Info de Cisco

Módulo 3: Recopilación de información y análisis de vulnerabilidades

3.3.7 Desafíos a tener en cuenta al ejecutar un análisis de vulnerabilidades

Las secciones anteriores han abordado una serie de cosas diferentes que deben tener en cuenta la forma en que realiza el escaneo. Las secciones siguientes brindan más detalles sobre algunas de las cuestiones específicas que debe tener en cuenta al crear una política de escaneo y realizar los escaneos. Para obtener más información, seleccione cada uno de los siguientes desafíos para tener en cuenta.

Consideración del mejor momento para realizar un escaneo

El momento en el que se debe ejecutar un escaneo suele ser lo más preocupante cuando se analiza una red de producción. Si está escaneando un dispositivo en un entorno de laboratorio, normalmente no hay mucha preocupación porque el entorno de laboratorio no está siendo utilizado por aplicaciones críticas. Hay algunas razones por las que la ejecución de un escaneo en una red de producción debe realizarse con cuidado. En primer lugar, el tráfico de red generado por un escaneo de vulnerabilidades puede causar y causará mucho ruido en la red. También puede causar una congestión significativa, especialmente cuando los escaneos atraviesan varios saltos de red. (Hablaremos de esto en breve).

Otra consideración al elegir un momento para ejecutar un escaneo es el hecho de que muchas de las opciones o complementos que se realizan en un escaneo de vulnerabilidades pueden bloquear el dispositivo objetivo y la infraestructura de la red. Por este motivo, debe asegurarse de que, al escanear en una red de producción, lo haga en los momentos que tendrán el menor impacto posible en los usuarios finales y los servidores. La mayoría de las veces, es mejor escanear en las primeras horas del día, cuando nadie está usando la red para fines críticos.

Determinar qué protocolos están en uso

Una de las primeras cosas que debe saber sobre una red o un dispositivo de destino antes de comenzar a ejecutar escaneo de vulnerabilidades es qué protocolos se utilizan. Si un dispositivo de destino utiliza protocolos TCP y UDP para los servicios en ejecución, y solo ejecuta un escaneo de vulnerabilidades en los puertos TCP, se perderán las vulnerabilidades que puedan encontrarse en los servicios UDP.

Topología de la red

Como se mencionó anteriormente, la topología de la red siempre debe considerarse cuando se trata del escaneo de vulnerabilidades. Por supuesto, nunca se recomienda escanear a través de una conexión WAN porque afectaría significativamente a cualquiera de los dispositivos a lo largo de la ruta. La regla general al determinar en qué parte de la topología de la red se debe ejecutar un escaneo de vulnerabilidades es que siempre se debe realizar lo más cerca posible del objetivo. Por ejemplo, si está escaneando un servidor de Windows que se encuentra dentro de su subred filtrada (anteriormente conocida como zona desmilitarizada o DMZ), la mejor ubicación para el escáner de vulnerabilidades es junto al

servidor en la subred filtrada. Al colocarlo allí, puede eliminar cualquier preocupación sobre el impacto de los dispositivos que atraviesa el tráfico de su escáner.
Además del impacto en la infraestructura de la red, otra preocupación es que cualquier dispositivo que atraviese también podría afectar los resultados del escáner. Esto es más preocupante al atravesar un dispositivo de cortafuegos; Además, otros dispositivos de la infraestructura de red también podrían afectar los resultados.

Limitaciones del ancho de banda

Tomemos un momento para considerar los efectos de las limitaciones de ancho de banda en el escaneo de vulnerabilidades. Obviamente, cada vez que inunde una red con una gran cantidad de tráfico, se producirá un problema con la cantidad de ancho de banda disponible. Como profesional de pruebas de penetración, debe conocer cómo afecta el ancho de banda de las redes o los sistemas que está escaneando. Específicamente, según la cantidad de ancho de banda que tenga entre el escáner y el objetivo, es posible que deba ajustar la configuración del escáner para adaptarse a situaciones de menor ancho de banda. Si está escaneando un enlace de VPN o WAN que probablemente tenga un ancho de banda limitado, querrá ajustar sus opciones de escaneo para no causar problemas de consumo de ancho de banda. Las configuraciones que deben ajustarse suelen ser las relacionadas con los ataques de tipo desbordamiento y denegación de servicio (DoS).

Limitación de consultas

Para solucionar el problema de las limitaciones de ancho de banda y el escaneo de vulnerabilidades, a menudo puede ser útil ralentizar el tráfico creado por el escáner. Esto a menudo se denomina limitación de consultas y, por lo general, se puede lograr modificando las opciones de la política de escaneo. Una forma de hacerlo es reducir la cantidad de subprocesos de ataque que se envían al objetivo al mismo tiempo. No hay una regla general específica para la cantidad de subprocesos. Realmente depende de la solidez del objetivo. Algunos objetivos son más frágiles que otros. Otra forma de lograr esto es reducir el alcance de los complementos/ataques que el escáner está buscando. Si sabe que el dispositivo de destino es un servidor Linux, puede deshabilitar los ataques para otros sistemas operativos, como Windows. Aunque los ataques no funcionarán contra el servidor Linux, aún necesita recibir y responder al tráfico. Este tráfico adicional puede causar un cuello de botella en el procesamiento y el consumo de tráfico de red. Limitar la cantidad de solicitudes a las que el objetivo debería responder reduciría el riesgo de causar problemas, como bloquearse en el objetivo, y dar como resultado un escaneo más exitoso.

Sistemas frágiles/activos no tradicionales

Al utilizar un escáner de vulnerabilidades en su red interna, debe tener en cuenta los dispositivos de la red que podrían no resistir el tráfico que les arroja un escáner de vulnerabilidades. Para estos sistemas, es posible que deba ajustar las opciones de escaneo para reducir el riesgo de bloqueo de los dispositivos o eximir por completo los dispositivos específicos del escaneo. Desafortunadamente, al eximir los dispositivos específicos, se reduce la seguridad general del entorno.

Las impresoras a menudo se consideran "sistemas frágiles". Históricamente, han sido dispositivos que no han podido resistir los intentos de escaneo de vulnerabilidades. Con el aumento de los dispositivos de IoT, hoy en día hay muchos más dispositivos que pueden considerarse frágiles y debe tenerlos en cuenta al planificar el escaneo de vulnerabilidades. La forma típica de abordar los dispositivos frágiles es eximirlos de un escaneo; sin embargo, estos dispositivos pueden suponer un riesgo para el entorno y deben analizarse. Para solucionar este problema, puede "limitar" la frecuencia de escaneo y las opciones utilizadas en la política de escaneo para reducir la probabilidad de que el dispositivo falle.

CONSEJO

El tiempo de ejecución de los escaneos también puede estar determinado por la persona o la empresa que lo contrató para realizar la prueba de penetración. En algunos casos, es posible que no se le permita realizar el escaneo durante el horario comercial.

3.3.7 Desafíos

Desafíos a Tener en Cuenta al Ejecutar un Análisis de Vulnerabilidades

El análisis de vulnerabilidades es una tarea crítica dentro de cualquier programa de seguridad ofensiva o defensiva. Sin embargo, su correcta ejecución requiere tener en cuenta diversos factores que pueden afectar tanto la precisión de los resultados como la estabilidad de la infraestructura evaluada. A continuación se detallan los principales desafíos y consideraciones clave que deben contemplarse al momento de planificar y llevar a cabo un escaneo de vulnerabilidades:

---

1. Consideración del Mejor Momento para Realizar un Escaneo

Uno de los aspectos más importantes en la planificación de un escaneo es el **momento de su ejecución**, especialmente cuando se trabaja sobre una red de producción. A diferencia de un entorno de laboratorio —donde no se ejecutan aplicaciones críticas—, en redes reales el escaneo puede generar un alto volumen de tráfico que:

- Produce **ruido** en la red, dificultando otras operaciones.
- Puede **saturar enlaces** si atraviesa múltiples saltos de red.
- **Bloquea servicios** o incluso dispositivos, especialmente cuando se activan ciertos complementos o scripts agresivos.

Recomendación: Realizar los escaneos durante **horas de baja actividad**, como la madrugada o fines de semana, para minimizar el impacto en la disponibilidad de servicios críticos. Además, el tiempo de ejecución puede estar regulado por el cliente o la organización contratante, quienes pueden restringirlo fuera del horario comercial.

---

2. Determinar Qué Protocolos Están en Uso

Antes de iniciar cualquier escaneo, es fundamental **identificar los protocolos activos** en los dispositivos destino. Muchos servicios importantes pueden estar utilizando **UDP además de TCP**. Si el escaneo sólo considera puertos TCP, se podrían pasar por alto vulnerabilidades críticas presentes en servicios UDP, como DNS o SNMP.

Recomendación: Incluir tanto escaneos TCP como UDP para obtener una visión más completa del estado de seguridad.

---

3. Topología de Red y Ubicación del Escáner

La **topología de red** influye directamente en la eficacia del escaneo. Ejecutar escaneos a través de una conexión WAN, VPN o segmentos remotos puede:

- Generar **latencias y pérdidas** de paquetes.
- Afectar los resultados debido al filtrado por dispositivos intermedios como firewalls.
- Generar **congestión innecesaria** que puede ser evitada.

Recomendación: Ubicar el escáner **lo más cerca posible del objetivo**, idealmente dentro de la misma subred. Por ejemplo, si se va a escanear un servidor en la DMZ, el escáner debe estar ubicado también en la DMZ para evitar distorsión del tráfico.

---

4. Limitaciones del Ancho de Banda

El escaneo de vulnerabilidades genera una considerable cantidad de tráfico, lo que puede suponer un problema en entornos con **ancho de banda limitado**, como enlaces WAN o conexiones VPN.

Recomendación: Ajustar la configuración del escáner para limitar el consumo de ancho de banda. Esto puede implicar:

- Evitar módulos de escaneo agresivos como ataques DoS o fuzzing masivo.
- Establecer límites en la velocidad de escaneo y concurrencia.

---

5. Limitación de Consultas (Query Throttling)

Una técnica clave para mitigar el impacto del escaneo es la **limitación de consultas**, que consiste en reducir la carga generada por el escáner. Esto puede realizarse mediante:

- Disminución del número de **hilos simultáneos** de ataque.
- Reducción del número de **complementos o plugins** activados, ajustándolos al sistema operativo o servicio detectado.

Ejemplo: Si se escanea un servidor Linux, no tiene sentido activar plugins destinados a Windows, ya que solo generan tráfico innecesario que consume recursos y ancho de banda.

---

6. Consideración de Sistemas Frágiles y Activos No Tradicionales

Algunos dispositivos de red, conocidos como **sistemas frágiles**, no están diseñados para soportar tráfico de escaneo intensivo. Entre estos destacan:

- Impresoras.
- Dispositivos IoT (cámaras, sensores, asistentes digitales).
- Equipamiento industrial (ICS/SCADA).

Recomendación:

- **Excluir** estos dispositivos del escaneo o, si se incluyen, aplicar políticas de escaneo **personalizadas**, menos agresivas.
- Implementar escaneos de baja frecuencia o utilizar escaneos pasivos si se desea evaluar la seguridad sin impacto.

Resumen Final

A la hora de llevar a cabo un análisis de vulnerabilidades, el profesional de ciberseguridad debe actuar con **criterio técnico, planificación estratégica y responsabilidad operacional**. No basta con ejecutar herramientas de forma automática; es necesario comprender:

- La infraestructura de red.
- La sensibilidad del entorno.
- Las capacidades de los equipos analizados.
- Las limitaciones técnicas y humanas del cliente o la organización.

Con una adecuada configuración del escáner y una política de escaneo bien definida, se puede obtener un análisis útil, preciso y seguro, que aporte valor real al programa de seguridad de cualquier empresa.

Tareas

🔐 Desafíos al ejecutar un análisis de vulnerabilidades

1. Falsos positivos y falsos negativos

- **Falsos positivos**: Son vulnerabilidades reportadas que en realidad **no existen**. Esto puede generar una carga innecesaria de trabajo y provocar desconfianza en los resultados.
- **Falsos negativos**: Son vulnerabilidades reales que el escáner **no detecta**, dejando puertas abiertas sin saberlo.

💡 *Solución recomendada:* Complementar los escaneos automatizados con validación manual y herramientas distintas (Nessus, OpenVAS, Nmap scripts, Nikto, etc.).

---

2. Configuración incorrecta del escáner

Muchos escáneres requieren ajustes según:

- El tipo de red o sistema operativo objetivo.
- El entorno (producción, desarrollo, etc.).
- El nivel de profundidad del análisis (rápido vs. completo).

💡 *Solución recomendada:* Crear perfiles de escaneo personalizados y realizar pruebas en entornos controlados antes de aplicar en producción.

---

3. Impacto en el sistema analizado

Algunos escaneos agresivos pueden:

- Causar caídas del servicio.
- Generar lentitud o bloqueos.
- Alterar logs o comportamientos del sistema.

💡 *Solución recomendada:* Planificar los escaneos fuera del horario productivo y realizar pruebas en entornos aislados (laboratorios).

---

4. Acceso insuficiente o incompleto

Los escáneres necesitan permisos para acceder a ciertos servicios o configuraciones (por ejemplo, escaneos autenticados). Sin permisos adecuados, los resultados serán **superficiales** o **incompletos**.

💡 *Solución recomendada:* Configurar credenciales de usuario con permisos limitados pero suficientes para realizar escaneos autenticados.

---

5. Entornos complejos o distribuidos

En sistemas con microservicios, contenedores o múltiples VLANs, un escáner puede no alcanzar todos los activos, especialmente si hay firewalls internos o segmentaciones.

💡 *Solución recomendada:* Usar escáneres distribuidos, realizar análisis por segmentos, y mapear previamente toda la red y activos críticos.

---

6. Falta de contexto o priorización

No todas las vulnerabilidades tienen el mismo riesgo. Algunas son **bajas en criticidad**, pero aparecen en la lista junto con otras más peligrosas, lo cual **puede confundir** o hacer perder tiempo.

💡 *Solución recomendada:* Priorizar según CVSS, impacto en el negocio y facilidad de explotación (usando matrices de riesgo).

---

7. No integración con el ciclo de vida del software (SDLC)

En entornos DevOps o CI/CD, si el análisis no se automatiza ni se integra en el pipeline, se detectan fallos demasiado tarde.

💡 *Solución recomendada:* Integrar herramientas de análisis estático y dinámico en cada fase del desarrollo.

---

8. Desactualización de la base de datos de firmas

Si la herramienta de análisis no tiene su base de datos de vulnerabilidades actualizada, es probable que **no detecte amenazas recientes** (como 0-days conocidos recientemente).

💡 *Solución recomendada:* Mantener siempre actualizado el escáner y validar contra fuentes como NVD, CVE Details o feeds de seguridad.

---

9. Falta de interpretación técnica

A veces, los informes generados no son claros para el equipo técnico o no están en lenguaje comprensible para directivos.

💡 *Solución recomendada:* Traducir los hallazgos a un lenguaje accesible para los stakeholders y acompañarlos de recomendaciones prácticas.

---

10. Cumplimiento normativo y ético

Ejecutar un análisis sin permisos o en redes ajenas puede violar leyes como el RGPD, la LOPD o normas internas de las empresas.

💡 *Solución recomendada:* Tener siempre una **autorización por escrito** antes de ejecutar cualquier tipo de análisis.

🧭 En resumen:

Categoría	Desafíos clave
Técnicos	Falsos positivos/negativos, configuración errónea, impacto en el sistema
Operativos	Escaneos incompletos, entornos complejos, integración deficiente
Organizativos	Priorización, interpretación, cumplimiento legal

Desafíos a Tener en Cuenta al Ejecutar un Análisis de Vulnerabilidades

El análisis de vulnerabilidades es una tarea crítica dentro de cualquier programa de seguridad ofensiva o defensiva. Sin embargo, su correcta ejecución requiere tener en cuenta diversos factores que pueden afectar tanto la precisión de los resultados como la estabilidad de la infraestructura evaluada. A continuación se detallan los principales desafíos y consideraciones clave que deben contemplarse al momento de planificar y llevar a cabo un escaneo de vulnerabilidades:

---

1. Consideración del Mejor Momento para Realizar un Escaneo

Uno de los aspectos más importantes en la planificación de un escaneo es el **momento de su ejecución**, especialmente cuando se trabaja sobre una red de producción. A diferencia de un entorno de laboratorio —donde no se ejecutan aplicaciones críticas—, en redes reales el escaneo puede generar un alto volumen de tráfico que:

- Produce **ruido** en la red, dificultando otras operaciones.
- Puede **saturar enlaces** si atraviesa múltiples saltos de red.
- **Bloquea servicios** o incluso dispositivos, especialmente cuando se activan ciertos complementos o scripts agresivos.

Recomendación: Realizar los escaneos durante **horas de baja actividad**, como la madrugada o fines de semana, para minimizar el impacto en la disponibilidad de servicios críticos. Además, el tiempo de ejecución puede estar regulado por el cliente o la organización contratante, quienes pueden restringirlo fuera del horario comercial.

---

2. Determinar Qué Protocolos Están en Uso

Antes de iniciar cualquier escaneo, es fundamental **identificar los protocolos activos** en los dispositivos destino. Muchos servicios importantes pueden estar utilizando **UDP además de TCP**. Si el escaneo sólo considera puertos TCP, se podrían pasar por alto vulnerabilidades críticas presentes en servicios UDP, como DNS o SNMP.

Recomendación: Incluir tanto escaneos TCP como UDP para obtener una visión más completa del estado de seguridad.

---

3. Topología de Red y Ubicación del Escáner

La **topología de red** influye directamente en la eficacia del escaneo. Ejecutar escaneos a través de una conexión WAN, VPN o segmentos remotos puede:

- Generar **latencias y pérdidas** de paquetes.
- Afectar los resultados debido al filtrado por dispositivos intermedios como firewalls.
- Generar **congestión innecesaria** que puede ser evitada.

Recomendación: Ubicar el escáner **lo más cerca posible del objetivo**, idealmente dentro de la misma subred. Por ejemplo, si se va a escanear un servidor en la DMZ, el escáner debe estar ubicado también en la DMZ para evitar distorsión del tráfico.

---

4. Limitaciones del Ancho de Banda

El escaneo de vulnerabilidades genera una considerable cantidad de tráfico, lo que puede suponer un problema en entornos con **ancho de banda limitado**, como enlaces WAN o conexiones VPN.

Recomendación: Ajustar la configuración del escáner para limitar el consumo de ancho de banda. Esto puede implicar:

- Evitar módulos de escaneo agresivos como ataques DoS o fuzzing masivo.
- Establecer límites en la velocidad de escaneo y concurrencia.

---

5. Limitación de Consultas (Query Throttling)

Una técnica clave para mitigar el impacto del escaneo es la **limitación de consultas**, que consiste en reducir la carga generada por el escáner. Esto puede realizarse mediante:

- Disminución del número de **hilos simultáneos** de ataque.
- Reducción del número de **complementos o plugins** activados, ajustándolos al sistema operativo o servicio detectado.

Ejemplo: Si se escanea un servidor Linux, no tiene sentido activar plugins destinados a Windows, ya que solo generan tráfico innecesario que consume recursos y ancho de banda.

---

6. Consideración de Sistemas Frágiles y Activos No Tradicionales

Algunos dispositivos de red, conocidos como **sistemas frágiles**, no están diseñados para soportar tráfico de escaneo intensivo. Entre estos destacan:

- Impresoras.
- Dispositivos IoT (cámaras, sensores, asistentes digitales).
- Equipamiento industrial (ICS/SCADA).

Recomendación:

- **Excluir** estos dispositivos del escaneo o, si se incluyen, aplicar políticas de escaneo **personalizadas**, menos agresivas.
- Implementar escaneos de baja frecuencia o utilizar escaneos pasivos si se desea evaluar la seguridad sin impacto.

Resumen Final

A la hora de llevar a cabo un análisis de vulnerabilidades, el profesional de ciberseguridad debe actuar con **criterio técnico, planificación estratégica y responsabilidad operacional**. No basta con ejecutar herramientas de forma automática; es necesario comprender:

- La infraestructura de red.
- La sensibilidad del entorno.
- Las capacidades de los equipos analizados.
- Las limitaciones técnicas y humanas del cliente o la organización.

Con una adecuada configuración del escáner y una política de escaneo bien definida, se puede obtener un análisis útil, preciso y seguro, que aporte valor real al programa de seguridad de cualquier empresa.

Consideraciones a tener

🛡️ Consideraciones prácticas para establecer una política de escaneo de vulnerabilidades

Diseñar una política de escaneo efectiva no es solo cuestión de elegir herramientas o automatizar procesos. Se trata de **analizar cuidadosamente el entorno**, los activos, la criticidad del servicio y el impacto potencial que un escaneo puede generar sobre la red. A continuación, se detallan aspectos clave que toda política de escaneo debe contemplar, seguidos de **ejemplos prácticos** para aplicarlos en distintos entornos.

🕰️ 1. Consideración del mejor momento para realizar un escaneo

El **momento en que se ejecuta el escaneo** es crítico, especialmente en redes de producción. Un escaneo mal programado puede:

- Saturar la red,
- Inutilizar servidores temporalmente,
- Generar falsos positivos o incompletos por bloqueos de tráfico.

✔ Ejemplo práctico:

Empresa de logística con actividad 24/7:

- Política: Escaneos se ejecutan los domingos entre 04:00 y 06:00, bajo supervisión del administrador de red.
- Razón: Durante ese horario, el sistema de gestión de flotas no está operativo y hay menor carga.

Laboratorio académico:

- Política: Escaneos pueden ejecutarse en cualquier momento, ya que el entorno es de prueba y no hay servicios críticos en producción.

🌐 2. Detección de protocolos activos

Es fundamental identificar qué protocolos están en uso: TCP, UDP, ICMP, etc. Ignorar alguno puede significar **omitir vulnerabilidades importantes**.

✔ Ejemplo práctico:

Servidor de juegos en línea (UDP + TCP):

- Política: El escáner debe estar configurado para detectar servicios UDP (por ejemplo, en el puerto 27015 para servidores de Steam) además de TCP.
- Ajuste: Se activa un plugin específico para detección de vulnerabilidades en servicios UDP como SNMP o DNS.

🧭 3. Topología de red y ubicación del escáner

Escanear desde ubicaciones lejanas o a través de múltiples saltos puede:

- Distorsionar resultados (por firewalls, NAT, etc.),
- Cargar innecesariamente routers intermedios,
- Bloquear el tráfico.

✔ Ejemplo práctico:

Empresa con DMZ separada:

- Política: El escáner se instala en una máquina virtual dentro de la misma subred que los servidores web en la DMZ.
- Resultado: Evita interferencias del firewall perimetral y mejora la precisión.

📶 4. Limitaciones de ancho de banda

Si la red tiene enlaces de baja velocidad (como VPN o WAN), el escaneo puede consumir el ancho de banda, afectando usuarios.

✔ Ejemplo práctico:

Sucursal remota conectada por VPN:

- Política: Escaneo limitado a 20 conexiones simultáneas. Se desactivan plugins de pruebas de DoS y fuzzing.
- Configuración: Intervalos de espera más amplios entre paquetes.

🧵 5. Limitación de consultas (Query Throttling)

Reducir la intensidad del escaneo puede prevenir bloqueos en sistemas sensibles.

✔ Ejemplo práctico:

Escaneo de un switch gestionable antiguo:

- Política: Se limita el número de hilos de escaneo a 5 y se establece una latencia mínima entre peticiones.
- Resultado: El dispositivo no se sobrecarga ni se reinicia durante el análisis.

⚠️ 6. Sistemas frágiles o activos no tradicionales

Dispositivos como **impresoras, cámaras IP, sensores IoT o PLCs** pueden bloquearse ante escaneos agresivos.

✔ Ejemplo práctico:

Red de impresoras y cámaras IP:

- Política: Excluir las impresoras HP antiguas y cámaras Dahua del escaneo automático.
- Alternativa: Se realiza un escaneo manual mensual con configuraciones personalizadas y baja intensidad.

🧑‍💼 7. Restricciones impuestas por el cliente o la organización

La política de escaneo debe respetar **acuerdos legales, operativos y de disponibilidad**.

✔ Ejemplo práctico:

Contrato con empresa bancaria:

- Política: Escaneos permitidos solo de lunes a viernes de 00:00 a 05:00. Todos los logs deben ser entregados encriptados.
- Herramienta: Se utiliza Nessus con política personalizada, reportando solo al jefe de seguridad de TI.

📋 Ejemplos completos de políticas de escaneo

🔹 Política A — Red corporativa con servicios críticos

```
Nombre: Política Corporativa de Escaneo Programado
Frecuencia: Semanal
Horario: Domingo, 03:00 – 05:00
Herramienta: OpenVAS / Nessus
Protocolos: TCP y UDP (limitado)
Configuración:
  - Desactivar ataques DoS
  - Limitar a 25 hilos
  - Topología: Escáner dentro de la red interna
Exclusiones:
  - Cámaras IP
  - Impresoras de red
  - PLCs en producción
```

🔹 Política B — Red de laboratorio educativo

```
Nombre: Política de Escaneo Intensivo en Entorno de Pruebas
Frecuencia: Diario
Horario: Libre
Herramienta: Nmap + scripts NSE + Nikto
Protocolos: Todos los disponibles
Configuración:
  - Pruebas de fuzzing y DoS habilitadas
  - Escaneo de puertos completo (1–65535)
  - Escaneo de versiones y vulnerabilidades
Exclusiones: Ninguna
```

🧠 Recomendación final

Antes de implementar cualquier política, es imprescindible:

- **Mapear los activos**: Saber qué hay en la red y su nivel de criticidad.
- **Establecer prioridades**: Qué sistemas son clave y deben estar más protegidos.

- **Obtener permisos formales**: Especialmente en pruebas de caja negra o entornos productivos.

3.4 Comprender

3.4 Comprender cómo analizar los resultados del análisis de vulnerabilidades

Intro:

El reconocimiento es importante para comprender los recursos y la superficie de ataque de nuestros clientes. Sin embargo, el reconocimiento no identifica necesariamente las vulnerabilidades reales. Es posible que conozcamos las plataformas y los servicios a los que pueden acceder los agentes de amenazas, pero ¿existen vulnerabilidades conocidas en esas plataformas y servicios?

Los escaneo de vulnerabilidades ofrecen una forma automatizada de vincular la información del escaneo con los detalles de las vulnerabilidades que existen para los resultados del escaneo. Con esta información, es posible crear exploits que pueden tener consecuencias graves, como violaciones de datos e interrupciones del servicio. Con una recopilación de estas vulnerabilidades, podemos avanzar hacia la penetración real de la red y la evaluación de los riesgos que plantean tales exploits para las empresas.

3.4.1 Descripción general

Como ya sabrá, ejecutar un escaneos de vulnerabilidades es realmente la parte fácil del proceso de recopilación de información e identificación de vulnerabilidades. La mayor parte del trabajo se dedica al análisis de los resultados que obtiene de las herramientas que utiliza para el escaneos de vulnerabilidades. Estas herramientas no son infalibles; pueden proporcionar falsos positivos y los falsos positivos deben clasificarse para determinar cuáles son las vulnerabilidades reales.

Por ejemplo, supongamos que forma parte de un equipo de seguridad de la información que realiza escaneoss internos de vulnerabilidades en su red. Ejecuta la herramienta de escaneos de vulnerabilidades que desee y luego exporta un informe con los resultados del escaneos. A continuación, entrega el informe al equipo de terminales para que aborde todos los problemas indicados en el informe. El equipo de terminales comienza a abordar los problemas uno por uno. Es probable que su proceso incluya una investigación de un terminal para determinar la mejor manera de mitigar un hallazgo al respecto. Si el informe que proporciona incluye falsos positivos, el equipo de terminales terminará perdiendo mucho tiempo persiguiendo problemas que realmente no existen. Obviamente, esto puede causar algunos problemas entre el equipo de seguridad y el equipo de terminales. Este escenario también se puede aplicar a otras situaciones.

Cuando proporciona un informe como entrega de una asignación de prueba de penetración paga, es especialmente importante que el informe sea preciso. Supongamos que lo contrataron para identificar vulnerabilidades en la red de un cliente. Su entrega es proporcionar un informe completo de los problemas de seguridad que deben abordarse para proteger el entorno del cliente. Entregar un

informe que incluye falsos positivos hará perder el tiempo al cliente y probablemente perderá el negocio habitual del cliente. Como puede ver en este escaneos, es muy importante reducir los falsos positivos en los escaneos de vulnerabilidades.

Entonces, ¿cómo se eliminan los falsos positivos? El proceso implica una revisión detallada y exhaustiva de los resultados que ha proporcionado su herramienta de escaneos de vulnerabilidades. Supongamos que los resultados de un escaneos revelan que hay una posible vulnerabilidad de ejecución remota de código en el servidor web Apache que se ejecuta en el servidor de destino. Es probable que este tipo de hallazgo se marque como una vulnerabilidad de alta gravedad y, por lo tanto, debe tener prioridad. Para determinar si este es un hallazgo válido, primero debe echar un vistazo a lo que hizo el escáner de vulnerabilidades para llegar a esta conclusión. ¿Extrajo la información de la versión directamente del sistema mediante un escaneos con credenciales o se determinó mediante la conexión remota al puerto? Como sabe, los resultados de un escaneos con credenciales tienen más probabilidades de ser válidos que el escaneos remoto.

Debido a que el método de recopilación de información de versión varía según el escáner y el servicio, debe poder ver los detalles de los hallazgos en un informe para determinar cómo se recopiló la información. Desde allí, si es posible, querrá conectarse directamente al destino que informa una vulnerabilidad en particular e intentar determinar manualmente la información de la versión de ese servicio. Una vez que valida que la versión informada por el escáner realmente coincide con la del sistema, también debe profundizar en los detalles de la vulnerabilidad. Cada vulnerabilidad normalmente se correlacionará con uno o varios elementos de la lista de vulnerabilidades y exposiciones comunes (CVE). Debe observar los detalles de esos elementos CVE para comprender los criterios porque una vulnerabilidad puede marcarse en función de un solo dato (como el número de versión del servidor Apache extraído del anuncio). Al profundizar en los detalles de CVE, es posible que para que la vulnerabilidad sea explotable, esta versión de Apache debe ejecutarse en una versión o distribución específica de Linux. La mayoría de los escáneres de vulnerabilidades pueden correlacionar varias piezas de información para tomar una determinación. Sin embargo, algunos sistemas operativos Linux, como Red Hat, informan una versión anterior de un servicio que realmente ha sido parcheado para la vulnerabilidad específica. Esto se denomina backporting. Entonces, como puede ver, hay más que solo ejecutar un escaneos. Por supuesto, el método número uno para validar un hallazgo de un escaneos de vulnerabilidades es aprovechar la vulnerabilidad, como se analiza en muchos de los próximos módulos.

3.4.2 Fuentes para una mayor investigación de vulnerabilidades

Las siguientes secciones describen algunas fuentes útiles para una mayor investigación de las vulnerabilidades que puede encontrar durante los escaneos.

US-CERT
El Equipo de preparación para emergencias informáticas de EE. UU. (US-CERT) se estableció para proteger la infraestructura de Internet de los Estados Unidos. El objetivo principal de US-CERT es trabajar con agencias del sector público y privado para aumentar la eficiencia del intercambio de datos sobre vulnerabilidades. El trabajo realizado por US-CERT tiene como objetivo mejorar la postura de ciberseguridad de la nación. US-CERT opera como una entidad dependiente del Departamento de Seguridad Nacional como parte del Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC). Puede acceder a los recursos de US-CERT visitando https://www.us-cert.gov.

División del CERT de la Universidad Carnegie Mellon
La División CERT del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon es un centro de ciberseguridad cuyos expertos ayudan a coordinar las divulgaciones de vulnerabilidades en toda la industria. CERT investiga las vulnerabilidades de seguridad y contribuye a muchos esfuerzos diferentes de ciberseguridad en la industria. El CERT también desarrolla y ofrece capacitación a muchas organizaciones para ayudarlas a mejorar sus prácticas y programas de ciberseguridad. Puede obtener información adicional sobre el CERT en https://cert.org.

NIST
El Instituto Nacional de Normas y Tecnología (NIST) es una agencia del Departamento de Comercio de EE. UU. Su enfoque principal es promover la innovación y la competitividad industrial. NIST es responsable de la creación del marco de ciberseguridad de NIST (NIST CSF; consulte https://www.nist.gov/cyberframework). Este marco incluye una política de orientación sobre seguridad informática. La versión 1 del marco de NIST se publicó en 2014 con el fin de orientar la seguridad de la infraestructura crítica; sin embargo, la industria privada lo utiliza comúnmente como orientación en la gestión de riesgos. En 2018, NIST lanzó la versión 1.1, que está diseñada para ayudar a las organizaciones a evaluar los riesgos que enfrentan. En general, el marco describe los estándares y las mejores prácticas de la industria que pueden utilizarse para mejorar la postura de ciberseguridad de las organizaciones. Cualquiera que sea responsable de tomar decisiones relacionadas con la ciberseguridad en una organización debe consultar este marco para obtener orientación sobre los estándares y las mejores prácticas.

JPCERT
De manera similar al US-CERT, el Equipo de respuesta ante emergencias informáticas de Japón (JPCERT) es una organización que trabaja con proveedores de servicios, de seguridad y agencias gubernamentales y del sector privado para brindar capacidades de respuesta a incidentes, aumentar la conciencia sobre la ciberseguridad, incidentes de seguridad y trabajar con otros equipos internacionales de CERT. El JPCERT es responsable de las actividades del Equipo de respuesta a incidentes de seguridad informática (CSIRT) en la región de Japón y Asia Pacífico. Puede acceder a los recursos de JP-CERT visitando https://www.jpcert.or.jp/english/.

CAPEC
La enumeración y clasificación de patrones de ataque común (CAPEC) es un esfuerzo impulsado por la comunidad para catalogar los patrones de ataque vistos en la naturaleza para que puedan usarse para identificar amenazas activas de manera más eficiente. CAPEC, mantenido por MITRE, actúa como un diccionario de ataques conocidos que se han visto en el mundo real.

CVE
Vulnerabilidades y exposiciones comunes (CVE) es un esfuerzo que llega a las comunidades internacionales de ciberseguridad. Fue creado en 1999 con la idea de consolidar herramientas y bases de datos de ciberseguridad. Una ID de CVE se compone de las letras CVE seguidas por el año de publicación y cuatro o más dígitos en la parte del número de secuencia de la ID (por ejemplo, CVE-AAAA-NNNN con cuatro dígitos en el número de secuencia, CVE-AAAA-NNNNN con cinco dígitos en el número de secuencia, CVE-YYYY-NNNNNNN con siete dígitos en el número de secuencia, etc.). Puede obtener información adicional sobre CVE en https://cve.mitre.org.

CWE
La enumeración de debilidades comunes (CWE), en un nivel alto, es una lista de debilidades de software. El propósito de CWE es crear un lenguaje común para describir las debilidades de seguridad del software que son la causa raíz de determinadas vulnerabilidades. CWE proporciona una línea de base común para la identificación de debilidades para ayudar en el proceso de mitigación. Puede obtener información adicional sobre CWE en el sitio de MITRE: https://cwe.mitre.org.

CVSS
Cada vulnerabilidad representa un riesgo potencial que los agentes de amenazas pueden utilizar para comprometer sus sistemas y su red. Cada vulnerabilidad conlleva una cantidad asociada de riesgo. Uno de los estándares más adoptados para calcular la gravedad de una vulnerabilidad determinada es el Sistema común de puntuación de vulnerabilidades (CVSS), que tiene tres componentes:

puntuaciones básicas, temporales y ambientales. Cada componente se presenta como una puntuación en una escala de 0 a 10.

CVSS es un estándar de la industria mantenido por el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) que es utilizado por muchos Equipos de Respuesta a Incidentes de Seguridad de Productos (PSIRT) para transmitir información sobre la gravedad de las vulnerabilidades que divulgan a sus clientes. En CVSS, una vulnerabilidad se evalúa según tres aspectos, con una puntuación asignada a cada uno de ellos:

El grupo base representa las características intrínsecas de una vulnerabilidad que son constantes en el tiempo y no dependen de un entorno específico del usuario. Esta es la información más importante y el único aspecto obligatorio para obtener una puntuación de vulnerabilidad. El grupo temporal evalúa la vulnerabilidad a medida que cambia con el tiempo.
El grupo de entornos representa las características de una vulnerabilidad, teniendo en cuenta el entorno de la organización.

La puntuación para el grupo base está entre 0 y 10, donde 0 es la menos grave y 10 se asigna a las vulnerabilidades muy críticas. Por ejemplo, una vulnerabilidad muy crítica podría permitir que un atacante comprometa de forma remota un sistema y obtenga el control total. Además, la puntuación se presenta en forma de una cadena de vectores que identifica cada uno de los componentes utilizados para componer la puntuación. La fórmula utilizada para obtener la puntuación tiene en cuenta varias características de la vulnerabilidad y cómo el atacante puede aprovechar estas características.

CVSS define varias características para los grupos base, temporal y ambiental. El grupo base define métricas de explotabilidad que miden cómo se puede aprovechar la vulnerabilidad, así como métricas de impacto que miden el impacto en la confidencialidad, la integridad y la disponibilidad. Además de estas dos métricas, se usa una métrica llamada Cambio de alcance (S) para transmitir el impacto en otros sistemas que pueden verse afectados por la vulnerabilidad, pero que no contienen el código vulnerable. Por ejemplo, si un enrutador es susceptible a una vulnerabilidad de DoS y experimenta un bloqueo después de recibir un paquete diseñado por el atacante, se cambia el alcance, ya que los dispositivos detrás del enrutador también experimentarán la condición de denegación de servicio. FIRST proporciona ejemplos adicionales en https://www.first.org/cvss/.

📌 Resumen Esquemático - Escaneo de Vulnerabilidades

🔍 1. Introducción al Escaneo de Vulnerabilidades

- **Reconocimiento**: Ayuda a conocer la superficie de ataque, pero **no identifica vulnerabilidades** por sí solo.
- **Escaneo de vulnerabilidades**: Automatiza la detección de debilidades conocidas asociadas a servicios y plataformas detectadas.
- **Objetivo final**: Identificar riesgos reales → facilitar el **exploitation controlado** → evaluar impacto.

🧰 2. Descripción General del Proceso (3.4.1)

- **Fase sencilla**: Ejecutar el escaneo.
- **Fase crítica**: Analizar resultados → identificar **falsos positivos**.

⚠️ Problemas derivados de falsos positivos:

- Pérdida de tiempo.
- Conflictos entre equipos técnicos.
- Pérdida de confianza del cliente en auditorías externas.

✅ Validación de hallazgos:

- Revisar **cómo** el escáner obtuvo los datos (¿con credenciales o sin ellas?).
- Conectarse directamente al sistema afectado y comprobar:
    - Versión del servicio.
    - Coincidencia con CVEs.

- Considerar el **backporting** (ej.: Red Hat puede reportar versión vulnerable pero estar parcheado).

🧪 **Validación final:**

- Intentar **explotar** la vulnerabilidad (cuando esté permitido y controlado).

📚 3. Fuentes para Investigación de Vulnerabilidades (3.4.2)

Fuente	Descripción	Enlace
US-CERT	Coordina divulgación de vulnerabilidades en EE.UU.	us-cert.gov
CERT CMU	Investigación y formación en ciberseguridad (Carnegie Mellon)	cert.org
NIST	Normas y mejores prácticas. Desarrolla el NIST CSF.	nist.gov/cyberframework
JPCERT	Similar a US-CERT pero en Japón/Asia-Pacífico.	jpcert.or.jp
CAPEC	Catálogo de patrones de ataque.	capec.mitre.org
CVE	Listado de vulnerabilidades comunes (identificador único).	cve.mitre.org
CWE	Catálogo de debilidades de software.	cwe.mitre.org
CVSS	Sistema de puntuación para clasificar gravedad de vulnerabilidades.	first.org/cvss

---

📏 4. CVSS (Common Vulnerability Scoring System)

- **Escala**: 0 a 10.
- **Componentes**:
    - **Base**: Intrínseco a la vulnerabilidad (obligatorio).
    - **Temporal**: Cambia con el tiempo.

    - **Ambiental**: Según el entorno donde se encuentra.

Métricas clave:

- **Explotabilidad**: Facilidad para ser aprovechada.
- **Impacto**: Confidencialidad, Integridad y Disponibilidad (CIA).
- **Cambio de Alcance (Scope)**: Si afecta a sistemas relacionados, no directamente vulnerables.

Escaneo de Vulnerabilidades en Ciberseguridad

Introducción

El escaneo de vulnerabilidades es una fase esencial en cualquier proceso de evaluación de seguridad, ya sea en pruebas de penetración internas o auditorías externas. Su propósito es identificar de manera automatizada las debilidades potenciales en los sistemas, servicios y aplicaciones que conforman la superficie de ataque de una organización. Sin embargo, ejecutar un escaneo es solo el primer paso; el verdadero valor reside en el análisis, la validación y la priorización de los hallazgos para una respuesta eficaz.

Importancia del Escaneo de Vulnerabilidades

Aunque el reconocimiento previo proporciona una visión general de los recursos expuestos, no necesariamente identifica vulnerabilidades explotables. El escaneo de vulnerabilidades automatiza la correlación entre los servicios descubiertos y las bases de datos de vulnerabilidades conocidas, como la CVE (Common Vulnerabilities and Exposures), permitiendo así detectar problemas de seguridad que podrían derivar en brechas de datos o interrupciones críticas del servicio.

Herramientas Comunes de Escaneo

Nessus: Uno de los escáneres más utilizados a nivel profesional. Ofrece una amplia cobertura de plugins, facilidad de uso, escaneos con y sin credenciales, y capacidades para generar informes detallados.

OpenVAS: Solución de código abierto con una comunidad activa. Es útil para entornos donde se requiere transparencia en los métodos de escaneo y una personalización detallada.

Ambas herramientas permiten escaneos automatizados, la gestión de políticas de escaneo, y la integración con sistemas de gestión de vulnerabilidades.

Flujo de Trabajo de un Escaneo de Vulnerabilidades

A continuación, se presenta un esquema general del proceso de escaneo y validación de vulnerabilidades:

Preparación:

Identificación del alcance: redes, hosts, rangos IP.

Elección de herramienta: Nessus, OpenVAS, Nexpose, etc.

Configuración del escaneo: con o sin credenciales, intensidad, tipo de pruebas.

Ejecución del escaneo:

Lanza el análisis sobre los objetivos definidos.

Recolecta información como versiones de software, puertos abiertos, servicios expuestos.

Revisión de resultados:

Clasificación de hallazgos por criticidad (CVSS score).

Detección de falsos positivos.

Validación manual en casos críticos.

Validación de vulnerabilidades:

Verificación manual de versiones y configuraciones.

Comparación con las condiciones descritas en las CVE.

Revisión de posibles casos de backporting (sistemas parcheados con versiones antiguas).

Informe y comunicación:

Redacción de informe técnico y ejecutivo.

Recomendaciones priorizadas.

Inclusión de evidencias y referencias.

Ejemplos Prácticos

Ejemplo 1: Falso Positivo por Versión de Apache

Un escaneo realizado con Nessus identifica una vulnerabilidad crítica en un servidor web Apache, alegando una ejecución remota de código basada en la versión detectada. Sin embargo, al revisar manualmente el sistema (por SSH o accediendo al banner del servicio), se descubre que aunque la versión parece vulnerable, el

sistema está parcheado mediante backporting, como es común en distribuciones como Red Hat o Debian.

Ejemplo 2: Validación de Escaneo con Credenciales

OpenVAS detecta múltiples vulnerabilidades en una máquina Linux expuesta. Se decide realizar un segundo escaneo con credenciales (SSH) para obtener información precisa del sistema. El segundo análisis reduce los falsos positivos y proporciona detalles exactos sobre los paquetes instalados y su estado de actualización.

Mejores Prácticas

Realizar escaneos con credenciales siempre que sea posible para obtener resultados más precisos.

Revisar manualmente los hallazgos críticos y los que puedan ser falsos positivos.

Mantener las herramientas actualizadas para aprovechar las últimas definiciones de vulnerabilidades.

Correlacionar los resultados con fuentes como NVD (National Vulnerability Database) o mitre.org.

Priorizar la remediación según el impacto y la exposición del activo afectado.

Conclusión

El escaneo de vulnerabilidades no debe considerarse una tarea puramente técnica o automatizable sin supervisión. Es un componente estratégico del proceso de seguridad defensiva, cuya eficacia depende en gran medida de la capacidad de análisis del profesional encargado. Validar los hallazgos y comprender el contexto en el que se presentan las vulnerabilidades son claves para minimizar riesgos, evitar pérdidas de tiempo y fortalecer la postura de seguridad de cualquier organización.

3.4.4 Cómo lidiar con una vulnerabilidad

Como evaluador de penetración, su objetivo es identificar las debilidades que pueden aprovecharse. Como se mencionó anteriormente, el escaneo de vulnerabilidades es un método para identificar posibles vulnerabilidades. Después

de identificar una vulnerabilidad, debe verificarla. Hay muchas maneras de determinar si los resultados de un escáner de vulnerabilidades son válidos. La validación final es la explotación.

Para determinar si una vulnerabilidad es aprovechable, primero debe identificar una forma de explotar o aprovecharse de esa vulnerabilidad. Supongamos que su escáner de vulnerabilidades informa que hay una versión desactualizada de Apache Struts que es vulnerable a un defecto no autenticado que se puede explotar de forma remota. Una de las primeras cosas que debe hacer es determinar si hay una explotación disponible. Muchas veces, esto se puede encontrar con un marco de explotación como Metasploit. Como regla general, si una vulnerabilidad tiene un módulo coincidente en Metasploit, casi siempre se debe considerar de alta gravedad. Dicho esto, también hay otros métodos para encontrar explotaciones, y siempre puede escribir sus propias explotaciones.

¿Cómo prioriza sus hallazgos para la siguiente fase de su prueba de penetración? Para determinar la prioridad, debe responder algunas preguntas:

- ¿Cuál es la gravedad de la vulnerabilidad?
- ¿A cuántos sistemas se aplica la vulnerabilidad?
- ¿Cómo se detectó la vulnerabilidad?
- ¿La vulnerabilidad se encontró con un escáner automatizado o manualmente?
- ¿Cuál es el valor del dispositivo en el que se encontró la vulnerabilidad?
- ¿Este dispositivo es fundamental para su empresa o infraestructura?
- ¿Cuál es el vector de ataque y se aplica a su entorno?
- ¿Existe una posible solución alternativa o mitigación?

Responder estas preguntas puede ayudarlo a determinar la prioridad que debe asignar a las vulnerabilidades encontradas. El protocolo estándar hace que comience con las vulnerabilidades de mayor gravedad que tienen la mayor probabilidad de ser explotadas. Si estas vulnerabilidades son realmente válidas, es posible que ya estén comprometidas. (Si en cualquier momento durante una prueba de penetración, descubre que un sistema está siendo explotado activamente, debe informarlo de inmediato al propietario del sistema). A continuación, debe abordar cualquier vulnerabilidad que se encuentre en los sistemas críticos,

independientemente del nivel de gravedad. Es posible que haya una cadena de explotaciones disponible para un atacante que permitiría que una vulnerabilidad de menor gravedad se vuelva crítica. Primero debe proteger los sistemas críticos. A continuación, es posible que desee establecer prioridades en función de la cantidad de sistemas afectados por el hallazgo. Si una gran cantidad de sistemas se ven afectados, esto aumentaría la prioridad porque muchas explotaciones en esta vulnerabilidad tendrían un mayor impacto en su entorno. Estas son pautas sugeridas, pero cuando se trata de priorizar la administración y mitigación de vulnerabilidades, realmente depende del entorno específico.

3.4.3 Práctica de laboratorio - Investigación de

3.4.3 Práctica de laboratorio - Investigación de fuentes de información de vulnerabilidades

Se ha trabajado mucho para crear una forma universal de compartir información sobre vulnerabilidades de ciberseguridad conocidas. Las herramientas de escaneo de vulnerabilidades asignan los resultados del escaneo a las vulnerabilidades relevantes en forma de números CVE, por lo que es importante saber qué representan los números CVE y cómo encontrar detalles sobre su gravedad y los sistemas y las versiones de software afectados.

Revise la información de esta práctica de laboratorio para asegurarse de tener claras las diferencias entre las fuentes de información sobre vulnerabilidades y cómo utilizarlas.

En esta práctica de laboratorio, utilizará varias fuentes útiles para investigar más a fondo las vulnerabilidades.

Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)
Parte 2: Explorar las enumeraciones de debilidades comunes (CWE)
Parte 3: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)
Parte 4: Investigar las vulnerabilidades en el sistema común de puntuación de vulnerabilidades (CVSS)

Práctica de laboratorio - Investigación de fuentes de información de vulnerabilidades

Objetivos

Utilice varias fuentes útiles para investigar más a fondo las vulnerabilidades.

- Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)
- Parte 2: Explorar las enumeraciones de debilidades comunes (CWE)
- Parte 3: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)
- Parte 4: Investigar las vulnerabilidades en el sistema común de puntuación de vulnerabilidades (CVSS)

Trasfondo / Escenario

En una práctica de laboratorio anterior, encontró varias vulnerabilidades después de escanear un sistema de destino. Ahora utilizará varias fuentes ampliamente disponibles para profundizar en los detalles de las vulnerabilidades. Asignará e investigará las vulnerabilidades en la lista de vulnerabilidades y exposiciones comunes (CVE), la enumeración de debilidades comunes (CWE), la base de datos nacional de vulnerabilidades del NIST y el sistema de puntuación de vulnerabilidades comunes (CVSS).

Recursos necesarios

- Computadora con conexión a Internet

Instrucciones

Parte 1: Investigue las vulnerabilidades y exposiciones comunes (CVE)

Paso 1: Explore las CVE.

a. Inicie el sitio web de CVE y vaya a www.cve.org.
b. Lea la descripción general del programa CVE.
    1. Seleccione About > Overview en el menú.
    2. Vea el video de descripción general del programa CVE.
    3. Consulte los podcasts disponibles para obtener información más detallada sobre el programa CVE.

¿Cuál es la misión del programa CVE?

Área de Respuesta

Identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas.

Ocultar respuesta

¿Quién asigna los ID de CVE?

Área de Respuesta

Las autoridades de numeración de CVE (CNA)

Ocultar respuesta

¿Cuáles son los dos objetivos principales del programa CVE?

Área de Respuesta

Escalar el programa para una adopción y cobertura más amplias, y producir más registros CVE más rápidamente (más cerca del tiempo real).

Ocultar respuesta

¿Quién opera la CVE?

Área de Respuesta

MITRE Corporation con financiación del Departamento de Seguridad Nacional de EE. UU. (DHS) y el Componente de administración de vulnerabilidades (VMC) de la Agencia de seguridad de infraestructura y ciberseguridad (CISA).

Ocultar respuesta

Paso 2: Utilice el programa CVE para recopilar información sobre las vulnerabilidades.

En una práctica de laboratorio anterior, analizó un sistema de destino en busca de vulnerabilidades. La lista de vulnerabilidades encontradas arrojó los siguientes seis CVE:

- CVE-2021-41617
- CVE-2020-14145
- CVE-2019-16905
- CVE-2019-6111
- CVE-2019-6110
- CVE-2019-6109

a. Ingrese CVE-2021-41617 en la ventana de búsqueda y haga clic en Find.

¿Qué versiones de OpenSSH están sujetas a esta vulnerabilidad?

Área de Respuesta

Versiones de la 6.2 a la 8.x, anteriores a la 8.8

Ocultar respuesta

¿Cuándo se actualizó por última vez este CVE?

Updated: 2024-08-04

14 de Febrero 2023.

Ocultar respuesta

b. En la parte inferior de la página, haga clic en CVE-2021-41617 para ver información adicional sobre la CVE de la Base de datos nacional de vulnerabilidades (NVD) del NIST.

¿Cuál es la puntuación de gravedad de CVSS 3.x para esta CVE?

Área de Respuesta

7.0 ALTO

Ocultar respuesta

c. Repita los pasos a y b. para revisar la información de las otras cinco CVE.

¿Cuál de estas CVE implica ataques de intermediario desde un servidor SCP malicioso?

Área de Respuesta

CVE-2019-6111

Ocultar respuesta

d. En el sitio de CVE (www.cve.org), ingrese CVE-2019-6111 en el cuadro de búsqueda y haga clic en Find.
e. Desplácese hasta la parte inferior de la página CVE y haga clic en CVE-2019-6111 para ver información adicional sobre el NVD.

f. En la página NVD para CVE-2019-6111, desplácese hacia abajo hasta la sección Weakness Enumeration.

¿Qué ID de CWE está asociado con esta CVE?

Área de Respuesta

CWE-22

Ocultar respuesta

Registre esta ID de CWE para usar en la Parte 2.

g. Repita los pasos del a al d. para obtener los ID de CWE asociados con las otras CVE devueltas.

¿Qué CWE están asociadas con cada una de las otras cinco CVE?

Área de Respuesta

CWE-203, CWE-190, CWE-116, CWE-838

Ocultar respuesta

Registre estas ID de CWE para usarlas en la Parte 2.

Parte 2: Explore la enumeración de debilidades comunes (CWE)

Paso 1: Explore CWE.

a. Inicie el sitio web de CWE y vaya a https://cwe.mitre.org.
b. Explore el programa CVE seleccionando About > Overview en el menú.

¿Cuál es el objetivo de CWE?

Área de Respuesta

Detener las vulnerabilidades en el origen mediante la educación de los arquitectos, diseñadores, programadores y adquirentes de software y hardware sobre cómo eliminar los errores comunes antes de la entrega de los productos.

Ocultar respuesta

¿Cuál es la diferencia entre una CVE y una CWE?

Área de Respuesta

Las respuestas pueden variar, pero las CVE identifican vulnerabilidades específicas, mientras que las CWE clasifican y describen tipos de debilidades que pueden generar vulnerabilidades.

Ocultar respuesta

c. ID que grabó en el paso 2 de la parte 1.
    1. Introduzca 22 en el cuadro ID Lookup en la parte superior derecha de la página de CWE. (Este es el ID de CWE para CVE-2019-6111)

¿Cuál es el título de esta CWE?

Área de Respuesta

Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’) (Limitación incorrecta de un nombre de ruta a un directorio restringido ('Recorrido de ruta'))

Ocultar respuesta

    2. Desplácese por la información disponible sobre esta CWE.
d. Repita el paso c. Busque los ID de CWE restantes que registró en la parte 1, paso 2g.

Parte 3: Investigue los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)

Paso 1: Explore el NIST.

a. Inicie el sitio web de NIST navegando a https://www.nist.gov.
b. Seleccione About NIST > About Us en el menú y revise la descripción general de NIST.

¿Cuál es la misión de NIST?

"Promover la innovación y la competitividad industrial de los Estados Unidos a través del avance de la ciencia, los estándares y la tecnología para mejorar la seguridad económica y la calidad de vida".

Ocultar respuesta

c. Explore la base de datos nacional de vulnerabilidad (NVD)
    1. Regrese a la página de inicio de NIST y seleccione Topics > Information Technology en el menú.
    2. Seleccione National Vulnerability Database en la lista Featured Content.
    3. Haga clic en General para ver y revisar la información general sobre el NVD.

¿Cuál es la relación entre NVD y CVE?

En la práctica

- Cuando usas herramientas como **OpenVAS**, **Nessus**, **Qualys** o **InsightVM**, muchas de ellas consumen los datos desde **NVD**, no directamente desde MITRE, por el nivel de detalle adicional.

- Como profesional o consultor, debes usar **ambas fuentes**:

- MITRE CVE para confirmar la existencia y legitimidad de una vulnerabilidad.

- NVD para evaluar su gravedad e impacto real.

El NVD realiza un escaneo de las CVE publicadas en el diccionario de CVE. El personal de NVD analiza las CVE y proporciona detalles adicionales.

Ocultar respuesta

4. Expanda el menú en General y haga clic en NVD Dashboard.

¿Cuántas vulnerabilidades de CVE contiene el NVD?

Según la información más reciente disponible, la **National Vulnerability Database (NVD)** contiene actualmente **291.022 registros de vulnerabilidades CVE**

La respuesta varía. En el momento de escribir este curso: 211116

Ocultar respuesta

¿Cuál es la vulnerabilidad puntuada más reciente y cuál es la calificación CVSS?

Según la información más reciente disponible en la National Vulnerability Database (NVD), la vulnerabilidad más recientemente publicada es:

CVE-2025-1675

Descripción: Esta vulnerabilidad se encuentra en la función dns_copy_qname del archivo dns_pack.c, donde se realiza una operación memcpy con un campo no confiable sin verificar si el búfer de origen es lo suficientemente grande para contener los datos copiados. Esto podría permitir a un atacante provocar una lectura fuera de límites.

NVD

Fecha de publicación: 25 de febrero de 2025

Calificación CVSS: Actualmente, no se ha asignado una puntuación CVSS para esta vulnerabilidad.

Es importante destacar que muchas de las vulnerabilidades recientes aún no tienen una puntuación CVSS asignada, lo que indica que están en proceso de análisis por parte del NVD.

Para mantenerte actualizado sobre las vulnerabilidades más recientes y sus calificaciones CVSS, puedes consultar regularmente el sitio oficial del NVD:

NVD

.

La respuesta variará, pero al momento de redactar este curso:
CVE-2023-20990 con una gravedad CVSS de 4,4 MEDIA

Ocultar respuesta

5. Vuelva a la página de la Base de datos nacional de vulnerabilidades https://nvd.nist.gov/.
6. Haga clic en Vulnerability Metrics en el menú a la izquierda de la página.

¿Qué método se utiliza para medir cualitativamente la gravedad de las vulnerabilidades?

El método más utilizado a nivel internacional para medir cualitativa y cuantitativamente la gravedad de las vulnerabilidades es el CVSS (Common Vulnerability Scoring System).

Sistema de puntuación de vulnerabilidades comunes (CVSS)

Ocultar respuesta

¿Cuántas clasificaciones de gravedad tiene CVSS v3.0 y cuáles son?

Relación con las puntuaciones CVSS

La puntuación final de CVSS v3.0 se calcula a partir de varias métricas, como el vector de ataque, el impacto y la complejidad. Dependiendo de los valores de estas métricas, se asignará una de estas clasificaciones.

Puntuación CVSS	Clasificación de gravedad
0.0	Ninguna
0.1 - 3.9	Baja
4.0 - 6.9	Media
7.0 - 8.9	Alta
9.0 - 10.0	Crítica

Cinco. Son: Ninguna, Baja, Media, Alta y Crítica.

Ocultar respuesta

Parte 4: Investigue las vulnerabilidades en el sistema común de puntuación de vulnerabilidades (CVSS)

Paso 1: Explore CVSS.

a. Inicie el sitio web de CVSS y vaya a https://first.org/cvss
b. Revise la información en CVSS.
c. Investigue las calificaciones CVSS haciendo clic en Specification Document en el menú de la izquierda.

¿Cuáles son las tres métricas que componen una calificación CVSS?

Las tres métricas principales para calcular la puntuación CVSS son:

1. **Métricas Base**: Factores fijos que describen la vulnerabilidad.

2. **Métricas Temporales**: Factores cambiantes, como la existencia de un parche.

3. **Métricas Ambientales**: Factores que dependen del contexto donde ocurre la vulnerabilidad.

Métrica básica, métrica temporal, métrica de entorno

Ocultar respuesta

¿Cuántas métricas componen el grupo de métricas base de un CVSS? ¿Cuáles son?

Resumen de las métricas base

Métrica	Descripción
Attack Vector	Método de explotación de la vulnerabilidad
Attack Complexity	Dificultad para explotar la vulnerabilidad
Privileges Required	Nivel de privilegios necesarios para explotar la vulnerabilidad
User Interaction	Si se requiere o no interacción del usuario
Confidentiality Impact	Impacto en la confidencialidad de los datos
Integrity Impact	Impacto en la integridad de los datos
Availability Impact	Impacto en la disponibilidad del sistema

Ocho: vector de ataque, complejidad de los ataques, privilegios requeridos, interacción del usuario, impacto en la confidencialidad, impacto en la integridad, impacto en la disponibilidad y alcance

Ocultar respuesta

1. Haga clic en Examples en el menú de la izquierda.
2. Haga clic en el enlace CVSS version 3.1 para ver ejemplos.
3. Desplácese hacia abajo en la página y revise los ejemplos de CVE y cómo se calcularon sus puntuaciones base de CVSS v3.1.

4. Observe los valores proporcionados para cada métrica que conforma la puntuación del CVSS.

d. Investigue las calificaciones CVSS de los CWE registradas en la parte 1, paso 2.
    1. Vaya a www.cve.org.
    2. En el cuadro de búsqueda, introduzca CVE-2021-41617 y haga clic en Find.
    3. Desplácese hasta la parte inferior de la página y haga clic en CVE-2021-41617 para ver información adicional sobre el NVD. Esto abre la base de datos nacional de vulnerabilidades para ver los detalles sobre la CVE.
    4. Desplácese hasta la sección Severity y asegúrese de seleccionar CVSS Version 3.x.

       Observe los valores de las ocho métricas base de CVSS en el Vector. La puntuación numérica correspondiente de estos valores se combina para dar una puntuación base de 7,0 ALTA.

    5. En una ventana separada del navegador, vaya a la calculadora de CVSS 3.1 en https://www.first.org/cvss/calculator/3.1.
    6. En la calculadora de puntuación base, haga clic en los nombres de las métricas que correspondan al vector en la página de NVD. (Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

¿Qué puntuación base calcula la calculadora CVSS?

Área de Respuesta

7.0

Ocultar respuesta

7. Repita los pasos 1 a 6 para las otras cinco CVE grabadas de la parte 1, paso 2.

Reflexión

¿Cuál es la relación entre CVE, CWE, NVD y CVSS?

La **CVE** es un identificador único para vulnerabilidades de seguridad, la **CWE** clasifica los tipos de debilidades de software, el **NVD** es una base de datos que contiene información detallada sobre las CVE, incluyendo su puntuación **CVSS**, que mide la gravedad de las vulnerabilidades.

CVE enumera las vulnerabilidades que se han descubierto, CWE las clasifica, NVD proporciona detalles y CVSS proporciona calificaciones de gravedad.

¿Conoces las vulnerabilidades y exposici. (CVE)?

¿Conoces las vulnerabilidades y exposiciones comunes (CVE)?

¿Qué es una CVE?

Una **CVE (Common Vulnerabilities and Exposures)** es un identificador único que se asigna a una **vulnerabilidad conocida** en un sistema informático, software o firmware. Estas identificaciones permiten que todos —fabricantes, analistas de seguridad, administradores de sistemas, etc.— hablen el **mismo idioma** cuando se refieren a una vulnerabilidad específica.

> 🌐 **Ejemplo real**:
>
> - **CVE-2021-44228** → más conocida como *Log4Shell*, una vulnerabilidad crítica en la biblioteca de Java Log4j que permitía ejecución remota de código (RCE). Afectó a miles de servidores y aplicaciones.

¿Para qué sirven?

Las CVE tienen múltiples finalidades prácticas:

- **Estandarizar la nomenclatura** de las vulnerabilidades.
- **Centralizar la información pública** sobre fallos de seguridad.
- **Permitir parches y mitigaciones rápidas**, ya que los fabricantes pueden publicar actualizaciones con referencia directa al número CVE.
- **Ayudar a priorizar riesgos**, al conocer la gravedad (score CVSS).

¿Quién mantiene las CVE?

Las CVE son gestionadas por una organización llamada **MITRE Corporation**, financiada por el Departamento de Seguridad Nacional de EE. UU. (DHS). MITRE colabora con cientos de empresas e instituciones, llamadas **CVE Numbering Authorities (CNA)**, que pueden registrar nuevas vulnerabilidades.

¿Cómo está estructurada una CVE?

El formato estándar es:

`CVE-AÑO-NÚMERO`

Ejemplo:

`CVE-2023-23397`

Esa es una vulnerabilidad crítica en Microsoft Outlook que permite a un atacante robar credenciales simplemente enviando un correo especialmente diseñado.

¿Dónde puedo consultar las CVE?

- 🔎 https://cve.mitre.org → Sitio oficial de MITRE.
- 🔐 https://nvd.nist.gov → Base de datos enriquecida con puntuación de gravedad (CVSS), referencias y soluciones.
- 🧰 https://www.cvedetails.com → Sitio muy práctico para filtrar por fabricante, producto, año, tipo de fallo, etc.

Consejo práctico para tu empresa y tus clientes

> Como representante de una empresa de servicio técnico, es importante que verifiques regularmente si los equipos que gestionáis tienen **software con CVE conocidas y sin parchear**. Esto puede ser una excelente ventaja competitiva si ofrecéis **auditorías básicas de vulnerabilidades** o mantenimientos preventivos.

¿Cuál es la misión del programa CVE?

🎯 Misión del programa CVE

La **misión oficial** del programa CVE es:

> **"Identificar, definir y catalogar públicamente las vulnerabilidades de ciberseguridad descubiertas en software y firmware para facilitar el intercambio de información y la gestión coordinada de la seguridad."**

📌 Objetivos fundamentales

1. **Proporcionar identificadores únicos para cada vulnerabilidad**

   Cada vulnerabilidad recibe un código único (por ejemplo, `CVE-2023-4863`) que la hace fácilmente reconocible y evitable de duplicar en informes de seguridad.

2. **Fomentar la transparencia**

   Al estar registradas públicamente, las CVEs permiten que cualquier persona —técnicos, fabricantes, investigadores o clientes— conozca y entienda los riesgos que afectan a los sistemas.

3. **Permitir la coordinación global**

   Los fabricantes de software, analistas de seguridad y proveedores de soluciones pueden trabajar en conjunto usando un **lenguaje común**, facilitando el **parcheo y mitigación eficiente**.

4. **Apoyar la gestión de riesgos**

   Integrando las CVEs en herramientas como gestores de parches, escáneres de vulnerabilidades o SIEMs, las organizaciones pueden **priorizar las amenazas reales** que afectan a sus activos.

5. **Favorecer la automatización y la interoperabilidad**

   Los identificadores CVE pueden integrarse en **sistemas automáticos de detección**, alertas, dashboards de seguridad, etc., gracias a su estandarización.

🧱 ¿Quién la ejecuta?

La misión es coordinada por la **MITRE Corporation**, que mantiene la base de datos y los estándares, en colaboración con:

- El **Departamento de Seguridad Nacional de EE.UU. (DHS)**
- La **Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA)**

- Más de **300 organizaciones CNA (CVE Numbering Authorities)** en todo el mundo (incluyendo Microsoft, Google, Cisco, Red Hat, etc.).

🛡️ ¿Por qué es importante para ti y tus clientes?

Porque permite:

- Identificar software vulnerable que debe ser parcheado.
- Informar con autoridad a los clientes sobre riesgos conocidos.
- Integrar prácticas de **gestión de vulnerabilidades basadas en estándares internacionales**.

¿Cuál es la relación entre NVD y CVE?

La relación entre **NVD (National Vulnerability Database)** y **CVE (Common Vulnerabilities and Exposures)** es **esencial** para entender cómo se gestionan y difunden las vulnerabilidades a nivel global. Vamos a explicarlo de forma clara y estructurada.

🔗 Relación entre NVD y CVE

1. 🧩 CVE es el identificador

El programa **CVE**, gestionado por MITRE Corporation, se encarga de:

- **Asignar un código único** a cada vulnerabilidad confirmada.
- Proporcionar una **descripción básica** y referencias del fallo.
- Actuar como el **registro oficial y estandarizado** de vulnerabilidades conocidas.

📘 Ejemplo:

- CVE-2021-34527 → Vulnerabilidad en Windows Print Spooler, también conocida como *PrintNightmare*.

---

2. 🏛️ NVD es la base de datos enriquecida

La **NVD (National Vulnerability Database)** es un servicio público del gobierno de EE.UU., mantenido por el **NIST (National Institute of Standards and Technology)**.

Una vez que MITRE **publica una nueva CVE**, **NVD la importa automáticamente** y realiza lo siguiente:

🔍 **Agrega información adicional:**

- **Puntuación de gravedad (CVSS v3.1)** → ¿Qué tan grave es?
- **Vectores de ataque** → ¿Cómo se explota?
- **Impacto en confidencialidad, integridad y disponibilidad (CIA Triad)**.
- **Soluciones, parches y mitigaciones**.
- **Clasificación por productos afectados (CPE)**.

---

3. 🔄 Flujo resumido

```
Investigador descubre vulnerabilidad
        ↓
MITRE la analiza y asigna un código CVE
        ↓
CVE se publica en cve.mitre.org
        ↓
NVD la recibe, analiza y enriquece con metadatos
        ↓
Organizaciones y herramientas consumen la CVE desde NVD para actuar
```

🎯 ¿Por qué es importante para la ciberseguridad?

Aspecto	CVE	NVD
Función	Registro e identificación	Análisis técnico profundo y enriquecido
Organización responsable	MITRE	NIST (EE.UU.)
Nivel de detalle	Básico: ID + descripción + referencias	Completo: gravedad, vectores, soluciones, etc.
Uso en herramientas automáticas	✅	✅ (más frecuente por su riqueza de datos)
Aplicación en empresas	Seguimiento y notificación	Gestión activa del riesgo y priorización de parches

---

🛠️ En la práctica

- Cuando usas herramientas como **OpenVAS**, **Nessus**, **Qualys** o **InsightVM**, muchas de ellas consumen los datos desde **NVD**, no directamente desde MITRE, por el nivel de detalle adicional.
- Como profesional o consultor, debes usar **ambas fuentes**:
    - MITRE CVE para confirmar la existencia y legitimidad de una vulnerabilidad.
    - NVD para evaluar su gravedad e impacto real.

¿Cuántas vulnerabilidades de CVE contiene el NVD?

Según la información más reciente disponible, la **National Vulnerability Database (NVD)** contiene actualmente **291.022 registros de vulnerabilidades CVE** .NVD

📊 Detalles adicionales

- **Total de CVE en NVD**: 291.022
- **Vulnerabilidades publicadas en 2024**: 40.300
- **Vulnerabilidades publicadas en 2023**: 29.066

🧠 ¿Por qué es relevante esta cifra?

El creciente número de vulnerabilidades registradas refleja tanto el aumento en la detección de fallos de seguridad como la expansión del ecosistema de software. Para empresas como la tuya, que ofrecen servicios de mantenimiento y asesoría informática, es crucial:

- **Mantenerse actualizado**: Revisar regularmente las vulnerabilidades más recientes para aplicar parches y mitigaciones oportunas.
- **Informar a los clientes**: Proporcionar información sobre riesgos potenciales en los sistemas que utilizan.
- **Priorizar acciones**: Utilizar herramientas que integren datos de NVD para identificar y abordar las vulnerabilidades más críticas.

¿Cuál es la vulnerabilidad puntuada más reciente y cuál es la calificación CVSS?

Según la información más reciente disponible en la National Vulnerability Database (NVD), la vulnerabilidad más recientemente publicada es:

🔐 CVE-2025-1675

- **Descripción**: Esta vulnerabilidad se encuentra en la función `dns_copy_qname` del archivo `dns_pack.c`, donde se realiza una operación `memcpy` con un campo no confiable sin verificar si el búfer de origen es lo suficientemente grande para contener los datos copiados. Esto podría permitir a un atacante provocar una lectura fuera de límites.NVD

- **Fecha de publicación**: 25 de febrero de 2025
- **Calificación CVSS**: Actualmente, no se ha asignado una puntuación CVSS para esta vulnerabilidad.

Es importante destacar que muchas de las vulnerabilidades recientes aún no tienen una puntuación CVSS asignada, lo que indica que están en proceso de análisis por parte del NVD.

Para mantenerte actualizado sobre las vulnerabilidades más recientes y sus calificaciones CVSS, puedes consultar regularmente el sitio oficial del NVD: NVD.

¿Qué método se utiliza para medir cualitativamente la gravedad de las vulnerabilidades?

El método más utilizado a nivel internacional para medir **cualitativa y cuantitativamente** la gravedad de las vulnerabilidades es el **CVSS (Common Vulnerability Scoring System)**. Vamos a desglosarlo con un enfoque claro y didáctico, adecuado tanto para formar a técnicos como para aplicarlo en entornos profesionales de ciberseguridad.

🎯 ¿Qué es CVSS?

CVSS es un estándar abierto creado por **FIRST (Forum of Incident Response and Security Teams)**. Su objetivo es:

- Evaluar la gravedad de las vulnerabilidades.
- Facilitar la **priorización de parches y medidas defensivas**.
- Establecer un lenguaje común entre técnicos, desarrolladores y responsables de seguridad.

📏 ¿Cómo mide CVSS la gravedad?

CVSS asigna una **puntuación numérica entre 0.0 y 10.0**, que se clasifica en niveles **cualitativos**:

Puntuación CVSS	Gravedad Cualitativa	Color habitual
0.0	Ninguna	🟢 Verde
0.1 - 3.9	Baja	🟢 Verde
4.0 - 6.9	Media	🟡 Amarillo
7.0 - 8.9	Alta	🟠 Naranja
9.0 - 10.0	Crítica	🔴 Rojo

🧪 ¿Qué factores evalúa CVSS?

CVSS tiene tres **grupos métricos**:

1. Base Metrics (Obligatorias)

Evalúan las características **invariables** de la vulnerabilidad:

- **Attack Vector (AV)**: ¿se explota localmente, en red, físicamente?
- **Attack Complexity (AC)**: ¿requiere condiciones especiales?
- **Privileges Required (PR)**: ¿necesita permisos previos?
- **User Interaction (UI)**: ¿requiere intervención del usuario?

- **Impacto en la Triada CIA**:
    - Confidencialidad
    - Integridad
    - Disponibilidad

2. Temporal Metrics

Factores que pueden **cambiar con el tiempo**, como:

- Exploit disponible
- Existencia de solución o parche

3. Environmental Metrics

Dependen del **entorno** donde se aplique:

- ¿Qué tan crítico es el sistema afectado?
- ¿Cuál es la importancia del activo?

> 🧠 **Nota**: La puntuación base es la más usada. Las demás se utilizan en análisis avanzados.

🛠️ Ejemplo práctico

Supongamos la vulnerabilidad **CVE-2021-34527 (PrintNightmare)**:

- **CVSS v3.1 Base Score**: 8.8
- **Gravedad**: Alta
- **Vectores**:
    - AV: Red

- AC: Baja
- PR: Baja
- UI: No requiere
- Impacto: Alto en Confidencialidad, Integridad y Disponibilidad

---

📌 ¿Dónde se consulta?

- En la **NVD (nvd.nist.gov)**
- En la **CVE de MITRE**
- A través de herramientas como **OpenVAS, Nessus, Qualys, etc.**

¿Cuántas clasificaciones de gravedad tiene CVSS v3.0 y cuáles son?

En **CVSS v3.0**, existen **5 clasificaciones de gravedad** para describir la importancia o el impacto de una vulnerabilidad en función de su puntuación. Estas clasificaciones se basan en el puntaje final, que puede oscilar entre **0.0 y 10.0**.

Las **5 clasificaciones** son:

---

1. Ninguna (None)

- **Puntuación**: 0.0
- **Descripción**: La vulnerabilidad no tiene impacto. No hay riesgo asociado.

2. Baja (Low)

- **Puntuación**: 0.1 - 3.9

- **Descripción**: La vulnerabilidad representa un bajo riesgo. Si se explota, el impacto es mínimo y no afecta de forma significativa la confidencialidad, integridad o disponibilidad del sistema.

3. Media (Medium)

- **Puntuación**: 4.0 - 6.9

- **Descripción**: La vulnerabilidad tiene un impacto moderado. Aunque la explotación podría comprometer el sistema, los efectos son generalmente limitados, o las condiciones de explotación son específicas y no siempre posibles.

4. Alta (High)

- **Puntuación**: 7.0 - 8.9

- **Descripción**: La vulnerabilidad presenta un alto riesgo. Su explotación podría tener un impacto significativo en la confidencialidad, integridad o disponibilidad del sistema, o puede ser fácil de ejecutar.

5. Crítica (Critical)

- **Puntuación**: 9.0 - 10.0

- **Descripción**: La vulnerabilidad es extremadamente grave. La explotación podría resultar en un compromiso total del sistema, comprometiendo los datos sensibles o controlando por completo el sistema afectado, con consecuencias severas.

🛠️ Relación con las puntuaciones CVSS

La puntuación final de **CVSS v3.0** se calcula a partir de varias métricas, como el vector de ataque, el impacto y la complejidad. Dependiendo de los valores de estas métricas, se asignará una de estas clasificaciones.

Puntuación CVSS	Clasificación de gravedad
0.0	Ninguna
0.1 - 3.9	Baja
4.0 - 6.9	Media
7.0 - 8.9	Alta
9.0 - 10.0	Crítica

Estas clasificaciones ayudan a priorizar las vulnerabilidades en función de su **impacto potencial** y **probabilidad de explotación**.

¿Cuáles son las tres métricas que componen una calificación CVSS?

En **CVSS v3.0**, la calificación de una vulnerabilidad se calcula en base a tres métricas principales. Estas métricas permiten evaluar de manera estructurada la **gravedad** y el **impacto potencial** de una vulnerabilidad. Las tres métricas son:

---

1. Métricas Base (Base Metrics)

Las **métricas base** son las más importantes, ya que describen las características inherentes de la vulnerabilidad que no cambian con el tiempo ni dependen del entorno. Estas métricas se utilizan para calcular la **puntuación CVSS básica**.

Principales componentes:

- **Vector de Ataque (Attack Vector - AV)**: Describe si el atacante necesita acceso físico al sistema afectado o si puede explotar la vulnerabilidad de forma remota.
    - **Valores posibles**:
        - **N** (Network): Explotable a través de la red.
        - **A** (Adjacent Network): Explotable solo a través de una red local adyacente.
        - **L** (Local): Explotable solo en el sistema local.
        - **P** (Physical): Explotable físicamente en el dispositivo afectado.
- **Complejidad del Ataque (Attack Complexity - AC)**: Indica la dificultad de explotar la vulnerabilidad.
    - **Valores posibles**:
        - **L** (Low): La explotación es fácil y no requiere condiciones especiales.
        - **H** (High): La explotación es difícil y requiere condiciones específicas.
- **Privilegios Requeridos (Privileges Required - PR)**: Mide el nivel de acceso necesario para explotar la vulnerabilidad.
    - **Valores posibles**:
        - **N** (None): No se requieren privilegios.
        - **L** (Low): Se requieren privilegios limitados (por ejemplo, un usuario estándar).

        - **H** (High): Se requieren privilegios elevados (por ejemplo, administrador o root).

- **Interacción de Usuario (User Interaction - UI)**: Indica si la explotación de la vulnerabilidad requiere la intervención de un usuario legítimo.
    - **Valores posibles**:
        - **N** (None): No se requiere interacción del usuario.
        - **R** (Required): Se requiere que el usuario realice una acción.
- **Impacto en la Confidencialidad (Confidentiality Impact - C)**: Evalúa el impacto de la vulnerabilidad en la confidencialidad de los datos afectados.
    - **Valores posibles**:
        - **N** (None): No hay impacto en la confidencialidad.
        - **L** (Low): Se compromete parcialmente la confidencialidad.
        - **H** (High): Se compromete completamente la confidencialidad.
- **Impacto en la Integridad (Integrity Impact - I)**: Evalúa el impacto de la vulnerabilidad en la integridad de los datos afectados.
    - **Valores posibles**:
        - **N** (None): No hay impacto en la integridad.
        - **L** (Low): Se compromete parcialmente la integridad.
        - **H** (High): Se compromete completamente la integridad.
- **Impacto en la Disponibilidad (Availability Impact - A)**: Evalúa el impacto de la vulnerabilidad en la disponibilidad del sistema afectado.
    - **Valores posibles**:
        - **N** (None): No hay impacto en la disponibilidad.
        - **L** (Low): Se compromete parcialmente la disponibilidad.

        - **H** (High): Se compromete completamente la disponibilidad.

---

2. Métricas Temporales (Temporal Metrics)

Estas métricas reflejan factores **que pueden cambiar con el tiempo**, como la existencia de una solución o la disponibilidad de un exploit. Son importantes para ajustar la gravedad según el contexto.

Principales componentes:

- **Exploitability (Exploitability - E)**: Define la facilidad con la que un atacante puede explotar la vulnerabilidad.
    - **Valores posibles**:
        - **U** (Unproven): No se ha demostrado que el exploit exista.
        - **P** (Proof-of-Concept): Existe un exploit parcialmente funcional.
        - **F** (Functional): El exploit es completamente funcional.
        - **H** (High): Hay un exploit ampliamente disponible y fácil de usar.
- **Parche o Mitigación (Remediation Level - RL)**: Define el nivel de solución disponible para mitigar la vulnerabilidad.
    - **Valores posibles**:
        - **O** (Official Fix): Un parche oficial está disponible.
        - **T** (Temporary Fix): Existe una solución temporal.
        - **W** (Workaround): Hay una mitigación que no resuelve completamente el problema.
        - **U** (Unavailable): No hay ninguna solución disponible.
- **Confianza del Análisis (Report Confidence - RC)**: Indica la confianza en la validez del análisis de la vulnerabilidad.

- **Valores posibles**:
  - **C** (Confirmed): Hay evidencia de que la vulnerabilidad existe.
  - **R** (Reasonable): La vulnerabilidad parece válida, pero no está confirmada.
  - **U** (Unconfirmed): La vulnerabilidad no está confirmada.

---

3. Métricas Ambientales (Environmental Metrics)

Estas métricas dependen del **entorno** específico donde se encuentra la vulnerabilidad. Toman en cuenta factores como la **importancia de los activos** afectados o el **entorno de implementación**.

Principales componentes:

- **Impacto en el Entorno (Environmental Impact - EI)**: Describe la gravedad del impacto en el entorno específico.
- **Modificadores de Impacto (Security Requirement - SR)**: Permite ajustar la calificación CVSS base según la importancia de la **confidencialidad**, **integridad** o **disponibilidad** en el contexto del sistema afectado.

Resumen

Las tres métricas principales para calcular la puntuación CVSS son:

1. **Métricas Base**: Factores fijos que describen la vulnerabilidad.
2. **Métricas Temporales**: Factores cambiantes, como la existencia de un parche.
3. **Métricas Ambientales**: Factores que dependen del contexto donde ocurre la vulnerabilidad.

Cada una de estas métricas es evaluada y combinada para determinar una **puntuación final** que se utiliza para clasificar la gravedad de la vulnerabilidad.

¿Cuántas métricas componen el grupo de métricas base de un CVSS? ¿Cuáles son?

El grupo de **métricas base** de **CVSS v3.0** consta de **7 métricas**. Estas métricas describen las características inherentes de la vulnerabilidad, y su valor no depende del tiempo ni del contexto del entorno donde se encuentra la vulnerabilidad.

Las **7 métricas base** son las siguientes:

---

1. Vector de Ataque (Attack Vector - AV)

- **Descripción**: Indica cómo un atacante puede explotar la vulnerabilidad.
- **Valores posibles**:
    - **N** (Network): Explotable a través de la red.
    - **A** (Adjacent Network): Explotable solo en redes locales adyacentes.
    - **L** (Local): Explotable solo en el sistema local.
    - **P** (Physical): Explotable físicamente.

---

2. Complejidad del Ataque (Attack Complexity - AC)

- **Descripción**: Mide cuán difícil es para un atacante explotar la vulnerabilidad.
- **Valores posibles**:
    - **L** (Low): Fácil de explotar, no requiere condiciones especiales.
    - **H** (High): Difícil de explotar, requiere condiciones específicas.

---

3. Privilegios Requeridos (Privileges Required - PR)

- **Descripción**: Indica el nivel de privilegios que un atacante necesita para explotar la vulnerabilidad.

- **Valores posibles**:

    - **N** (None): No se requieren privilegios.

    - **L** (Low): Se requieren privilegios limitados (por ejemplo, un usuario estándar).

    - **H** (High): Se requieren privilegios elevados (por ejemplo, administrador o root).

---

4. Interacción de Usuario (User Interaction - UI)

- **Descripción**: Indica si se requiere que un usuario legítimo interactúe para que el ataque sea exitoso.

- **Valores posibles**:

    - **N** (None): No se requiere interacción del usuario.

    - **R** (Required): Se requiere interacción del usuario.

---

5. Impacto en la Confidencialidad (Confidentiality Impact - C)

- **Descripción**: Mide el impacto en la confidencialidad de los datos afectados por la vulnerabilidad.

- **Valores posibles**:

    - **N** (None): No hay impacto en la confidencialidad.

    - **L** (Low): Compromete parcialmente la confidencialidad.

- **H** (High): Compromete completamente la confidencialidad.

---

6. Impacto en la Integridad (Integrity Impact - I)

- **Descripción**: Mide el impacto en la integridad de los datos afectados por la vulnerabilidad.
- **Valores posibles**:
  - **N** (None): No hay impacto en la integridad.
  - **L** (Low): Compromete parcialmente la integridad.
  - **H** (High): Compromete completamente la integridad.

---

7. Impacto en la Disponibilidad (Availability Impact - A)

- **Descripción**: Mide el impacto en la disponibilidad del sistema afectado por la vulnerabilidad.
- **Valores posibles**:
  - **N** (None): No hay impacto en la disponibilidad.
  - **L** (Low): Compromete parcialmente la disponibilidad.
  - **H** (High): Compromete completamente la disponibilidad.

Resumen de las métricas base

Métrica	Descripción
Attack Vector	Método de explotación de la vulnerabilidad

Attack Complexity	Dificultad para explotar la vulnerabilidad
Privileges Required	Nivel de privilegios necesarios para explotar la vulnerabilidad
User Interaction	Si se requiere o no interacción del usuario
Confidentiality Impact	Impacto en la confidencialidad de los datos
Integrity Impact	Impacto en la integridad de los datos
Availability Impact	Impacto en la disponibilidad del sistema

Estas métricas se combinan para calcular la puntuación CVSS, que evalúa la gravedad de la vulnerabilidad en una escala de **0.0 a 10.0**.

¿Cuál es la relación entre CVE, CWE, NVD y CVSS?

La **CVE** es un identificador único para vulnerabilidades de seguridad, la **CWE** clasifica los tipos de debilidades de software, el **NVD** es una base de datos que contiene información detallada sobre las CVE, incluyendo su puntuación **CVSS**, que mide la gravedad de las vulnerabilidades.

Documento Profesional: Vulnerabilidades, CVE, NVD

Documento Profesional: Vulnerabilidades, CVE, NVD y CVSS

Para Portafolio y Recurso Educativo

---

1. Introducción

En el campo de la ciberseguridad, es esencial comprender cómo se clasifican, catalogan y puntúan las vulnerabilidades de software. Los sistemas como **CVE (Common Vulnerabilities and Exposures)**, **CWE (Common Weakness Enumeration)**, **NVD (National Vulnerability Database)** y **CVSS (Common Vulnerability Scoring System)** desempeñan un papel crucial en la gestión de la seguridad informática. Este documento cubre las relaciones y características fundamentales de estos sistemas, proporcionando una base sólida de conocimientos para profesionales y estudiantes de ciberseguridad.

---

2. ¿Qué es CVE?

El **Common Vulnerabilities and Exposures (CVE)** es un sistema de identificación estándar para vulnerabilidades de seguridad en software y hardware. Cada vulnerabilidad registrada en CVE recibe un identificador único (por ejemplo, **CVE-2021-34527**) que se utiliza para referenciar la vulnerabilidad de manera uniforme en la industria. El propósito de CVE es facilitar la comunicación de vulnerabilidades entre diferentes herramientas, bases de datos y organizaciones.

---

3. ¿Qué es CWE?

El **Common Weakness Enumeration (CWE)** es una lista categorizada de las debilidades o fallos comunes en el software que pueden ser explotados por una vulnerabilidad. A diferencia de CVE, que se enfoca en las vulnerabilidades específicas, **CWE** clasifica las debilidades de programación que dan origen a las vulnerabilidades. Las CWE proporcionan un marco para entender y mitigar las fallas de seguridad en el software desde su fase de desarrollo.

---

4. ¿Qué es el NVD?

El **National Vulnerability Database (NVD)** es una base de datos pública mantenida por el gobierno de los EE. UU. que contiene información sobre las vulnerabilidades de seguridad, proporcionando detalles adicionales sobre cada **CVE**. El NVD incluye información adicional como la puntuación **CVSS**, descripciones detalladas de las vulnerabilidades y enlaces a recursos relacionados. Esta base de datos ayuda a los profesionales de la seguridad a evaluar la gravedad de las vulnerabilidades y tomar decisiones informadas sobre las acciones correctivas.

---

5. ¿Qué es CVSS?

El **Common Vulnerability Scoring System (CVSS)** es un sistema que permite puntuar las vulnerabilidades en función de su gravedad. CVSS utiliza una serie de métricas para calcular una puntuación numérica entre **0.0 y 10.0**, lo que ayuda a priorizar las acciones correctivas frente a las vulnerabilidades. La puntuación se desglosa en varias métricas, que se agrupan en tres categorías:

1. **Métricas Base (Base Metrics)**: Factores fijos que describen la vulnerabilidad.

2. **Métricas Temporales (Temporal Metrics)**: Factores que pueden cambiar con el tiempo, como la existencia de un exploit funcional.

3. **Métricas Ambientales (Environmental Metrics)**: Factores específicos del entorno que afectan la calificación de la vulnerabilidad.

---

6. Relación entre CVE, CWE, NVD y CVSS

- **CVE** proporciona un identificador único para vulnerabilidades, permitiendo su seguimiento en diferentes sistemas y plataformas.

- **CWE** clasifica las debilidades que dan origen a las vulnerabilidades, ayudando a los desarrolladores a prevenir problemas de seguridad desde el código.

- **NVD** es una base de datos pública que contiene información detallada sobre las CVE, incluyendo su puntuación CVSS, para facilitar la evaluación y mitigación de vulnerabilidades.

- **CVSS** se utiliza para calcular una puntuación numérica de la gravedad de una vulnerabilidad, permitiendo priorizar la gestión de riesgos en función del impacto potencial.

---

7. Métodos para Medir la Gravedad de las Vulnerabilidades

Para medir cualitativamente la gravedad de las vulnerabilidades, se utilizan herramientas como **CVSS**, que evalúa tres aspectos clave:

- **Impacto potencial** en la **confidencialidad**, **integridad** y **disponibilidad**.
- **Complejidad** del ataque necesario para explotar la vulnerabilidad.
- **Privilegios** requeridos para que un atacante explote la vulnerabilidad.

Este enfoque proporciona una manera estructurada de evaluar la gravedad de las vulnerabilidades.

---

8. Clasificaciones de Gravedad en CVSS v3.0

En **CVSS v3.0**, la gravedad de las vulnerabilidades se clasifica en **cuatro categorías**:

1. **Critical**: Puntuación entre **9.0 y 10.0**; vulnerabilidades que tienen un impacto severo y son de alta prioridad para la mitigación.
2. **High**: Puntuación entre **7.0 y 8.9**; vulnerabilidades significativas, pero con un menor impacto comparado con las críticas.
3. **Medium**: Puntuación entre **4.0 y 6.9**; vulnerabilidades que requieren mitigación, pero con un impacto moderado.
4. **Low**: Puntuación entre **0.1 y 3.9**; vulnerabilidades menores con bajo impacto.

---

9. Métricas Base de CVSS v3.0

El grupo de **métricas base** consta de **7 métricas** fundamentales que definen la gravedad de una vulnerabilidad:

1. **Attack Vector (AV)**: Método de explotación (Network, Local, etc.).
2. **Attack Complexity (AC)**: Dificultad para explotar la vulnerabilidad.

3. **Privileges Required (PR)**: Nivel de privilegios necesarios para explotar la vulnerabilidad.

4. **User Interaction (UI)**: Si se requiere interacción del usuario.

5. **Confidentiality Impact (C)**: Impacto en la confidencialidad de los datos.

6. **Integrity Impact (I)**: Impacto en la integridad de los datos.

7. **Availability Impact (A)**: Impacto en la disponibilidad del sistema.

Estas métricas combinadas proporcionan una puntuación que evalúa la **gravedad inherente** de la vulnerabilidad.

---

10. Conclusión

El conocimiento y la comprensión de cómo se gestionan las vulnerabilidades es fundamental para proteger sistemas y datos en un mundo cada vez más interconectado. El uso de **CVE**, **CWE**, **NVD** y **CVSS** permite a los profesionales de la ciberseguridad identificar, clasificar y mitigar vulnerabilidades de manera eficaz, priorizando las amenazas más graves y aplicando soluciones adecuadas.

Este documento proporciona una referencia completa sobre la clasificación de vulnerabilidades y su impacto, sirviendo como recurso educativo y guía para mejorar las estrategias de seguridad.

Fuente: Este documento está basado en la conversación y el análisis detallado de las vulnerabilidades, sistemas de puntuación y metodologías de evaluación de seguridad, ideales para profesionales y estudiantes del campo de la ciberseguridad.

3.5 Resumen Modulo

3.5.1 ¿Qué aprendí en este módulo?

Realizar reconocimiento pasivo

El reconocimiento es el paso inicial de un ciberataque en el que un atacante recopila información sobre el objetivo. Hay dos tipos de reconocimiento: activo y pasivo. El reconocimiento activo implica el envío de sondeos a la red o los sistemas de destino, mientras que el reconocimiento pasivo no interactúa directamente con el objetivo, sino que utiliza bases de datos de terceros y escucha el tráfico de la red.

Los métodos de reconocimiento activo comunes incluyen host, red, usuario, grupo, recurso compartido de red, página web, aplicación y enumeración de servicios, así como la elaboración de paquetes. Los métodos de reconocimiento pasivo incluyen la enumeración de dominios, la inspección de paquetes, la inteligencia de código abierto (OSINT), el reconocimiento y la escucha.

La realización de un reconocimiento activo generalmente comienza con una pequeña cantidad de información y luego se recopila más durante el escaneo, para luego pasar a diferentes tipos de escaneo y recopilar información adicional. Algunas técnicas utilizadas por los atacantes incluyen búsquedas de DNS, identificación de contactos técnicos y administrativos, extracción de medios sociales e inspección de fallas criptográficas en certificados SSL. La transparencia de los certificados es otra herramienta que los atacantes pueden utilizar para recopilar información sobre los subdominios y los sistemas de una organización.

Las violaciones a la seguridad pueden afectar directamente la reputación de una empresa. Los atacantes utilizan varios métodos para recopilar información, incluidos volcados de contraseñas, metadatos de archivos, análisis estratégico de motores de búsqueda, archivo de sitios web y repositorios de código fuente público. Herramientas como h8mail y WhatBreach aprovechan los repositorios de datos vulnerados, mientras que ExifTool revela los metadatos en los archivos. Los operadores de motores de búsqueda avanzados pueden descubrir información confidencial y el archivo de sitios web permite una vista histórica de los sitios web. La recopilación de inteligencia de código abierto (OSINT) implica la recopilación y el escaneo de información disponible públicamente, siendo Recon-ng un marco potente para este propósito. Shodan escanea Internet en busca de hosts vulnerables y otros sistemas expuestos.

Realizar reconocimiento activo

La realización de un reconocimiento activo implica la enumeración, que es el proceso de recopilación de información sobre un objetivo durante una prueba de penetración. El primer paso es identificar los hosts conectados a Internet del objetivo, seguido de un escaneo de puertos para enumerar los servicios que se ejecutan en esos hosts. Nmap es una herramienta popular para dichos escaneos,

incluidos los escaneos SYN, los escaneos de conexión TCP, los escaneos UDP y los escaneos FIN de TCP.

Un escaneo SYN envía un paquete TCP SYN al puerto de destino y analiza la respuesta para determinar si el servicio está escuchando. Los escaneos de conexión de TCP utilizan el mecanismo de red del sistema operativo para establecer una conexión TCP completa, lo que puede activar alarmas en los sistemas de detección de intrusiones. Los escaneos UDP son útiles para enumerar servicios como DNS, SNMP o DHCP, que utilizan UDP para la comunicación. Los escaneos FIN de TCP envían un paquete FIN al puerto de destino y, si no se recibe respuesta, el puerto se considera abierto.

Los escaneos de detección de host ayudan a determinar si un host está en línea y responde en una red. Nmap también proporciona seis plantillas de tiempo (-T 0-5) para determinar la agresividad de un escaneo, desde muy lento para la evasión de IDS hasta muy agresivo, que puede abrumar a los objetivos o perder puertos abiertos.

Las técnicas de enumeración utilizadas en la recopilación de información incluyen:

- Enumeración de host: se realiza interna y externamente, implica el escaneo de las direcciones IP de un objetivo mediante herramientas como Nmap o Masscan.
- Enumeración de usuarios: recopila una lista de usuarios válidos para descifrar las credenciales mediante la manipulación del protocolo de bloqueo de mensajes del servidor (SMB) en una red de Windows.
- Enumeración de grupos: ayuda a determinar los roles de autorización en el entorno de destino mediante la enumeración de los grupos de SMB mediante el guion NSE de Nmap smb-enum-groups.
- Enumeración de recursos compartidos de red: identifica los sistemas que comparten archivos, carpetas e impresoras en una red mediante el guion NSE smb-enum-Sharts.
- Enumeración de páginas web / Enumeración de aplicaciones web: asigna la superficie de ataque de una aplicación web mediante el guion NSE http-enum de Nmap y otras herramientas como Nikto.
- Enumeración de servicios: identifica los servicios que se ejecutan en un sistema remoto, principalmente a través de la funcionalidad de escaneo de puertos de Nmap.
- Enumeración mediante la elaboración de paquetes: Scapy, un marco de trabajo basado en Python, se puede utilizar para realizar el reconocimiento de la red mediante la generación de paquetes.

Además, la inspección de paquetes y la escucha clandestina se pueden realizar con herramientas como Wireshark, tshark y tcpdump, lo que ayuda en el reconocimiento pasivo durante las pruebas de penetración.

Comprender el arte de realizar escaneo de vulnerabilidades

El escaneo de vulnerabilidades es el proceso de identificación de debilidades en un sistema al sondear servicios para determinar si son vulnerables. Los escáneres de vulnerabilidades utilizan diferentes métodos, pero generalmente siguen un proceso de cuatro pasos: detección, identificación de software / versión, correlación de vulnerabilidades y generación de informes. Sin embargo, estos informes pueden contener falsos positivos, por lo que la validación es crucial.

Hay varios tipos de escaneo de vulnerabilidades, entre ellos:

- no autenticado (el escáner funciona sin credenciales)
- autenticado (el escáner utiliza credenciales de acceso de nivel raíz)
- detección (el escáner identifica la superficie de ataque de un objetivo)
- completo (el escáner habilita todas las opciones de escaneo)
- furtivo (el escáner minimiza el ruido para evitar la detección)
- pasivo (el escáner supervisa y analiza el tráfico de red)
- cumplimiento (el escáner verifica el cumplimiento de las regulaciones de la industria).

Cada tipo de escaneo tiene sus propios puntos fuertes y sus limitaciones. Por ejemplo, los escaneos no autenticados solo muestran servicios de red expuestos, mientras que los escaneos autenticados proporcionan información más completa. Los escaneos furtivos son útiles para los entornos de producción, pero es posible que no detecten todas las vulnerabilidades. Los escaneos de cumplimiento abordan requisitos específicos del sector, pero pueden ser difíciles debido a las diferentes interpretaciones de las regulaciones.

Los desafíos a tener en cuenta al ejecutar un escaneo de vulnerabilidades en una red o dispositivo incluyen:

- Mejor momento para ejecutar un escaneo: los escaneos en las redes de producción deben realizarse con cuidado para minimizar el impacto en los usuarios y los servidores, generalmente durante las primeras horas cuando el uso de la red es bajo.
- Determinación de los protocolos en uso: identifique si el dispositivo de destino utiliza TCP, UDP o ambos, para evaluar las vulnerabilidades en ambos servicios.
- Topología de red: los escaneos deben realizarse lo más cerca posible del destino para evitar afectar los dispositivos a lo largo de la ruta y afectar los resultados del escaneo.
- Limitaciones de ancho de banda: es posible que la configuración del escáner deba ajustarse para situaciones de ancho de banda bajo para evitar problemas de consumo de ancho de banda.

- Limitación de consultas: reducir el tráfico del escáner puede ayudar a administrar las limitaciones de ancho de banda. Esto se puede lograr reduciendo los hilos de ataque o el alcance de los complementos / ataques.
- Sistemas frágiles / Recursos no tradicionales: es posible que los escáneres de vulnerabilidades deban ajustar las opciones de escaneo de los sistemas frágiles, como impresoras o dispositivos de IoT, para evitar su falla. Alternativamente, estos dispositivos pueden estar exentos de escaneo, pero esto podría reducir la seguridad general.

Ejecutar un escaneo de vulnerabilidades es la parte fácil de identificar amenazas potenciales; el principal desafío radica en el escaneo de los resultados. Las herramientas de escaneo de vulnerabilidades pueden producir falsos positivos, que deben eliminarse para identificar con precisión las vulnerabilidades reales. Reducir los falsos positivos es particularmente importante al proporcionar un informe para una asignación de prueba de penetración pagada.

La eliminación de falsos positivos implica validar la información de la versión e investigar los detalles de la vulnerabilidad. Cada vulnerabilidad se asigna a elementos de la lista de vulnerabilidades y exposiciones comunes (CVE), que deben examinarse para comprender mejor los criterios.

Varias organizaciones y recursos, como US-CERT, la División CERT de la Universidad Carnegie Mellon, NIST, JPCERT, CAPEC, CVE, CWE y CVSS, proporcionan información útil para una mayor investigación de las vulnerabilidades. Al lidiar con una vulnerabilidad, es importante determinar su prioridad evaluando su gravedad, la cantidad de sistemas afectados y otros factores.

En general, analizar correctamente los resultados del escaneo de vulnerabilidades implica un examen detallado de los hallazgos de la herramienta y priorizar las vulnerabilidades para su mitigación en función de su gravedad y posible impacto.

3.5.2 Preguntas de reflexión

Una vez que se firma el contrato y la participación en las pruebas de penetración está en curso, es hora de aprender lo más posible sobre la red, las aplicaciones y los sistemas del cliente. El reconocimiento pasivo es una buena manera de comenzar. ¿Qué tipo de información valiosa se puede encontrar en el reconocimiento pasivo? El reconocimiento activo es más intrusivo que el reconocimiento pasivo. Debido a esto, ¿por qué un evaluador debe tener cuidado al realizar un reconocimiento activo?

Muchos escáneres de vulnerabilidades están automatizados. Si bien los escáneres de vulnerabilidades suelen ser precisos, es importante verificar manualmente algunos resultados. ¿Por qué es esto cierto? Al analizar los resultados del escaneo de vulnerabilidades, ¿por qué es importante estar familiarizado con CVE, CWE y CVSS?

Pestaña 10

🛡️ Documento Profesional: Reconocimiento y Escaneo de Vulnerabilidades

---

1. 🧭 Introducción

En el ámbito de las pruebas de penetración y la ciberseguridad ofensiva, los procesos de **reconocimiento** y **escaneo de vulnerabilidades** son esenciales para identificar activos expuestos y debilidades explotables dentro de una infraestructura. Este documento sintetiza los aspectos clave de dichas técnicas, organizado como material de consulta profesional y educativo.

---

2. 🔍 Reconocimiento Pasivo

- **Definición:** Recolección de información sin interacción directa con el objetivo.
- **Fuentes comunes:** Bases de datos de terceros, escuchas de red, redes sociales, metadatos de archivos, certificados SSL, fuentes OSINT.
- **Herramientas relevantes y ejemplos de uso:**
    - 📨 **h8mail / WhatBreach:** Verificar si un correo electrónico ha sido expuesto en filtraciones de datos.
    - 🖼️ **ExifTool:** Extraer metadatos de imágenes/documentos (ubicación, autor, fecha).
    - 🕵️ **Recon-ng:** Automatizar la recolección de inteligencia pública sobre dominios o identidades.
    - 🌐 **Shodan:** Identificar dispositivos accesibles desde Internet (cámaras IP, routers, etc.).

---

3. 🚨 Reconocimiento Activo

- **Definición:** Implica enviar paquetes o realizar sondeos al sistema objetivo.

- **Técnicas comunes:**
    - 🌐 **Escaneo de red y puertos:** Nmap (SYN, TCP, UDP, FIN)
    - 📈 **Análisis de tráfico:** Wireshark, tcpdump
    - ⚙️ **Paquetes personalizados:** Scapy
    - 🔍 **Enumeración:** Identificar usuarios, grupos, recursos compartidos, servicios web, etc.
- **Consideraciones:**
  Es más intrusivo y detectable. Puede activar IDS (sistemas de detección de intrusos).

---

4. 🧪 Escaneo de Vulnerabilidades

- **Objetivo:** Detectar servicios, identificar versiones y correlacionarlas con vulnerabilidades conocidas (CVE).
- **Etapas típicas del escaneo:**
    - 📡 Detección de servicios
    - 🔎 Identificación de versiones
    - 📚 Correlación con bases de datos de vulnerabilidades
    - 📝 Generación de informes
- **Tipos de escaneo:**
    - 🚫 **No autenticado:** Sin credenciales. Simula un atacante externo.
    - ✅ **Autenticado:** Acceso interno con credenciales. Análisis más profundo.
    - 🔍 **Completo:** Examina todos los puertos y servicios disponibles.
    - 🕶️ **Furtivo:** Usa técnicas para evitar detección (escaneo lento, fragmentación).
    - 💤 **Pasivo:** Solo observación del tráfico, sin enviar paquetes.

    - 🛠️ **Cumplimiento:** Verifica conformidad con normativas como PCI-DSS, HIPAA, etc.

- **Desafíos comunes:**
    - ⚠️ Falsos positivos (requieren validación manual)
    - 🛑 Limitaciones de red y ancho de banda
    - 💣 Sistemas frágiles (IoT, impresoras)
- **Recursos de apoyo:**
    - 📌 **CVE:** Common Vulnerabilities and Exposures
    - 🔍 **CWE:** Common Weakness Enumeration
    - 📊 **CVSS:** Sistema de puntuación de vulnerabilidades
    - 🗒️ **Otros:** US-CERT, NIST, JPCERT, CAPEC

---

5. ⚠️ Consideraciones Críticas

- 🕵️ El reconocimiento pasivo puede revelar subdominios, correos, contactos técnicos y configuraciones expuestas.
- 🚨 El reconocimiento activo debe realizarse con autorización explícita y consciente del posible impacto operativo.
- 🔎 El análisis de resultados debe minimizar los falsos positivos para generar valor accionable.

---

6. ✅ Recomendaciones Finales

- Familiarízate con los estándares **CVE, CWE y CVSS** para clasificar vulnerabilidades.
- Combina herramientas automáticas con validaciones manuales para mayor precisión.
- Programa los escaneos en horarios controlados para evitar interrupciones.

- Documenta claramente cada fase del proceso.
- Mantente al día sobre nuevas amenazas, vectores de ataque y herramientas emergentes.

---

7. 🏁 Conclusión

El dominio del reconocimiento y el escaneo de vulnerabilidades permite a los profesionales de ciberseguridad **anticiparse a amenazas**, **evaluar superficies de ataque** y **mitigar riesgos de forma eficaz**. Es un proceso estructurado que constituye la base de una prueba de penetración profesional.

📄 **Documento preparado por:** Mitxel Macias
🎯 **Propósito:** Consulta profesional y formación