Tarea 6 Seguridad Informática Básica – Gpo. 2 Fecha de entrega: 07 /11/ 23

Equipo 4 || Integrantes:

Castelan Ramos Carlos	**317042711**
Martínez González Héctor Eduardo	**316322122**
Martínez Sánchez Berenice Vianney	**317581223**
Pineda González Rodrigo	**317224397**
Vega Alvarez Marcos	**420054432**

9

Investigué qué es y cuáles son las características principales de:

1. **Metasploit**

   Metasploit Framework es una herramienta de código abierto que se ha convertido en un pilar en el campo de la seguridad informática. Inicialmente desarrollado en Perl y posteriormente reescrito en Ruby para mejorar su eficiencia, Metasploit es ampliamente utilizado en el mundo del hacking ético y la evaluación de vulnerabilidades. Su característica más destacada son los exploits, que son piezas de código diseñadas para aprovechar vulnerabilidades conocidas en sistemas y aplicaciones. Estos exploits permiten a los profesionales de seguridad realizar pruebas de penetración en sistemas para identificar posibles debilidades y tomar medidas correctivas. Metasploit ofrece una amplia gama de exploits y módulos adicionales, como payloads y codificadores, que le dan versatilidad en la post explotación y la evasión de sistemas de detección. Metasploit es una herramienta esencial para aquellos que desean evaluar y mejorar la seguridad de sistemas informáticos al aprovechar y analizar exploits de manera controlada y ética.

   Otras de sus características son:

   - **Automatización y modularidad:** La plataforma es altamente modular y permite la automatización de tareas, lo que ahorra tiempo y esfuerzo en pruebas de penetración y evaluación de seguridad.

   - **Interfaz de línea de comandos y GUI:** Metasploit ofrece una interfaz de línea de comandos (CLI) para usuarios avanzados y una interfaz gráfica de usuario (GUI) llamada Armitage para facilitar su uso a los principiantes.

   - **Compatibilidad multiplataforma:** Metasploit es compatible con una amplia gama de sistemas operativos y plataformas, lo que lo hace versátil para probar la seguridad en diferentes entornos.

- **Base de datos integrada:** Cuenta con una base de datos que permite el registro y seguimiento de información relevante, como exploits utilizados, hosts, servicios y resultados de pruebas de penetración.

- **Comunidad activa y soporte:** Metasploit cuenta con una comunidad activa de usuarios y desarrolladores que contribuyen con exploits, módulos y actualizaciones. También ofrece documentación y soporte a los usuarios.

- **Funcionalidades avanzadas:** Además de los exploits, Metasploit incluye módulos para payloads, codificadores y otras herramientas que son esenciales en las pruebas de penetración y la explotación de sistemas.

2. **Metodología OSSTM v3**

   El OSSTMM (Manual de Metodología de Pruebas de Seguridad de Código Abierto) proporciona una metodología exhaustiva para llevar a cabo evaluaciones de seguridad rigurosas. Una auditoría OSSTMM representa una medición precisa de la seguridad en términos operativos, eliminando suposiciones y basándose en evidencia sólida.

   El manual se actualiza cada seis meses aproximadamente, para seguir siendo relevante para el estado actual de las pruebas de seguridad. El Instituto de Seguridad y Metodologías Abiertas (ISECOM) dice que su principal objetivo con el OSSTMM es proporcionar un proceso científico para la caracterización precisa de la seguridad operativa que se puede utilizar para pruebas de penetración, piratería ética y otras pruebas de seguridad.
   Algunas de sus características son las siguientes:

   - **Amplitud de Cobertura:** La versión 3 del OSSTMM abarca una amplia variedad de canales de prueba, incluyendo aspectos humanos, físicos, inalámbricos, de telecomunicaciones y redes de datos.

   - **Versatilidad Tecnológica:** Esta metodología es extremadamente versátil y puede aplicarse a la computación en la nube, infraestructuras virtuales, middleware de mensajería y comunicaciones móviles.

   - **Inclusividad en la Seguridad:** Es apta para auditar ubicaciones de alta seguridad, recursos humanos, sistemas de cómputo confiables y procesos lógicos que involucran todos estos canales.

   - **Métricas de Superficie de Ataque (RAVS):** Incluye un conjunto de métricas de superficie de ataque que proporciona una herramienta poderosa y altamente flexible.

- **Integración con Paneles de Control:** Lo que facilita pruebas internas y externas y permite la comparación y combinación de resultados.

- **Gestión Cuantitativa de Riesgos:** Permite realizar una gestión cuantitativa de riesgos a través de informes detallados, lo que da como resultado una evaluación más precisa y libre de errores, mejorando la toma de decisiones en seguridad.

3. **Pentesting**

El pentesting es un ataque malicioso simulado contra los sistemas informáticos que se usa para encontrar y verificar posibles vulnerabilidades. Este tipo de exámenes y pruebas son comunes en el contexto de la seguridad en las aplicaciones y páginas web. Se hacen pentesting para mejorar el firewall y proteger la información recopilada por las distintas apps. Es el resultado de unir dos conceptos: penetration y testing.

Existen varios tipos de Pentesting que se clasifican según el tipo de información que se tenga a la hora de realizar los test:

Pentesting de caja blanca o “White Box”: el Pentester o Auditor conoce todos los datos sobre el sistema: Estructura, contraseñas, IPs, firewalls… y suele formar parte del equipo técnico de la empresa. Es el más completo y forma parte de un análisis integral de la estructura. Gracias a toda esta información preliminar es relativamente fácil saber qué puede ser modificado o mejorado dentro de la arquitectura del sistema.

Pentesting de caja negra o “Black Box”: es el tipo de pentesting más “*real*” ya que, el Pentester tiene muy pocos datos sobre la organización y actúa como un ciberdelincuente más. Por eso, como si fuera una prueba “*a ciegas*” se debe descubrir las vulnerabilidades y amenazas en la estructura de la red.

Pentesting de caja gris o “Grey Box”: puede definirse como la mezcla de los dos anteriores, el Auditor posee cierta información a la hora de realizar el test, la suficiente para no partir de cero. Es el tipo de pentest más recomendado ya que se necesitará tiempo y medios para poder realizar este test de penetración en su totalidad. Las cinco fases del Pentesting son:

**Recopilación y planificación.

**Análisis de vulnerabilidades.

**Modelado de amenazas.

**Explotación del sistema.

**Elaboración de los informes.

Entre las características a las que favorece tenemos las siguientes:

- **Encontrar vulnerabilidades y fallos** en los sistemas informáticos.

- **Determinar cuan robustos son los controles de seguridad** implementados en el desarrollo de aplicaciones.

- **Ayudar en el cumplimiento de las normas** de seguridad y privacidad de datos.

- **Proporcionar ejemplos cualitativos y cuantitativos del estado de seguridad** actual y, con ello, ayudar a determinar cuáles son las prioridades presupuestarias para su gestión.

4. **Robo de identidad**

   El robo de identidad o usurpación de identidad, consiste en que una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de ésta última, usualmente para cometer un fraude o delito.

   La identidad la constituyen los datos personales: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y de seguridad social, incluyendo información financiera o médica, así como cualquier otro dato que permita identificar a una persona.

   En muchos casos el ladrón de identidad utiliza la información ilegalmente adquirida para contratar productos y servicios financieros a nombre de la víctima.

   Es posible sospechar de ser víctima de este delito, si ocurre alguna de las siguientes características:

   - **Recibe facturas** de productos que no compró.

   - Llaman para **cobrarle deudas** de cuentas que no abrió.

   - Aparece una **información** en su informe de crédito **que no le resulta familiar**.

   - **Rechazaron sus solicitudes** de préstamo.

   - **Deja de recibir el correo con sus cuentas** o no lo encuentra en su buzón.

5. **Ataques a firewalls**

   Un ataque a un firewall es un intento de comprometer la seguridad de un firewall, lo que podría permitir al atacante acceder a una red o sistema protegidos. Los ataques a firewalls pueden ser muy variados, pero algunos de los más comunes incluyen:

Ataques de fuerza bruta: Estos ataques consisten en intentar adivinar la contraseña de un firewall mediante el uso de un programa automatizado.
Ataques de inyección: Estos ataques consisten en introducir código malicioso en un paquete de datos que se envía a un firewall.
Ataques de denegación de servicio: Estos ataques consisten en sobrecargar un firewall con tráfico de red, lo que lo hace inoperable.

Las características principales de los ataques a firewalls son las siguientes:

- Son cada vez más sofisticados: Los atacantes están constantemente desarrollando nuevas técnicas para comprometer la seguridad de los firewalls.
- Pueden tener un impacto significativo: Un ataque exitoso a un firewall podría permitir al atacante acceder a una red o sistema protegidos, lo que podría provocar la pérdida de datos, el robo de información o la interrupción de los servicios.
- Para protegerse de los ataques a firewalls, es importante mantener el firmware del firewall actualizado, utilizar contraseñas seguras y aplicar las últimas actualizaciones de seguridad. También es importante implementar medidas de seguridad adicionales, como un firewall de aplicaciones web (WAF) o un sistema de detección de intrusiones (IDS).

Consejos para proteger su firewall de ataques:

- Mantenga el firmware del firewall actualizado: Los fabricantes de firewalls suelen publicar actualizaciones de seguridad para abordar las vulnerabilidades conocidas.
- Utilice contraseñas seguras: Las contraseñas débiles son una de las principales causas de los ataques a firewalls. Utilice contraseñas seguras y únicas para cada cuenta.
- Aplique las últimas actualizaciones de seguridad: Los fabricantes de software suelen publicar actualizaciones de seguridad para abordar las vulnerabilidades conocidas.
- Implemente medidas de seguridad adicionales: Además de un firewall, también puede implementar medidas de seguridad adicionales, como un WAF o un IDS.

- Los ataques a firewalls son una amenaza importante para la seguridad de las redes y sistemas informáticos. Al seguir estos consejos, puede ayudar a proteger su firewall de ataques y mantener su red segura.

6. Engaño a detectores de intrusos

El engaño a detectores de intrusos (IDS) es una técnica utilizada por los atacantes para evitar que sus actividades sean detectadas por los IDS. Los IDS son sistemas de seguridad que monitorean el tráfico de red en busca de actividad maliciosa.

Hay varias técnicas que los atacantes pueden usar para engañar a los IDS. Algunos de los métodos más comunes incluyen:

- Camuflaje: Los atacantes pueden disfrazar su tráfico malicioso para que parezca tráfico legítimo. Esto se puede hacer cambiando los encabezados de los paquetes de datos o utilizando técnicas de ofuscación.
- Evasión: Los atacantes pueden evitar que los IDS detecten su tráfico malicioso enviando el tráfico a través de un túnel cifrado o utilizando técnicas de segmentación de red.
- Inundación: Los atacantes pueden enviar un gran volumen de tráfico de red a un IDS para sobrecargarlo y evitar que detecte su tráfico malicioso.

Las características principales del engaño a IDS son las siguientes:

- Es una amenaza creciente: Los atacantes están constantemente desarrollando nuevas técnicas para engañar a los IDS.
- Es difícil de detectar: Los IDS están diseñados para detectar tráfico malicioso, no tráfico que ha sido disfrazado o evadido.
- Puede tener un impacto significativo: Los atacantes que pueden engañar a los IDS pueden llevar a cabo ataques exitosos sin ser detectados.

Para protegerse del engaño a IDS, es importante implementar una combinación de medidas de seguridad, como:

- Un IDS de múltiples sensores: Un IDS de múltiples sensores puede ayudar a detectar el tráfico malicioso que ha sido disfrazado o evadido.

- Un sistema de prevención de intrusiones (IPS): Un IPS puede ayudar a bloquear el tráfico malicioso antes de que llegue a un sistema.
- Un firewall: Un firewall puede ayudar a bloquear el tráfico malicioso de llegar a una red.
- Una conciencia situacional sólida: Es importante estar al tanto de las últimas técnicas de ataque para poder detectarlas y tomar medidas.

El engaño a IDS es una amenaza importante para la seguridad de las redes y sistemas informáticos. Al implementar una combinación de medidas de seguridad, puede ayudar a protegerse de este tipo de ataques.

7. **Ataques a contraseñas**
   Los "ataques a contraseñas" son intentos de acceder a una cuenta o sistema protegido por una contraseña sin conocerla legítimamente. Estos ataques pueden llevarse a cabo de diversas formas y tienen como objetivo descifrar o adivinar la contraseña para obtener acceso no autorizado a una cuenta o sistema. Algunas de las características principales de los ataques a contraseñas incluyen:

   - Intentos de acceso no autorizado: Los atacantes tratan de ingresar a una cuenta o sistema sin permiso legítimo, ya sea con fines maliciosos, como el robo de información o la realización de actividades fraudulentas.
   - Uso de herramientas y técnicas: Los atacantes utilizan software, herramientas o técnicas específicas para intentar adivinar o descifrar contraseñas. Estas herramientas pueden incluir diccionarios de contraseñas, fuerza bruta, ataques de diccionario, ataques de rainbow tables, entre otros.
   - Variabilidad en el método: Existen diferentes métodos para realizar ataques a contraseñas, lo que puede incluir la adivinanza de contraseñas débiles, la obtención de contraseñas almacenadas en texto claro o encriptadas, y la manipulación de cookies de sesión, entre otros.

   Los ataques a contraseñas se pueden clasificar en varias categorías, que incluyen:

- Fuerza Bruta: En este tipo de ataque, un atacante intenta todas las posibles combinaciones de contraseñas hasta encontrar la correcta. Es un método lento pero efectivo si la contraseña es débil y corta.
- Ataques de Diccionario: Los atacantes utilizan una lista de palabras o frases comunes (un diccionario) para intentar adivinar la contraseña. Pueden combinar palabras, realizar variaciones y probar palabras de un idioma específico.
- Ataques de Rainbow Tables: En este enfoque, se utilizan tablas precalculadas que contienen combinaciones de contraseñas y sus correspondientes valores hash. Los atacantes buscan en estas tablas para encontrar una coincidencia y obtener la contraseña original.
- Ataques de Adivinanza: Los atacantes intentan adivinar la contraseña basándose en información personal o conocimiento sobre la víctima, como fechas de nacimiento, nombres de familiares, etc.
- Ataques de Fuerza Bruta Distribuida: En este caso, múltiples sistemas o dispositivos se utilizan para realizar ataques de fuerza bruta simultáneamente, acelerando el proceso de adivinanza de contraseñas.

Es importante destacar que la seguridad de las contraseñas es fundamental para proteger cuentas y sistemas, y se recomienda el uso de contraseñas fuertes y medidas adicionales, como la autenticación de dos factores (2FA), para protegerse contra los ataques a contraseñas. Además, los sistemas deben estar configurados para detectar y bloquear intentos de acceso no autorizados y limitar el número de intentos fallidos de inicio de sesión.

8. **Debilidades de los protocolos de red.**
   Las debilidades de los protocolos de red se refieren a las vulnerabilidades o puntos débiles en los protocolos de comunicación utilizados en redes de computadoras. Estas debilidades pueden ser explotadas por atacantes para comprometer la seguridad de la red o para llevar a cabo actividades maliciosas. Algunas de las características principales de las debilidades de los protocolos de red incluyen:

   - Vulnerabilidades: Las debilidades suelen ser vulnerabilidades en el diseño, la implementación o la configuración de los protocolos de red. Estas vulnerabilidades pueden permitir a los atacantes acceder a la red, interceptar datos, modificar la información transmitida o llevar a cabo otros tipos de ataques.
   - Exposición a amenazas: Las debilidades de los protocolos exponen a la red a diversas amenazas, como ataques de denegación de servicio (DDoS), interceptación de datos, suplantación de identidad y muchos otros tipos de ataques cibernéticos.

- Impacto en la seguridad: La explotación de debilidades en los protocolos de red puede tener un impacto significativo en la seguridad de la red y los sistemas conectados. Puede resultar en la pérdida de datos confidenciales, la interrupción de servicios, la degradación del rendimiento y la exposición a riesgos cibernéticos.

Las debilidades de los protocolos de red se pueden clasificar en varias categorías, algunas de las cuales incluyen:

- Vulnerabilidades de autenticación: Incluyen debilidades en los mecanismos de autenticación que permiten a los atacantes suplantar identidades legítimas.
- Vulnerabilidades de cifrado: Estas debilidades se relacionan con problemas en los algoritmos de cifrado utilizados para proteger la confidencialidad de los datos transmitidos.
- Vulnerabilidades de enrutamiento: Implican problemas en los protocolos de enrutamiento que podrían permitir a un atacante redirigir el tráfico o llevar a cabo ataques de denegación de servicio.
- Vulnerabilidades de protocolo: Se refieren a debilidades en los propios protocolos de red, como el Protocolo de Control de Mensajes de Internet (ICMP) o el Protocolo de Resolución de Direcciones (ARP).
- Vulnerabilidades de seguridad inalámbrica: Estas debilidades se encuentran comúnmente en las redes inalámbricas y pueden permitir a los atacantes interceptar o comprometer las comunicaciones inalámbricas.

9. Fingerprinting

El "Fingerprinting" es un término que se utiliza en diversos contextos para referirse a la identificación y seguimiento de entidades, ya sea en el mundo digital o en otros campos. Las características principales y su clasificación pueden variar según el contexto en el que se aplique. Aquí te proporcionaré una descripción general de lo que es el "Fingerprinting" en algunos contextos comunes:

Fingerprinting digital:

- Definición: En el ámbito digital, el "Fingerprinting" se refiere a la técnica de recopilar información única de un dispositivo, navegador web o usuario para identificarlo de manera única y realizar un seguimiento en línea.
- Características:
    - Identificación única: El objetivo principal es crear un identificador único para un dispositivo o usuario en línea.
    - Recopilación de datos: Se recopilan datos como la configuración del navegador, información de hardware,

direcciones IP, cookies, entre otros, para crear una huella digital única.
    - Seguimiento en línea: Se utiliza para rastrear la actividad en línea de un usuario, a menudo con fines publicitarios o de análisis.

- Clasificación:
    - Fingerprinting de navegador: Se basa en la recopilación de información sobre el navegador web y su configuración para crear una huella digital única.
    - Fingerprinting de dispositivo: Se enfoca en la información de hardware y software de un dispositivo, como el sistema operativo, resolución de pantalla, tiempo de actividad, etc.
    - Fingerprinting de usuario: Se centra en la recopilación de datos sobre el comportamiento del usuario en línea, como patrones de navegación, preferencias y más.

Fingerprinting forense:

- Definición: En el contexto forense, el "Fingerprinting" se refiere a la recopilación y análisis de pruebas físicas o digitales para identificar personas o dispositivos en una investigación criminal.
- Características principales:
    - Identificación de pruebas: Se busca identificar huellas dactilares, ADN, balas, marcas de herramientas o cualquier otra evidencia que pueda vincular a un sospechoso con un delito.
    - Análisis forense: Se utiliza para recopilar pruebas que puedan ser presentadas en un tribunal como parte de una investigación criminal.
- Clasificación:
    - Fingerprinting dactilar: Se refiere a la identificación de personas a través de sus huellas dactilares.
    - Fingerprinting de balística: Implica la comparación de balas y cartuchos para vincular armas de fuego a incidentes específicos.
    - Fingerprinting de ADN: Se utiliza para identificar a individuos basándose en su material genético.

La clasificación y las características del "Fingerprinting" pueden variar según el contexto en el que se aplique, pero en general, se refiere a la técnica de identificación única a través de la recopilación de datos específicos. Es importante destacar que en el ámbito digital, el "Fingerprinting" también plantea preocupaciones sobre la privacidad y la ética, ya que puede utilizarse para el seguimiento en línea sin el consentimiento de los usuarios.

Referencias.

Berry, J., & Stoney, D. A. (2001). *The history and development of fingerprinting*. Advances in fingerprint Technology, 2, 13-52.

Ciberseg. (2021, Junio 29). *¿Qué es OSSTMM? Definición, historia y características*. Ciberseguridad. https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/

DragoN. (2014, Diciembre 4). *Manual de Metasploit Framework en Español. DragonJAR* - Servicios De Seguridad Informática. https://www.dragonjar.org/manual-de-metasploit-framework-en-espanol.xhtml

Gobierno de México. (2016). *¿Sabes qué es el Robo de Identidad?*. https://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad?idiom=es

Gómez, P. (2021, 18 junio). *¿Qué es un sistema de detención de intrusiones?* ICM. https://www.icm.es/2021/06/07/ids-intrusiones/

KeepCoding, R. (2023, octubre 12). *¿Qué es Metasploit?*. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

NortonLifeLock Inc. (2021). *¿Cómo proteger tus contraseñas?* Norton. Cómo proteger sus contraseñas (norton.com)

Nowak, S. (2022). *¿Qué es el Pentesting?. Tipos, fases y herramientas.* Nuclio Digital School. https://nuclio.school/que-es-el-pentesting/

¿Qué es y en qué consiste el pentesting?. (2022). Tokio School. https://www.tokioschool.com/noticias/pentesting/

Radware. (s. f.). *7 tipos de ataques más comunes para los que está diseñado el firewall de aplicaciones web (WAF)* | Radware. https://es.radware.com/cyberpedia/application-security/7-most-common-attack-types/#:~:text=Un%20WAF%20protege%20las%20aplicaciones%20web%20de%20ataques%20como%20la,la%20inyecci%C3%B3n%20SQL%2C%20entre%20otros.

Ramírez, H. (2022, 6 junio). *El Sistema de Detección de Intrusiones (IDS)*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/sistema-deteccion-intrusiones-ids/

Robo de identidad. (2023). USAGov en español. https://www.usa.gov/es/robo-identidad

Wagner, N. R. (1983, April). *Fingerprinting*. In 1983 IEEE Symposium on Security and Privacy (pp. 18-18). IEEE.

Walton, A. (2022, 3 noviembre). *Vulnerabilidades y amenazas a la Seguridad* CCNA. CCNA desde Cero. https://ccnadesdecero.es/amenazas-y-vulnerabilidades-redes/