INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Autor

Toledo Marcelo Alejandro

Licenciado en Sistemas.

Profesor Adjunto.

Seguridad de la Información.

Licenciatura en Sistemas de Información.

Facultad de Ingeniería y Tecnología.

Sede Formosa.

toledomarceloalejandro@gmail.com

Palabras claves: Hacking Ético–Vulnerabilidad – Malware –Ataques – Atacantes

Introducción

Una de las ventajas que la informática ha introducido a la vida del hombre es la capacidad de tener prácticamente todo al alcance de unos clics. Actualmente, las actividades de ocio, la comunicación, la formación de nuevas relaciones con otras personas pueden realizarse desde la comodidad de nuestra casa con distintos dispositivos como celulares, tabletas, computadoras o consolas de videojuegos. La economía también se ha transformado al mercado digital, permitiéndonos conseguir una gran variedad de productos y servicios, como así también llevar control de nuestros gastos e inversiones bancarias desde internet. Sin embargo, todo esto es posible gracias a que se transmite y almacena continuamente una inmensa cantidad de información sensible. Una vulnerabilidad en el sistema en el cual circula esta información sensible la dejaría desprotegida ante algún ente malintencionado. Es aquídonde entra en juego la seguridad de la información, la cual permite prevenir, detectar y corregir estas vulnerabilidades para evitar las posibles amenazas.

SEGURIDAD FÍSICA Y LÓGICA

La seguridad física refiere a los equipos informáticos como computadoras, servidores, dispositivos de networking, etc. Ésta se ve amenazada por eventos como los desastres naturales, robos y fallos en el suministro de electricidad por ejemplo.

La seguridad lógica refiere a las aplicaciones que se ejecutan en estos dispositivos. La misma se ve amenazada por virus, troyanos y malware, la pérdida de información y los ataques a las aplicaciones. (Roa Buendía, 2013)

La seguridad pasiva la integran aquellos mecanismos que permiten recuperarnos cuando ya ocurrió algún evento. Por ejemplo, la activación de un UPS ante un corte en el suministro eléctrico. La seguridad activa es la que protege frente a los ataques adoptando medidas de protección. Por ejemplo, un antivirus bloqueando una conexión sospechosa en Internet. (Roa Buendía, 2013)

Vulnerabilidad

Una vulnerabilidad es un defecto de software que puede ser aprovechado por un ente malintencionado. Al ser descubierta, podría crearse un nuevo software que se aproveche de esa vulnerabilidad, es decir un malware, para tomar el control del sistema o realizar operaciones no autorizadas, o un exploit.

Existen tres tipos de vulnerabilidades:

1. Las reconocidas para las que existe una corrección definitiva.
2. Las reconocidas para las que no existe una solución definitiva, pero existe una manera de sortear el problema de manera temporal.
3. Las no reconocidas, que son las peores al dejar expuesto al sistema durante largos periodos sin saberlo.

Los fabricantes solucionan estas vulnerabilidades con actualizaciones periódicas del sistema.

Malware

En cuanto al malware, existe una gran variedad de tipos, aunque se suelen resumir en:

1. Virus: su función es inutilizar el sistema infectado pudiendo actuar al momento o de manera programada.
2. Gusanos: su función es acaparar recursos del sistema, deteriorando su rendimiento paulatinamente.
3. Troyanos: su función es habilitar puertas traseras, o backdoors, que permiten a otro equipo tomar el control parcial o total del sistema infectado para intenciones malintencionadas.

Estos tres tipos de malware tienen en común un objetivo principal que es replicarse para contaminar la mayor cantidad de sistemas posibles. Para evitar esto hay que instalar software únicamente de sitios de confianza, evitar sitios de dudosa actividad o procedencia y mantener actualizados nuestros sistemas operativos y actualizaciones. Además, se recomienda contar con software anti-malware en caso de ser necesaria una protección activa. (Roa Buendía, 2013)

Tipos de Ataque y Técnicas de Ataque

Una vez que un ente malintencionado decide perpetrar un ataque a un sistema, puede hacerlo de distintas maneras:

1. Por interrupción, cortando la prestación de un servicio, como un servidor web.
2. Por intercepción, accediendo a los canales de comunicación y sustrayendo la información que se está transmitiendo.
3. Por modificación, alterando la información para que ocasione alguna reacción anormal en su destino.
4. Por fabricación, haciéndose pasar por el destinatario de la transmisión, engañando para obtener información valiosa.

Para lograr sus objetivos, un atacante emplea varias técnicas. Entre las mismas se encuentran:

1. La Ingeniería Social, es una técnica donde el atacante se vale del conocimiento sobre aspectos de la su víctima, como fechas de cumpleaños, el nombre de sus familiares o sus deportistas favoritos para intentar dar con una contraseña. También implica valerse de la confianza de la víctima para acceder a su sistema y alterarlo para su beneficio.
2. El Phishing, es una técnica de ataque en línea, generalmente a través de correo electrónico o páginas web, donde el atacante se hace pasar por una persona que tenga relación con alguna empresa o servicio a la que la víctima conoce, solicitando información sensible que luego utilizará para otros fines.
3. Los Keyloggers, son herramientas de hardware o software que toman nota de todo lo que la víctima ingresa por teclado en el sistema y luego envía dicha información en intervalos programados hasta el atacante.
4. Los Ataques de Fuerza Bruta, donde el atacante prueba todas las combinaciones posibles una a una hasta dar con una contraseña o clave de acceso, muchas veces valiéndose de diccionarios de contraseñas comunes y conocidas. Si bien ningún sistema es inmune a este ataque, utilizar contraseñas largas, variando caracteres y símbolos y cambiándola periódicamente hace que este tipo de ataques sea inviable ya que tomaría años o siglos para dar con una contraseña segura mediante un ataque secuencial, aún con las computadoras más potentes.
5. El Ransomware, es un software que encripta particiones de disco enteras solicitando un pago, a menudo a través de criptomonedas, para devolver la información.
6. El Spoofing, es una técnica que implica suplantar la identidad de un componente del sistema para fines criminales.
7. El Sniffing, es una técnica donde el atacante se infiltra en la comunicación entre su víctima y destinatario, accediendo a sus conversaciones.
8. La denegación de servicio (DoS) y la denegación distribuida de servicio (DDoS), que consiste en inutilizar un servidor de un servicio enviando una gran cantidad de peticiones falsas acaparando todo el tráfico y recursos del mismo. Puede realizarse desde un solo equipo, en el caso de la DoS, o desde una red de equipos, como es el caso de la DDoS.

Tipos de Atacantes

Al atacante de un sistema informático se lo conoce comúnmente como hacker, sin embargo, el concepto de atacante es más amplio y se pueden distinguir, entre otros:

1. Hacker. Es quien realiza el ataque a un sistema solo por el reto que impone. Si tiene éxito, suele dar aviso a los desarrolladores sobre las fallas del sistema para que estas sean solucionadas.
2. Cracker. Es quien ataca a un sistema con fines malintencionados, como robo o alteración de información, suspensión de servicios, extorsión, etc.
3. Script Kiddie. Es un aprendiz de hacker o cracker, es peligroso tanto para un sistema como para él mismo, ya que la falta de experiencia en la materia no lo hace medir los peligros y consecuencias de sus actos.

4. Programador de malware. Es un programador experto capaz de aprovechar vulnerabilidades de algún software para generar otro software que le permita atacar.
5. Sniffer. Es un experto en protocolos de comunicaciones, opera capturando tráfico para analizar la información sensible que este contiene.
6. Ciberterrorista. Es un cracker con intereses políticos o económicos a gran escala.

Hacking Ético

El hacking ético, también conocido como prueba de vulnerabilidad y penetración, se vale de las mismas herramientas que los hackers criminales utilizan, solo que, con una diferencia fundamental. En este caso no se habla de una víctima sino de un "objetivo profesional". El objetivo del hacking ético es descubrir vulnerabilidades desde el punto de vista de un atacante criminal para mejorar la seguridad de un sistema. Las pruebas de vulnerabilidad y penetración son parte de un amplio programa de gestión de riesgos que impulsan mejoras en la seguridad. Estas pruebas también sirven para que los vendedores puedan especificar que la seguridad de sus productos de software es óptima y legítima.

Según lo mencionado en el párrafo anterior, es normal la confusión entre el hacking ético y la auditoría de seguridad. Estos dos conceptos se diferencian en sus objetivos. La auditoría de seguridad implica comparar las políticas de seguridad de una compañía con las prácticas que esta está llevando a cabo en la realidad. Su intención es validar que existan controles de seguridad y, a menudo, implica revisar procesos del negocio. Es, entonces, un listado de requerimientos que se deben cumplir para lograr una certificación. (Beaver, 2018)

HISTORIA

El término hacking ético se oyó por primera vez en 1995 por parte de John Patrick, vicepresidente de IBM, sin embargo, el concepto es todavía más antiguo.

El termino hacking, en el sentido amplio, proviene del Instituto Tecnológico de Massachusetts (MIT). Durante la década del 60, los estudiantes de ingeniería del MIT lo utilizaban para describir varios métodos de optimización de sistemas y equipos. En ese entonces no era más que un hobby para gente muy inteligente. Por lo tanto, la idea del hacking ético precede a la del hacking criminal.

Al crecer la popularidad de las computadoras en los años 70, también creció la cantidad de personas expertas en lenguajes de programación que empezaron a ver beneficios a la hora de probar un sistema para evaluar su potencial. Al mismo tiempo, empresas y dependencias gubernamentales empezaron a ver el beneficio que podría traer tener este tipo de expertos que pudieran encontrar debilidades en sus sistemas.

Durante los años 80 y los 90 se empezó a escuchar el término hacker asociado a la actividad delictiva. La computadora personal ya era una herramienta muy popular tanto para personas como para las empresas, lo que significaba que ya existieran grandes cantidades de información sensible almacenada en ellas. Los hackers descubrieron el beneficio de robar esa información para actividades fraudulentas o de espionaje.

Estos son los llamados hackers de sombrero negro, quienes solo utilizan sus destrezas para fines malintencionados y de los que más se oye en los medios.

Los hackers de sombrero blanco utilizan las mismas técnicas que los de sombrero negro, pero lo hacen para encontrar vulnerabilidades en un sistema para solucionarlas o dar aviso a las empresas para que tomen medidas al respecto.

Para desempeñar correctamente, los hackers éticos son contratados en secreto por las empresas. Esto les permite trabajar como lo haría un hacker criminal para intentar hackear un sistema valiéndose de técnicas de penetración, ingeniería social y pruebas de fuerza bruta. (Bradley, 2019)

TIPOS DE HACKERS

Un hacker puede ser cualquier persona que utiliza el conocimiento sobre hardware y software que ha adquirido para atravesar medidas de seguridad de una computadora, red o dispositivo. En sí mismo, el hacking no es ilegal a menos que no se cuente con el premiso explícito de la persona o empresa.

Metafóricamente se clasifican a los hackers según un color de sombrero, en blancos, grises o negros, una terminología que data de los Spaghetti Western donde los buenos usaban sombreros blancos y los malos sombrero negro.

Hackers de Sombrero Negro

Como todos los hackers tienen gran conocimiento sobre el compromiso de sistemas de computadoras, redes de comunicación y el salto de medidas de seguridad. También son el tipo de hacker que programa malware y virus.

Su motivación es económica o personal, y su experiencia varía entre principiantes y expertos. Por lo general no solo se limitan al robo de información, también la alteran para otros cometidos maliciosos.

Hackers de Sombrero Blanco

Tienen el mismo nivel de conocimiento y experiencia, pero optan por utilizarlo para el bien. Son los también llamados hackers éticos, y a menudo son empleados por empresas para identificar vulnerabilidades en sus sistemas.

Se valen de las mismas tácticas que los hackers de sombrero negro, pero cuentan con el permiso de los propietarios del sistema. Realizan pruebas de penetración, evaluación de vulnerabilidades y de sistemas ya instalados. Existen cursos para convertirse en un hacker ético certificado.

Hackers de Sombrero Gris

Este tipo de hackers son una mezcla entre los dos anteriores. Buscan vulnerabilidades en un sistema sin el permiso del propietario, pudiendo reportarlas y ofreciendo repararlas, a menudo bajo cierto costo. De no lograr su cometido, pueden hacer públicas las vulnerabilidades para todo el mundo.

Los hackers de sombrero gris no suelen tener intenciones maliciosas, solamente quieren ser remunerados por sus hallazgos. A pesar de que la mayoría no haga públicas las vulnerabilidades que han hallado, o que no provoque daños en los sistemas en cuestión, esta sigue siendo considerada una forma ilegal de hacking. (Bradley, 2019)

Bibliografía

- Beaver, K. (2018). *Hacking for Dummies* (Sexta ed.). Hoboken, Nueva Jersey, Estados Unidos de América: John Wiley & Sons, Inc. Recuperado el 20 de Marzo de 2019.
- Bradley, P. (2019). *Hacking with Kali Linux: A Comprehensive, Step-By-Step Beginner's Guide to Learn Ethical Hacking With Practical Examples to Computer Hacking, Wireless Network, Cybersecurity and Penetration Testing.*Estados Unidos de América: Publicación Independiente. Recuperado el 20 de Marzo de 2019.
- Roa Buendía, J. F. (2013). *Seguridad Informática*. Madrid: McGraw-Hill Interamericana de España S.R.L. Recuperado el 20 de Marzo de 2019.