ETHICAL HACKING: UNA ESTRATEGIA DE DEFENSA PROACTIVA

Ariza Bonces Diana Marcela
marcelaariza_22@hotmail.com
Universidad Piloto de Colombia

Resumen **-** Las empresas hoy en día tienen dos grandes debilidades respecto a la seguridad informática y ciber seguridad, el primero es que no cuentan con departamentos o personal calificado en esta materia, y el segundo es que no hacen revisión de seguridad periódicamente para saber cómo están realmente preparados ante un eventual ataque informático. Sí las empresas han realizado pruebas de seguridad es con el acompañamiento de terceros o ejecutando herramientas solo para obtener un informe para demostrar la evidencia ante las auditorias o entidades que vigilan dichas actividades. Aunque probablemente sean menos formales, incluso los piratas informáticos del tipo más básico hacen preparativos de algún tipo antes de atacar a sus víctimas. Tomar tiempo para preparar una prueba de seguridad antes de la ejecución, es la única forma de obtener buenos resultados a largo plazo. La información de este articulo abarca la importancia de realizar un análisis de vulnerabilidades y pruebas de penetración, que se debe tener en cuenta, como preparase y como hacer seguimiento, con el objetivo de implementar estrategias que deberían tenerse en cuenta para endurecer la seguridad informática y ciber seguridad en las compañías.

Abstract **-** Companies today have two major weaknesses regarding computer security and cybersecurity, the first is that they do not have departments or qualified personnel in this matter, and the second is that there is no possible computer attack, and yes, companies they have carried out security tests with the accompaniment of third parties or executing tools only to obtain a report to demonstrate the evidence before the audits or entities that monitor these activities. Although they are probably less formal, even hackers of the most basic type make preparations of a type before attacking their victims. Taking the time to prepare a safety test before execution is the only way to obtain good long-term results. The information in this article covers the importance of conducting vulnerability analysis and penetration tests, which must be taken into account, how to prepare and how to follow up, with the aim of implementing strategies that must be taken into account to strengthen computer security and cybersecurity in the companies.

Índice de términos **-** activo, amenaza, ataque, ciber seguridad, consecuencias, controles, información, impacto, políticas, probabilidad, riesgo, seguridad, vulnerabilidad.

I. INTRODUCCIÓN

La seguridad de la información y la informática, tienen que ser foco de las compañías para proteger su información tanto desde adentro de la compañía hasta saber cómo estar protegidos desde afuera. La información es considerada uno de los activos más importantes para una empresa, desde transacciones bancarias, aplicaciones, páginas web hasta bases de datos, son gestionados a través de sistemas computarizados. Un mal uso de estos sistemas, junto a empleados que no están capacitados, son un punto débil en las empresas, y un punto a favor no solamente para curiosos, sino también para la competencia y delincuentes.

Las entidades lideradas por sus dueños no saben que es un hacking ético, por ello es importante contar con espacios con la gerencia en donde puedan explicar y poner en contexto a los directivos de la importancia de utilizar una estrategia práctica y proactiva de defensa en materia de ciber seguridad y protección de la información.

La utilización de los conocimientos de seguridad en informática para realizar reconocimiento y pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de ser reportadas para tomar medidas sin poner en riesgo el sistema y dotar de mayor seguridad el entorno, se conoce como Ethical Hacking. Lo que se pretende es estar constantemente adelante de aquellos que intentan agredir haciendo pruebas y ataques propios con la ayuda de los expertos informáticos, los cuales han sido entrenados con mentalidad delictiva de los piratas informáticos así como en las diferentes técnicas de ataque digital. Sin duda es un procedimiento muy ventajoso para las empresas, ya

que pueden anticiparse a posibles delitos cada vez más comunes en la actualidad, no solo a nivel externo, sino a nivel de la propia empresa, ya que cada vez se dan más casos de hacking por parte de los propios empleados. Con un apropiado, oportuno y constante uso de un hacking ético, se pueden detectar quien está haciendo uso inadecuado de los sistemas de información de la entidad.

La filtración de datos confidenciales puede poner en juego a toda una empresa, sea ésta del tipo que sea, en el sentido en que puede afectar a sus cimientos y hacer tambalear sus buenos resultados y estabilidad, o cuanto menos, su imagen y reputación. Y es que de todos es sabido que la clave del éxito empresarial es uno de los secretos mejor guardados y protegidos.

Lo que se pretende con este artículo es dar a conocer de manera muy superficial como se debe realizar un hacking ético, que se debe tener en cuenta y como sacar el mayor provecho a esta estrategia de defensa.

II. LAS VULNERABILIDADES ESTÁN PRESENTES EN TODAS PARTES

Cada sistema informático será en algún momento vulnerable al ataque. Las vulnerabilidades a menudo se introducen erróneamente en un sistema por errores de código sobre la aplicación. Como no hay un sistema informático estándar, no hay errores estándar. Los sistemas y redes de computadoras modernas tienden a ser altamente sofisticados, a menudo también confían en hacer conexiones de red e intercambiar datos con sistemas y usuarios que no pueden ser controlados por una sola organización, empresa, estado-nación, etc. Dicha complejidad, y la falta de control general, hace que sea difícil implementar cualquier tipo de sistema de la manera más segura posible.

Otra razón importante por la que se pueden encontrar vulnerabilidades en la mayoría de los sistemas informáticos es que la prioridad principal de un sistema no es estar seguro. La principal prioridad de cualquier sistema es operar de una manera que satisfaga a su propietario y sus usuarios. Si eso se puede hacer de una manera segura, genial, pero agregar controles de seguridad a un sistema tiende a ser una idea de último momento.

Ningún sistema útil puede ser 100% seguro, pero encontrar el equilibrio adecuado entre los controles de seguridad y la facilidad de uso solo se puede hacer al saber cómo cobran vida las vulnerabilidades y cómo pueden abordarse.

Los hackers diseñan aplicaciones para explotar vulnerabilidades y afectar los sistemas, un gusano llamado slammer o sapphire fue el gusano más rápido de la historia, ya que se estima que hasta el 90% de los servidores vulnerables en línea se infectaron en diez minutos, esto ocurrió en enero de 2003, este gusano provocó una denegación de servicio en algunos servidores de internet e hizo dramáticamente más lento el tráfico de internet en general. Obligó a muchos sistemas de misión crítica a detenerse por completo explotando versiones vulnerables del servidor SQL de Microsoft y saturando el ancho de banda disponible. Además de la velocidad de infección sin precedentes del gusano, un aspecto interesante del gusano slammer es que se propago en un momento en que un parche para la vulnerabilidad que había sido explotada, Microsoft la tenía disponible seis meses atrás cuando se presentó este ataque. El parche “MS02-039” debería haberse instalado idealmente en los servidores vulnerables mucho antes de que el gusano comenzara su viaje caótico a través de internet.

La dura verdad es que la administración adecuada de parches habría salvado a muchas organizaciones de los efectos del gusano informático. Igualmente cierto es que, incluso sin una rutina sólida de administración de parches, una prueba de seguridad realizada hasta medio año antes del ataque del gusano slammer probablemente habría alertado a los propietarios del sistema sobre el problema.

III. ¿QUÉ ES UNA PRUEBA DE SEGURIDAD?

Las pruebas de seguridad son un tipo de evaluación de vulnerabilidad, el responsable de seguridad asume el papel de un pirata informático y hace todo lo posible por penetrar en el entorno de TI de la organización. El propósito de tal prueba es encontrar cualquier vulnerabilidad dentro del entorno de TI de una organización y cómo podrían explotarse las vulnerabilidades en un ataque de piratas informáticos en el mundo real. La idea subyacente es que una buena prueba de seguridad debe revelar como un atacante podría trabajar a través de los sistemas de la organización antes de que realmente suceda.

Con el conocimiento de cómo se pueden comprometer los sistemas de la organización, abordar los problemas encontrados es más manejable y rentable que simplemente esperar a que ocurra el accidente. Una entrega estándar al final de una prueba de seguridad es un informe que describe las vulnerabilidades encontradas durante las pruebas y cómo estas vulnerabilidades fueron explotadas. El informe también debe contener sugerencias sobre cómo corregir cualquiera de los agujeros de seguridad descubiertos.

IV. TIPOS DE HACKERS

Los piratas informáticos vienen en todas las formas, desde el estereotipo clásico del adolescente solitario que irrumpe en las computadoras de otras personas desde el sótano de la casa de sus padres, hasta soldados altamente calificados y disciplinados como parte de la defensa cibernética de una nación. Si bien es difícil categorizar adecuadamente cada tipo de pirata informático, las siguientes secciones son un intento de explicar lo que puede ser un pirata informático.

A. White hat Hackers

Este término se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas. Estos hackers cuando encuentran una vulnerabilidad inmediatamente se comunican con el administrador de la red para comunicar la situación con el objetivo de que sea resuelto lo más pronto posible.

B. Black hat Hackers

Este término se utiliza a menudo específicamente para los hackers que se infiltran en redes y computadoras con fines maliciosos. Los hackers de sombrero negro continúan superando tecnológicamente a los sombreros blancos. A menudo se las arreglan para encontrar el camino de menor resistencia, ya sea debido a un error humano o pereza, o con un nuevo tipo de ataque.

A diferencia de un hacker de sombrero blanco, el hacker de sombrero negro se aprovecha de las vulnerabilidades con el objetivo de destruir o robar información.

C. Personal patrocinado por el estado

A diferencia de otros tipos de piratas informáticos, los piratas informáticos patrocinados por el estado se esfuerzan por volar muy por debajo del radar para permanecer lo más secreto posible. Sin embargo, existen casos de ataques patrocinados por el estado que fueron todo menos secreto, independientemente del enfoque los ataques patrocinados por el estado están respaldados por fondos masivos. Es probable que este tipo de piratería se convierta en una parte cada vez más importante de la defensa militar de cualquier país.

D. Delincuentes informáticos

Debido a que la mayoría de las transacciones financieras involucran el procesamiento por computadora en algún momento, este es otro camino para que algunos delincuentes lleven su atención con el objetivo de robar el dinero ganado por la gente, usar computadoras en lugar de un cuchillo es otra opción para robar.

E. Hacktivistas

Un hacktivista es alguien que adopta un enfoque del siglo XXI para manifestarse frente al gobierno. Pero en lugar de pararse en medio de una manifestación grupal con pancartas y gritos de consigna, un hacktivista hace que su protesta se haga desde la comodidad de su hogar.

Tradicionalmente, el hacktivismo ha involucrado ataques de denegación de servicio contra sitios web

y modificación de sitios web, donde las páginas del sitio web han sido reemplazadas por mensajes que se adapta mejor a los hacktivistas. Dos aspectos clave que diferencian a los hacktivistas de otros tipos de hackers son que generalmente no buscan beneficiarse de sus proyectos de piratería, en segundo lugar, también quieren que el resultado de sus actividades de piratería sea visto por la mayor cantidad de personas posibles.

F. Insider

La amenaza de un ataque interno es quizás la más difícil de prever y gestionar, los mecanismos de control, como los controles administrativos, los controles físicos y los controles técnicos, probablemente no se impongan tan firmemente a un interno como lo son, o deberían serlo, a un extraño. Esto significa que una persona con información privilegiada podría salir por la puerta con los datos más valiosos de la organización sin tener que abrirse camino en ningún sistema ya que esa persona ya cuenta con el acceso requerido.

G. Scrip kiddies

Los script kiddies son aquellos piratas informáticos que no tienen conocimientos profundos de programación y seguridad informática pero siempre están intentando vulnerar la seguridad de los sistemas de información utilizando herramientas desarrolladas por los verdaderos hackers.

Se pueden encontrar hoy en día innumerables herramientas “script kiddies” que permiten a cualquier persona sin muchos conocimientos de informática jaquear un computador que tenga instalado un sistema con una vulnerabilidad conocida. Debido a la facilidad de uso de estos programas, hay cientos de miles (o millones) de los script kiddies en internet. Cualquier máquina que se conecta directamente a internet con una conexión de alta velocidad es probable que vea un buen número considerables de ataques contra su sistema utilizando estos script kiddies.

Si bien estos novatos pueden carecer incluso de la comprensión más fundamental de la seguridad, el resultado de sus acciones no debe ser subestimado de ninguna manera. Al igual que una persona que no sabe cómo funciona una pistola puede dañar a alguien, un script kiddies puede causar un gran daño a un sistema.

V. TIPOS DE PRUEBAS DE SEGURIDAD

En general, hay tres tipos de pruebas de seguridad: caja blanca, caja gris y caja negra. La idea detrás de la terminología monocromática es que cuanto más sepa el encargado de realizar el ethical hacking sobre los secretos internos de la compañía objetivo, más claro se vuelve el color.

Esto significa que cuando el encargado ha tenido acceso completo a los planos de red, a los diagramas de flujo de datos, a los algoritmos de hashing de contraseñas y a todas las demás cosas que permiten dejar en evidencia al sistema de destino, el tipo de prueba es una prueba de caja blanca. Posteriormente, esto también significa que cuando el responsable de llevar a cabo el ethical hacking tiene muy poca información sobre el objetivo previsto, se considera que es una prueba de caja negra.

Una prueba de caja gris lógicamente caería en algún lugar entre una caja negra y una prueba de caja blanca. Un ejemplo de prueba de caja gris sería la situación en la que se solicitó al profesional de seguridad que pruebe un equipo que ejecuta una aplicación web que acepta archivos de imagen como entrada para el procesamiento interno. Pero el tipo de formato de imagen que la aplicación web está configurada para aceptar y procesar, es desconocido para el profesional de seguridad al comienzo de la prueba.

Los tres tipos tienen sus respectivas ventajas y desventajas. Algunos de estos beneficios y limitaciones son los siguientes:

Prueba de caja negra

- Ventaja. La simulación más realista de un pirata informático que intenta romper o entrar en un sistema.
- Desventaja. Tiende a ser innecesariamente lento para el probador por lo tanto, costoso para el actor.

Prueba de caja blanca

• Ventaja. Muy eficiente para el probador.

• Desventaja. Por lo general, no es una simulación realista de un ataque de un pirata informático, ya que el probador tiene conocimiento interno del sistema.

Prueba de caja gris

• Ventaja. Un buen equilibrio entre un ataque de pirata informático realista y el ahorro de tiempo al proporcionar al probador un conocimiento interno de cómo funciona el sistema objetivo.

• Desventaja. Es posible que el probador no tenga acceso al código fuente de la aplicación de destino u otros datos importantes.

Cuanto menos sepa el probador de seguridad sobre el objetivo, mayor será el factor de conjetura y cuanto más sepa el probador de seguridad sobre el objetivo, menor será el factor de conjetura. El factor de conjetura puede verse como la cantidad de trabajo que debe realizar el evaluador de seguridad para descubrir la comprensión más básica del objetivo.

La figura 1 ilustra cómo el factor de conjetura aumenta a medida que el tipo de prueba de seguridad elegido pasa de las pruebas de caja blanca, a las pruebas de caja gris y finalmente a las pruebas de caja negra.

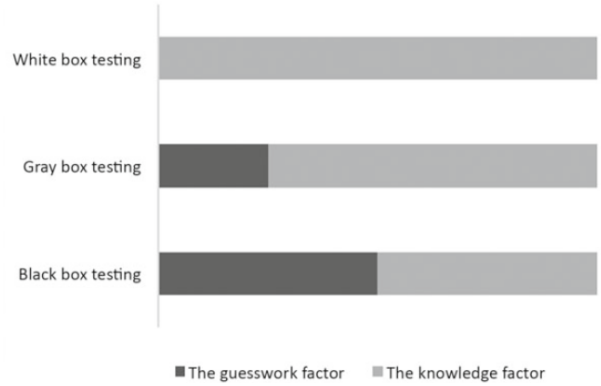

Fig. 1. Factor de conocimiento vs. Factor de conjetura
Fuente: From Hacking to Report Writing

VI. ¿QUÉ ES UNA AMENAZA?

Todo sistema está expuesto a amenazas, un centro de cómputo ubicado en un área donde los cortes de energía son comunes tendrá dificultades para cumplir con cualquier promesa de entrega continua. Un servidor que se ejecuta en una serie de discos duros que han alcanzado años más allá de su esperanza de vida diseñada es un desastre de pérdida de datos que está por suceder. Y un sistema orientado a internet que no se ha configurado para instalar automáticamente actualizaciones de seguridad es básicamente una invitación permanente a todo tipo de pirata informático imaginable.

Las amenazas a los sistemas informáticos se pueden dividir en las siguientes cuatro categorías:

1. Natural. La madre naturaleza hace lo que le plazca, como crear tormentas de nieve, tormentas eléctricas, huracanes, erupciones volcánicas, terremotos, maremotos.
2. Hecho por el hombre. Las acciones deliberadas de los seres humanos, como ataques de piratas informáticos, sabotaje y disturbios.
3. Técnico. Fallas relacionadas con sistemas técnicos como la pérdida de datos, falla de disco y cortocircuitos.
4. Sistema de suministro. Calefacción, ventilación, agua y cualquier otro tipo de sistema de suministro necesario para un sistema completamente operativo.

Sin embargo, la mayor amenaza para un sistema es una amenaza hecha por el hombre, más específicamente, una amenaza hecha por el hombre que involucra un ataque de hackers deliberado.

VII. ¿QUÉ ES UNA VULNERABILIDAD?

Antes de que aprendan a buscar vulnerabilidades, deben tener una comprensión sólida de lo que es una vulnerabilidad en el mundo de TI. Según la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA), una vulnerabilidad es "la existencia de una debilidad en el diseño o en una implementación que puede llevar a un evento inesperado e indeseable que comprometa la seguridad del sistema informático, la

red, la aplicación, o el protocolo involucrado".

Otra definición de qué es una vulnerabilidad proviene de internet engineering taskforce (IETF), "una falla o debilidad en el diseño, implementación, operación y administración de un sistema que podría ser explotada para violar la política de seguridad del sistema".

Una descripción más abstracta de lo que es una vulnerabilidad podría ser algo como lo siguiente, “acto que hace posible que alguien obligue a su computadora a hacer algo que no quiere que haga”. Algunos ejemplos menos abstractos incluyen los siguientes:

- Un complemento, extensión, complemento de navegador web que permite que un sitio web malintencionado infecte una computadora visitante con malware.
- Un recurso compartido de archivos que contiene documentos secretos a los que todas las personas en la red tienen acceso cuando no deberían hacerlo.
- Un servidor web público con la contraseña mal elegida como 12345678 para su interfaz administrativa.

La idea después de tener claro el concepto de qué es una vulnerabilidad, es identificar su posible impacto desde la perspectiva de la CID. El CID es un acrónimo que significa confidencialidad, integridad y disponibilidad, se utiliza para describir los componentes fundamentales de la seguridad de la información.

La confidencialidad tiene como objetivo evitar que la información confidencial caiga en las manos equivocadas. Los datos de la tarjeta de crédito, los registros médicos y los nombres de usuario, contraseñas son tres ejemplos de dicha información. Cuando se ha violado la confidencialidad de un sistema, el propietario de la información debe (o al menos debe) hacer todo lo posible por limitar el daño causado.

La integridad busca evitar que la información sea alterada por usuarios no autorizados. Un ejemplo sería un sistema de comercio electrónico en línea donde un cliente puede ver y cambiar la información de pedidos de otros clientes sin dejar rastro de hacerlo. Cuando se ha violado la integridad de un sistema, la información que procesa ya no puede ser completamente confiable.

Disponibilidad tiene como objetivo mantener la información accesible cuando sea necesario. Los cortes de energía o la denegación de servicio distribuida (DDOS) son dos ejemplos de cómo la disponibilidad de un sistema puede verse afectada. Cuando se viola la disponibilidad de un sistema, el sistema ya no puede realizar su función prevista.

La idea detrás del concepto de la CID es que los tres aspectos deben tomarse en consideración al tratar de mantener un nivel de seguridad aceptable. No todos los tres aspectos son igual de importantes para cada tipo de sistema, algunos sistemas pueden funcionar bien sin uno o incluso dos de ellos, pero los propietarios del sistema siempre deben considerar los tres.

En la figura 2 se puede ver una ilustración de la importancia del concepto del tridente CID (o CIA correspondiente al acrónimo en inglés). El palacio de securitas maxima, que debe ser sólido como una roca, está a punto de convertirse en una ruina debido a la vulnerabilidad que está acabando con la estabilidad del pilar de la disponibilidad. A pesar de que los otros dos pilares siguen intactos, el sistema en su conjunto ya no puede realizar su función prevista si el pilar de Disponibilidad dañado se deja desatendido.

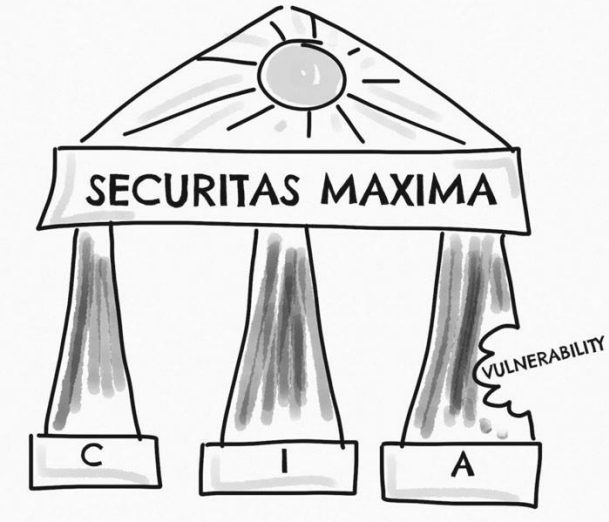

Fig. 2. Relaciones de riesgo, líneas de base y contramedidas
Fuente: From Hacking to Report Writing

La figura 3 busca ilustrar cómo encontrar y mitigar las imperfecciones del software es un proceso continuo, se le conoce como la rueda de la vulnerabilidad. A continuación una breve descripción de cada pieza de la rueda.

Software defectuoso. Un software en lanzamiento de un proveedor que contiene errores relacionados con la seguridad.

Hackers. Los hackers identifican los errores relacionados con la seguridad en el software.

Código de explotación. Los hackers desarrollan un código que puede explotar los errores en el software.

Respuesta del proveedor. El proveedor de software se da cuenta de la situación y emite un parche para corregir los errores.

Respuesta del usuario. Los usuarios aplican el parche a su sistema para que estén seguros por el momento.

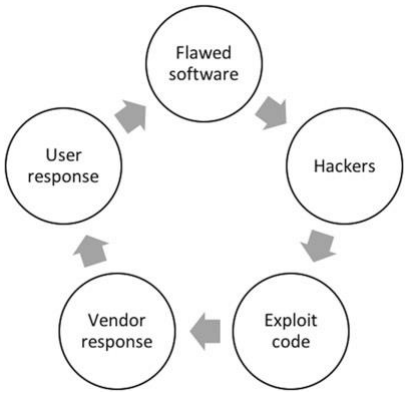

Fig. 3. Rueda de la vulnerabilidad
Fuente: From Hacking to Report Writing

Como se ilustra aquí, los hackers buscan sin cesar las vulnerabilidades de software para explotarlas. La forma más eficiente para que los usuarios realicen un seguimiento de los errores recientemente descubiertos en el software que utilizan es prestar atención a los anuncios de seguridad del proveedor y estar instalando los parches y actualizaciones de seguridad.

Algunos proveedores de software responden rápidamente a las vulnerabilidades que se encuentran en su software. De hecho, algunos proveedores de software informan a sus clientes tan pronto como se descubre una vulnerabilidad. Tal notificación a veces ocurre antes de que haya un parche disponible del proveedor para corregir el problema. La razón de esto es para que sus clientes puedan intentar mitigar el problema antes de que el proveedor de software lance un parche de corrección.

Los ejemplos para mitigar el problema antes de que un parche del proveedor esté disponible incluyen el ajuste detallado de los sistemas de detección de intrusos para identificar el tráfico de red sospechoso que podría estar relacionado con una vulnerabilidad, o para deshabilitar temporalmente el componente vulnerable hasta que un parche confiable esté disponible.

VIII. ¿CÓMO SE CLASIFICAN Y CALIFICAN LAS VULNERABILIDADES?

Todo sistema tiene, o pronto tendrá, vulnerabilidades, estas pueden ser explotadas por

los piratas informáticos, son tan diversas como los sistemas que afectan. La diversidad a veces puede dificultar la medición de la gravedad de una cierta vulnerabilidad. Igualmente desafiante es la tarea de categorizar las vulnerabilidades de una manera útil. Esto hace que, por ejemplo, sea sorprendentemente difícil responder a esta pregunta, ¿son los sistemas de la organización más seguros ahora que hace un año? O, ¿cuál de estas vulnerabilidades es la peor?

Una forma de tratar de resolver el problema es usar el sistema de puntuación de vulnerabilidad común (CVSS - Common Vulnerability Scoring System). El CVSS fue creado para proporcionar una manera de capturar las características principales de una vulnerabilidad y establecer una puntuación numérica que refleje su gravedad, así como una representación textual de esa puntuación.

Lo que esto significa es que puede aplicar el CVSS a una vulnerabilidad y obtener la calificación correspondiente. El puntaje de CVSS oscila entre 0 a 10. Cuanto más grave es una vulnerabilidad, mayor es el número.

Una buena manera de calcular un valor CVSS es usar la calculadora CVSS en el siguiente link: https://www.first.org/cvss/calculator/3.0
Se puede considerar que CVSS es la manera estándar de la industria de medir la gravedad de las vulnerabilidades, un evaluador de seguridad debe hacer un esfuerzo para usar siempre este sistema de puntuación cuando se reportan vulnerabilidades.

IX. MÉTRICAS DE SEGURIDAD

Los colores y los números son una excelente manera de visualizar y cuantificar el posible impacto de las vulnerabilidades. También es una excelente manera de organizar y priorizar el trabajo de manejo de ellos. Sí se usa en consecuencia y con el tiempo, el caso de las métricas de seguridad también le ayudará a comprender si nuestro trabajo relacionado con la seguridad hace que la organización sea más segura. Las métricas comunes incluyen lo siguiente:

- ✓ Número de incidentes.
- ✓ Tiempo medio entre incidentes de seguridad.
- ✓ Cobertura de escaneo de vulnerabilidad.
- ✓ Porcentaje de sistemas sin vulnerabilidades graves conocidas.
- ✓ Cumplimiento de la política de parches.
- ✓ Número de solicitudes.
- ✓ Porcentaje de aplicaciones críticas.
- ✓ Cobertura de pruebas de seguridad.
- ✓ Porcentaje de cambios con revisiones de seguridad.
- ✓ Porcentaje de cambios con excepciones de seguridad.

Los colores en las métricas normalmente indican el rango de tiempo en el que deben abordarse según la calificación de la vulnerabilidad, se puede utilizar un esquema de color monocromático como por ejemplo así:

- ✓ Gris oscuro: La vulnerabilidad debe abordarse en un plazo de 3 días.
- ✓ Gris: La vulnerabilidad debe ser tratada dentro de 7 días.
- ✓ Gris claro: La vulnerabilidad debe abordarse dentro de los 14 días.
- ✓ Blanco: No se debe realizar ninguna acción.

Por otro lado, no todas las vulnerabilidades pueden solucionarse al mismo tiempo, por lo que la codificación de colores que usted escoja puede ser útil para decidir dónde comenzar.

X. PRUEBAS DEL LADO DEL CLIENTE Y DEL LADO DEL SERVIDOR

La mayoría de las metodologías de pruebas de seguridad están enfocadas a encontrar las vulnerabilidades de seguridad en el lado del servidor. Si bien los dispositivos conectados a una red en la actualidad pueden tomar la forma de cualquier cosa, desde un reloj pequeño hasta un enorme grupo de computadoras, después de todo, es muy probable que los días en que los clientes o usuarios no eran más que terminales sin sentido que debían comunicarse con un servidor. Pero separar al atacante (como cliente) y la víctima (como servidor)

hace que sea más fácil explicar cómo se han llevado a cabo los ataques históricamente.

Es importante que recuerde sobre que una vulnerabilidad es una vulnerabilidad, independientemente de dónde se encuentre en el espectro cliente-servidor. También es importante recordar que los piratas informáticos pueden dirigirse a las aplicaciones vulnerables del lado del cliente para obtener más tarde los datos del lado del servidor.

XI. FASES DE UN ETHICAL HACKING

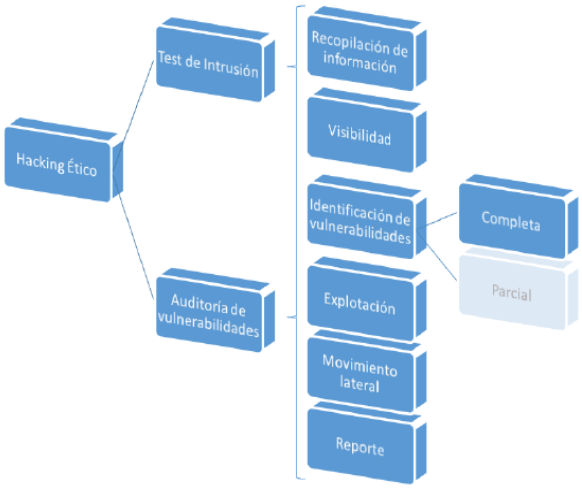

Fig. 4. Fases de un Ethical Hacking
Fuente: From Hacking to Report Writing

A. Recopilación de información

La fase de reconocimiento inicial es una faceta extremadamente importante de un ataque. Se centra en investigar la organización objetivo mediante información pública fácilmente disponible. Se puede obtener una gran cantidad de información sobre el objetivo con solo acceder a la página web de la empresa. Aquí se incluye información importante sobre el personal clave, así como otra información que puede utilizarse al intentar usar tácticas de ingeniería social. También se puede obtener información de los usuarios de la organización de fuentes abiertas, como por ejemplo de redes sociales como LinkedIn, Facebook, Twitter, etc.

Como cualquier persona puede acceder a este tipo de información, se puede recopilar una gran cantidad de información que puede ser utilizadas: revistas comerciales, motores de búsqueda web, artículos de periódicos, anuncios e incluso fuentes tan simples y retrogradas como un directorio telefónico. La información que al parecer no pueda tener algún sentido, puede resultar muy valiosa en combinación con otros datos aparentemente inofensivos. Con este levantamiento de información el atacante o los profesionales encargados de dicha labor, pueden comenzar a pintar una imagen más clara de la empresa objetivo.

B. Visibilidad

Se conoce también como la determinación del servicio o fase de exploración, es la fase en donde se intenta obtener información sobre los diversos servicios de escucha y los puertos que actualmente están operativos en la red del cliente. Aquí se hace una identificación de servicios, por lo general se debe hacer una inspección de red, el especialista determinará y descubrirá todas aquellas aplicaciones que ofrecen conexiones UDP o TCP en los sistemas auditados, conformando un mapa de los posibles puntos débiles que el equipo de intrusión utilizará como input.

Identificación de aplicaciones. Los auditores de seguridad proceden a identificar las aplicaciones que ofrecen sus servicios a la red de la entidad, determinando versiones y nivel de aplicación de parches de seguridad, todo ello con el objetivo de establecer una estrategia de intrusión y configurar adecuadamente las herramientas de auditoría.

Identificación de sistemas. Los servicios de los aplicativos están sustentados por el sistema operativo; por tanto, en esta fase el grupo de seguridad identificará hasta donde técnicamente sea posible, el sistema base, el nivel de parcheo y los subsistemas que pudieran dar soporte al principal.

Identificación de usuarios. Esta fase se focaliza en la identificación y preparación de la estrategia de intrusión vía phishing por correo electrónico, física en las instalaciones, mediante USB abandonados, interacción lógica con los equipos de los usuarios, etc.

A partir de esta información, el equipo de penetración debe poder determinar el tipo de sistema operativo que utiliza el cliente. Los diferentes sistemas operativos tienen características únicas en cuanto a que puertos tienen abiertos y facilita descubrir que sistema operativo está utilizando.

C. Identificación de vulnerabilidades

Se debe hacer una identificación de vulnerabilidades de red, como salida obtenida en los dos módulos anteriores el equipo de análisis está en disposición de establecer un listado de las posibles vulnerabilidades que pudieran afectar a los sistemas auditados, mediante el uso de herramientas automáticas y pruebas manuales, que afecten a entornos no Web.

Identificación de vulnerabilidades específicas web. Dada la importancia de este tipo de servicios se debe llevar a cabo pruebas específicas con herramientas orientadas a la revisión de la seguridad de esta tecnología.

El escaneo de vulnerabilidades emplea software que busca fallas de seguridad basadas en una base de datos de fallas conocidas, prueba los sistemas para detectar la ocurrencia de estas fallas y genera un informe de los hallazgos que una persona o empresa puede usar para reforzar la seguridad de la red.

Con la información suministrada en esta fase, un atacante puede capitalizar una vulnerabilidad pero por otro lado, cuando se hace de manera proactiva, el equipo de TI puede identificar oportunamente las vulnerabilidades y pueden tomar acciones al respecto para mitigar o eliminar los riesgos asociados a ellas.

D. Explotación

Explotación de vulnerabilidades. Una vez identificadas las vulnerabilidades en los sistemas, el quipo auditor deberá explotar dichas debilidades con el objetivo de ganar acceso a los sistemas bajo análisis.

Compromiso de los equipos de usuario. Esta fase perteneciente al test de intrusión trata de utilizar los equipos de usuarios comprometidos como pasarela a la información crítica de la organización. El objetivo de esta fase es establecer un punto de apoyo en la red interna del objetivo para ir a la fase final que corresponde a la escala de privilegios.

E. Movimiento lateral

Una vez que el equipo ya está en la red de la víctima, en esta fase el atacante intentara obtener privilegios administrativos o de nivel raíz en el sistema del cliente para obtener el control completo. Una vez obtenido el acceso a un sistema, el equipo auditor procederá a ejecutar la propagación al entorno interno de la entidad, para obtener acceso al mayor número de activos e información posible. La idea es simular las acciones de un atacante que forme parte de un grupo de amenazas persistentes avanzadas.

Restauración del entorno. Finalizado la auditoría de Hacking Ético y antes del reporte final es necesario volver a dejar los entornos comprometidos en su estado inicial, eliminando cualquier software adicional o puerta trasera habilitada en el sistema.

F. Reporte

Esta fase perteneciente al test de intrusión utilizará canales encubiertos para la ex filtración de evidencias tal y como los nuevos atacantes están realizando actualmente.

Reporte. Por último debe proceder a documentar el análisis realizado, incluyendo las evidencias tomadas como resultado del test. Este punto se detalla en mayor profundidad en el Plan de pruebas.

XII. CONCLUSIONES

Las pruebas de seguridad son el arte de evaluar la postura de seguridad de una organización al asumir el papel de hacker. Un analista de seguridad utilizará muchas de las mismas herramientas y técnicas que un hacker usaría para abrirse camino en el sistema. Sin embargo, una diferencia importante entre un ataque de hackers y una prueba de seguridad es que este último es parte de un proceso mayor para encontrar y mitigar problemas de seguridad.

Una prueba de seguridad bien planificada y bien

ejecutada puede ayudar a señalar cómo podría ocurrir una intrusión de hacker antes de que realmente ocurra. Un aspecto clave de las pruebas de seguridad es tratar de mantenerse un paso por delante de los delincuentes, al buscar proactivamente las vulnerabilidades dentro de un sistema y hacer algo al respecto.

El hacking ético es una parte fundamental dentro del mundo empresarial actual. La necesidad de las empresas de sentirse seguras en un entorno digital para poder ejercer su actividad de negocio hace que la aportación del hacking ético sea imprescindible para poder ayudar a mejorar dicha seguridad y por lo tanto, la actividad de negocio.

REFERENCIAS

[1] Robert Svensson. (2016). From Hacking to Report Writing - An Introduction to Security and Penetration Testing. Apress.
[2] OWASP Top Ten Project (2017) | OWASP. Sitio web: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[3] El hacking ético y su importancia para las empresas (2014, Febrero 28) | Enter CO. Sitio web: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/
[4] La inteligencia predictiva ayudará a mejorar la ciber seguridad (2018, Octubre 31) | Panda Security. Sitio web: https://www.pandasecurity.com/spain/mediacenter/seguridad/pablo-gonzalez-firma-invitada-ii/
[5] Common Vulnerabilities and Exposures (2018) | CVE. Sitio web: http://cve.mitre.org/
[6] Informe anual Pandalabs 2017 (2017, Noviembre) | Panda Security. Sitio web: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/11/Informe_Anual_PandaLabs_2017.pdf
[7] Blueprint: Building a better pen tester (2017) | SANS. Sitio web:https://blogs.sans.org/pen-testing/files/2017/12/PENT-PSTR-SANS18-BP-V1_web.pdf
[8] High-Value Penetration Testing (2018) | SANS Penetration testing. Sitio web: https://pen-testing.sans.org/value
[9] Blueprint: Building a better pen tester (2017) | SANS. Sitio web:https://blogs.sans.org/pentesting/files/2017/12/Blueprint_Wallpaper_Pre-EngRecon.png
[10] Current CVSS Score Distribution for All Vulnerabilities (2018) | CVE Details. Sitio web: http://www.cvedetails.com/

AUTOR

Diana Marcela Ariza Bonces nació en la ciudad de Bogotá, Colombia. Se graduó como Pedagoga en Electrónica en la Universidad Pedagógica y como Ingeniera electrónica en la Escuela Colombiana de Carreras Industriales, actualmente se encuentra culminando la Especialización en Seguridad Informática en la Universidad Piloto de Colombia.

Actualmente está laborando como analista de datos en Col pensiones.