Análisis de Vulnerabilidades

Laboratorio

Contenido

ANÁLISIS DE VULNERABILIDADES

1. Vulnerabilidades

Una vulnerabilidad en el contexto de la seguridad informática es una debilidad o fallo en un sistema, red, aplicación, o dispositivo que puede ser explotada por un atacante para comprometer la integridad, confidencialidad o disponibilidad de los recursos afectados. Las vulnerabilidades pueden ser introducidas por errores de diseño, implementación, configuración o incluso por fallos en la administración y mantenimiento de los sistemas.

Tipos Comunes de Vulnerabilidades

1. **Vulnerabilidades de Software:**
    - **Errores de Código (Bugs):** Fallos en el código fuente de un software que pueden ser explotados para ejecutar código malicioso, obtener acceso no autorizado, etc.
    - **Buffer Overflows:** Ocurre cuando un programa escribe más datos en un buffer (memoria temporal) de los que este puede manejar, permitiendo al atacante sobrescribir memoria adyacente.
    - **SQL Injection:** Una vulnerabilidad en las aplicaciones web que permite a los atacantes inyectar sentencias SQL maliciosas en las consultas de bases de datos.
2. **Vulnerabilidades de Configuración:**
    - **Configuraciones Inseguras:** Uso de configuraciones predeterminadas, como contraseñas por defecto o servicios no necesarios habilitados.
    - **Permisos Inadecuados:** Permisos de archivos, directorios o sistemas mal configurados que permiten accesos no autorizados.
3. **Vulnerabilidades de Red:**
    - **Open Ports:** Puertos abiertos innecesarios que pueden ser utilizados por atacantes para acceder a servicios no protegidos.
    - **Protocolos No Seguros:** Uso de protocolos de comunicación sin cifrar (como HTTP en lugar de HTTPS), exponiendo datos sensibles en tránsito.

4. **Vulnerabilidades Físicas:**
    - **Acceso Físico No Autorizado:** Riesgos asociados con el acceso físico a los servidores, estaciones de trabajo o dispositivos de red.

Consecuencias de las Vulnerabilidades

Las vulnerabilidades, si son explotadas, pueden llevar a una variedad de consecuencias negativas, tales como:

- **Acceso No Autorizado:** Los atacantes pueden obtener acceso a datos y sistemas que no deberían estar disponibles para ellos.
- **Pérdida de Datos:** Datos sensibles pueden ser robados, modificados o eliminados.
- **Interrupción de Servicios:** Ataques que explotan vulnerabilidades pueden causar la interrupción de servicios críticos, afectando la disponibilidad de los sistemas.
- **Compromiso del Sistema:** Un sistema comprometido puede ser utilizado como un punto de partida para atacar otros sistemas dentro de la red.

1.1. Categorización de vulnerabilidades

Common Vulnerability Scoring System (CVSS) es un framework abierto y universalmente utilizado que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad IT.

Componentes del CVSS

CVSS se compone de tres grupos métricos que contribuyen a la puntuación final:

1. **Métricas Base:**
    - **Vector de Ataque (AV):** Define la manera en que se puede explotar la vulnerabilidad (Red, Adyacente, Local o Físico).
    - **Complejidad del Ataque (AC):** Evalúa la dificultad de realizar el ataque (Baja o Alta).
    - **Privilegios Requeridos (PR):** Indica el nivel de privilegios necesarios para explotar la vulnerabilidad (Ninguno, Bajo, Alto).

- **Interacción del Usuario (UI):** Determina si se requiere interacción del usuario para explotar la vulnerabilidad (Ninguna o Requerida).
- **Alcance (S):** Evalúa si la vulnerabilidad afecta sólo al componente vulnerable o a otros componentes (Sin Cambios o Cambiado).
- **Impacto:**
  - **Confidencialidad (C):** Mide el impacto sobre la confidencialidad de los datos (Ninguno, Bajo, Alto).
  - **Integridad (I):** Evalúa el impacto sobre la integridad de los datos (Ninguno, Bajo, Alto).
  - **Disponibilidad (A):** Mide el impacto sobre la disponibilidad de los servicios (Ninguno, Bajo, Alto).

2. **Métricas Temporales:**
   - **Explotabilidad (E):** Indica la facilidad con la que se puede explotar la vulnerabilidad en el entorno actual (No definido, Prueba de Concepto, Funcional, No explotable).
   - **Madurez de la Remediación (RL):** Mide la disponibilidad y efectividad de soluciones para la vulnerabilidad (No definido, Solución Oficial, Solución Temporal, No disponible).
   - **Reportes de Confianza (RC):** Evalúa la confianza en la existencia de la vulnerabilidad (No definido, Confirmado, Razonablemente Confirmado, No confirmado).
3. **Métricas de Entorno:**
   - **Relevancia del Confidencialidad (CR):** Evalúa la importancia de la confidencialidad en el entorno específico (No definido, Baja, Media, Alta).
   - **Relevancia de la Integridad (IR):** Evalúa la importancia de la integridad en el entorno específico (No definido, Baja, Media, Alta).
   - **Relevancia de la Disponibilidad (AR):** Evalúa la importancia de la disponibilidad en el entorno específico (No definido, Baja, Media, Alta).
   - **Modificación de las Métricas Base:** Permite ajustar las métricas base según el entorno específico (Ataque, Complejidad, Privilegios, Interacción del Usuario, Alcance, Confidencialidad, Integridad, Disponibilidad).

1.2. Puntuación CVSS

La puntuación CVSS se calcula combinando las métricas mencionadas, resultando en un valor numérico que generalmente varía entre 0 y 10. Este valor se clasifica en niveles de severidad:

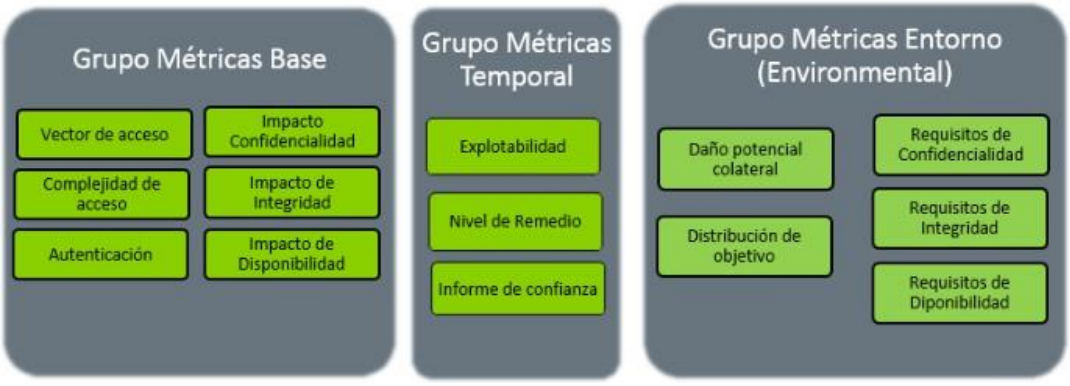
- **Baja (0.1 - 3.9):** Vulnerabilidades que tienen un impacto limitado.
- **Media (4.0 - 6.9):** Vulnerabilidades con un impacto moderado.
- **Alta (7.0 - 8.9):** Vulnerabilidades que tienen un impacto significativo.
- **Crítica (9.0 - 10.0):** Vulnerabilidades con un impacto severo y generalmente explotables de forma remota sin necesidad de autenticación.

Interpretación y Uso

El CVSS es ampliamente utilizado por organizaciones y profesionales de la ciberseguridad para:

- **Priorizar Remediaciones:** Focalizando los recursos en las vulnerabilidades más críticas primero.
- **Evaluar Riesgos:** Proporcionando una métrica común para evaluar el riesgo en diferentes entornos y sistemas.

Al categorizar y puntuar vulnerabilidades a través de CVSS, las organizaciones pueden gestionar de manera más efectiva sus riesgos de seguridad y tomar decisiones informadas sobre la mitigación de vulnerabilidades.

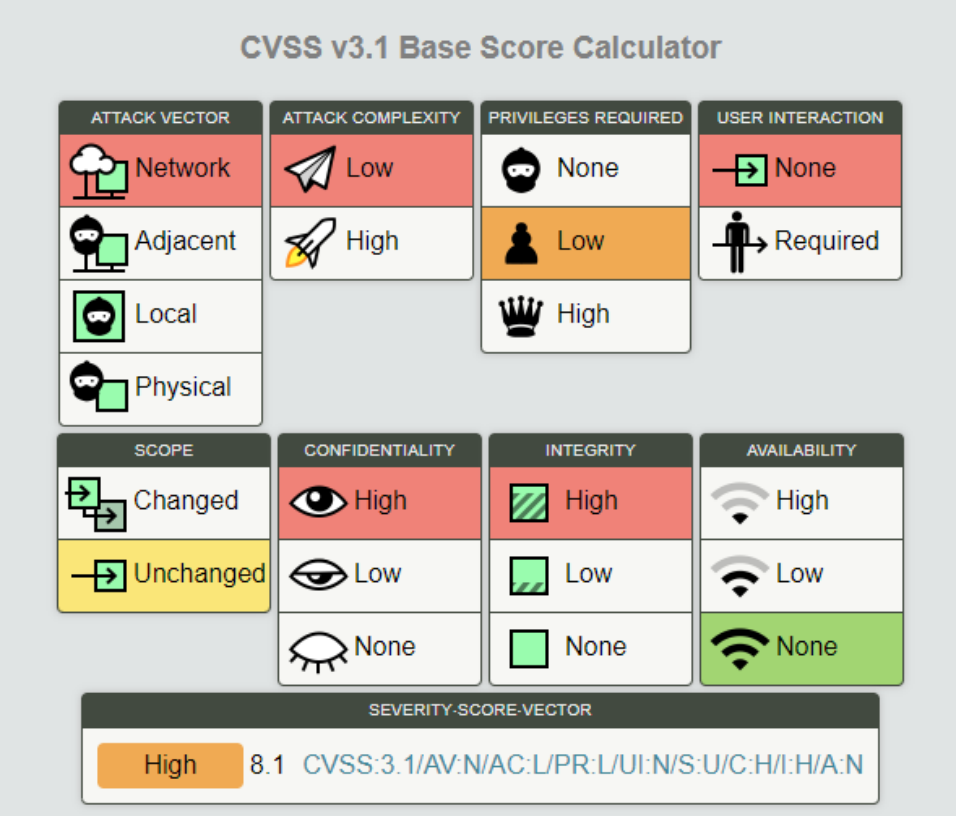


https://www.cyberseguridad.net/calificacion-de-vulnerabilidades-cvss

Common Vulnerabilities and Exposures (CVE): Es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente, categorizando su criticidad basada en las métricas de CVSS y asignándole un ID a cada una de ellas.

Puedes practicar como se categoriza una vulnerabilidad, a través de una calculadora CVSS gratuita:

https://chandanbn.github.io/cvss/



https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

1.3. Ejemplos de vulnerabilidades

- **Ejecución de código remoto en VMware vCenter (CVE-2021-21985)**
  Esto permite a un atacante leer y modificar el contenido del servidor, sus ambientes y su información.
- **ProxyLogon (CVE-2021-26855)**
  Una vulnerabilidad crítica de Microsoft Exchange permite a un atacante obtener privilegios de administrador del servidor. En su

mayoría estos ataques son el primer componente para acceder de manera no autorizada a una organización e infectar equipos dentro de la red con ransomware.

- **PwnKit escalada de privilegios local Linux (CVE-2021-4034)**

La vulnerabilidad se encuentra en el componente pkexec de PolKit, que está en la configuración por defecto de la mayoría de distribuciones Linux.

- **PrintNightmare (CVE-2021-1675)**
  Se le da este nombre a componentes de servicios de impresión de Windows que habilitan a un atacante con el control total del servidor.
- **Log4Shell - Módulos para guardar bitácoras del servidor Apache (log4j) (CVE-2021-44228, CVE-2021-45046 y CVE-2021-45105)**
  Esto permite a un atacante controlar el sistema en su totalidad con un ataque muy simple que afectó a miles de aplicaciones.
- **Eternalblue (ms17-010)**

Es un exploit supuestamente desarrollado por la NSA. Fue filtrado por el grupo de hackers Shadow Brokers el 14 de abril de 2017

- **Zerologon CVE-2020-1472**

Es una vulnerabilidad en la criptografía del proceso de Netlogon de Microsoft que permite un ataque hacer un volcado del ntds de los controladores de dominio.

- **Follina (CVE-2022-30190)**

La vulnerabilidad Follina, permite la explotación de la herramienta Microsoft Support Diagnostic Tool mediante los archivos de MS Office, esto permite a un atacante ejecutar comandos de forma remota.

1.4. Proceso de gestión de vulnerabilidades

La gestión de vulnerabilidades es el proceso de identificar los sistemas y redes que tienen vulnerabilidades conocidas o identificadas, como exploits, fallos, brechas de seguridad, puntos de entrada de acceso inseguros y los errores de configuración del sistema, para así generar un

plan de acción permita remediarlos antes que sean explotados por un actor de amenaza.

Comúnmente son procesos automatizados que utilizan tecnologías que se basan en la identificación de versiones de servicios.

Para mitigar los riesgos asociados con las vulnerabilidades, se utilizan estrategias de gestión de vulnerabilidades, que incluyen:

1. **Identificación y Evaluación:**
    - **Escaneos de Vulnerabilidades:** Utilización de herramientas como Nessus, OpenVAS, o Qualys para identificar y evaluar vulnerabilidades en los sistemas.
    - **Pruebas de Penetración:** Simulación de ataques para identificar debilidades y evaluar la efectividad de las medidas de seguridad.
2. **Mitigación:**
    - **Parches y Actualizaciones:** Aplicación regular de parches de seguridad y actualizaciones de software.
    - **Configuración Segura:** Asegurar configuraciones seguras y deshabilitar servicios innecesarios.
3. **Monitoreo y Respuesta:**
    - **Monitoreo Continuo:** Utilización de sistemas de detección de intrusiones (IDS) y monitoreo continuo para detectar y responder rápidamente a intentos de explotación.
    - **Planes de Respuesta a Incidentes:** Desarrollo e implementación de planes de respuesta a incidentes para mitigar los efectos de las explotaciones exitosas.
4. **Educación y Concientización:**
    - **Capacitación:** Entrenamiento regular del personal en prácticas de seguridad y concientización sobre amenazas y vulnerabilidades.

https://www.b-secure.co/recursos/infografias/proceso-de-gestion-de-vulnerabilidades-seguridad

1.5. Técnicas y herramientas para el análisis de vulnerabilidades

Captura de Banners

La captura de banners es una técnica fundamental en el reconocimiento de redes, utilizada para recolectar información sobre los servicios que se están ejecutando en un host. Un "banner" es una respuesta generada por un servidor o un dispositivo que puede incluir detalles sobre el software y la versión que está ejecutando, así como el sistema operativo subyacente. Esta información es valiosa porque permite a los analistas de seguridad y a los atacantes potenciales identificar vulnerabilidades específicas asociadas con ciertas versiones de software.

- **Telnet**: Una herramienta de línea de comandos que permite a los usuarios conectarse a servicios remotos. Al conectarse a un puerto específico (por ejemplo, puerto 80 para HTTP), Telnet puede revelar el banner del servicio.

- **Netcat**: Similar a Telnet, pero más versátil y poderosa. Puede ser utilizada para conectar a diferentes puertos y servicios, facilitando la captura de banners.
- **Nmap**: Aunque más conocida por el escaneo de puertos, Nmap puede realizar capturas de banners utilizando scripts específicos (por ejemplo, nmap --script banner).

Identificación del Sistema Operativo de un Servidor Web

La identificación del sistema operativo de un servidor web es un paso crucial en el análisis de vulnerabilidades. Conocer el sistema operativo ayuda a los analistas a enfocar sus esfuerzos de seguridad en las debilidades específicas de ese sistema.

- **Telnet**: Al conectar a un servidor web (por ejemplo, utilizando telnet <IP> 80), el banner de respuesta puede incluir información sobre el sistema operativo.
- **Nmap**: Utiliza técnicas avanzadas de huella digital del sistema operativo (OS fingerprinting) para identificar el sistema operativo subyacente. Esto se hace enviando paquetes especialmente diseñados y analizando las respuestas.
- **HTTP Headers**: Los encabezados HTTP de respuesta pueden contener información valiosa. Herramientas como curl o extensiones de navegador pueden extraer estos encabezados.

Exploraciones de Red Personalizadas

Las exploraciones de red personalizadas son esenciales para entender la estructura y los servicios de una red. Permiten a los analistas descubrir hosts activos, identificar puertos abiertos y determinar qué servicios están operativos.

- **Nmap**: Es la herramienta más versátil para exploraciones de red. Permite escaneos básicos (identificación de hosts y puertos abiertos) y avanzados (detección de servicios, huella digital del sistema operativo, scripts de vulnerabilidades).
- **Zenmap**: Optimizada para escaneos rápidos de grandes redes. Aunque menos detallada que Nmap, es útil para obtener una visión general rápidamente.

- **Masscan**: Similar a Zmap, es capaz de escanear toda la Internet en cuestión de minutos.

Bandera en un Paquete

En el contexto de TCP/IP, las banderas (flags) son bits específicos en el encabezado del paquete que controlan o notifican ciertas condiciones de la conexión.

Principales Banderas TCP:

- **URG (Urgent)**: Indica que los datos marcados son urgentes.
- **ACK (Acknowledgment)**: Confirma la recepción de datos.
- **PSH (Push)**: Solicita que los datos sean transmitidos inmediatamente.
- **RST (Reset)**: Reinicia la conexión.
- **SYN (Synchronize)**: Inicia una conexión.
- **FIN (Finish)**: Finaliza una conexión.

Ataque SYN

Un ataque SYN es un tipo de ataque de denegación de servicio (DoS) que explota la forma en que se establece una conexión TCP.

Funcionamiento del Ataque SYN:

- El atacante envía una serie de solicitudes SYN al servidor.
- El servidor responde con un SYN-ACK y espera una respuesta ACK del atacante.
- El atacante no responde con un ACK, dejando la conexión incompleta.
- Esto consume recursos del servidor, que quedan ocupados esperando la finalización de conexiones que nunca ocurren, lo que puede llevar a una denegación de servicio.

Uso de Tor

Tor (The Onion Router) es una red que permite a los usuarios navegar por Internet de manera anónima. En lugar de conectarse directamente a los sitios web, las conexiones son enrutadas a través de una serie de nodos voluntarios, cada uno de los cuales aplica una capa de cifrado.

Ventajas de Usar Tor:

- **Anonimato**: Oculta la dirección IP del usuario.
- **Privacidad**: Cifra el tráfico, protegiendo contra la vigilancia.
- **Acceso a Contenido Restringido**: Permite el acceso a sitios web bloqueados o censurados.

Uso de Proxies

Un proxy actúa como intermediario entre el usuario y el destino al que quiere acceder. Utilizar un proxy durante un escaneo de red puede ofrecer varias ventajas.

Ventajas de Usar Proxies:

- **Anonimato**: Oculta la IP del escáner, dificultando la identificación del origen del escaneo.
- **Evasión de Firewalls**: Algunos proxies pueden eludir reglas de firewall que bloquean el tráfico directo.
- **Acceso a Recursos Restringidos**: Permiten acceder a recursos que pueden estar restringidos por ubicación.

Método para Analizar Vulnerabilidades

Un análisis de vulnerabilidades efectivo sigue un enfoque sistemático para identificar y evaluar posibles debilidades en un sistema.

Pasos Clave:

- **Identificación de Puertos Abiertos**: Utilizar herramientas como Nmap para encontrar puertos accesibles.
- **Detección de Servicios**: Determinar qué servicios están corriendo en esos puertos.

- **Análisis de Versiones**: Identificar las versiones de los servicios para comparar con bases de datos de vulnerabilidades conocidas (por ejemplo, CVE).
- **Evaluación de Vulnerabilidades**: Utilizar herramientas como Nessus o OpenVAS para automatizar el proceso de correlación de servicios y versiones con vulnerabilidades conocidas.

Escaneo Requerido para Nmap

Nmap es principalmente una herramienta de escaneo de puertos, pero también ofrece muchas otras capacidades.

Tipos de Escaneo con Nmap:

- **Escaneo de Puertos**: Identifica puertos abiertos en un host o red.
- **Escaneo de Servicios**: Determina qué servicios están corriendo en los puertos abiertos y sus versiones.
- **Detección de Sistemas Operativos**: Utiliza huellas digitales para identificar el sistema operativo de los hosts.
- **Scripts NSE (Nmap Scripting Engine)**: Permiten ejecutar scripts personalizados para detectar vulnerabilidades específicas, realizar auditorías, y más.

Funcionamiento de una Herramienta de Análisis de Vulnerabilidades

Las herramientas de análisis de vulnerabilidades automatizan el proceso de identificar debilidades en un sistema o red.

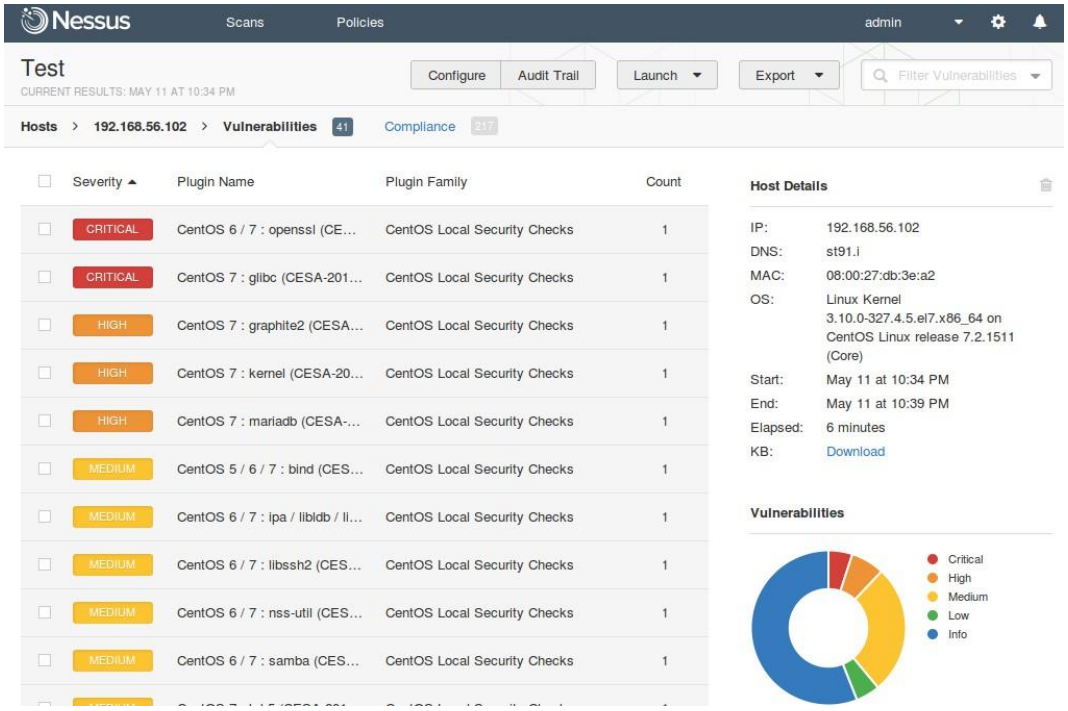
Funcionamiento General:

- **Escaneo de Red**: Detectan hosts y puertos abiertos.
- **Enumeración de Servicios**: Identifican los servicios corriendo en los puertos abiertos y sus versiones.
- **Comparación con Bases de Datos de Vulnerabilidades**: Utilizan bases de datos como CVE, NVD, y otros repositorios para correlacionar las versiones de los servicios con vulnerabilidades conocidas.

- **Generación de Informes**: Proveen informes detallados con las vulnerabilidades encontradas, su criticidad, y recomendaciones para mitigarlas.

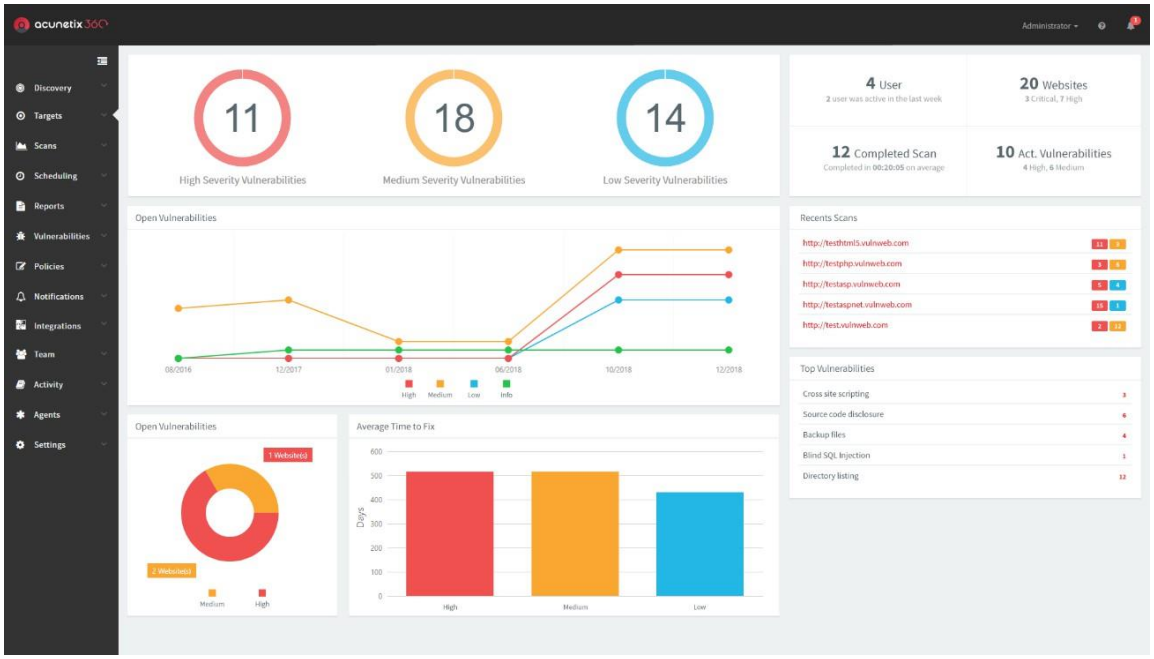
Ejemplos de Herramientas:

- **Nessus**: Muy popular en la industria, conocido por su amplia base de datos de vulnerabilidades.



- **OpenVAS**: Una opción de código abierto, derivada de Nessus.

- **Acunetix**: Ofrece servicios basados en la nube para el análisis de vulnerabilidades.



2. Pon a prueba tus conocimientos

A continuación, te presentamos un test en el que puedes medir tus conocimientos. Tienes la solución en el anexo I.

Actividad Teórica

Pregunta 1: ¿Cómo funciona una herramienta de análisis de vulnerabilidades?

- A) Escanea las políticas del equipo.
- B) Analiza las versiones de los servicios y puertos abiertos para relacionar vulnerabilidades conocidas.
- C) Hace un ataque de denegación de servicio.
- D) Hace una inyección de comandos.

Pregunta 2: ¿Indique un buen método para analizar vulnerabilidades?

- A) Encuentra puertos abiertos
- B) Encuentra debilidades

- C) Encontrar sistemas operativos
- D) Identificar el hardware

Pregunta 3: ¿Qué tipo de escaneo realiza Nmap?

- A) Escaneo de puertos
- B) Análisis de vulnerabilidades
- C) Escaneo de servicio
- D) Análisis de amenazas

Pregunta 4: ¿Cuál de los siguientes se utiliza para captar banners?

- A) Telnet
- B) FTP
- C) SSH
- D) Wireshark

Pregunta 5: ¿Cuál de los siguientes se utiliza para identificar un sistema operativo de servidor web?

- A) Telnet
- B) Redes sociales
- C) Fragroute
- D) Wireshark

Pregunta 6: ¿Cuál de los siguientes se utiliza para realizar enumeraciones de red personalizadas?

- A) Nessus
- B) Wireshark
- C) AirPcap
- D) Nmap

Pregunta 7: ¿Cuál de las siguientes no es una bandera en un paquete?

- A) URG
- B) PHS
- C) RST
- D) FIN

Pregunta 8: ¿Qué protocolo utiliza un ataque SYN?

- A) TCP
- B) UDP
- C) HTTP
- D) Telnet

Pregunta 9: ¿Para qué se utiliza Tor?

- A) Para ocultar la navegación web
- B) Para ocultar el proceso de escaneo
- C) Para automatizar el escaneo
- D) Para ocultar el banner en un sistema

Pregunta 10: ¿Por qué necesitaría utilizar un proxy para realizar el escaneo?

- A) Para mejorar el anonimato
- B) Para engañar a los firewalls
- C) Realizar exploraciones semiabiertas
- D) Para realizar exploraciones completamente abiertas

Ver respuestas correctas en el Anexo I

3. Laboratorio Práctico – Ejecución de Escaneo de Vulnerabilidades

Vamos a utilizar una de las herramientas más populares y poderosas en el campo de la ciberseguridad: Nessus. Te guiaremos a través de los pasos para **configurar y ejecutar un escaneo de vulnerabilidades** con Nessus, así como interpretar los resultados obtenidos.

Instalación y configuración de Nessus

Primero, necesitamos instalar Nessus en nuestra máquina. Para ello, visita el sitio web oficial de Tenable, descarga el instalador correspondiente a tu sistema operativo y sigue las instrucciones de instalación. Una vez instalado, abre tu navegador y navega a https://localhost:8834 para acceder a la interfaz web de Nessus.

Creación de un nuevo escaneo

Una vez que Nessus esté listo, vamos a crear un nuevo escaneo. Haz clic en el botón 'Nuevo Escaneo' y selecciona el tipo de escaneo que deseas realizar. Para este laboratorio, utilizaremos el perfil 'Basic Network Scan'.

Dale un nombre a tu escaneo, por ejemplo, 'Escaneo de Red Local', y especifica la dirección IP o el rango de direcciones IP de los sistemas

que deseas escanear. Puedes ingresar una sola dirección IP, un rango de direcciones o una subred completa.

Configuración de opciones avanzadas

A continuación, vamos a ajustar algunas opciones avanzadas. En la pestaña 'Configuración', puedes especificar credenciales para escaneos autenticados, ajustar los niveles de rendimiento y configurar alertas. Para este laboratorio, dejaremos las opciones predeterminadas, pero es importante saber que estas configuraciones existen y pueden ser muy útiles en entornos más complejos.

Ejecución del escaneo

Con todas las configuraciones listas, haz clic en 'Guardar' y luego en 'Iniciar Escaneo'. Nessus comenzará a analizar la red y buscará posibles vulnerabilidades en los sistemas especificados. Este proceso puede tardar desde unos pocos minutos hasta varias horas, dependiendo del tamaño de la red y el número de dispositivos.

Análisis de resultados

Una vez completado el escaneo, podrás ver un resumen de los resultados en el panel de Nessus. Haz clic en el nombre del escaneo para ver detalles más específicos. Los resultados se organizan por niveles de severidad: Crítica, Alta, Media y Baja.

Revisa cada vulnerabilidad detectada. Nessus proporciona descripciones detalladas, incluyendo el impacto potencial, las soluciones recomendadas y enlaces a recursos adicionales para obtener más información.

Mitigación y corrección de vulnerabilidades

El siguiente paso es mitigar o corregir las vulnerabilidades encontradas. Esto puede incluir aplicar parches, configurar correctamente los sistemas, actualizar software obsoleto o implementar medidas de seguridad adicionales.

Recuerda documentar cada acción tomada y realizar escaneos de seguimiento para asegurarte de que las vulnerabilidades hayan sido efectivamente corregidas.

4. Caso práctico: Análisis de vulnerabilidades

Objetivo:

Realizar un análisis de vulnerabilidades a un equipo Windows utilizando Nessus para identificar posibles riesgos de seguridad y aplicar medidas correctivas.

Pre-requisitos:

1. Equipo Windows con acceso a Internet.
2. Nessus instalado y configurado en el equipo o en otro dispositivo dentro de la misma red. (tenable.com)
3. Credenciales administrativas del equipo Windows a analizar.

Paso 1: Instalación y Configuración de Nessus

1. **Descargar Nessus:**
    - Visita el sitio oficial de Tenable y descarga el instalador de Nessus correspondiente a tu sistema operativo.

https://www.tenable.com/downloads/nessus?loginAttempted=true

    - Sigue las instrucciones de instalación y, una vez completado, abre tu navegador y navega a https://localhost:8834.
2. **Crear una Cuenta y Activar Nessus:**
    - Regístrate y activa tu producto con licencia "Home" usando el código proporcionado.
    - Espera a que Nessus descargue los últimos plugins y actualizaciones.

Paso 2: Preparación del Escaneo

1. **Iniciar Sesión en Nessus:**
    - Abre la interfaz web de Nessus e inicia sesión con tus credenciales.
2. **Crear un Nuevo Escaneo:**

- Haz clic en 'Nuevo Escaneo' y selecciona 'Basic Network Scan'.
- Asigna un nombre a tu escaneo, por ejemplo, 'Escaneo Windows'.
- En 'Targets', ingresa la dirección IP de tu equipo Windows. Si estás escaneando desde el mismo equipo, puedes usar 127.0.0.1.

3. **Configurar Escaneo Autenticado:**
   - Ve a la pestaña 'Credentials' y selecciona 'Windows'.
   - Ingresa las credenciales administrativas de tu equipo Windows para permitir un escaneo autenticado, lo que proporcionará resultados más detallados.

Paso 3: Ejecutar el Escaneo

1. **Guardar y Ejecutar el Escaneo:**
   - Revisa las configuraciones y haz clic en 'Save'.
   - Inicia el escaneo haciendo clic en 'Launch'.
   - Espera a que el escaneo se complete. El tiempo puede variar según el número de vulnerabilidades y la configuración del sistema.

Paso 4: Análisis de Resultados

1. **Ver Resultados del Escaneo:**
   - Una vez finalizado el escaneo, haz clic en el nombre del escaneo para ver los resultados detallados.
   - Nessus mostrará una lista de vulnerabilidades organizadas por niveles de severidad: Crítica, Alta, Media y Baja.
2. **Interpretar los Resultados:**
   - Examina cada vulnerabilidad detectada. Nessus proporciona una descripción, el impacto potencial, las soluciones recomendadas y enlaces a recursos adicionales.

Paso 5: Mitigación de Vulnerabilidades

1. **Aplicar Parches y Actualizaciones:**
    - Instala los parches de seguridad recomendados por Nessus.
    - Actualiza cualquier software obsoleto que Nessus haya identificado como vulnerable.
2. **Revisar y Documentar:**
    - Documenta todas las acciones correctivas que tomaste.

Paso 6: Reescaneo y Confirmación

1. **Ejecutar un Escaneo de Seguimiento:**
    - Realiza un nuevo escaneo en Nessus para confirmar que todas las vulnerabilidades han sido corregidas.
    - Verifica que no se detecten nuevas vulnerabilidades o que las existentes hayan sido mitigadas.

4. ¿Qué has aprendido?

A lo largo de este bloque de contenido, has aprendido:

- Conceptos básicos sobre vulnerabilidades
- Como calcular la criticidad de una vulnerabilidad a través de CVSS
- Herramientas para realizar análisis de vulnerabilidades
- Ejercicios prácticos para aplicar los conocimientos obtenidos.
- Ejemplos de Vulnerabilidades y CVE
- Técnicas para un análisis de Vulnerabilidades
- Ciclo de vida de un proceso de Gestión de Vulnerabilidades

5. Preguntas frecuentes

1. ¿Cuál es la diferencia entre un escaneo de vulnerabilidades y una prueba de penetración (pentesting)?

Respuesta: Un escaneo de vulnerabilidades es un proceso automatizado que utiliza herramientas para identificar debilidades conocidas en sistemas, redes o aplicaciones. Este escaneo proporciona una lista de vulnerabilidades potenciales, clasificadas por severidad, y generalmente no intenta explotar estas vulnerabilidades.

Por otro lado, una prueba de penetración (pentesting) es un enfoque más profundo y manual que simula ataques reales para no solo identificar, sino también explotar vulnerabilidades en un entorno controlado. Los pentesters emplean técnicas similares a las de los atacantes para evaluar la seguridad de los sistemas, permitiendo una comprensión más precisa del riesgo y la efectividad de las defensas de seguridad.

2. ¿Qué debo hacer después de identificar vulnerabilidades en los sistemas?

Respuesta: Una vez que has identificado vulnerabilidades en tu sistema, sigue estos pasos para mitigar los riesgos:

1. Priorizar Vulnerabilidades:

Utiliza la clasificación de severidad proporcionada por herramientas como Nessus y el puntaje CVSS para priorizar las vulnerabilidades críticas y de alta severidad.

2. Aplicar Parches:

Instala parches y actualizaciones de seguridad proporcionados por los proveedores de software para corregir las vulnerabilidades identificadas.

3. Configurar Correctamente los Sistemas:

Ajusta configuraciones de seguridad según las mejores prácticas recomendadas para reducir el riesgo de explotación.

4. Implementar Medidas de Mitigación:

Considera soluciones temporales o adicionales, como reglas de firewall,

políticas de acceso más restrictivas o deshabilitar servicios vulnerables, mientras se aplican parches definitivos.

5. Realizar Escaneos de Seguimiento:

Realiza nuevos escaneos para asegurarte de que las vulnerabilidades hayan sido efectivamente mitigadas y que no se hayan introducido nuevas debilidades.

6. Documentar y Comunicar:

Registra todas las acciones tomadas y los resultados obtenidos. Informa a las partes interesadas sobre el estado de las vulnerabilidades y las medidas adoptadas.

6. Glosario

- ✓ CVSS (Common Vulnerability Scoring System): - Un estándar para evaluar la severidad de las vulnerabilidades en sistemas informáticos, proporcionando un puntaje de 0 a 10 que ayuda a priorizar la mitigación.
- ✓ Escaneo de Vulnerabilidades: - Proceso automatizado que utiliza herramientas para buscar debilidades conocidas en un sistema, red o aplicación.
- ✓ Explotación: - Técnica utilizada por los atacantes para aprovechar una vulnerabilidad en un sistema para ejecutar código malicioso, acceder a datos o interrumpir servicios.
- ✓ Falsos Positivos: - Resultados del análisis de vulnerabilidades que indican la presencia de una vulnerabilidad cuando en realidad no existe.
- ✓ Falsos Negativos: - Fallas en el análisis de vulnerabilidades que no detectan una vulnerabilidad existente en el sistema.
- ✓ Parche de Seguridad: - Actualización de software diseñada para corregir una vulnerabilidad de seguridad específica.
- ✓ Penetration Testing (Pentesting): - Prueba de seguridad que simula un ataque real para identificar y explotar vulnerabilidades en un sistema.
- ✓ Riesgo: - Combinación de la probabilidad de que ocurra un incidente de seguridad y el impacto potencial de dicho incidente.
- ✓ Remediación: - Proceso de corregir una vulnerabilidad o debilidad en un sistema para mitigar riesgos de seguridad.

- ✓ Mitigación: - Medidas y controles implementados para reducir la probabilidad o el impacto de una vulnerabilidad de seguridad.
- ✓ Privilegios Requeridos (PR): - Nivel de acceso necesario para explotar una vulnerabilidad. Puede ser ninguno, bajo o alto.
- ✓ Vector de Ataque (AV): - Forma en que un atacante puede explotar una vulnerabilidad, como a través de la red, localmente, adyacente, o físicamente.
- ✓ Complejidad del Ataque (AC): - Nivel de dificultad requerido para explotar una vulnerabilidad, puede ser bajo o alto.
- ✓ Interacción del Usuario (UI): - Indica si la explotación de una vulnerabilidad requiere la interacción de un usuario legítimo del sistema.
- ✓ Alcance (S): - Evalúa si una vulnerabilidad afecta solo al componente vulnerable o también a otros componentes del sistema.

- ✓ Impacto: - Efecto de la explotación de una vulnerabilidad en la confidencialidad, integridad y disponibilidad de los datos o servicios.
- ✓ Exploit: - Herramienta, técnica o código utilizado para aprovechar una vulnerabilidad en un sistema.
- ✓ Ingeniería Social: - Técnica de ataque que utiliza la manipulación psicológica de las personas para obtener información confidencial o acceso no autorizado a sistemas.
- ✓ Evaluación de Seguridad: - Proceso sistemático de revisar y analizar la seguridad de un sistema, red o aplicación para identificar vulnerabilidades y riesgos.
- ✓ Gestión de Vulnerabilidades: - Proceso continuo de identificación, evaluación, tratamiento y monitoreo de las vulnerabilidades en los sistemas de una organización.
- ✓ Prueba de Concepto (PoC): - Demostración técnica que muestra cómo se puede explotar una vulnerabilidad, sin causar daño significativo.
- ✓ Reporte de Vulnerabilidades: - Documento que detalla las vulnerabilidades identificadas durante un análisis, incluyendo su severidad, impacto y recomendaciones de mitigación.

✓ Sistema de Gestión de Seguridad de la Información (SGSI): - Marco de políticas y procedimientos que incluye todos los controles de seguridad y gestión de riesgos necesarios para la protección de la información.

7. Anexo I - Respuestas

Respuestas:

- Pregunta 1 - Respuesta: B
- Pregunta 2 - Respuesta: A
- Pregunta 3 - Respuesta: A
- Pregunta 4 - Respuesta: A
- Pregunta 5 - Respuesta: A
- Pregunta 6 - Respuesta: D
- Pregunta 7 - Respuesta: B
- Pregunta 8 - Respuesta: A
- Pregunta 9 - Respuesta: B
- Pregunta 10 - Respuesta: A

Autor de esta guía

Julián David Delgado Piraquive

Head of Offensive Security & MDR

Julián es un experto en ciberseguridad, especializado en seguridad ofensiva y respuesta ante incidentes. Lidera equipos de Red Team y MDR en Factum Information Technologies, además es docente de Máster de Ciberseguridad.

Ver más contenido de este autor

Puedes encontrar más contenido como este en www.cylum.tech

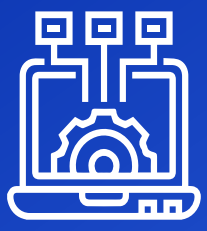
Cylum

CYBERSECURITY AS A SERVICE

Simplificamos la ciberseguridad

Soluciona tus necesidades de protección ante riesgos digitales. Cumple con la regulación.

Personal Experto



Tecnología

Cumplimiento normativo

Protección 24x7

Una solución de

FACTUM

15 años protegiendo empresas