Hacking Ético: Una herramienta para la seguridad informática

Medina Rojas, Edwin Ferney
efmedinar@gmail.com
Universidad Piloto de Colombia

Resumen— La expresión "hacker" es frecuentemente utilizada para hacer referencia a un individuo que intenta ingresar a un sistema de información o que de otro modo utiliza el conocimiento experto y la programación para actuar de manera maliciosa. Este proceder es conocido como hacking. Es por esto que proteger adecuadamente los activos de información de la organización se hace prioritario. Una prueba de hacking ético normalmente es ejecutada por una o varias personas contratadas por la organización que solicita la prueba. Es importante tener claro que es posible que una prueba de hacking ético no identifique todas las vulnerabilidades, ni que ofrece garantía absoluta de que la información de la organización está segura.

El hacking ético son pruebas de penetración que la organización autoriza para simular las actividades de hackers que intentan acceder a sus activos de información y es por esta razón que se puede decir que es una herramienta para la seguridad informática.

Abstract-- **The term "hacker" is often used to refer to an individual who attempts to enter an information system or otherwise use the expertise and programming to act maliciously. This procedure is known as hacking. It is for this reason that adequately protects information assets of the organization is a priority. A test of ethical hacking is usually performed by one or more persons engaged by the organization requesting the test. It is important to understand that you may ethical hacking test does not identify all vulnerabilities, or provides absolute assurance that the organization information is secure.**

Ethical hacking are penetration testing that organization authorized to simulate the activities of hackers attempting to access their information assets and for this reason we can say it is a tool for computer security.

Índice de términos--Ethical hacker, ethical hacking, cracker, vulnerabilidad, pruebas de penetración, backdoor, remediación.

I. INTRODUCCIÓN

Las personas, los sistemas de información y los datos que estos almacenan, son actualmente los activos más valiosos de cualquier organización. El vertiginoso crecimiento y uso de las tecnologías de la información y las telecomunicaciones, trae consigo la aparición de agentes (internos o externos) que pueden aprovechar vulnerabilidades en dichos sistemas y de este modo poner en riesgo la seguridad de la infraestructura de comunicación, los sistemas de información, de los datos allí contenidos e incluso, de las personas. Es por esto que es de vital importancia proteger tanto la información, como la infraestructura de las tecnologías de la información.

Dicho lo anterior y para que una organización pueda minimizar la probabilidad de pérdidas de activos de información por causa de la exposición a amenazas, se hace necesario el uso de herramientas como Sistemas de Gestión de la Seguridad de la Información, análisis de riesgos, gestión de vulnerabilidades, hacking ético, entre otras [1].

II. ANTECEDENTES

Conforme avanza la tecnología, también se incrementan las vulnerabilidades y los ataques a los activos informáticos tanto

de las organizaciones como de las personas en general; es así que existen casos como el del gestor de noticias Feedly o Evernote, quienes vieron afectado sus servicios al ser secuestrada su información por piratas informáticos quienes solicitaban un pago para revertir el ataque y devolver la información [2].
Es entonces cuando toma un rol diferencial el Hacking Ético o Ethical Hacking, una herramienta de la seguridad de la información que se basa en la premisa de que para implementar protección se debe saber cómo piensan y qué métodos o herramientas usan los hackers, de este tema nos ocuparemos en las siguientes secciones.

III. HACKING ÉTICO O ETHICAL HACKING

A. ¿Qué es el hacking ético?

Para atrapar a un intruso, hay que pensar como un intruso, bajo esta premisa se puede dar una base al concepto de hacking ético, el conocimiento del enemigo es una tarea vital ya que con el veloz desarrollo de la tecnología, también aumenta el número de hackers y el número de vulnerabilidades de los sistemas que pueden ser explotadas por ellos. A medida que pasa el tiempo, la infraestructura, los sistemas de información y las aplicaciones se vuelven susceptibles de ser atacadas, es así que proteger estos activos de los hackers se vuelve crítico.

Los hackers atacan las malas prácticas en materia de seguridad y vulnerabilidades de día cero. Los firewalls, la criptografía y el uso de contraseñas pueden crear una falsa sensación de seguridad, estas herramientas normalmente no cubren todos los frentes necesarios para tener realmente un nivel de seguridad aceptable. Atacar la infraestructura y los sistemas de información propios de la organización para descubrir debilidades ayuda a mejorar la seguridad.

Se puede decir y sin temor a equivocaciones que el hacking ético o ethical hacking es en gran medida el único método probado de aseguramiento de los sistemas de información contra los ataques, si no se identifican las vulnerabilidades, es solo cuestión de tiempo que estas sean explotadas. En resumen, el ethical hacking permite a las organizaciones conocer las debilidades en su infraestructura y sistemas de información de modo que puedan ser tratadas para disminuir el riesgo de pérdidas.

B. ¿Qué es y que hace un hacker ético?

Un hacker ético es la persona que usa habilidades como: conocimientos en programación, redes de computadoras, instalación y mantenimiento de infraestructuras basadas en los sistemas operativos más conocidos y usados como lo son Unix1 y Windows NT2, el ingenio, el pensar como un intruso, la paciencia, la constancia, el auto-estudio y la capacitación entre otras para hacer pruebas de penetración o hacking ético de forma controlada, con el respectivo permiso sobre la infraestructura y los sistemas de información de una organización sin hacer daño alguno, de modo que pueda detectar debilidades y

[1] Marca comercial o marca registrada de The Open Group.
[2] Marca comercial o marca registrada de Microsoft Corporation.

sugerir contramedidas y recomendaciones para su remediación y aseguramiento.

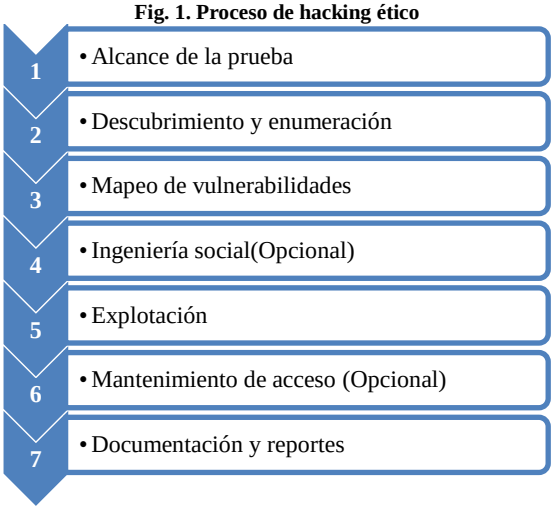
El objetivo del hacker ético es en esencia el mismo que el de un cracker: tratar de determinar lo que un intruso puede obtener en una infraestructura o sistema de información objetivo y que puede hacer con esa información. Cabe recalcar que la palabra ética en el mundo del hacking implica una gran responsabilidad ya que la persona encargada de realizar la actividad puede tener acceso a información privilegiada, privada, confidencial, reservada, etc. Que mal manejada puede acarrear problemas legales y hasta causar un gran perjuicio en la organización.

Existen tres modelos de pruebas que un hacker ético puede ejecutar sobre el sistema de información, estas son:

- Caja blanca: Pruebas de caja blanca es cuando el equipo de pruebas tiene acceso a diagramas de red, registros de activos, y otra información útil. Este método se utiliza cuando el tiempo es esencial y cuando los presupuestos y el número de horas autorizadas son limitados. Este tipo de prueba es el menos realista, en términos de lo que un atacante puede hacer [3].
- Caja gris: Como se puede suponer, están en algún lugar entre pruebas de caja blanca y pruebas de caja negra. Esta es la mejor forma de hacer pruebas de penetración, donde al equipo de pruebas se le da información limitada y sólo si es necesaria. Así, a la hora de trabajar su camino desde el exterior, se concede mayor acceso a la información para acelerar el proceso. Este método de pruebas maximiza el realismo sin dejar de ser agradable y económico [3].
- Caja negra: Es que cuando no se da absolutamente ninguna información al equipo de pruebas de penetración. De hecho, usando este método de prueba, al equipo de pruebas de penetración sólo se le podrá dar el nombre de la empresa. Otras veces, se les puede dar un rango de direcciones IP y otros parámetros para limitar el potencial daño colateral Este tipo de pruebas representa más exactamente lo que un atacante puede hacer y es el más realista [3].

Un hacker ético se guía por un modelo de referencia definido para llevar a cabo las actividades dentro de las pruebas de penetración o pen testing como se muestra en la Fig. 1:

Fig. 1. Proceso de hacking ético



Fuente: El autor

La Fig. 1 será tratada con más detalle en

las siguientes secciones.

IV. PROCESO DEL HACKING ÉTICO

El proceso del hacking ético viene dado por una serie de etapas que el hacker ético debe seguir para alcanzar el objetivo de la actividad a saber.

A. Alcance de la prueba

Con el alcance de la prueba se determinan los activos que se van a evaluar durante el ejercicio. Lo primero es conseguir la aprobación del cliente, en muchos países, la intrusión abusiva en infraestructuras y sistemas de información es un delito, por lo que obtener un permiso escrito de parte del cliente es esencial. El siguiente paso es definir un plan detallado que puede incluir los siguientes ítems entre otros:

1. Seleccionar los sistemas a atacar: Esto incluye los sistemas y procesos más críticos y los que son sospechosos de ser más vulnerables.
2. Evaluar el riesgo: Implica tener un plan de choque en caso de que algo salga mal; como por ejemplo respaldos de la base de datos, respaldos de configuración de aplicativos, entre otras.
3. Fechas, horas y duración de las pruebas: Saber en qué momento del día se van a realizar las pruebas de modo que el hacker ético pueda estar preparado y no afecten la continuidad del negocio.
4. Conocimiento del sistema antes de empezar la prueba: Esto abarca el tipo de prueba que el cliente quiera realizar, ya sean de caja blanca, caja gris o caja negra.
5. Acciones cuando se descubren vulnerabilidades críticas: Se debe continuar con el ataque para ver hasta dónde se puede llegar sin causar daños en el sistema, cuando esto ocurre, lo que se debe hacer es informar al cliente para que pueda hacer el respectivo tratamiento de la vulnerabilidad antes de que sea explotada por alguien malicioso.
6. Definir las actividades que finalizan las pruebas: Las actividades o eventos que desencadenarán la conclusión de las pruebas de penetración deben describirse claramente en la definición del alcance del plan detallado. Dichas actividades o eventos dependen de los objetivos específicos de la prueba, pero podrían, existir otros desencadenantes. En algunos casos, puede ser apropiado definir una ventana de tiempo en la que la prueba debe ser completada.

El ideal del plan detallado es definir lo más claramente posible los límites de la prueba para no llegar a afectar el normal funcionamiento de la organización.

B. Descubrimiento y enumeración

Para tener éxito en el reconocimiento, el hacker ético debe tener una estrategia; casi todos los métodos de recopilación de información, aprovechan el poder de Internet, una estrategia típica debe incluir tanto el reconocimiento pasivo como el reconocimiento activo.

Reconocimiento pasivo: Este método de recolección de información busca hacerlo de la manera más silenciosa posible,

puede hacerse de manera sencilla como observando el comportamiento de los empleados de la organización, horarios de entrada y salida y sobre ellos hacer ingeniería social; también se puede acudir a herramientas informáticas como buscadores donde se puede recopilar información del objetivo, sniffers en modo escucha para observar el tráfico circulante por la red de la organización.

Reconocimiento activo: Cuando se utiliza este método de recolección de información, el hacker ético es más vulnerable a ser detectado ya que se interactúa directamente con el objetivo. El reconocimiento activo da al hacker ético información del sistema como hosts, servicios, puertos o direcciones IP sobre la red.

Ambos métodos de recolección de información, ayudan a obtener datos útiles que luego son utilizados como insumo base en el momento de lanzar el ataque contra el sistema objetivo. Algunas de las herramientas utilizadas para hacer descubrimiento y enumeración son: WhoIs, Nslookup, Maltego, ARIN (American Registry of Internet Numbers), TraceRoute, Smart/Whois, Sam Spade, entre otras [4].

C. Mapeo de vulnerabilidades

Ahora que se tiene una lista de direcciones IP, puertos abiertos, y servicios, entre otras detecciones en cada máquina, es el momento de escanear los objetivos en busca de vulnerabilidades. Una vulnerabilidad es una debilidad en el software o sistema de configuración que puede ser explotada. Las vulnerabilidades pueden venir en muchas formas, pero más a menudo están asociadas con parches faltantes [1].

El software y los sistemas sin parches a menudo conducen a pruebas de penetración rápidas porque algunas vulnerabilidades permiten la ejecución remota de código. La ejecución remota de código es definitivamente uno de los santos griales del hacking [1]. La búsqueda de estas vulnerabilidades se puede hacer en dos escenarios macro a saber: escenario interno, que no es más que la búsqueda de vulnerabilidades desde adentro de la organización, escenario externo, que es la búsqueda de vulnerabilidades desde el exterior de la organización.

Hoy en día existen muchas herramientas en las cuales un hacker ético se puede apoyar para buscar dichas vulnerabilidades como pueden ser: Nessus (Herramienta de software libre), Microsoft Baseline Security Analyzer, Retina, Network Security Scanner, Qualys o Acunetix, SAINT, entre otras [4]. Los resultados obtenidos del escaneo de vulnerabilidades se usarán en el siguiente paso del proceso de hacking ético; cabe también aclarar que las herramientas usadas pueden ser capaces de sugerir soluciones a las vulnerabilidades (proceso llamado remediación) que son las que se incluirán finalmente en el informe final que se discutirá en una sección posterior.

D. Ingeniería social [5]

La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de

la persona objetivo.

La Ingeniería Social se sustenta en un sencillo principio: "el usuario es el eslabón más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla.

La Ingeniería Social es un arte que pocos desarrollan debido a que no todas las personas tienen "habilidades sociales". Aun así, hay individuos que desde pequeños han demostrado tener la aptitud y con un poco de entrenamiento convertirla en el camino ideal para realizar acciones maliciosas. Por ejemplo, hay crackers que en vez de perder horas rompiendo una contraseña, prefieren conseguirla preguntando por teléfono a un empleado de soporte técnico.

Algunas herramientas utilizadas en la ingeniería social son: Vigilancia, Pishing, suplantación de identidad, llamada telefónica, correo electrónico, SMS, entre otras.

E. Explotación

En la etapa de explotación se logra el acceso a la infraestructura o sistema de información evaluado, la explotación es la ejecución de un exploit que no es otra cosa que un código que se puede aprovechar de una vulnerabilidad permitiendo alterar la funcionalidad normal del software.

Esta tarea es ardua, ya que puede tomar demasiado tiempo explotar las vulnerabilidades encontradas hasta escalar privilegios. El escalamiento de privilegios permite al atacante tomar el control de una máquina con permisos de administración para poder ejecutar todo tipo de tareas sin restricciones. Es en este paso donde se recolectará todo tipo de evidencia que se incluirá en el reporte final del ejercicio.

F. Mantenimiento de acceso

En algunos casos para completar el ejercicio se instala un backdoor con el cual el hacker ético puede tener acceso al sistema en cualquier momento, este paso puede ser no deseado por el cliente ya que un hacker malicioso podría encontrar esta puerta y acceder al sistema de información causando daños y perjuicios a la organización. En mi opinión es una actividad que no se debería llevar a cabo o que se debería deshacer justo después de su ejecución para evitar posibles ataques. Las herramientas que se pueden utilizar para logra el acceso permanente al sistema de información pueden ser: Troyanos y backdoors entre otros.

G. Documentación y reportes

Finalmente y como conclusión del ejercicio, entramos en la etapa de documentación y reportes, aquí vamos a recopilar toda la evidencia obtenida en las actividades previas. Los reportes deben ser presentados de manera asertiva, ordenada, clara, completa y considerando el perfil, conocimiento e interés del receptor.

Como primera medida y si el trato con el cliente lo requiere, se debe presentar un plan de remediación de las vulnerabilidades detectadas que puede ser generado automáticamente por la herramienta o desarrollado manualmente con la información arrojada por la misma, esto cobija información como la descripción de la vulnerabilidad, código CVE, impacto, solución, etc.

Acto seguido se sugiere entregar dos reportes más, un reporte técnico dirigido al personal netamente técnico de la organización como los grupos encargados de la remediación, los líderes de TI o de seguridad, etc. Y un reporte ejecutivo que va dirigido al personal administrativo de la organización (Gerentes y directores). Básicamente los dos informes deben tener las mismas secciones (Introducción, objetivos, alcance, metodología, resultados y conclusiones y recomendaciones), el informe técnico tiene mayor detalle, un lenguaje técnico y sirve como herramienta para la toma de decisiones de tipo técnico; por el otro lado, el informe ejecutivo tiene un uso mínimo de lenguaje técnico especializado ya que debe ser comprensible para las personas sin conocimientos del tema; en algunos casos puede servir para tomar decisiones gerenciales.

V. CONCLUSIONES

1. El continuo y vertiginoso crecimiento de los aplicativos y sistemas de información hace que aparezcan más vulnerabilidades y por ende más personas maliciosas que podrían atacarlos, es por esto que el hacking ético se convierte en una herramienta indispensable en la evaluación de la seguridad.

2. La protección adecuada de los activos de información de una organización es una tarea vital. La ejecución de pruebas de penetración es una parte eficaz y rentable de la estrategia de seguridad de la organización y que provee información sobre la facilidad de que un intruso pueda obtener acceso no autorizado a sus sistemas de información e información y que además sirve para probar la seguridad de la información y capacidad de respuesta ante un ataque.

3. El hacking ético es una herramienta de la que cualquier organización preocupada por la información debe echar mano ya que metódicamente detecta debilidades, las explota y hace recomendaciones en pro de mejorar la seguridad de la infraestructura y los sistemas de información de una organización.

4. Para que una prueba de hacking ético produzca el efecto deseado, a nivel organizacional, debe haber conciencia sobre la importancia de la seguridad de la información, lo cual, en conjunto con el Sistema de Gestión de Seguridad de la Información permite minimizar el número de vulnerabilidades y así mismo el riesgo asociado a ellas.

VI. REFERENCIAS

[1] (2014, Junio) Revista semana. [Online]. http://www.semana.com/tecnologia/novedades/articulo/los-peores-ataques-informaticos-de-2014/391376-3

[2] Allen Harper et al., Gray Hat Hacking, Tercera ed., Michael Baucom, Ed. New York, USA: McGraw Hill, 2011.

[3] Russell Dean Vines. (2008, Junio) Network penetration testing: Ethical hacking tools and techniques. [Online]. http://searchitchannel.techtarget.com/tip/Network-penetration-testing-Ethical-hacking-tools-and-techniques

[4] Patrick Engebretson, The Basics of Hacking and Penetration Testing, Primera ed., James Broad, Ed. Waltham, USA: Elsevier, 2011.

[5] Edgar Jair Sandoval Castellanos, "Ingeniería Social: Corrompiendo la mente humana," Seguridad, vol. I, no. 10, Mayo 2011, http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana#_ftn1.