# 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 nos permita llevar un orden en nuestro trabajo para optimizar nuestro tiempo en la fase de explotación, además de aplicar nuestro sentido común y experiencia. Y aunque lamentablemente la experiencia y el sentido común no se pueden transferir en un libro, haré mi mejor esfuerzo por trasmitirles la metodología y las buenas prácticas que he adquirido a lo largo de los años de ejercer la profesión de auditora de seguridad informática.

## Fases 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 - Fases 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.

## Tipos de hacking

Cuando efectuamos un hacking ético es necesario establecer el alcance del mismo para poder elaborar un cronograma de trabajo ajustado a la realidad y, en base a él, realizar la propuesta económica al 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. Por citar un ejemplo, en una encuesta sobre seguridad informática realizada a un grupo de empresarios en el Reino Unido, cuando se les preguntó quiénes eran los atacantes se obtuvieron estas cifras: externos 25%, internos 75% 1.

## 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, 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, en fin... Debido a que el

consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también.

## 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 2 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 sobre hacking.

## 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.

## 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, 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 me creo Lara Croft, así que ni loca ofrezco este último servicio.

## 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.

## Recursos útiles

■Libro: Proposal writing from three perspectives: Technical Communication, Engineering, and science3.

■Libro: Handbook For Writing Proposals4.

■Libro: Persuasive Business Proposals: Writing to Win More Customers, Clients, and Contracts5.

■Libro: PMI (Project Management Institute), PMBOK Guide and Standards. Recuperado el 15 de mayo de 2013 de http://www.pmi.org/PMBOK-Guide-and-Standards.aspx6.

■Curso: Formulación y Evaluación de Proyectos de Tecnología7