TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN

Ataques de red, hardware y software

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

Tabla de contenidos

Aprendizaje esperado 5

Introducción 6

1. Introducción al Ethical Hacking 6

1.1 Visión general de la seguridad de la información 6

1.2 Terminología esencial del hacking 8

1.3 Elementos de la seguridad de la información basado en los principios del ethical hacking 10

1.4 Triángulo del ethical hacking 10

2. Vectores de Ataques y Vectores de amenazas en seguridad de la información 14

2.1 Motivos, metas y objetivos de los ataques de seguridad 14

2.2 Ranking de vectores de ataques en seguridad de la información 14

2.3 Categorías en las amenazas de seguridad de la información 16

2.4 Tipos de ataques a los sistemas 17

3. Definiciones de Hacker 26

3.1 Fases del Hacking 28

4. Controles de seguridad 29

4.1 Aseguramiento de la información 29

4.2 Programa de administración de la seguridad de la información 29

4.3 Network Security Zoning 29

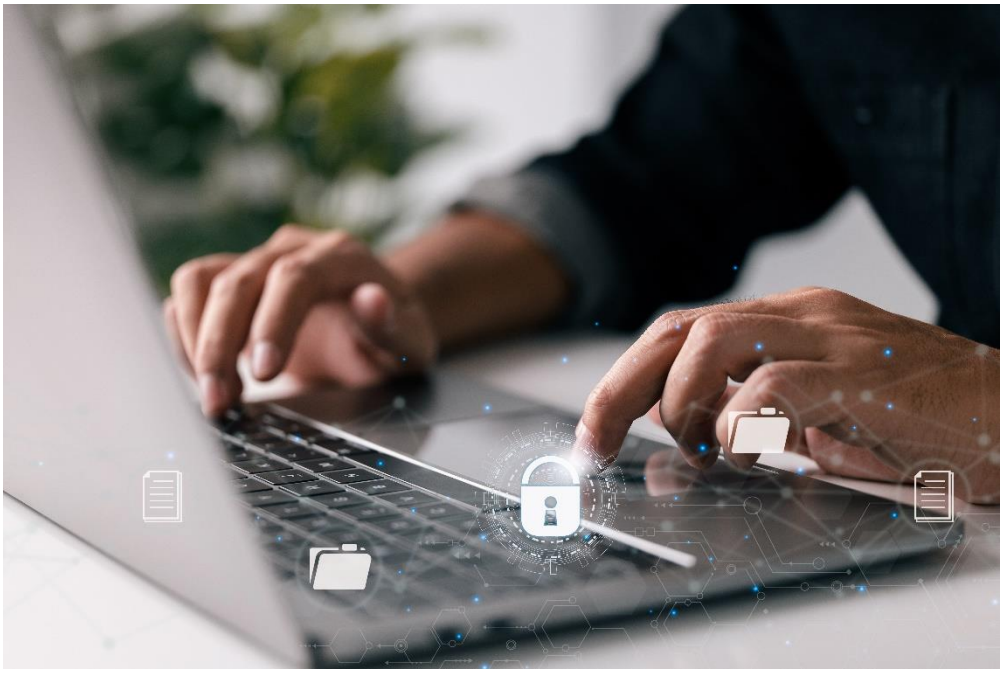
4.4 Políticas de seguridad de la información 30

Cierre 31

Referencias 32

Aprendizaje esperado

Identifican conceptos relacionados a Ethical Hacking, considerando estándares de la industria.



Introducción

En esta semana, se estarán revisando los diferentes conceptos de ethical hacking desde una visión general de la seguridad de la información, identificando los distintos vectores de ataque y amenaza que puede realizar un hacker de acuerdo a su clasificación. Además, se podrán observar los distintos controles de seguridad mediante el establecimiento de políticas programadas.

1. Introducción al Ethical Hacking

1.1 Visión general de la seguridad de la información

En los últimos años, nos hemos hecho cada día más dependientes de la tecnología. Esto es válido tanto para una organización que necesita desarrollar sus actividades habituales o bien para uso personal, que se traduce en una importante dependencia de esta. Si pensamos en los inicios del acceso masivo a internet hace bastantes años atrás, una caída de internet o un mal funcionamiento eran algo molesto, pero no crítico. En la actualidad, perder acceso a la red significa que una organización queda prácticamente inutilizada.

Día a día la información que se almacena en la red crece exponencialmente, junto al crecimiento de las telecomunicaciones y el intercambio de información utilizando medios digitales, el uso las

plataformas comerciales electrónicas y las transacciones bancarias nos dan un claro ejemplo de hiperconectividad.

Teniendo en cuenta todo lo anterior, ser afectados por robo o pérdida de información cada vez es más frecuente. Muchos ciberdelincuentes utilizan la tecnología como medio para obtener información de interés. Dentro de estas herramientas se encuentran los malware, pero también existen programas diseñados para el robo de información y por ello los profesionales de la seguridad deben estar atentos, ante nuevas amenazas.

Por lo expuesto es extremadamente necesario establecer prácticas y herramientas orientadas a proteger la infraestructura informática y la información que ésta contiene tanto de personas como de organizaciones, todo esto se conoce como seguridad informática.

Para poder comenzar a tratar temas relacionados con la seguridad informática, es importante conocer exactamente a qué nos referimos cuando hablamos de este concepto. Si nos remitimos a la bibliografía existente y a la información que circula por internet para su consulta, vamos a ver que existe una infinidad de definiciones y conceptos de seguridad informática.

Nos vamos a centrar en un concepto elegante y acertado para lo que vamos a estudiar: la seguridad informática es un conjunto de medidas de prevención, detección y corrección que se orientan a proteger la confidencialidad, la integridad y la disponibilidad de los recursos.

1.2 Terminología esencial del hacking

Hacker: para entender este concepto hay que considerar que existe mucha desinformación ya que muchas personas piensan que un hacker es una un criminal o una persona malintencionada que anda por el mundo robando datos, destruyendo la reputación de las empresas y un sinfín de actos delictivos. Si bien, efectivamente existen ciberdelincuentes, un hacker por lo general es una persona curiosa, autodidacta, que adquiere conocimientos sobre ciberseguridad constantemente, para darles un buen uso como detectar fallos de seguridad en organizaciones, y así colaborar en la corrección de estos para poder mejorar la seguridad y evitar que los ciberdelincuentes, que son como se les llama a las personas que usan su conocimiento sobre ciberseguridad para cometer actos delictivos, se aproveche de esas vulnerabilidades y las aproveche para un beneficio propio.

Amenaza (Threat): se le llama amenaza al posible incidente que puede generar una brecha de seguridad. Cuando se realiza un análisis de seguridad son los hackers éticos quienes buscan y dan prioridad a las amenazas. El uso malicioso de software y las técnicas de hacking en sí mismas son amenazas de seguridad para la información de una organización.

Vulnerabilidad: es la presencia de un error en el diseño de la lógica, de un defecto de software, o una falla en una aplicación que puede conllevar a un evento inesperado e indeseable al ejecutar instrucciones malintencionadas o perjudiciales para el sistema.

Ataque: un ataque se produce cuando un sistema posee una vulnerabilidad. Por lo general estos se realizan a través de un exploit. Los hackers éticos poseen herramientas para lograr detectar vulnerabilidades y a partir de esa información prevenir posibles ataques.

Hack Value: el término hack value se refiere a un objetivo que denota atractivo, interés o algo que vale la pena. El valor de este objetivo describe el nivel de atracción de estos para el hacker.

Ataque de día cero: es el uso de un exploit de día cero para causar daños o robar datos a un sistema afectado por una vulnerabilidad.

Exploit: es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. Por lo general, los exploits toman la forma de un programa de software o una secuencia de código previsto para hacerse con el control de los ordenadores o robar datos de red.

Daisy Chaining: Los procesos de producción en plantas interconectadas a menudo se organizan en un patrón lineal. Este tipo de topología también se llama cableado de bus o Daisy Chain. Significa que varios componentes están conectados en serie uno tras otro.

Doxxing (o doxing): es la revelación de la información personal confidencial de alguien mediante su publicación en línea. Los hackers lo utilizan para acosar, amenazar o vengarse de alguien en línea.

1.3 Elementos de la seguridad de la información basado en los principios del ethical hacking

En la actualidad la información constituye uno de los activos más preciados de las organizaciones ya que están expuestos a amenazas de diferentes tipos como es el caso de robos, incendios, fallas de hardware, virus, etc. Entonces las organizaciones deben proteger estos activos ya que corresponde a activos críticos de las empresas. Una de las medidas más importantes para la protección de los datos es establecer las políticas adecuadas para la protección de la información.

1.4 Triángulo del ethical hacking

A la hora de elaborar un pentesting es necesario saber a quién o qué evaluaremos, ya que la respuesta a esas preguntas guiará el tipo de desarrollo que deberemos seguir a fin de que nuestra auditoria se adapte de mejor forma a la realidad.

Partiendo de allí, es pertinente hablar de un triángulo muy curioso, que básicamente busca aclarar esas dudas para el desarrollo, el triángulo FSU, un acrónimo de Funcionalidad-Seguridad-Usabilidad, tres cosas fundamentales a la hora de realizar una auditoria.

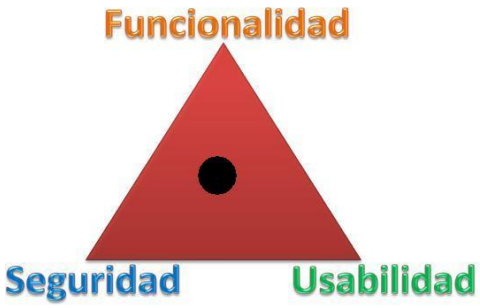


Figura 1. Triangulo de ethical hacking

Fuente: culturatics.wordpress.com (s.f)

Dependiendo de a quién o qué evaluaremos, uno de estos tres aspectos podría explotarse más que otro, el punto negro que está en medio del triángulo define que tan seguro, funcional y usable es nuestra auditoria. Dicho punto puede movilizarse a una esquina del triángulo según sea la necesidad, pero mientras más se acerca a una esquina evidentemente se aleja de las otras.

Seguridad: es lo referido a la protección de los datos y, especialmente, al procesamiento que se hace de los mismos, con el objetivo de evitar la manipulación de información y procesos por personas no autorizadas.

Funcionalidad: se refiere a la capacidad de un dispositivo o programa de computador de llevar a cabo una determinada tarea (p. ej. «el programa incluye la funcionalidad reloj»)

Usabilidad: ISO/IEC 9126 "La usabilidad se refiere a la capacidad de un software de ser comprendido, aprendido, usado y ser atractivo para el usuario, en condiciones específicas de uso". Esta definición se refiere a los atributos internos y externos del producto, los cuales contribuyen a su funcionalidad y eficiencia.

Triada CID

Figura 2. Triada CID

Fuente: b-one-informatica.blogspot.com (s.f)

La imagen anterior es conocida como la "Triada CID" o el triángulo de la ciberseguridad, representa los tres pilares de la información.

Confidencialidad: la confidencialidad es la propiedad que asegura el acceso a la información solo a aquellas personas o sistemas que cuenten con la debida autorización.

Por ejemplo, cuando realizamos una transacción en línea nos encontramos generalmente con que tenemos que validar nuestras credenciales: Banco con que se realizará la transacción, usuario y contraseña, número de tarjeta, medio de validación (tarjeta de coordenadas o generador de código). Si existe una vulneración y acceso a estos datos se ha perdido la confidencialidad. Esto puede lograrse de varias maneras, incluso con formas menos sofisticadas como una mirada por encima del hombro.

Integridad: cuando hablamos de integridad nos referimos a mantener los datos libres de modificaciones no autorizadas o de adulteraciones. La integridad es el mantener inmaculada la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Si un miembro de la organización, programa o proceso (por accidente o, mala intención) altera o elimina parte de la información, estamos hablando de perdida de Integridad.

Así mismo, mediante protocolos, se puede lograr que el contenido permanezca inalterado y que sea modificado solo por personal autorizado. Esta modificación debe ser registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad, como por ejemplo firmas digitales o revisión de metadatos.

Disponibilidad: al hablar de disponibilidad nos referimos a la característica, cualidad o condición de la información que debe estar a disposición de quienes están autorizados a acceder a ella, ya sean personas, procesos o aplicaciones. Dicho de forma más simple, la disponibilidad es acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Se deben establecer protocolos para el resguardo de la disponibilidad de la información que deben ajustarse a normas y estándares internacionales.

2. Vectores de Ataques y Vectores de amenazas en seguridad de la información

No todos los ataques son iguales, existe una infinidad de ataques informáticos en la práctica y todos los días surgen otros nuevos por el avance de la tecnología. En este punto, nos vamos a centrar, desde el punto de vista técnico, en los ataques al sistema operativo, a las aplicaciones, a las configuraciones y a los protocolos.

2.1 Motivos, metas y objetivos de los ataques de seguridad

Los hackers suelen actuar por distintas razones. Vulnerar la seguridad informática en ocasiones obedece al deseo de obtener un beneficio monetario, a un medio de protesta por alguna causa, entretenimiento personal, ego o a una combinación de estos factores. Cualquiera de ellos puede ser la motivación de los hackers.

2.2 Ranking de vectores de ataques en seguridad de la información

En la actualidad los 4 vectores de ataques más utilizados:

El correo electrónico: el correo electrónico es la vía de ataque más utilizada para la propagación de virus y la realización de ingeniería social. Aquí se realizan desde campañas de spam hasta ciberataques personalizados de Phishing.

La mejor forma de evitar este tipo de ataques de generar cultura de seguridad informática dentro de la organización, con una capacitación constate de los miembros de esta.

Ataque con macros: los ataques con macro son vectores de ataque muy comunes en ciberseguridad. Estos malware se insertan en el código de archivos de Office, como documentos de Word o Excel, y se ejecutan cuando el usuario hace clic en el botón «habilitar edición» del documento.

El código escrito en lenguaje Visual Basic inserto abre la puerta para la instalación de código malicioso cuando la víctima abre el documento. Los ataques con macro son sumamente comunes, generalmente tienen consecuencias graves, como el robo persistente de información.

Descarga de archivos maliciosos: es muy frecuente que un usuario inexperto instale softwares piratas en su computador para para no pagar licencia. Sin embargo, cuando lo hace no sabe es que estas descargas son uno de los tipos de vectores de ataque más comunes en ciberseguridad. Por medio de estos programas, descargados de fuentes desconocidas, suelen instalar malwares que utilizan la capacidad de procesamiento del host para ejecutar tareas como, por ejemplo, minar

criptomonedas, o hacer un ataque de denegación de servicios distribuido (DDoS).

Ingeniería social: ¿para qué esforzarse en diseñar software si puedes aprovechar el fallo humano? Esta es la premisa de la ingeniería social, que se centra en manipular al usuario para que entregue credenciales y accesos voluntariamente. Este es uno de los vectores de ataque más comunes en ciberseguridad. Hablaremos con mayor profundidad de este tipo de vector más adelante.

2.3 Categorías en las amenazas de seguridad de la información

De forma general, podemos agrupar las amenazas informáticas en dos bloques principales:

- Amenazas físicas
- Amenazas lógicas

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- Personas
- Programas o aplicaciones específicas
- Catástrofes naturales

2.4 Tipos de ataques a los sistemas

Ataques al sistema operativo

El ataque al sistema operativo es el más clásico que se puede sufrir, en razón de que la búsqueda de fallas se centra en el propio sistema operativo, que es la base de todo el resto del software que se encuentra instalado sobre él y, a su vez, es el almacenaje de la información. Por eso, muchas veces los hackers toman control del sistema operativo antes de concretar el ataque puntual.

Tenemos tres líneas principales de ataque de este tipo, en razón de que globalmente existentes sistemas operativos principales:

1. En primera línea está Windows, el más atacado. Ya desde sus inicios, fue centro de ataque debido a su masificación y a lo simple que era acceder a su núcleo, incluso sin contar con su código fuente.

2. Los sistemas operativos Linux o derivados de UNIX, que, por tener código abierto, son un punto de ataque peor que Windows (cuando sufre intrusión), ya que los ataques son posibles también a nivel de código.

3. Los sistemas operativos MacOS, que sufren ataques en menor medida, por ser menos populares. De todos modos, últimamente son blanco de los atacantes por haberse extendido a una variedad considerable de dispositivos (teléfonos, tabletas, computadoras), lo que

hace que año a año se descubra un mayor número de vulnerabilidades y los atacantes las exploten.

Ataques a las aplicaciones

En el caso de las aplicaciones, la variedad de ataques es mucho mayor, ya que existen miles y miles de aplicaciones de software y programas de todo tipo disponibles para su utilización. Cuando hablamos de ataques a las aplicaciones, se debe tener en cuenta como sucede con los sistemas operativos y cuán masivas son estas. Los atacantes siempre buscan aplicaciones de uso masivo, ya que hay documentación de ataques a estas y los fallos que poseen ya se conocen en el ambiente de los atacantes. Además, al tener un uso masivo, tienen más llegada a las personas y empresas, con lo cual tienen mayor potencial el ataque. Por eso se dice que un programa utilizado por miles de millones de personas va a ser mejor objetivo que uno empleado por pocos usuarios.

El objetivo de atacar una aplicación es ampliar la superficie de ataque de un sistema, por lo que siempre es indispensable evitar instalar software que no se requiera. Este es uno de los principales puntos de la seguridad informática.

Existen casos donde se falsifican programas que, a simple vista, poseen las mismas funciones, pero dentro tienen fallos en la operatoria que sirven para comprometer el software base y llevar adelante un ataque informático a gran escala.

Es importante siempre tener en cuenta con qué privilegios se ejecutan las diferentes aplicaciones. De esto dependerá cuán grave pueda ser el ataque directo al sistema. Existe la posibilidad de realizar un ataque a una aplicación y luego escalar privilegios hasta llegar y comprometer el sistema operativo base. Si los privilegios ya son elevados desde un primer momento, van a ser utilizados para realizar un ataque más grande y a otro nivel de una forma más sencilla.

Es importante destacar que, por medio del ataque a cualquier programa o aplicación, se genera un ataque mucho más grande, ya que los atacantes utilizan como puerta de entrada los sistemas de las organizaciones de software de uso popular.

Ataques a las configuraciones

Las configuraciones pueden ser del sistema operativo o de las aplicaciones, y constituyen otro punto sensible, ya que, por más seguro que sea un software, una mala configuración puede transformarlo en totalmente inseguro y fácil de manejar por un atacante. Vamos a ver un ejemplo pequeño, pero muy común.

Pensemos en un software antivirus, si se configura de forma deficiente, su función sería cumplida en forma escasa o poco efectiva, lo que daría como resultado que una buena herramienta de software sea una mala solución y, por ende, una brecha de seguridad y puerta de entrada para un atacante.

Por eso podemos decir que ni siquiera las herramientas de seguridad o los softwares de protección son 100 % fiables solo por su función. Para minimizar al máximo los problemas de seguridad, el profesional de seguridad informática debe realizar configuraciones extra y adecuadas, para evitar que se produzcan ataques graves. Un atacante siempre, como primera medida, trata de aprovecharse de las configuraciones estándar de las aplicaciones, los equipos informáticos, los dispositivos de red, etcétera.

Vamos a suponer que un sitio de administración web se instala con las credenciales por defecto, es decir que se realiza la instalación y se dejan las contraseñas que vienen de fábrica, sin modificación alguna. Entonces ingresa un atacante, que conoce cuáles son las credenciales por defecto, e ingresa sin ningún tipo de esfuerzo a nuestros sistemas. Este es un error de configuración que provoca un ataque a un sistema. A su vez, se debe tener en cuenta que en internet existe una gran cantidad de sitios que recopilan información de contraseñas por defecto de programas, aplicaciones y dispositivos, y que estos sitios son muy utilizados por atacantes para acortar caminos.

Ataques a protocolos

El ataque a protocolos es otro problema, dentro de la seguridad informática de una organización, menos frecuente, pero más grave si contamos con errores en los protocolos. Esto implica que sin importar la implementación que se haya realizado, el sistema operativo que se esté utilizando en la organización, ni la configuración, algo que se componga

del protocolo erróneo se puede ver afectado. Veamos un ejemplo clásico. El conocido protocolo TCP/IP (transmission control protocol (protocolo de control de transmisión) /internet protocol (protocolo de internet) es un paquete de protocolos efectivos y flexibles que perduran en el tiempo y continúan utilizándose. Cuando nació este protocolo, no era muy utilizado y tampoco contenía medidas de seguridad, pero con el tiempo no solo continuó su utilización, sino que se comenzó a usar para fines que no habían sido pensados, hasta transformarse en un arma de ataque.

Si bien este protocolo se fue ajustando con el tiempo para mitigar los posibles ataques, es un protocolo de uso tan masivo que vuelve imposible su reemplazo, por lo que es susceptible de ser atacado. Si bien no constituye un verdadero error, hay que tenerlo en cuenta. El diseño del protocolo TCP/IP es altamente efectivo, al punto de que el modelo de referencia OSI (interconexión de sistemas abiertos) se basa en él.

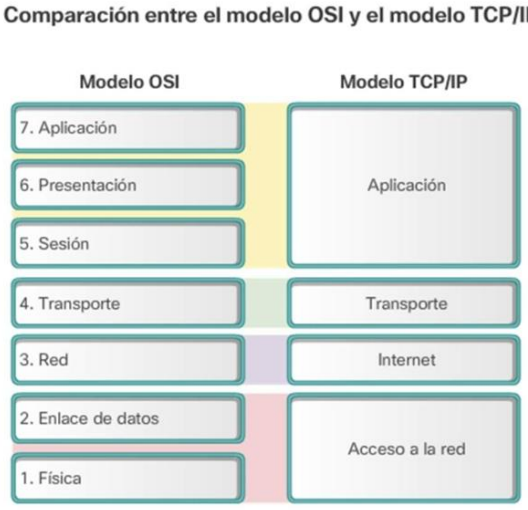


Figura 3. Comparación entre el modelo OSI y el modelo TCP/IP

Fuente: Interpolados.worpress.com (2017)

Amenazas informáticas

Cuando hablamos de amenazas informáticas debemos considerar que pueden ser deliberadas, y con la finalidad generar daños en la organización, tales como es el caso del robo de información usando diferentes técnicas. También pueden ser del tipo no intencionales, generadas por acciones u omisiones que, si bien no buscan explotar una vulnerabilidad en particular, ponen en riesgo la seguridad de la información y que podrían dañar a la organización, usando a los usuarios como amenaza.

Ingeniería social

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos con la finalidad de obtener información confidencial que a la postre puede servir para preparar algún tipo de ataque. En muchas oportunidades los atacantes se aprovechan del desconocimiento de los usuarios y de lo incauto que pueden ser ellos.

La mejor forma de protegerse de la ingeniería social es por medio de una buena educación; los usuarios deben aprender que no deben hacer clic en links desconocidos que pueden ser sospechosos, siempre deben proteger sus credenciales de inicio de sesión, en el trabajo y en el hogar. Cuando las personas deben enfrentar situaciones complejas o aterradoras, la primera reacción es actuar y, luego, pensar. La ingeniería social se basa en esta "vulnerabilidad" para que los ataques sean exitosos, generalmente se aprovechan de las emociones de las

personas. Cuando hay un problema, todos queremos ayudar y esto constituye otra vulnerabilidad explotada por los atacantes.

Trashing: una técnica dentro de ingeniería social que se refiera al tratamiento y manejo de la basura. No es una técnica relacionada directamente con los sistemas de información, pues los atacantes se valen de otra forma de ingeniería social y para ello, el mecanismo utilizado, es la búsqueda en los contenedores de la basura o en los sitios donde se desechan papeles y documentos de extractos bancarios, facturas, recibos, borradores de documentos, etc., y posteriormente utilizarla según convenga, elaborando un perfil de la víctima para Ataques informáticos.

Pretextos: se crea un escenario ficticio para que la víctima revele una información que, en circunstancias normales, no revelaría. Normalmente la creación de escenarios ficticios requiere una investigación previa de la víctima para conseguir datos personales sensibles y hacer así más creíble la suplantación y hacer creer a la víctima que es legítima.

Phishing: se denomina así a este ataque que está dentro de las técnicas de ingeniería social, su finalidad es la obtención de forma fraudulenta de los datos confidenciales de un usuario específico en especial aquellos de tipo financieros, a través de la confianza que se tiene en los servicios tecnológicos, el escaso conocimiento de cómo se realiza esta técnica y las pocas medidas de seguridad hacen presa fácil de este tipo de ataque. En la actualidad un ataque de este tipo incluye una serie

sofisticadas técnicas sustentadas en las tecnologías como es el caso de correo electrónico y sitios Web falsos que suplantan originales.

Shoulder surfing: se refiere al acto de obtener información personal o privada a través de la observación directa, esto implica mirar por encima del hombro de una persona para recopilar información pertinente mientras la víctima no se da cuenta. Esto es especialmente efectivo en lugares con mucha gente donde una persona usa un computador, un teléfono inteligente, un cajero automático, etc. Si esta técnica se realiza cuando hay muy pocas personas, el acto se vuelve sospechoso muy rápidamente. También se utilizan binoculares, cámaras de video y dispositivos para mejorar la visión, dependiendo de la ubicación y la situación.

Ataques de repetición: este tipo de ataque es aquel en donde el atacante captura la información que viaja por la red, como los comandos de acceso a un sistema para luego enviarla a otro destinatario, sin que se percate que ha sido capturado. Si el sistema es vulnerable a este tipo de ataque, se ejecutará el comando desde otro lugar como si fuera el verdadero enviando la respuesta al atacante de manera tal que de esta forma se puede acceder al sistema, por medio de un suplantador.

Ataques de modificación: es un ataque contra la integridad de un sistema de información por medio de la manipulación. Este tipo de ataque es considerado uno de los más dañinos, ya que puede eliminar

o modificar parte de la información, en algunos casos llegando a inutilizar sistemas o haciendo que funcionen de manera distinta.

Ataque DoS: uno de los ataques más antiguos en el repertorio del hacker es el ataque Denial-of-the Service. Esta es la técnica simple pero efectiva de atacar un sistema o servicio con solicitudes que comprometen los recursos hasta el punto de que no se puedan cumplir las solicitudes legítimas. Algunos ataques en este género harán que un sistema o servicio falle de manera incontrolada y detenga el procesamiento, lo que no es un buen estado para un servidor web. Como se mencionó anteriormente, los servidores web y las aplicaciones que se ejecutan en ellos son ampliamente accesible por el hecho de que queremos que las personas accedan a ellos. Aunque en el pasado ha habido casos altamente publicitados de vulnerabilidades en los servidores web, la mayoría de los hackeos que se realizan hoy en día están explotando las aplicaciones web que se ejecutan en la parte superior de los servidores web en el nivel de la aplicación, atentando contra el tráfico de los servidores.

Ataque de diccionario: un ataque de diccionario es una técnica para adivinar contraseñas en la que el atacante intenta determinar la contraseña de un usuario probando palabras sucesivas de un diccionario generado a partir de diferentes combinaciones con la esperanza de que una de estas propuestas sea la contraseña real del usuario.

3. Definiciones de Hacker

A continuación, presentaremos algunos términos asociados a las prácticas de seguridad, con lo que podremos relacionar estas acciones con el tipo de ataque.

Hacker: en informática este término se utiliza para referirse a una persona experta o con gran conocimiento técnico e informático capaz de vulnerar sistemas, pero en el mundo de la seguridad informática es considerado un título de honor relacionado con sus conocimientos y habilidades técnicas.

Aquí podemos clasificarlos en 3 tipos:

Los hackers de sombrero negro: ciberdelincuentes que se introducen en redes informáticas para llevar a cabo algún acto maligno. Además, se dedican a robar contraseñas, números de tarjetas de crédito y otro tipo de información relevante, toman sistemas de rehén o propagan malware diseñado para borrar o dañar archivos.

Los hackers de sombrero blanco: son aquellos que usan sus conocimientos para detectar vulnerabilidades en los sistemas ayudar a las organizaciones a resguardarse de probables ataques de hackers peligrosos. Algunas empresas contratan en forma directa a estos hackers porque están puntualmente interesadas en conocer sus puntos vulnerables.

Los hackers de sombrero gris: son una mezcla híbrida entre los hackers de sombrero blanco y los hackers de sombrero negro. Es decir, no tienen problema en infringir alguna ley o precepto ético, pero no actúan con la malicia que caracteriza al hacker de sombrero negro.

Crackers: este término, aplicado a la informática, hace referencia a una persona que viola o rompe la seguridad de un sistema. Si bien es similar al concepto de hacker, el cracker (intruso) tiene otros fines. Generalmente, se llama cracker a aquella persona que, de forma ilegal, utiliza ingeniería inversa para desproteger un software (conjunto de programas) o sistema. Un ejemplo muy común de este tipo de personas es el de aquellos que rompen las claves o keys de una licencia de software para utilizarlas de modo ilegal, es decir, sin adquirirlas.

Newbie: este término es conocido en el ambiente informático para definir a los principiantes.

Lammers: las personas llamadas bajo este término informático son aquellas que presumen tener conocimientos de ataques informáticos, pero en realidad no poseen conocimiento alguno.

Phreaker: estos son un tipo de hacker, pero orientados más a los sistemas telefónicos que informáticos. Cuando se habla de sistemas telefónicos, no se hace referencia a smartphones, sino a telefonía propiamente dicha.

Script kiddie: es un personaje que se dice hacker, pero utiliza programas de terceros para realizar ataques sin conocer su funcionamiento, razón por la cual suelen ser víctimas de ataques ellos mismos.

3.1 Fases del Hacking

Fase 1 – Reconocimiento (Footprinting): es la fase donde el hacker utiliza varias técnicas para investigar y recolectar toda la información necesaria de su objetivo para preparar el ataque.

Fase 2 – Escaneo (Scanning): la información recolectada en la Fase de Reconocimiento es utilizada para identificar vulnerabilidades específicas.

Fase 3 – Obtener Acceso (Gaining Access): aquí es cuando se lleva a cabo la explotación de la vulnerabilidad para lograr la penetración a este, en esta fase el hacker explota las vulnerabilidades que encontró en la Fase de Escaneo.

Fase 4 – Mantener Acceso (Maintaining Access): aquí es prioridad del hacker mantener el acceso al sistema vulnerable sin ser detectado.

Fase 5 – Limpiar Huellas (Clearing Tracks): el hacker destruye (en la medida de sus capacidades) toda evidencia de su presencia y de las actividades no autorizadas, así, si no es descubierto, puede volver a lograr acceso al sistema vulnerado nuevamente, además de lograr no ser descubierto por agentes de la ley.

4. Controles de seguridad

4.1 Aseguramiento de la información

En la actualidad la información constituye uno de los activos más preciados de las organizaciones ya que están expuestos a amenazas de diferentes tipos como es el caso de robos, incendios, fallas de hardware, virus, etc. Entonces las organizaciones deben proteger estos activos ya que corresponde a activos críticos de las empresas. Una de las medidas más importantes para la protección de los datos es establecer las políticas adecuadas para la protección de la información.

4.2 Programa de administración de la seguridad de la información

Se refiere al conjunto de medidas preventivas y reactivas que adoptan las organizaciones para sus sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

4.3 Network Security Zoning

La zonificación de seguridad en las redes es la práctica de dividir en sub redes la misma, para limitar las comunicaciones entre Host dentro de una red. Las direcciones IP se utilizan para mapear las subredes asociándolas de manera predecible con un solo sistema o grupo de sistemas con la

misma política de control de acceso. Una zona de seguridad de red puede contener una única dirección IP o cualquier combinación de direcciones IP y subredes. Todas las direcciones IP en una zona de seguridad deben tener la misma etiqueta de seguridad, aunque no es necesario que todas las direcciones IP con la misma etiqueta de seguridad estén en la misma zona de seguridad.

4.4 Políticas de seguridad de la información

Son todos los protocolos destinados a resguardar la seguridad de la información, sobre todo un atributo muy importante: la Confidencialidad, es decir, que la información sea conocida únicamente por personas autorizadas. Además, estas políticas también deben hacer resguardo de la Disponibilidad de la información, es decir, la capacidad de estar siempre disponible para ser procesado por personas autorizadas.

Existen varios tipos de políticas de seguridad, ya que al ser un conjunto de que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización tendrán incluidas áreas como la seguridad física, personal, administrativa y de la red. Ejemplo de política de seguridad:

Para mayor información, se recomienda visitar el sitio web (https://www.csirt.gob.cl/matrices-de-politicas/) del equipos de

respuestas ante incidentes de seguridad informática, quien nos brinda diversas políticas de seguridad de la información.

Cierre

Después de analizados y estudiados los conceptos establecidos en el contenido, se puede resaltar lo siguiente:

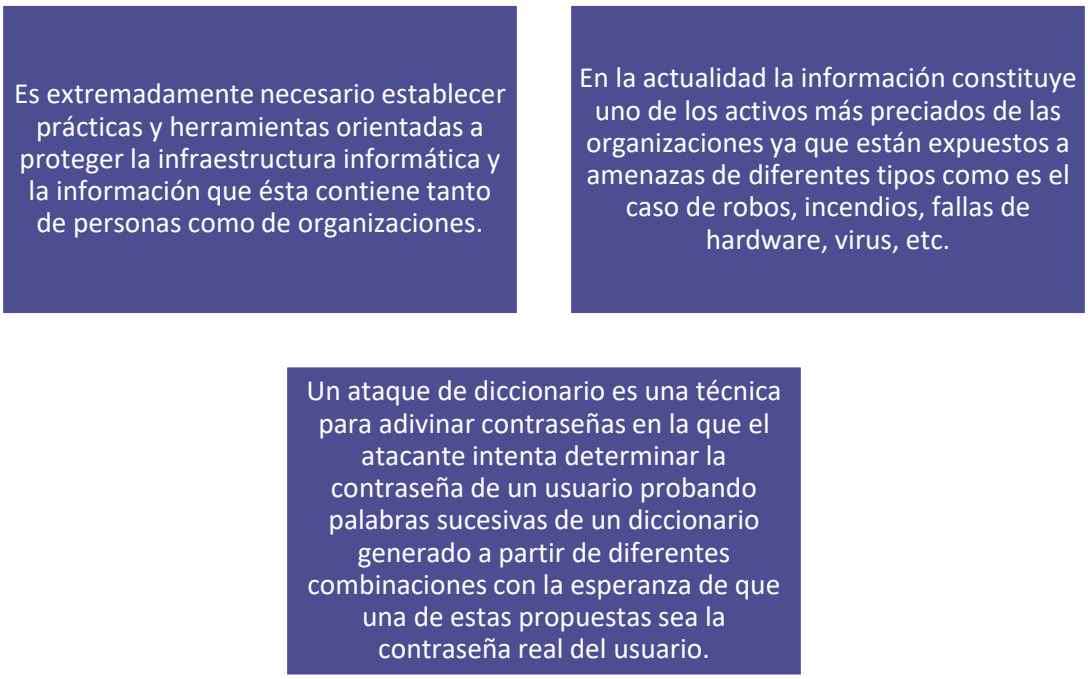


Figura 4. Ideas clave semana 1

Fuente: Moran, E. (2022)

Referencias

Albors, J. (2020). Qué es un ataque de fuerza bruta y cómo funciona.

Recuperado de https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/

Astudillo, K. (2013). Hacking ético 101. ¡Cómo hackear profesionalmente en 21 días o menos! Recuperado de https://eduarmandov.files.wordpress.com/2017/05/security-hacking-etico-101.pdf

Beetrack. (s. f.). Tipos de trazabilidad: ventajas y desventajas [+ Ejemplos]. Recuperado de https://www.beetrack.com/es/blog/tipos-de-trazabilidad-ventajas

Benchimol, D. (Coord.). (2011). Hacking. Buenos Aires, AR: Fox Andina. Blanco, D. y Cattafesta, M. F. (s. f.). Evaluación integral de seguridadinformática del centro de datos y comunicaciones (Trabajo final de grado).

Bortnik, S. (2010). Defensa en profundidad: qué es. Recuperado de https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

Forsenergy. (s. f.). Establecer los permisos de un recurso compartido. Recuperado de https://forsenergy.com/es-es/aclui/html/fc747cd7-e7ca-4544-b485-3c40230d848c.htm

Funnel MKT Experts. (s. f.). Productividad. Recuperado de https://www.i-s.com.mx/productividad/

Giannone, A. O., Rodríguez, D. y Amatriain, H. (2018). Método de inclusión de hacking ético en el proceso de testing de software (Trabajo final de maestría). Universidad Tecnológica Nacional, Buenos Aires, AR. Recuperado de https://ria.utn.edu.ar/bitstream/handle/20.500.12272/4068/Tesis%20Maestria%20GIANNONE%20Ariel%20.pdf?sequence=1&isAllowed=y

GlosarioIT. (s. f.). Autenticidad [Definición]. Recuperado de https://www.glosarioit.com/Autenticidad

Gobierno de Canarias. (s. f.). Seguridad y Alta Disponibilidad. Recuperado de https://www3.gobiernodecanarias.org/medusa/ecoblog/flopmarl/seguridad-y-alta-disponibilidad/

International Organization for Standarization/International ElectronicComision (ISO/IEC). (2005). Information Security Management (NormaISO/IEC 27001). Recuperado de https://www.iso.org/isoiec-27001-information-security.html

Interpolados. (2017). Comparación entre el modelo OSI y el modelo TCP/IP. Recuperado de https://interpolados.wordpress.com/2017/03/01/comparacion-entre-el-modelo-osi-y-el-modelo-tcpip/

Jara, H. y Pacheco, F. G. (2012). Ethical hacking 2.0. Buenos Aires, AR: Fox Andina. José Ignacio. (s. f.). Los 6 ciber ataques más comunes en un eCommerce. Recuperado de https://www.actualidadecommerce.com/los-6-ciber-ataques-mas-comunes-en-un-ecommerce/

Junta de Andalucía. (s. f.). Gestionar las líneas base y peticiones de cambio a los requisitos del sistema. Recuperado de http://www.juntadeandalucia.es/servicios/madeja/contenido/libro-pautas/188

Paterva. (2014). Maltego (Versión 4.2.19) [Software de computación]. Noguera, B. (s. f.). ¿Qué es una denegación de servicio? Recuperado de https://culturacion.com/que-es-una-denegacion-de-servicio/

Panda Security. (s. f.). Exploit. Recuperado de https://www.pandasecurity.com/es/security-info/exploit/ Rodríguez, F. (s. f.). Phreakers: Los hackers de los sistemas telefónicos.

Portinos. (2020). ¿Quiénes son las personas detrás de los sistemas? Recuperado de https://culturacion.com/phreakers-los-hackers-de-los-sistemas-telefonicos/

Ramírez Ferreira, R. R. (2016). Ante los sueños irrealizados. ¿Más poder y más tiempo? Recuperado de https://acento.com.do/opinion/ante-los-suenos-irrealizados-mas-poder-mas-tiempo-8398536.html

Rodríguez Ruiz, S. (s. f.). ¿Qué es una contraseña o password? -Definición de contraseña o password. Recuperado de https://www.masadelante.com/faqs/password

Tecnología para los negocios. (s. f.). Qué es el hacking ético. Recuperado de https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

Universidad Complutense de Madrid. (2015). Generalidades sobre Criptografía, Certificación y Firma. Recuperado de https://www.ucm.es/faq/generalidades-sobre-criptografia-certificacion-y firma/que-significa-no-repudio-o-irrenunciabilidad

Universidad Internacional de Valencia. (2018). ¿Qué es la seguridad informática y cómo puede ayudarme? Recuperado de https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme