker es cool**: tal vez suene a broma, pero le aseguro al lector que después de las frases "soy millonario" o "soy una celebridad", la frase "soy hacker" es una de las que genera más curiosidad, admiración y respeto por parte del público. Y claro, si la temática se mantiene fuera de los detalles técnicos aburridos, puede ser una excelente apertura para mantener una conversación interesante con nuevos conocidos en una reunión.

---

1 C. (2018, June 13). Cybersecurity Jobs Report 2018-2021. Retrieved from https://cybersecurityventures.com/jobs/

2 PayScale. (n.d.). Penetration Tester Salary. Retrieved 2018, from https://www.payscale.com/research/US/Job=Penetration_Tester/Salary

¿CÓMO ESTÁ DIVIDIDO EL LIBRO?

El libro se desarrolla en 8 capítulos y hemos calculado que el estudiante deberá invertir alrededor de 21 días para completar el contenido a cabalidad y practicar los laboratorios, con un tiempo de dedicación mínimo de 2 horas diarias. Sin embargo, el lector es libre de avanzar a su propio paso y tomarse mayor o menor tiempo.

Mi única sugerencia es que deben realizarse todos los laboratorios propuestos, inclusive con diferentes sistemas operativos víctimas a los referidos por esta servidora. Es en la variación de escenarios y en la práctica continua que se gana experiencia.

El ***Capítulo 1 – Introducción al Hacking Ético*** cubre conceptos básicos acerca de esta profesión y describe los diferentes tipos de pruebas de intrusión posibles. En él se incluyen asimismo consejos acerca de cómo conducir la fase inicial de levantamiento de información para elaborar una propuesta ajustada a las necesidades de nuestro cliente.

En el ***Capítulo 2 – Reconocimiento o Footprinting*** se revisan metodologías que ayudarán al hacker ético a descubrir el entorno de la red objetivo y los elementos en ella contenidos, así como herramientas de software útiles y comandos para ayudarlo durante la ejecución de la auditoría. Se hace énfasis en el uso de *Maltego* y técnicas de *Google Hacking* para conducir con éxito esta fase.

Durante los ***Capítulos 3 y 4, Escaneo*** **y** ***Enumeración****,* respectivamente, se describen técnicas utilizadas por los crackers y hackers éticos para detectar los servicios presentes en los equipos auditados y discernir qué sistemas operativos y versiones de aplicaciones usan nuestras víctimas. La ejecución exitosa de estas fases facilitará al pentester la enumeración de recursos como cuentas de usuarios, grupos, carpetas, claves del registro y demás, a propósito de detectar huecos de seguridad potenciales que puedan explotarse con posterioridad. Aquí se estudian herramientas de software populares como el scanner de puertos *NMAP* y los analizadores de vulnerabilidades *OpenVAS* y *Nessus,* bajo el conocido ambiente *Kali Linux* (antes *Backtrack*).

En el ***Capítulo 5 – Explotación o Hacking***, se cubren conceptos claves como los frameworks de explotación y mecanismos de ataques y se realizan laboratorios paso a paso haciendo uso del *Metasploit Framework* y las interfaces *msfconsole* y *Armitage*. Se incluyen además talleres detallados para la realización de ataques de claves, hombre en el medio, phishing, inyección de malware, ataques a redes inalámbricas, etc. En los laboratorios se utilizan aplicaciones populares como *Ettercap*, *Wireshark* y la suite *Aircrack-ng*.

A continuación, en el ***Capítulo 6 - Post Explotación*** cubrimos comandos y técnicas que nos ayudarán a sacar un mayor provecho de los equipos que hayamos conseguido explotar previamente. En él se cubren temas como escalamiento de privilegios, cómo buscar información relevante en un host víctima, cómo mantener el acceso en un sistema implantando puertas traseras (backdoors), cómo ir más allá del equipo víctima usándolo como pivote para descubrir nuevas redes y cómo cubrir rastros si el tipo de auditoría que efectuemos lo requiere.

Luego en el ***Capítulo 7 - Escribiendo el informe de auditoría sin sufrir un colapso mental***, se sugiere una sistemática para hacer que esta fase sea lo más indolora posible para el consultor, mientras se crea un entregable de calidad, claro y conciso para la alta gerencia y que aporta sugerencias de remediación útiles para la organización cliente.

Posteriormente en el ***Capítulo 8 – Certificaciones internacionales relevantes***, realizamos una revisión de las certificaciones generales de seguridad informática y aquellas específicas de hacking ético que son imprescindibles en el currículum de un pentester experto.

Creímos también que, a pesar de tratarse de un libro de hacking, el mismo no podía estar completo sin incluir en cada fase de ataque los mecanismos de defensa pertinentes que podrían sugerirse al cliente dentro del informe de auditoría como medidas de remediación.

¡Gracias por adquirir esta obra! Desde ya le deseo muchos éxitos en su nueva carrera como **Hacker Ético Profesional**.

REGALO PARA EL LECTOR

En agradecimiento por haber adquirido esta obra, quiero obsequiarle mi **Guía Gratuita de Wireless Hacking**.

Puede descargarla sin costo desde: *http://bit.ly/WiFiHackingGuiaSP*

CAMBIOS EN LA 3ª EDICIÓN

En esta edición hemos actualizado los laboratorios previos a la última versión de *Kali Linux*[3] y hemos agregado nuevas secciones y laboratorios en casi todos los capítulos.

3 A la fecha de escritura de este libro: septiembre 2018.

Se reorganizaron además diversas secciones y laboratorios para que guarden un orden progresivo y consistente, eliminando algunos de los laboratorios que usaban el descontinuado *Windows XP* como víctima y reemplazándolo por víctimas como *Metasploitable* o nuevas versiones de *Windows*. En total los laboratorios paso a paso suman 24 en esta edición.

Hemos agregado además un capítulo nuevo para cubrir una fase muy importante pero poco abordada en los textos introductorios de hacking: la fase de Post Explotación, la cual entra en el área gris de Mantener el Acceso y Borrar Huellas del famoso Círculo del Hacking. Aquí hemos tratado de cubrir conceptos avanzados de la forma más sencilla posible para dar luces a los auditores neófitos sobre tópicos complejos como la elevación de privilegios, rootkits y backdors, pivoteo, limpieza de rastros, etc.

Finalmente, ¡queremos aprovechar la oportunidad para comentarle que dentro de poco verá la luz el tercer tomo de la serie "Cómo Hackear" a través de la publicación del libro "Web Hacking 101 – ¡Cómo hackear aplicaciones web!", así que lo invitamos a mantenerse informado de la fecha de publicación de esta y otras obras agregando a la autora en la red social de su predilección.

La información de contacto se halla en la sección "Acerca de la autora".

¡Sin más preámbulos a hackear se ha dicho!

1

INTRODUCCIÓN AL HACKING ÉTICO

Cuando hablamos de hacking ético nos referimos a la acción de efectuar **pruebas de intrusión controladas** sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole - en algunos casos - acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente.

Es importante enfatizar que, aunque es indudable que el pentester debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una auditoría de este tipo. Se requiere además seguir una metodología que le permita al auditor llevar un orden en su trabajo para optimizar el tiempo en la fase de explotación, además de aplicar el sentido común y la experiencia.

Y aunque lamentablemente la experiencia y el sentido común no se pueden transferir en un libro, haré mi mejor esfuerzo por trasmitirle al lector la metodología y las buenas prácticas que he adquirido a lo largo de los años de ejercer la profesión de consultora de seguridad informática.

1.1 EL CÍRCULO DEL HACKING

Tanto el auditor como el cracker siguen un orden lógico de pasos al momento de ejecutar un hacking, a estos pasos agrupados se los denomina fases.

Existe un consenso generalizado entre las entidades y profesionales de seguridad informática de que dichas fases son 5 en el siguiente orden:

1-> Reconocimiento 2-> Escaneo 3-> Obtener acceso 4-> Mantener acceso 5-> Borrar huellas

Usualmente dichas fases se representan como un ciclo al que se denomina comúnmente **Círculo del Hacking** (ver Figura 1) con el ánimo de enfatizar que el cracker luego de borrar sus huellas puede pasar nuevamente a realizar un reconocimiento y de esta manera continuar con el proceso una y otra vez. No obstante, el auditor de seguridad informática que ejecuta un servicio de hacking ético presenta una leve variación en la ejecución de las fases de esta forma:

1-> Reconocimiento 2-> Escaneo 3-> Obtener acceso 4-> Escribir Informe 5-> Presentar Informe

De esta manera el hacker ético se detiene en la fase 3 del círculo del hacking para reportar sus hallazgos y realizar recomendaciones de remediación al cliente.

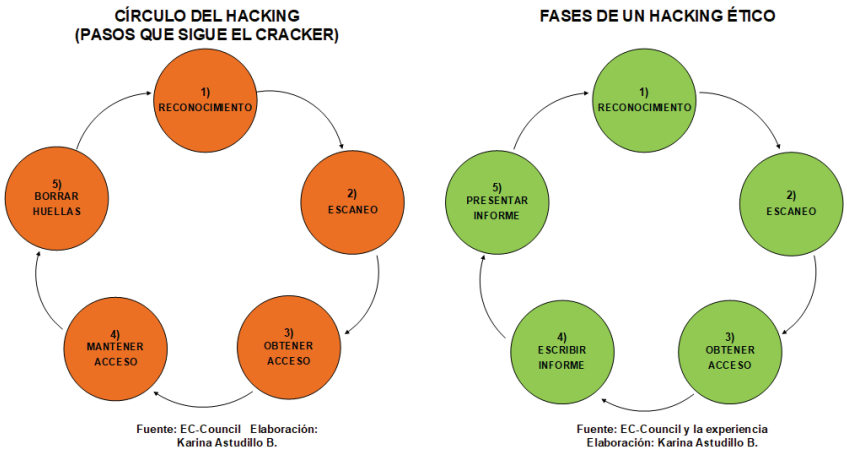


Figura 1. Círculo del Hacking

En los capítulos subsiguientes explicaremos en qué consiste cada fase y aplicaremos el uso de herramientas de software y nuestro sentido común, unido a la experiencia, para ejecutar un hacking ético de principio a fin de forma profesional.

1.2 TIPOS DE HACKING

Cuando efectuamos un hacking ético es necesario establecer el alcance del mismo para poder realizar un cronograma de trabajo ajustado a la realidad y elaborar

la propuesta económica para el cliente. Y para determinar el alcance requerimos conocer como mínimo tres elementos básicos: el **tipo de hacking** que vamos a efectuar, **la modalidad** del mismo y **los servicios adicionales** que el cliente desea incluir junto con el servicio contratado.

Dependiendo desde dónde se ejecutan las pruebas de intrusión, un hacking ético puede ser externo o interno.

Hacking ético externo

Este tipo de hacking se realiza desde Internet sobre la infraestructura de red pública del cliente; es decir, sobre aquellos equipos de la organización que están expuestos a Internet porque brindan un servicio público. Ejemplo de equipos públicos: enrutador, firewall, servidor web, servidor de correo, servidor de nombres, etc.

Hacking ético interno

Como su nombre sugiere, este tipo de hacking se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empresa, un consultor, o un asociado de negocios que tiene acceso a la red corporativa.

En este tipo de pruebas de intrusión se suele encontrar más huecos de seguridad que en su contraparte externa, debido a que muchos administradores de sistemas se preocupan por proteger el perímetro de su red y subestiman al atacante interno. Esto último es un error, puesto que estudios demuestran que la mayoría de ataques exitosos provienen del interior de la empresa.

1.3 MODALIDADES DEL HACKING

Dependiendo de la información que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de tres modalidades: black-box hacking, gray-box-hacking o white-box-hacking. La modalidad escogida afectará el costo y la duración de las pruebas de intrusión, puesto que, a menor información recibida, mayor el tiempo invertido en investigar por parte del auditor.

Black box hacking

También llamado **hacking de caja negra**. Esta modalidad se aplica a pruebas de intrusión externas. Se llama de este modo porque el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que éste obra a ciegas, la infraestructura de la organización es una **caja negra** para él.

Si bien este tipo de auditoría se considera más realista, dado que usualmente un agresor externo que elige una víctima X no tiene más información al inicio que el nombre de la organización a atacar, también es cierto que requiere una mayor inversión de tiempo y por ende el costo incurrido es superior también. Adicionalmente, se debe notar que el hacker ético - a diferencia del cracker - no cuenta con todo el tiempo del mundo para efectuar las pruebas de intrusión, por lo que la fase preliminar de indagación no puede extenderse más allá de lo que en términos prácticos sea posible para el cliente en razón del costo/tiempo/beneficio.

Gray box hacking

O **hacking de caja gris**. Esta modalidad suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. Empero, algunos auditores también le llaman **gray-box-hacking** a una prueba externa en la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como la dirección IP y el tipo/función del equipo (router, web-server, firewall, etc.).

Cuando el término se aplica a pruebas internas, se denomina así porque el consultor recibe por parte del cliente solamente los accesos que tendría un empleado de la empresa sin mayores privilegios, es decir un punto de red para la estación de auditoría y datos de configuración de la red local (dirección IP, máscara de subred, gateway y servidor DNS); pero no le revela información adicional como, por ejemplo: usuario/clave para unirse a un dominio, la existencia de subredes anexas, etc.

White box hacking

Este es el denominado **hacking de caja blanca**, aunque en ocasiones también se le llama **hacking transparente**. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma porque la empresa cliente le da al consultor información completa de las redes y los sistemas a auditar.

Es decir, que además de brindarle un punto de red e información de configuración para la estación de auditoría, como en el hacking de caja gris, el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información de subredes remotas, etc. Debido a que el consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking podría tomar menos tiempo para ejecutarse y por ende reduciría costos también; sin embargo, esto es relativo, porque en un hacking de caja blanca es usual que se le pida al consultor probar varios escenarios (ej.: sin credenciales, con credenciales de un perfil de usuario X o Y, etc.).

1.4 SERVICIOS DE HACKING ADICIONALES

Dependiendo de la experiencia del consultor o de la empresa auditora, es posible que se le ofrezca al cliente servicios opcionales que pueden incluirse con el servicio de hacking ético externo o interno.

Entre los servicios adicionales más populares tenemos: ingeniería social, wardialing, wardriving, equipo robado y seguridad física.

Ingeniería social

La ingeniería social se refiere a la obtención de información a través de la manipulación de las personas, es decir que aquí el hacker adquiere datos confidenciales valiéndose del hecho bien conocido de que el eslabón más débil en la cadena de seguridad de la información son las personas.

De mi experiencia les puedo contar que hubo ocasiones en que me encontraba frustrada en la conducción de un hacking ético externo, porque el administrador de sistemas en efecto había tomado las precauciones del caso para proteger el perímetro de su red, y dado mi nivel de estrés y obsesión decidí aplicar técnicas de ingeniería social, consiguiendo el objetivo fácilmente, en muchos casos. Ejemplos de ingeniería social: envío de correos electrónicos falsos con adjuntos maliciosos, llamadas al personal del cliente fingiendo ser un técnico del proveedor de Internet, visitas a las instalaciones de la empresa pretendiendo ser un cliente para colocar un capturador de teclado (keylogger), etc.

Wardialing

Durante los primeros años de Internet el acceso a la misma se daba mayoritariamente a través de módems y era común que las empresas tuvieran un grupo de estos dispositivos (pool de módems) conectados a una central telefónica (PBX) para responder las llamadas de quienes requerían acceso a la red local de la empresa. Dichos módems se conectaban a un servidor de acceso remoto (RAS), el cual a través de un menú de ingreso (nombre de usuario y clave) y haciendo uso de protocolos como el histórico SLIP o el PPP, permitían que los usuarios autorizados se conectaran como si estuviesen en la red local y tuvieran acceso a los recursos compartidos de la empresa.

En aquella época la seguridad no era algo en lo que los administradores meditaban mucho, por lo que muchos de esos módems no estaban adecuadamente protegidos, lo que los hizo presa fácil de los primeros programas de wardialing. Lo que hacían estos programas era marcar números de teléfono consecutivos, en

base al valor inicial proporcionado por el usuario, y registrar aquellos en los cuales respondía un módem en lugar de una persona; luego el cracker llamaba manualmente a los números identificados y ejecutaba comandos AT[4] para ganar acceso al módem o corría programas de fuerza bruta para vencer las claves puestas por el administrador de sistemas. Posteriormente estos programas se fueron sofisticando, pudiendo realizar desde una misma aplicación y de forma automática el descubrimiento de módems y el ataque de fuerza bruta.

En la actualidad nuestro modo de conectarnos a Internet ha cambiado, sin embargo, es un hecho a notar que muchos administradores utilicen aún conexiones vía módem como respaldo para conectarse remotamente a dar soporte, en el caso de que la red falle. Por lo consiguiente, no deberíamos descartarlo como un punto vulnerable de ingreso a la red del cliente.

Wardriving

El término wardriving se deriva de su antecesor el wardialing, pero aplicado a redes inalámbricas. El hacker entabla una guerra inalámbrica desde las inmediaciones de la empresa cliente/víctima, usualmente parqueado desde su auto con una laptop y una antena amplificadora de señal.

El objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente e identificar vulnerabilidades que permitan el ingreso al hacker. Sobre este tema haremos un par de laboratorios muy interesantes en el Capítulo 5.

Equipo robado

Aquí el objetivo es comprobar si la organización ha tomado las medidas necesarias para precautelar la información confidencial contenida en los equipos portátiles de los ejecutivos clave en caso de hurto o robo. Se simula el robo del equipo, para lo cual los ejecutivos elegidos entregan su equipo por espacio de un día como máximo al consultor y éste utiliza herramientas de hardware/software, sumadas a su técnica, para intentar extraer información sensible.

Debido a lo delicado de la operación se debe recomendar siempre al cliente realizar un respaldo de su información previo a la ejecución de este servicio.

---

4 AT (abreviatura de la palabra de origen inglés attention, que significa atención): los comandos AT son instrucciones codificadas utilizadas para comunicarse con un módem.

Auditoría de seguridad física

Aunque la seguridad física es considerada por muchos expertos como un tema independiente de las auditorías de hacking ético, existen empresas especializadas que pueden integrarla como parte del servicio.

Este tipo de auditoría entraña dificultades y riesgos de los que se debe estar consciente para evitar situaciones que pongan en peligro a las personas implicadas. Les indico esto porque una auditoría de seguridad física puede conllevar desde algo tan simple como realizar una inspección acompañados de personal del cliente llenando formularios de un estándar como por ejemplo el SAS-70, algo más complejo como probar si podemos llegar a la sala de juntas y colocar un dispositivo espía haciéndonos pasar por un cliente perdido, hasta algo tan delicado como intentar burlar guardias armados e ingresar por una puerta trasera. En mi caso no pretendo ser *Lara Croft* - bueno tal vez en mis sueños, pero eso no es de su incumbencia - así que ni loca ofrezco este último servicio.

1.5 ELABORACIÓN DE LA PROPUESTA E INICIO DE LA AUDITORÍA

Finalmente, una vez que hemos obtenido del cliente la información requerida – tipo de hacking, modalidad y servicios opcionales – estamos listos para elaborar una propuesta que defina claramente: el alcance del servicio, el tiempo que nos tomará ejecutar el hacking ético, el entregable (un informe de hallazgos y recomendaciones), costos y forma de pago.

Discutir técnicas de elaboración de propuestas, dimensionamiento de proyectos y valoración de costos está fuera del alcance de este texto, pero les dejo algunos enlaces relacionados en la sección "Recursos Útiles" al final de este capítulo.

Quizás una sola recomendación en este punto: asesórese de un buen abogado para que lo ayude a elaborar una plantilla de contrato. En el Capítulo 7 incluyo más información acerca de por qué esto es una buena idea.

1.6 CREANDO NUESTRO LABORATORIO DE HACKING

En los distintos capítulos del libro se realizarán prácticas usando como plataforma de hacking tanto *Windows* como *Kali Linux*. Y las víctimas pueden ser dispositivos de red como routers inalámbricos, o bien equipos con sistemas operativos *Windows, Android, iOS, Mac OS, Unix, Linux, etc*.

Pero sin importar el sistema operativo host que tengamos en el PC, mi recomendación es que instalemos software de virtualización como *VMWare* o *Virtual Box*, y sobre éste configuremos máquinas virtuales para usarlas como plataformas de hacking. Lo mismo aplica si queremos practicar con máquinas víctimas.

¿Por qué recomiendo virtualizar? Primero porque resulta económico, virtualizando podemos tener en un solo equipo físico tanto las estaciones hacker como las máquinas víctimas. Y segundo, porque es más seguro. De este modo no se toca al sistema operativo principal y si ocurriera algún fallo en una máquina virtual, siempre se puede restaurar una copia de la misma o simplemente reinstalarla.

Hay que poner especial cuidado en este tema sobre todo si en algún momento queremos experimentar con una herramienta *underground* de cuyo origen no tengamos mayor confianza, recordemos que una herramienta "gratis" hecha por crackers puede traer software troyano, "gratuito" en efecto. Si jugamos con nuestra máquina virtual y por error introducimos virus o malware, al tenerla aislada de nuestro sistema principal nos aseguramos de que no afecte nuestra información.

Si el lector decide hospedar en una sola máquina física todas las máquinas virtuales requeridas para realizar los talleres, entonces se recomienda que dicho equipo tenga como mínimo 8GB de RAM. De igual forma, es importante que el procesador sea rápido (dual-core mínimo, quad-core recomendado).

¿En dónde conseguimos los instaladores de los OS's requeridos?

Comencemos por los sistemas *Linux* dado que por ser distribuciones de código abierto (open source) no implican ningún costo de licenciamiento.

Estos son los enlaces de descarga:

- *Kali Linux*: *http://www.kali.org/downloads/*
- *Metasploitable*: *http://sourceforge.net/projects/metasploitable/files/Metasploitable2/*

Revisemos ahora los sistemas *Windows*. Sería genial contar con los recursos monetarios para comprar todas las versiones requeridas para los laboratorios y si el lector los tiene enhorabuena, ¡por favor contráteme! :-D Pero si no, existe esta alternativa sin costo, legítima:

- Sitio de descarga de máquinas virtuales de sistemas *Microsoft (Windows 7, 8 y 10):*[5] *https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/#downloads*

Este sitio es mantenido principalmente para proveer a los desarrolladores web formas de probar sus aplicaciones en diferentes navegadores y sistemas operativos de *Microsoft*, pero no hay ningún impedimento legal para que lo usemos para realizar pruebas de intrusión. Dado que son máquinas virtuales para pruebas, la licencia otorgada es de carácter temporal. Sin embargo, de requerirse un mayor tiempo de prueba, podemos volver a realizar el proceso de importación. El proceso de importación ya sea en *VmWare* o *VirtualBox* es sencillo de realizar, pero los detalles se pueden revisar en el documento de release notes incluido en el sitio web.

Otra forma de acceder a licencias legales de *Windows*, tanto de versiones de escritorio como de servidor, es inscribirse en el programa *Microsoft Imagine* (*https://imagine.microsoft.com/es-es*), disponible para estudiantes y profesores de las instituciones académicas suscritas a dicho programa.

1.7 RECURSOS ÚTILES

- ✓ Libro: Northcut, K.M., Crow, M.L. y Mormile, M. (Julio, 2009). Proposal writing from three perspectives: Technical Communication, Engineering, and science. Professional Communication Conference, 2009. IPCC 2009. IEEE International.
- ✓ Libro: Baugh, R. H. (2011). Handbook for writing proposals, second edition. McGraw-Hill.
- ✓ Libro: Sant, T. (2012). Persuasive business proposals: Writing to win more customers, clients, and contracts. New York: AMACOM.
- ✓ Libro: A guide to the project management body of knowledge: (PMBOK® guide). (2017). Newtown Square, PA, USA: Project Management Institute.

5 Antes era posible obtener Windows XP desde este lugar, pero debido a que Microsoft retiró el soporte para dicha versión, la descarga ya no está disponible. Para usar esta versión como máquina víctima, al momento hay dos opciones: 1) Comprar el medio de reinstalación de Windows XP en sitios que aún lo venden como por ejemplo Amazon - esto requiere contar con una licencia previa y 2) Conseguir un instalador y licencia viejos de algún amigo o de una Academia Microsoft. No le recomiendo al lector descargar XP ni ningún otro software desde sitios de descarga no oficiales, porque - aparte de ser ilegal - hay una alta posibilidad (por no decir probabilidad = 1) de que esos medios estén infectados con malware, lo cual pondría en riesgo su información. Le recuerdo que los antivirus tradicionales no detectan las amenazas avanzadas (malware de día cero).

2

RECONOCIMIENTO O FOOTPRINTING

El reconocimiento, como vimos en el capítulo previo, es la primera fase en la ejecución de una prueba de intrusión y consiste en descubrir la mayor cantidad de información relevante de la organización cliente o víctima.

En un hacking de caja negra el consultor no sabe nada sobre el cliente, salvo el nombre de la organización, por lo que necesita averiguar a qué se dedica la empresa, dónde están ubicadas sus oficinas, nombres de funcionarios, correos electrónicos, cuál es el dominio de Internet que usa la compañía, cuáles son los bloques de direcciones IP públicas asignados por el ISP, cuáles son los hosts activos dentro del rango de IP's públicas, cuáles son los nombres de dichos hosts, etc.

Por otro lado, en un hacking de caja gris externo o interno, el consultor ya cuenta con información provista por el cliente y eso le da una ventaja, pero no por ello debe dejar de investigar. En todos los casos, mientras más sepamos de nuestro objetivo será mejor para la conducción de la auditoría, sobre todo si esta incluye ingeniería social.

Debido a que de la magnitud y certidumbre de la información recopilada dependerá que hagamos un buen análisis posterior, es muy importante que le dediquemos nuestro mejor esfuerzo y cabeza a esta fase y que invirtamos todo el tiempo necesario en realizar un buen levantamiento de información.

"Si tuviera 9 horas para cortar un árbol, le dedicaría 6 horas a afilar mi hacha", Abraham Lincoln.

Les enfatizo esto, porque es importante seguir una buena metodología para la ejecución de pruebas de intrusión y en muy pocos textos se le da la relevancia del caso a la fase de reconocimiento. No obstante, con un reconocimiento escueto realizado al apuro para llegar rápido a las fases consideradas "más interesantes" de un hacking no se logra nada positivo, por el contrario, un reconocimiento incompleto

hará que el consultor pierda tiempo en las fases subsiguientes, teniendo que volver en muchos casos al inicio del círculo del hacking.

Además, el reconocimiento no tiene por qué ser aburrido, a mí en lo personal esta fase me hace sentir como si estuviera en una serie policíaca y tuviese que tomar el rol de detective para encontrar pistas sobre un caso.

Ahora bien, dependiendo de si existe o no interacción con el objetivo, las técnicas de reconocimiento pueden ser activas o pasivas.

2.1 RECONOCIMIENTO PASIVO

Decimos que el reconocimiento es pasivo cuando no tenemos una interacción directa con el cliente o víctima. Por ejemplo, entramos a un buscador como *Google* e indagamos por el nombre de la empresa auditada, entre los resultados conseguimos el nombre de la página web del cliente y descubrimos que el nombre del servidor web es *www.empresax.com*, luego hacemos una búsqueda DNS y obtenemos que la dirección IP de ese servidor es la 200.20.2.2 (dirección ficticia por supuesto).

Algunos ejemplos de reconocimiento pasivo:

- *Buscar en el periódico por anuncios de ofertas de empleo en el departamento de sistemas de la empresa X.* Si resulta que buscan un DBA experto en *Oracle*, eso nos da una pista sobre qué base de datos utilizan, o si quieren un Webmaster que conozca sobre administración de *Apache* ya sabemos qué webserver utilizan.
- *Consultas de directorios en Internet*. Cuando una empresa registra un nombre de dominio, el proveedor de hosting publica información de contacto en un base de datos pública denominada Who-Is, por lo que consultándola se puede obtener información valiosa como el nombre de la empresa dueña del dominio, dirección y teléfonos de la oficina matriz, correo electrónico del administrador, rangos de direcciones IP asignados, en fin. Es posible pagar para mantener esta información privada, pero muchas empresas que adquieren un nombre de dominio no contratan el servicio de privacidad de información.
- *Búsquedas en redes sociales*. Sitios como *Facebook, Linkedin, Twitter,* entre otros, tienen joyas de información gratuita para los hackers que pueden ser usadas fácilmente en un ataque de ingeniería social.
- *Recuperación de información desde la basura*. A este método para nada agradable se lo conoce también como **dumpster diving**, pero, aunque suene repulsivo puede resultar muy útil a la hora de adquirir información

confidencial de una empresa. Aún en esta época de inseguridad son pocas las empresas que usan trituradores e incineradores para destruir información confidencial y aunque suene de *Ripley,* son muchos los empleados que "reciclan" hojas impresas de informes que salieron mal o que botan notas post-it con claves a la basura.

2.2 RECONOCIMIENTO ACTIVO

En este tipo de reconocimiento hay una interacción directa con el objetivo o víctima.

Ejemplos de reconocimiento activo:

- *Barridos de ping* para determinar los equipos públicos activos dentro de un rango de IP's.
- *Conexión a un puerto de un aplicativo* para obtener un *banner* y tratar de determinar la versión.
- *Uso de ingeniería social* para obtener información confidencial.
- *Hacer un mapeo de red* para determinar la existencia de un firewall o router de borde.

2.3 HERRAMIENTAS DE RECONOCIMIENTO

Existen un sinnúmero de aplicativos sofisticados que nos pueden ayudar a la hora de realizar un reconocimiento. Pero, aunque dichas herramientas nos ahorran tiempo, no significa que no podamos hacer un footprinting si no las tenemos a la mano. En lo personal, a mí me gusta empezar un reconocimiento por lo más simple: una línea de comandos y un navegador.

La plataforma de sistema operativo hacker puede ser *Windows, Linux/Unix o MacOS*, según su preferencia, pero si me preguntan, prefiero usar *Kali Linux* para mis auditorías. Empero, existen muchas otras plataformas Linux de pentesting como: Backbox, Parrot, WiFiSlax, Samurai, Knoppix, etc.

Para mayores detalles de los requisitos a nivel de sistema operativo para la realización de los laboratorios, por favor revise la sección "Creando nuestro laboratorio de hacking" del Capítulo 1.

Hecha esta aclaración y sin más preámbulos, ¡pasemos a realizar nuestro primer reconocimiento!

2.4 FOOTPRINTING CON GOOGLE

Aunque existen muchos otros buscadores en Internet, sin duda *Google* es el más utilizado gracias a su tecnología de clasificación de páginas web (*Page Rank*), la cual nos permite realizar búsquedas de forma rápida y acertada.

Para nuestro ejemplo de reconocimiento con *Google*[6] iniciaremos con lo más simple: buscando por el nombre de la empresa víctima, la cual será por ahora el proyecto *Scanme* de *Nmap*[7].

Scanme es un sitio mantenido gratuitamente por *Fyodor*, el creador del escáner de puertos *NMAP*. Sobre este estamos autorizados a realizar pruebas de reconocimiento y escaneo solamente[8], más adelante para los laboratorios de hacking usaremos máquinas virtuales víctimas provistas para tales efectos.

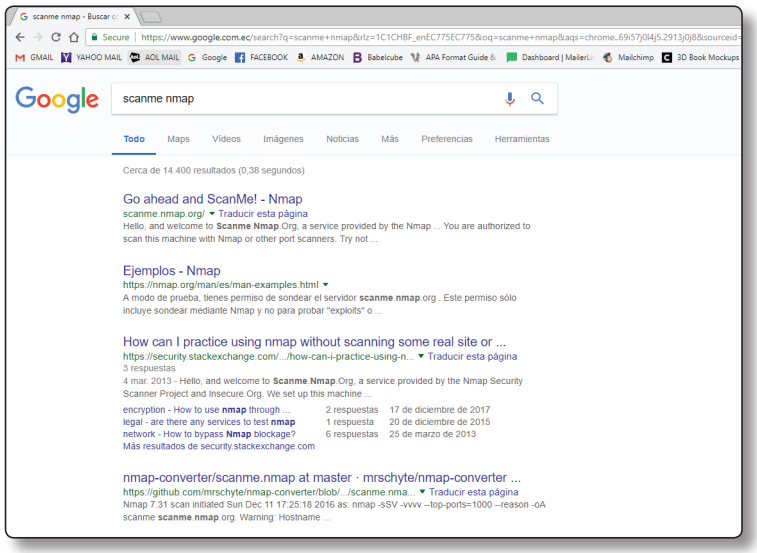


Figura 2. Footprinting con Google

6 Al uso de operadores de Google para hacer reconocimiento o footprinting se le denomina Google Hacking.

7 Nmap Security Scanner Project, http://www.nmap.org.

8 La autorización proviene de Fyodor el creador de NMAP, puesto que el sitio scanme.nmap.org fue creado específicamente con el propósito de servir como objetivo de pruebas de escaneo de puertos.

Nota

Un hacker ético jamás realiza pruebas de intrusión sobre sistemas, a menos que haya obtenido autorización de la organización propietaria de los mismos. Ni la autora, ni la editorial se hacen responsables por el mal uso derivado de las técnicas de hacking provistas en este libro.

Como podemos observar en la Figura 2, la búsqueda ha arrojado cerca de 14 mil resultados, pero el que nos interesa está ubicado primero en la lista. Esto no siempre es tan fácil, hay empresas que tienen nombres muy comunes o tienen sitios que no están bien indexados, por lo que, no aparecerán entre los primeros resultados.

Por ello, para mejorar nuestras búsquedas nos valdremos de los operadores provistos por *Google*. Revisemos algunos de los más importantes.

- Operadores de ***Google :***
  - **+ (símbolo más):** se utiliza para incluir palabras que por ser muy comunes no son incluidas en la búsqueda por *Google*. Por ejemplo, digamos que queremos buscar ***la empresa X***, dado que el artículo "la" es muy común, usualmente se excluye de la búsqueda. Si queremos que sea incluido entonces lo escribimos así ***+la empresa X***
  - **- (símbolo menos):** es usado para excluir resultados que incluyan el término al que se antepone el símbolo. Por ejemplo, si estamos buscando entidades bancarias podríamos escribir: ***bancos seguros -muebles***
  - **"" (dobles comillas):** si queremos buscar un texto de forma literal lo enmarcamos en dobles comillas. Ejemplo: **"la empresa X"**
  - **~ (virgulilla):** al colocar este símbolo antepuesto a una palabra, se incluye en la búsqueda sinónimos de la misma. Por ejemplo, buscar por ***la ~empresa X*** incluirá también resultados para ***la organización X***
  - **OR**: esto permite incluir resultados que cumplan con uno o ambos criterios de búsqueda. Por ejemplo: ***"Gerente General" OR "Gerente de Sistemas" empresa X***
  - **site:** permite limitar las búsquedas a un sitio de Internet en particular. Ejemplo: ***Gerente General site:empresaX.com***
  - **link:** lista las páginas que contienen enlaces al sitio indicado. Por ejemplo, al buscar ***link:empresaX.com*** obtendremos páginas que contienen enlaces hacia la empresa X.

- **filetype:** o **ext:** permite hacer búsquedas por tipos de archivos. Ejemplo: ***rol + pagos ext:pdf site:empresax.com***
- **allintext:** obtiene páginas que contienen las palabras de búsqueda dentro del texto o cuerpo de las mismas. Ejemplo: ***allintext: la empresa X***
- **inurl:** muestra resultados que contienen las palabras de búsqueda en la dirección de Internet (URL). Ejemplo: ***inurl: empresaX***

Por supuesto existen más operadores que podemos usar con *Google*,[9] pero considero que estos son los imprescindibles.

Regresando a nuestro ejemplo de reconocimiento, hemos encontrado entre los resultados algunas páginas relacionadas con la organización *NMAP*, pero la que nos interesa es **scanme.nmap.org.** Esto nos lleva a nuestra siguiente herramienta: la resolución de nombres DNS.

2.5 LAB: CLONANDO WEBSITES

La información contenida en el sitio web del objetivo puede resultar muy útil como parte del reconocimiento, motivo por el cual podría ser de interés de un hacker descargar todo el sitio web para analizarlo después de forma offline.

Otra razón para realizar una copia idéntica o clon de un sitio web, es para efectuar ataques de suplantación o también llamados ataques de "phishing".

Pero independiente de las razones detrás del clonado de un sitio web, existen herramientas que permiten efectuar esta tarea de forma fácil. Estas son algunas de las más populares:

- **Grab-a-Site:** Licencia Comercial. Plataforma Windows. Versión de prueba disponible. Sitio web: *http://www.bluesquirrel.com/products/grabasite/*
- **HTTrack:** Licencia de código abierto (open source). Plataformas Windows, Linux y Android. Sitio web: *http://www.httrack.com/*
- **SiteSucker:** Licencia Comercial. Plataformas Mac e iOS. Versión de prueba disponible. Sitio web: *http://ricks-apps.com/osx/sitesucker/index.html*

9 Google dentro de Google. (2016). Operadores de Búsqueda – Ayuda de Web Search. Recuperado de https://support.google.com/websearch/answer/136861?p=adv_operators&hl=es.

- **Website eXtractor:** Licencia Comercial. Plataforma Windows. Versión de prueba disponible. Sitio web: *http://www.esalesbiz.com/extra/*
- **Web Site Downloader:** Licencia comercial. Plataforma Windows. Sitio web: *http://www.web-site-downloader.com*

De estas, la única aplicación de software libre, compatible con *Kali Linux* es *HTTrack*, la cual ya viene pre-instalada en las últimas versiones.[10] Para usarlo podemos escogerlo desde el menú "**Applications -> Web Application Analysis -> httrack"**, o bien, escribiendo directamente el comando desde un terminal.

La sintaxis básica es la siguiente:

```
httrack <URLs> [-opción] [+<FILTRO_URL>] [-<FILTRO_URL>]

Parámetros:
<URLs>: es la lista de direcciones web que queremos clonar,
separadas por espacios entre sí
+<FILTRO_URL>: para agregar los tipos de archivos que quere-
mos copiar. Ej: +*.png/*.jpg
-<FILTRO_URL>: para indicar los tipos de archivos que desea-
mos excluir de la copia. Ej: -*.zip

Opción más usada:
-O ruta_directorio: aquí debemos indicar la ruta (path) al
directorio en donde queremos que se copien los archivos del
sitio web. Ej: -O /root/clon
```

Nota

Para ver todos los parámetros y opciones acuda al manual (man httrack).

En el siguiente ejemplo clonamos el sitio web del proyecto *WebScanTest*, el cual ha sido diseñado a propósito para ser auditado y escaneado en busca de vulnerabilidades en sus aplicaciones web. Véase la Figura 3.

Ejemplo (como root o anteponiendo sudo): httrack http://www.webscantest.com -O /root/clone.

10 Si no estuviese instalado, es tan fácil como agregarlo con 1) sudo apt-get update y 2) sudo apt-get install httrack.

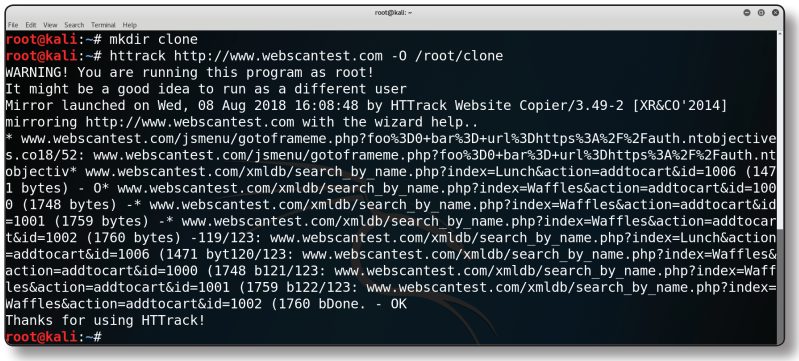


Figura 3. Clonado de WebScanTest con HTTrack

El tiempo para efectuar la copia puede variar dependiendo del tamaño del sitio web objetivo, desde unos pocos segundos hasta varios minutos. Cuando httrack finaliza el proceso, veremos un mensaje que dice "Thanks for using *HTTrack*!" (gracias por usar *HTTrack*). A partir de esto ya podremos revisar la estructura y las páginas del sitio web usando un navegador. En *Kali* viene incluido *Firefox*, el cual podemos ejecutar haciendo clic en el ícono respectivo de la barra de programas situada a la izquierda de la pantalla, o desde el menú "**Applications -> Favorites > Firefox ESR"**.

Una vez abierto *Firefox*, presionaremos la tecla ALT para que se muestre el menú y escogeremos la opción "**File -> Open File"** para abrir el archivo de índice (usualmente index.html) del website, desde la ruta que usamos como salida para la copia (en el ejemplo previo: /root/clone). Véase la Figura 4.

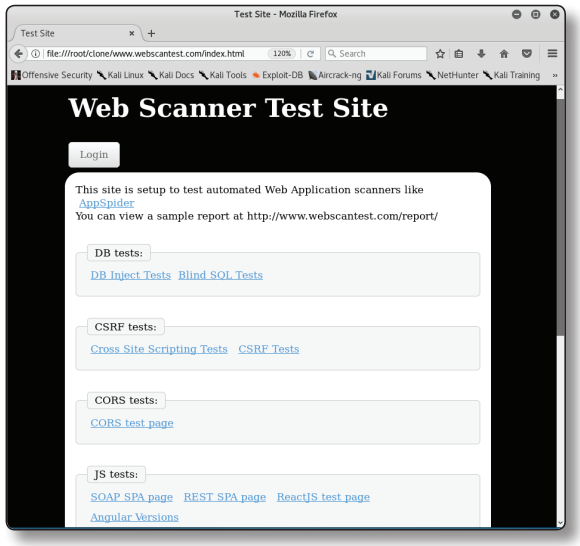


Figura 4. Página de inicio del sitio website clonado

Podremos además explorar tanto la estructura del sitio web como los archivos descargados, desde la línea de comandos o con el explorador de archivos de Kali, tal y como se observa en la Figura 5.

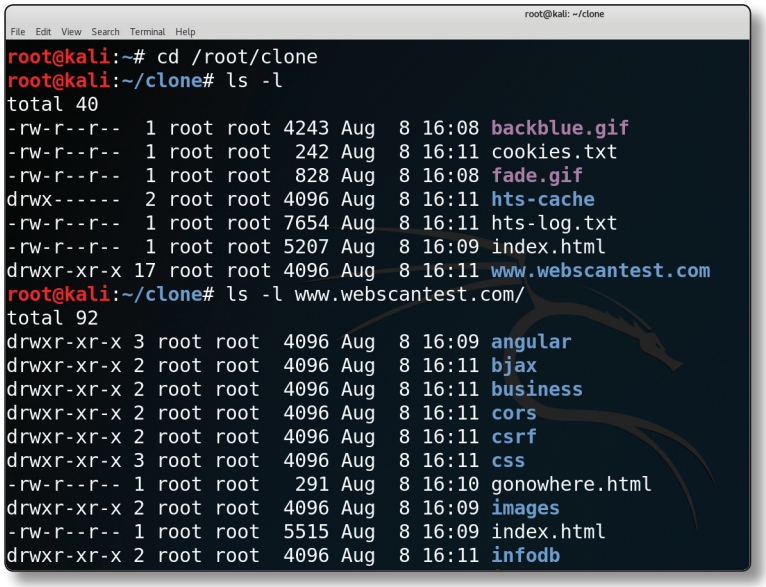


Figura 5. Explorando la estructura del clon

La línea de comandos tiene la ventaja de que nos permite usar utilidades como grep y cut, para efectuar búsquedas de patrones dentro de los archivos. Esto nos permitirá extraer información valiosa como direcciones de hosts, por citar un ejemplo.

```
Ejemplo (como root o anteponiendo sudo): grep href * .html |
cut -d "/" -f 3 | grep "\." | cut -d '"' | sort -u
```

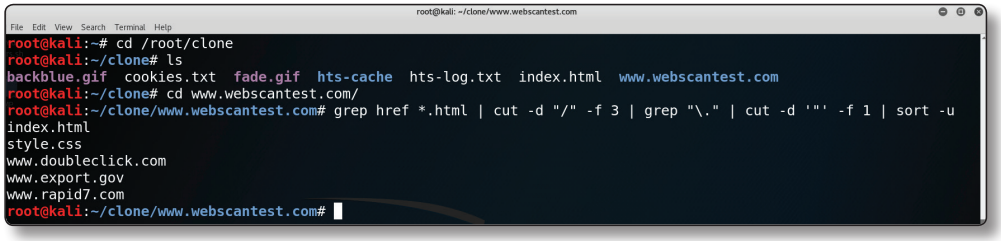


Figura 6. Buscamos patrones de texto con grep y otros comandos de Linux