Introducción al hacker ético

Betancourt, Jhonny.
JsasukeJ@gmail.com
Universidad Piloto de Colombia

Abstract— The evolution of internet has brought many good events such as electronic commerce, easy access to study materials, technological advances, e-mail, and new ways for advertising and information distribution. But not everything can be perfect; there is also the dark side of technology too; cyber-attacks caused by "hackers". Governments, companies and citizens around the world are afraid that some "hacker" interfere with a web server and can gain remote access, read emails, steal credit card numbers, among others. With these concerns, the ethical hacker originated; which can help against the threat. This paper describes ethical hackers and malicious hackers; their skills, their attitudes, different types of attacks and how they go about helping their customers find and implement security vulnerabilities will also be described.

Key words—Attack, hacker, hacker's phases, security.

Resumen— La evolución de internet ha traído muchos sucesos buenos como el comercio electrónico, fácil acceso a material de estudio, avances tecnológicos, e-mail, y nuevos caminos para la publicidad y la distribución de la información. Sin embargo no todo puede ser perfecto; también existe el lado oscuro de la tecnología; los ataques cibernéticos causados por "hackers". Los gobiernos, empresas y ciudadanos de todo el mundo tienen miedo de que algún "hacker" interfiera en un servidor web y logre tener acceso remoto, leer correos electrónicos, robar números de tarjetas de crédito, entre otros. Con estas preocupaciones, dio origen el hacker ético; el cual puede ayudar contra dicha amenaza. Este artículo describe los hackers éticos de los hackers maliciosos; también se describirá sus habilidades, sus actitudes, los diferentes tipos de ataques y cómo van en ayudar a sus clientes a encontrar e implementar las vulnerabilidades en la seguridad.

Índice de Términos—Ataques, fases de un hacker, hacker, seguridad.

I. INTRODUCCIÓN

La mayoría de las personas creen que los hackers poseen sorprendentes habilidades y conocimientos que les permiten acceder en los sistemas informáticos. Un profesional de la seguridad se orienta como un hacker ético. Este hacker ético debe entender cómo opera un sistema informático y a su vez, conocer qué herramientas utiliza con el fin de encontrar vulnerabilidades. Con el crecimiento de internet, la seguridad informática se ha convertido en una preocupación importante para las empresas y las personas. Hoy en día el internet es vital para cualquier organización, ya sea para el comercio electrónico, la publicidad o la distribución de información. Y por estar asociados a internet, esto aumenta la preocupación de ser "hackeado" [1].

La manera de afrontar dicho problema, es una vez que las organizaciones comprendan que una de las mejores maneras de evaluar la amenaza de intrusión, es contar con un grupo de profesionales en seguridad informática para atacar y acceder a los sistemas informáticos [1]. El esquema en estos profesionales en seguridad informática es similar a tener auditores independientes en una organización para verificar los registros de contabilidad. En el caso de la seguridad informática, a estos profesionales se les denominan "hackers éticos" donde emplean las mismas herramientas y técnicas como los intrusos, pero no perjudicarían los sistemas de la organización, ni robarían la información dentro de la misma; En su lugar, se evaluará la seguridad de los sistemas y se reporta a los propietarios las vulnerabilidades halladas [1].

II. TIPOS DE HACKER

A. Hackers de sombrero Blanco

Los hackers de sombrero blanco son los hackers éticos que utilizan sus experiencias de hacker, con el objetivo de tomar medidas defensivas. Los hackers del sombrero blanco suelen ser

profesionales de la seguridad con la comprensión del hacking y el uso de herramientas para llevar a cabo estas tareas y a su vez, usan este conocimiento para hallar vulnerabilidades y detectar las respectivas contramedidas. Los hacker de sombreros blanco realizan un ataque hacker con el permiso del dueño del negocio u organización. Es de vital importancia obtener el permiso antes de comenzar cualquier actividad hacking; debido a que es la manera correcta en la que operan los profesionales de la seguridad contra un hacker malicioso [2], [3], [6], [8].

B. Hackers de sombrero negro

Los hackers de sombrero negro son los malos: los hackers maliciosos utilizan sus habilidades para fines ilícitos o perjudiciales. Rompen la seguridad para vulnerar la integridad del sistema, con malas intenciones y buscan la manera de obtener acceso no autorizado. Los hackers de sombrero negro intentan destruir datos vitales o activos del negocio; también, tratan de negar el servicio a los usuarios legítimos. Los hackers de sombrero negro pueden ser fácilmente diferenciados de los hackers sombrero blanco porque sus acciones son maliciosas [2], [3], [6], [8].

C. Hackers de sombrero gris

Los hackers de sombrero gris son los hackers que pueden trabajar de manera ofensiva o defensiva, dependiendo del escenario en el que se encuentre. Esta es la línea en la que se divide del bien y del mal o del hacker y del cracker. Los hackers de sombrero gris sólo buscan estar interesados en las herramientas y tecnologías del hacking. Los hackers de sombrero gris pueden ser, o se consideran hackers éticos, debido a que el interés de las herramientas de hacking no los impulsa a realizar actos ilícitos o maléficos, y solo ven las herramientas de manera curiosa [2], [3], [6], [8].

Los hackers de sombrero gris acceden a sistemas no autorizados sin el respectivo permiso del titular; pero en lugar de cometer un acto malicioso, destacan los problemas de seguridad en un sistema o educan a las víctimas para que aseguren sus sistemas correctamente. Estos hackers les están haciendo a sus "víctimas" un favor. La diferencia entre los sombreros blancos y sombreros grises es el permiso para realizar la actividad hacking. Aunque sombreros grises pueden tener buenas intenciones, sin el permiso correcto ya no pueden ser considerados como hackers éticos; es decir, de los tres tipos de hackers vistos, el único que puede considerarse un hacker ético, es el hacker de sombrero blanco [2], [3], [6], [8].

III. TIPOS DE ATAQUE

Existe una gran cantidad formas de atacar un sistema. Esto se puede conseguir mediante el aprovechamiento de vulnerabilidades, debilidades conocidas o halladas por el uso de uno o varios software de hacking, o incluso el simple aprovechamiento de una política de seguridad mal establecida. Los tipos de ataques que se mencionan en este artículo son los más comunes; sin embargo existen otros tipos de ataques, y con el paso del tiempo existirán nuevos tipos de ataques [1].

A. Ataques de desbordamiento de búfer

Ataques de desbordamiento de búfer o más conocido como buffer overflow aprovechan el software mal escrito por los desarrolladores para condescender a los atacantes ejecutar código aleatorio en el sistema objetivo y tener acceso. Los desbordamientos pueden suceder en el software del servidor que esté disponible para los usuarios en la red [4], [5].

B. Ataques de denegación de servicio

Ataques de denegación de servicio o DoS por sus siglas en inglés (Denial of Service) resulta en un servicio específico que puede afectar a los usuarios y generalmente estos ataques suelen tener tres objetivos [5]:

1) La conexión de red que proporciona acceso al servicio.
2) El sistema operativo que aloja el servicio.
3) El programa de nivel de aplicación que proporciona el servicio.

C. Ataques de denegación de servicio distribuidos

Los ataques de denegación de servicio distribuidos o conocido como DDoS por sus siglas en inglés (Distributed Denial of Service); estos ataques tienen el mismo objetivo como el ataque de denegación de servicio, pero utilizan una arquitectura diferente para lograrlo. Un solo host lanza un ataque a nivel de red o aplicación frente a un objetivo, pero este se ve limitado por los recursos del ancho de banda de la red y del hardware disponible; por otro lado, un grupo de máquinas puede ser más eficaz en un ataque concertado; donde se puede concluir que, la cantidad marca la diferencia [5].

D. Error de configuración

Muchos de los ataques exitosos son llevados por abusar de los errores de configuración comunes en los servicios de red. Los servicios de la red siempre deben estar configurados con una política de "no permitir el acceso por defecto". Lo que normalmente hacen caso omiso a dicha política; lo que resulta un gran número de servicios que son realmente vulnerables a un ataque malicioso [5].

E. Abuso de confianza

Los protocolos de red no ponen mucho énfasis en el cifrado y la autenticación, debido a que se utilizan en redes relativamente pequeñas. A medida que estas redes y sistemas forman parte del internet, se hace posible la explotación de vulnerabilidades en estos protocolos. Un ejemplo es el uso de una dirección IP origen como un medio para establecer una relación de confianza entre los dos sistemas mediante TCP. Sppofing es un tipo de ataque común que explota esta vulnerabilidad y por lo tanto logra tener acceso al sistema y los recursos de la organización [5].

F. Ataques de fuerza bruta

Estos ataques están dirigidos a obtener acceso a un sistema mediante intentos repetidos de autenticación. La mayoría de los servicios requieren un nombre de usuario y contraseña; es decir, se requiere de credenciales válidas para obtener una correcta autenticación; Pero muchas de estas, no disponen de instalación de bloqueo de cuentas, lo que los vuelven vulnerables a este tipo de ataque. Los ataques de fuerza bruta se utilizan comúnmente para descifrar contraseñas, debido a que existen muchas herramientas que pueden realizar este tipo de ataque [5].

G. Puertas traseras y troyanos

Los virus troyanos y programas de puertas traseras (backdoors) son un método popular para obtener acceso no autorizado a sistemas remotos. Las puertas traseras ofrecen al atacante una manera fácil de acceder a un sistema remoto sin tener que depender de la explotación a determinadas vulnerabilidades de seguridad. Una herramienta de uso común es NetCat, que está disponible en las plataformas Windows y Unix [5].

IV. PROCESO DE UN HACKER ÉTICO

Al igual que prácticamente cualquier proyecto de TI (Tecnología de la información), El hacking ético necesita ser planificado de antemano. Las estratégicas y tácticas en el proceso de hacking ético deben ser determinadas y acordadas desde el inicio [7].

A. Formulación de plan

La aprobación de hacking ético es esencial. Para asegurarse que el procedimiento realizado sea conocido y visible para la organización o al menos para los que toman las decisiones. Se requiere de al menos una persona para que apoye y firme el plan. De lo contrario, las pruebas y el trabajo realizado pierden validez si alguien afirma que nunca se obtuvo dicho permiso para realizar las respectivas pruebas. Una vez aprobado el plan se deberá realizar el análisis de vulnerabilidades para hallar debilidades; normalmente se utiliza ataques de ingeniería social para medir el nivel de capacitación de los miembros dentro de la organización. Si un ataque de ingeniería social tiene éxito puede causar la pérdida de integridad de los datos y la mala publicidad a la organización [7].

B. Selección de herramientas

La simple idea de utilizar las herramientas adecuadas, no significa que se van a descubrir todas

las vulnerabilidades; Se debe conocer las limitaciones, tanto personales como técnicas. Muchas de las herramientas de seguridad generan falsos positivos; también estas herramientas se centran en pruebas específicas, pero ninguna herramienta puede hacer de todo. Por este motivo se debe usar un conjunto de herramientas que permitan completar la respectiva identificación de vulnerabilidades; cuantas más herramientas se tienen, los análisis de hacking ético lograrán ser más efectivos [7].

V. Fases de un hacker ético

Las etapas del hacker ético se dividen en cinco fases secuenciales. Un hacker ético sigue estos pasos como un cracker o hacker malicioso para obtener y mantener la entrada en un sistema informático, con la excepción de que el hacker ético informará los hallazgos encontrados [1].

1) Reconocimiento

Esta primera etapa implica la recopilación de información sobre un objetivo partiendo desde cero. Normalmente los hackers usan el internet como medio de búsqueda de información sobre el objetivo que puede ser desde una persona hasta una organización. La ingeniería social también se considera otro método de recopilación de información debido a que el atacante o hacker que realice ingeniera social, puede lograr obtener valiosa información que será utilizada para la etapa de reconocimiento. Sniffing es otro medio de reconocimiento y puede proporcionar información útil, como rangos de direcciones IP, servidores ocultos, redes u otros servicios disponibles en el sistema. Las herramientas de Sniffing son simples, fáciles de usar y generan una gran cantidad de información valiosa. Muchas veces esto incluye nombres de usuario, contraseñas y otros datos sensibles lo que conduce a graves problemas de seguridad en manos equivocadas [1], [2].

2) Escaneo

La fase de escaneo consiste en tomar la información obtenida durante la etapa de reconocimiento y usarlo para examinar la red. Las herramientas que un hacker ético se pueden emplear durante la fase de escaneo; las que incluyen [1], [2]:

- Escaneo de puertos
- (ICMP) escáneres de Protocolo de mensajes de control de Internet
- barridos ping
- Mapeos de red
- (SNMP) barredoras de protocolo simple de administración de red
- Los scanners de vulnerabilidades

Los hackers ético están buscando cualquier información que pueda ayudarles a realizar un ataque contra el objetivo como:

- Nombres de equipo
- Sistema operativo (OS)
- Software instalado
- Direcciones IP
- Cuentas de usuario

3) Ganar acceso

En esta tercera etapa es cuando el verdadero ataque hacking tiene lugar, debido a que hace la respectiva función de lograr ingresar a un sistema. Las vulnerabilidades expuestas durante la etapa de reconocimiento y la fase de escaneo que se encarga de la exploración para obtener acceso al sistema de destino. El ataque informático se puede enviar al sistema destino a través de una red de área local (LAN), ya sea por cable o inalámbrico (Wi-Fi) o fuera de línea (offline). El acceso es conocido en el mundo hacker como propietario del sistema, ya que una vez que un sistema ha sido hackeado, el hacker tiene el control y puede utilizar ese sistema como lo desee [1], [2].

4) Mantener acceso

Una vez que un hacker ha logrado obtener acceso al sistema objetivo, quieren mantener el acceso para una futura utilización al sistema de manera rápida y oculta. Esto se logra mediante uso de puertas traseras, rootkits o troyanos [1], [2].

5) Borrar huellas

Una vez que los hackers han sido capaces de

obtener acceso al sistema y también logran mantener el acceso al mismo, cubren sus pistas para evitar la detección por parte del personal de seguridad, para seguir utilizando el sistema. En esta etapa se busca eliminar la evidencia de la actividad hacking. Los hackers tratan de eliminar todos los rastros del ataque, tales como los archivos de registro en el sistema de detección de intrusos (IDS). Esta última etapa es usada normalmente por los hackers de sombrero negro. Un hacker ético o de sombrero blanco no se encargará de borrar las huellas; en su lugar generará un reporte donde especifique las fallas de seguridad halladas dentro de la organización [1], [2].

VI. Tipos de pruebas

Cuando se realiza una prueba de seguridad, un hacker ético utiliza uno o más tipos de pruebas en el sistema. Cada tipo de prueba representa a un atacante con diferentes niveles de conocimiento acerca de la organización objetivo [1], [2], [3]. Estos tipos de prueba son:

A. Caja negra

Las pruebas de caja negra implica la realización de una evaluación de seguridad y pruebas sin conocimiento previo de la infraestructura de red o sistema objetivo. Este tipo de prueba simula un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización. Las pruebas de caja negra puede tomar la mayor cantidad de tiempo y esfuerzo, debido a que no se conoce la información básica. Por lo tanto, la ventaja de este tipo de pruebas es que simula más los métodos de un verdadero ataque hacking; y se puede lograr obtener resultados de un atacante malintencionado como si este fuera real. Las desventajas de este tipo de prueba es principalmente la cantidad de tiempo y costo para realizar la prueba [1], [2].

B. Caja blanca

Las pruebas de caja blanca implica la elaboración de una evaluación de seguridad y prueba con un conocimiento completo sobre la infraestructura de red y del sistema objetivo. Esta prueba es mucho más rápida que las pruebas de caja negra y caja gris; debido a que el hacker ético puede saltar directamente a la fase de ataque porque ya se obtiene conocimiento sobre la misma. Muchas auditorías de seguridad consisten en la realización de pruebas de caja blanca para la reducción de tiempo y costo comparado con las pruebas de caja negra [1], [2].

C. Caja gris

Las pruebas de caja gris implica la realización de una evaluación de seguridad y pruebas internamente. Este tipo de prueba examina el grado de acceso de información a nivel de privilegios dentro de la red. El propósito de esta prueba es simular la forma más común de ataque; es decir, las que dan inicio dentro de la red. La idea es probar o auditar el nivel de acceso dado a los empleados o contratistas y ver si esos privilegios se pueden elevar a un nivel superior [1], [2].

VII. Realización de pruebas de penetración

Los hackers éticos utilizan sus habilidades para llevar a cabo evaluaciones de seguridad o pruebas de penetración [1]. Estas pruebas y evaluaciones se basan en tres fases:

A. Preparación

Esta fase radica en un acuerdo formal entre el hacker ético y la organización. Este acuerdo debe contener el alcance total de la prueba, los tipos de ataques que van a ser utilizados, y los tipos de pruebas [1].

B. Evaluación de conducta de la seguridad

Durante esta fase se realizan las pruebas, después se prepara un informe técnico y ejecutivo de las vulnerabilidades y otros hallazgos encontrados [1].

C. Conclusión

Los resultados se presentan a la organización en esta fase, junto con las recomendaciones para mejorar la seguridad [1].

Estos tres pasos son únicamente para la generación del informe sobre un análisis realizado, el hacker ético no "arregla" las vulnerabilidades

halladas, solo informa cómo se debe implementar la seguridad para evitar ser explotadas nuevamente. Este es un error común de llevar a cabo auditorías de seguridad o pruebas de penetración [1].

El objetivo final o entregable es realmente los resultados de la prueba y un análisis de los riesgos asociados. La prueba es lo que lleva a las conclusiones del informe final y deberá estar bien documentado en cada hallazgo encontrado con capturas de pantallas para tomar con total seriedad este rol [1].

VIII. Conclusiones

La aplicación de herramientas de hacking no forman a los profesionales de seguridad para ser hackers éticos; para ser un verdadero hacker ético no solo debe conocer las herramientas y lograr tener acceso no autorizado, sino que también utiliza todos los procedimientos vistos en el artículo donde incluyen los procesos de un hacker ético.

La documentación es la principal características de un hacker ético. Un profesional en la seguridad que no realice la respectiva documentación de los hallazgos encontrados, no se puede considerar un acto de hacker ético.

Es muy importante identificar los diferentes tipos de hackers que habitan alrededor del mundo; muchas personas usan la palabra “hacker” desde el punto de vista negativo. Pero la realidad es que el hacker ético se encarga de encontrar fallas en la seguridad para que esta puedan ser implementada y no ser vulnerada por un hacker malicioso que busca causar algún perjuicio o beneficio propio.

REFERENCIAS

[1] Kimberly Graves, 2010. CEH Certified Ethical Hacker Study Guide. [En linea] Disponible en: http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf

[2] Kimberly Graves, 2012. CEH Certified Ethical Hacker Review Guide. [En linea] Disponible en: http://www.it-docs.net/ddata/893.pdf

[3] www.redusers.com. Ethical Hacking. [En linea] Disponible en: http://img.redusers.com/imagenes/ebook/lpcu228/notagratis.pdf

[4] www.cdn.ttgtmedia.com, 2004. Buffer Overflow. [En linea] Disponible en: http://cdn.ttgtmedia.com/searchSecurity/downloads/ExploitingSoftware-Ch07.pdf

[5] www.hackbbs.org, 2000. Ethical Hacking Student Guide. [En linea] Disponible en:http://hackbbs.org/article/book/ethical%20hacking,%20student%20guide.pdf

[6] David M. Hafele, 2004. Three Different Shades of Ethical Hacking : Black, White and Gray. [En linea] Disponible en:http://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390

[7] www.media.techtarget.com. Chapter 1 Introduction to Ethical Hacking. [En linea] Disponible en:http://media.techtarget.com/searchNetworking/downloads/hacking_for_dummies.pdf

[8] Rafay Baloch. A beginners guide to Ethical Hacking. [En linea] Disponible en:http://x3n0n.com/wp-content/uploads/2014/02/A-Beginners-Guide-To-Ethical-Hacking.pdf