

En este módulo, los alumnos comprenderán el proceso de gestión de vulnerabilidades. Aprenderán sobre vulnerabilidades comunes. Desarrollarán una mentalidad de atacante examinando las formas en que las vulnerabilidades pueden convertirse en amenazas a la seguridad de los activos si son explotadas.

Objetivos de aprendizaje

- Diferencie entre vulnerabilidades y amenazas.
- Describa la estrategia de defensa en profundidad.
- Explique cómo MITRE identifica las exposiciones a vulnerabilidades comunes.
- Explique cómo se utilizan las evaluaciones de vulnerabilidad para evaluar el riesgo potencial.
- Analice una superficie de ataque.
- Desarrolle una mentalidad de atacante para reconocer las amenazas.

Enfoques para la exploración de vulnerabilidades

Anteriormente, usted aprendió acerca de una evaluación de vulnerabilidad, que es el proceso de revisión interna de los sistemas de Seguridad de una organización. Una organización realiza evaluaciones de vulnerabilidad para identificar debilidades y prevenir ataques. Las herramientas de exploración de vulnerabilidades se utilizan habitualmente para simular amenazas encontrando vulnerabilidades en una superficie de ataque. También ayudan a los Equipos de Seguridad a tomar medidas proactivas para implementar su estrategia de remediación.

Los escáneres de vulnerabilidades son herramientas importantes que probablemente utilizará sobre el terreno. En esta lectura, explorará cómo funcionan los escáneres de vulnerabilidades y los tipos de escaneos que pueden realizar.

¿Qué es un escáner de vulnerabilidades?

Un escáner de vulnerabilidades es un software que compara automáticamente las vulnerabilidades y exposiciones conocidas con las tecnologías de la red. En general, estas herramientas escanean los sistemas para encontrar errores de configuración o de programación.

Las herramientas de escaneado se utilizan para analizar cada una de las cinco superficies de ataque que conoció en [el vídeo sobre la estrategia de defensa en profundidad](#):

1. Capa de perímetro, como los sistemas de autenticación que validan la accesibilidad de los usuarios
2. Capa de red, que se compone de tecnologías como firewalls de red y otras
3. Capa de punto final, que describe los dispositivos de una red, como ordenadores portátiles, de sobremesa o servidores
4. Capa de aplicación, que implica el software con el que interactúan los usuarios

5. Capa de datos, que incluye cualquier información almacenada, en tránsito o en uso

Cuando comienza un escaneo de cualquier capa, la herramienta de escaneo compara los hallazgos con las bases de datos de amenazas a la seguridad. Al final de la exploración, la herramienta marca cualquier vulnerabilidad que encuentre y la añade a su base de datos de referencia. Cada exploración añade más información a la base de datos, lo que ayuda a la herramienta a ser más precisa en su análisis.

Nota: Las bases de datos de vulnerabilidades también son actualizadas rutinariamente por la empresa que diseñó el software de exploración.

Realización de exploraciones

Los escáneres de vulnerabilidades están pensados para no ser intrusivos. Es decir, no rompen ni se aprovechan de un sistema como lo haría un atacante. En su lugar, simplemente escanean una superficie y le alertan de cualquier puerta potencialmente desbloqueada en sus sistemas.

Nota: Aunque los escáneres de vulnerabilidades no son intrusivos, hay casos en los que un escáner puede causar problemas inadvertidamente, como bloquear un sistema.

Estas herramientas se utilizan de varias maneras para escanear una superficie. Cada enfoque corresponde a la vía que podría seguir un Agente de amenaza. A continuación, puede explorar cada tipo de escaneo para tener una idea más clara al respecto.

Externo frente a interno

Los escaneos externos e internos simulan el enfoque de un atacante.

Los escaneos *externos* prueban la capa perimetral fuera de la red interna. Analizan sistemas orientados al exterior, como sitios web y firewalls. Este tipo de exploraciones pueden descubrir puntos vulnerables, como puertos de red o servidores vulnerables.

Los escaneos *internos* parten del extremo opuesto, examinando los sistemas internos de una organización. Por ejemplo, este tipo de escaneado podría analizar el software de aplicación en busca de puntos débiles en la forma en que gestiona la entrada de datos de los usuarios.

Autenticación frente a no autenticación

Los escaneos autenticados y no autenticados simulan si un usuario tiene o no acceso a un sistema.

Los escaneos *autenticados* pueden probar un sistema registrándose con una cuenta de usuario real o incluso con una cuenta de administrador. Estas cuentas de servicio se utilizan para comprobar vulnerabilidades, como controles de acceso rotos.

Los escaneos *no autenticados* simulan agentes de amenaza externos que no tienen acceso a los recursos de su empresa. Por ejemplo, un escaneado podría analizar los recursos compartidos de archivos dentro de la organización que se utilizan para albergar documentos exclusivamente internos. Los usuarios no autenticados deberían recibir resultados de "acceso denegado" si intentaran abrir estos archivos. Sin embargo, se identificaría una vulnerabilidad si pudieran acceder a un archivo.

Limitado frente a exhaustivo

Los escaneos limitados y exhaustivos se centran en dispositivos concretos a los que acceden usuarios internos y externos.

Los escaneos *limitados* analizan dispositivos concretos de una red, como la búsqueda de errores de configuración en un firewall.

Los escaneos *exhaustivos* analizan todos los dispositivos conectados a una red. Esto incluye sistemas operativos, bases de datos de usuarios, etc.

Consejo profesional: La exploración de descubrimiento debe realizarse antes de las exploraciones limitadas o exhaustivas. La exploración de descubrimiento se utiliza para hacerse una idea de las computadoras, dispositivos y puertos abiertos que hay en una red.

Puntos clave

Encontrar vulnerabilidades requiere pensar en todas las posibilidades. Los escaneos de vulnerabilidad varían en función de las superficies que una organización esté evaluando. Por lo general, los profesionales de seguridad experimentados lideran el esfuerzo de configurar y realizar este tipo de escaneos para crear un perfil de la postura de seguridad de una empresa. Sin embargo, los analistas también desempeñan una función importante en el proceso. Los resultados de un escaneado de vulnerabilidad a menudo conducen a la renovación de los esfuerzos de cumplimiento, a cambios en los procedimientos y a la aplicación de parches en el sistema. Comprender los objetivos de los tipos comunes de escáneres de vulnerabilidad le ayudará a participar en estos ejercicios proactivos de Seguridad siempre que sea posible.

Consejo: Para explorar el software escáner de vulnerabilidades utilizado habitualmente en el sector de la ciberseguridad, en su navegador preferido introduzca términos de búsqueda similares a "software escáner de vulnerabilidades popular" y/o "software escáner de vulnerabilidades de código abierto utilizado en ciberseguridad".

1. ¿Qué es una exploración de vulnerabilidades?

Definición profesional:

Es el proceso sistemático de búsqueda de debilidades o errores de seguridad en sistemas, redes, aplicaciones o dispositivos, con el objetivo de anticiparse a un ataque.

¿Cómo se hace?

Mediante **herramientas de escaneo automatizadas** (scanners), que comparan el sistema actual con una base de datos de vulnerabilidades conocidas (como el CVE – *Common Vulnerabilities and Exposures*).

Enfoque mental del analista:

Cuando escaneas, te pones en la piel de un atacante: ¿Por dónde podría entrar? ¿Qué está mal configurado? ¿Qué error de software podría aprovechar?

2. ¿Qué es un escáner de vulnerabilidades?

Es una herramienta que...

- Recorre la red, sistema o aplicación.
- Compara lo que encuentra con bases de datos actualizadas (como NVD o la propia del fabricante del scanner).
- Identifica *errores de configuración, software obsoleto, servicios expuestos*, etc.

Bases de datos vivas:

Estas herramientas **actualizan constantemente sus firmas** y conocimientos. Por eso, es fundamental mantener el escáner actualizado.

💡 Ejemplo práctico:

Una empresa usa *Nessus* o *OpenVAS* para escanear semanalmente su red interna. Se detecta un servidor con SMBv1 habilitado (protocolo obsoleto y peligroso). El escáner lo detecta, alerta, y se toma acción.

🔒 3. Capas a analizar: la Defensa en Profundidad

Un buen escáner puede analizar cada una de estas **5 capas de seguridad** (según el enfoque de *defense in depth*):

Capa	¿Qué analiza?	Ejemplo de vulnerabilidad detectada
Perímetro	Firewalls, VPNs, autenticación	Contraseña débil o puerto abierto
Red	Protocolos, tráfico interno	SNMP habilitado sin seguridad
Punto final	PCs, portátiles, servidores	Antivirus desactualizado, software vulnerable
Aplicación	Sitios web, APIs	Inyección SQL, falta de validación
Datos	Archivos, bases de datos	Acceso no restringido, cifrado débil


📌 **Nota importante:** Ningún escáner analiza *todo perfectamente*, pero muchos cubren varias capas.

4. Tipos de escaneos

Los escaneos se pueden clasificar en función de cómo se realiza el análisis:


♦ a) Externo vs Interno

Tipo	Simula a...	Objetivo
Externo	Un atacante desde fuera	Detectar puntos vulnerables públicos
Interno	Un atacante dentro de la red	Ver qué podría hacer alguien con acceso parcial

 **Relevancia:** En muchos ciberataques reales, el atacante **ya está dentro** (empleado malicioso, malware, VPN comprometida...). Por eso, ambos tipos son esenciales.

♦ b) Autenticado vs No autenticado

Tipo	Acceso	Utilidad
Autenticado	Usuario con login	Detectar fallos profundos, privilegios mal gestionados
No autenticado	Sin login	Simular amenazas externas, acceso indebido a recursos públicos

 **Ejemplo:** Si un escaneo no autenticado detecta que un PDF con datos personales está accesible sin login, se trata de **una fuga de datos** grave.

♦ c) Limitado vs Exhaustivo

Tipo	Alcance	Ejemplo
Limitado	Dispositivos o sistemas específicos	Revisión puntual de un firewall
Exhaustivo	Todo el entorno	Análisis completo de red, PCs, servidores y aplicaciones

Consejo profesional:

Antes de hacer un escaneo limitado o exhaustivo, se realiza un **escaneo de descubrimiento** (*discovery scan*), que mapea todos los dispositivos y servicios visibles.

5. Riesgos y buenas prácticas

Aunque los escáneres **no son intrusivos**, pueden:

- Saturar la red si se malconfiguran.
- Hacer que un sistema reaccione mal (por ejemplo, bloqueos si el antivirus detecta el escaneo como sospechoso).

Recomendaciones para escanear como profesional:

1. **Planifica:** Nunca escanees en horario laboral sin avisar (riesgo de interrupciones).

2. **Etiqueta:** Documenta qué se escanea, cuándo, con qué credenciales.
 3. **Prioriza:** No intentes arreglar 100 fallos a la vez; prioriza por severidad y facilidad de explotación.
 4. **Corrige y vuelve a escanear:** Un buen escaneo termina cuando **se mitigan las vulnerabilidades**, no cuando se genera el informe.
-

6. En resumen (como lo explicaría un mentor)

- Un escáner de vulnerabilidades **no es un hacker**, sino un médico del sistema.
 - Su misión es encontrar puntos débiles *antes que lo hagan los atacantes*.
 - Hay distintos tipos de escaneos según el enfoque, nivel de acceso y profundidad.
 - Toda exploración debe integrarse en una estrategia de **defensa en profundidad**.
 - Las vulnerabilidades encontradas deben corregirse con base en un plan bien estructurado.
-

Recursos para explorar

Te sugiero que investigues sobre estas herramientas (todas relevantes y populares en ciberseguridad):

- **Nessus** (comercial, muy usado en empresas)
- **OpenVAS** (código abierto)
- **Qualys** (SaaS empresarial)
- **Nmap + NSE scripts** (para escaneos más técnicos)
- **Lynis** (para sistemas Linux)

La importancia de las actualizaciones

Es posible que en algún momento se haya preguntado: "¿Por qué necesitan actualizarse constantemente mis dispositivos?" Para los consumidores, las actualizaciones proporcionan mejoras en el rendimiento, la estabilidad e incluso ¡nuevas funciones! Pero desde el punto de vista de la Seguridad, sirven a un propósito específico. Las actualizaciones permiten a las organizaciones abordar las vulnerabilidades de seguridad que pueden poner en peligro a sus usuarios, dispositivos y redes.

En un vídeo, usted aprendió que las actualizaciones encajan en la estrategia de corrección de cualquier equipo de seguridad. Suelen tener lugar después de una evaluación de vulnerabilidades, que es el proceso de revisión interna de los sistemas de Seguridad de una organización. En esta lectura, aprenderá qué hacen las actualizaciones, cómo se suministran y por qué son importantes para la ciberseguridad.

Parchear las lagunas de seguridad

Una computadora anticuada se parece mucho a una casa con las puertas sin cerrar. Los actores maliciosos utilizan estas brechas en la Seguridad de la misma manera, para obtener accesibilidad no autorizada. Las actualizaciones de software son similares a cerrar las puertas para mantenerlos fuera.

Una actualización de parche es una actualización de software y del sistema operativo que aborda las vulnerabilidades de seguridad dentro de un programa o producto. Los parches suelen contener correcciones de errores que abordan vulnerabilidades y exposiciones de seguridad comunes.

Nota: Idealmente, los parches abordan las vulnerabilidades y exposiciones comunes antes de que los hackers maliciosos las encuentren. Sin embargo, los parches se

desarrollan a veces como resultado de un Día cero, que es un exploit desconocido hasta entonces.

Estrategias comunes de actualización

Cuando las actualizaciones de software están disponibles, los clientes y usuarios tienen dos opciones de instalación:

- Actualizaciones manuales
- Actualizaciones automáticas

Como aprenderá, cada estrategia tiene tanto beneficios como desventajas.

Actualizaciones manuales

Una estrategia de implementación manual depende de que los departamentos de TI o los usuarios obtengan las actualizaciones de los desarrolladores. Los entornos de oficina en casa o de pequeña empresa pueden requerir que usted mismo busque, descargue e instale las actualizaciones. En entornos empresariales, el proceso suele gestionarse con una herramienta de administración de configuraciones. Estas Herramientas ofrecen una serie de opciones para la implementación de actualizaciones, como a todos los clientes de su red o a un grupo selecto de usuarios.

Ventaja: Una ventaja de las estrategias de implementación manual de actualizaciones es el control. Esto puede ser útil si los desarrolladores no prueban a fondo las actualizaciones de software, lo que puede dar lugar a problemas de inestabilidad.

Desventaja: Una desventaja de la implementación manual de actualizaciones es que las actualizaciones críticas pueden olvidarse o ignorarse por completo.

Actualizaciones automáticas

Una estrategia de implementación automática adopta el enfoque opuesto. Con esta opción, el sistema o la aplicación pueden encargarse de buscar, descargar e instalar las actualizaciones.

Consejo profesional: La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) recomienda utilizar las opciones automáticas siempre que estén disponibles.

Es necesario que los usuarios o los grupos de TI habiliten ciertos permisos antes de que las actualizaciones puedan instalarse, o empujarse, cuando estén disponibles. Depende de los desarrolladores probar adecuadamente sus parches antes de publicarlos.

Ventaja: Una ventaja de las actualizaciones automáticas es que el proceso de implementación se simplifica. También mantiene los sistemas y el software al día con los últimos parches críticos.

Desventaja: Un inconveniente de las actualizaciones automáticas es que pueden producirse problemas de inestabilidad si los parches no han sido probados a fondo por el proveedor. Esto puede provocar problemas de rendimiento y una mala experiencia del usuario.

Software al final de su vida útil

A veces no hay actualizaciones disponibles para cierto tipo de software conocido como software de fin de vida útil (EOL). Todo software tiene un ciclo de vida. Comienza cuando se produce y termina cuando se publica una versión más reciente. En ese momento, los desarrolladores deben asignar recursos a las versiones más recientes, lo que da lugar al software EOL. Aunque el software más antiguo sigue siendo útil, el fabricante ya no le da soporte.

Nota: Los parches y las actualizaciones son muy diferentes de las mejoras. Las *actualizaciones* se refieren a versiones completamente nuevas de hardware o software que pueden adquirirse.

[CISA recomienda dejar de utilizar el software EOL](#) porque supone un riesgo irreparable para los sistemas. Pero esta recomendación no siempre se sigue. La sustitución de la tecnología EOL puede resultar costosa para las empresas y los usuarios individuales.

Los Riesgos que presenta el software EOL siguen creciendo a medida que más dispositivos conectados entran en el mercado. Por ejemplo, hay miles de millones de dispositivos de Internet de las cosas (IoT), como bombillas inteligentes, conectados a redes domésticas y de trabajo. En algunos entornos empresariales, todo lo que necesita un atacante es un único dispositivo sin parchear para acceder a la red y causar problemas.

Puntos clave

Actualizar el software y parchear las vulnerabilidades es una práctica importante en la que todo el mundo debería participar. Por desgracia, no siempre es así. Muchos de los mayores ciberataques del mundo podrían haberse evitado si los sistemas se hubieran mantenido actualizados. Un ejemplo es el ataque WannaCry de 2017. El ataque afectó a computadoras de más de 150 países y causó unos daños estimados en 4.000 millones de dólares. Los investigadores han descubierto desde entonces que WannaCry podría haberse evitado si los sistemas infectados hubieran estado actualizados con un parche de Seguridad que estuvo disponible meses antes del ataque. Mantener el software actualizado requiere esfuerzo. Sin embargo, los Beneficios que proporcionan hacen que merezca la pena.

Resumen esquemático: La importancia de las actualizaciones

1. ¿Por qué son importantes las actualizaciones?


- Mejoran:
 - Rendimiento
 - Estabilidad
 - Funcionalidades
 - Pero sobre todo **corrigen vulnerabilidades** que podrían ser explotadas por atacantes.
 - Forman parte clave de la estrategia de **corrección de vulnerabilidades** en ciberseguridad.
-

2. Parchear las lagunas de seguridad

- Un sistema sin actualizar = una casa con las puertas abiertas.
 - Los **parches** corrigen fallos conocidos (vulnerabilidades).
 - **Día cero**: vulnerabilidad que se explota antes de que exista un parche → muy peligrosa.
-

3. Estrategias comunes de actualización

A. Actualizaciones manuales

- Requieren intervención humana para buscar e instalar.
- Utilizadas por:
 - Usuarios domésticos
 - Administradores de sistemas (con herramientas de gestión)
-  Ventaja: mayor **control**

- ❌ Desventaja: riesgo de **olvido** o **desactualización**

B. Actualizaciones automáticas

- El sistema gestiona la búsqueda e instalación por sí solo.
 - Recomendadas por la **CISA** (Agencia de Ciberseguridad de EE.UU.)
 - ✅ Ventaja: mayor **rapidez y cobertura**
 - ❌ Desventaja: riesgo de **inestabilidad** si el parche está mal probado
-

⌚ 4. Software EOL (End of Life / Fin de vida útil)

- Ya **no recibe actualizaciones ni parches de seguridad**.
 - Representa un **riesgo crítico**.
 - CISA recomienda **no usar software EOL**.
 - Problema frecuente:
 - Empresas o usuarios siguen usando software obsoleto por **costes** de actualización.
-

🌐 5. Riesgos actuales: IoT y dispositivos obsoletos

- Ejemplo: bombillas inteligentes, cámaras, routers, etc.
 - Un solo dispositivo sin parchear puede comprometer toda una red.
-

📌 6. Caso real: WannaCry (2017)

- Ataque global que afectó a +150 países.
- Daños estimados: 4.000 millones de dólares.
- **Se pudo evitar**: existía un parche publicado **meses antes** del ataque.

✓ Conclusión

Mantener el software actualizado **no es opcional** en ciberseguridad.

Es una de las **formas más eficaces** de prevenir ataques y proteger los sistemas.

Pruebas de penetración

Un plan de Seguridad eficaz se basa en pruebas periódicas para encontrar los puntos débiles de una organización. Anteriormente, aprendió que las evaluaciones de vulnerabilidad, el proceso de revisión interna de los sistemas de Seguridad de una organización, se utilizan para diseñar estrategias de defensa basadas en las debilidades del sistema. En esta lectura, aprenderá cómo los Equipos de Seguridad evalúan la eficacia de sus defensas mediante pruebas de penetración.

Pruebas de penetración

Una prueba de penetración, o pen test, es un ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. El ataque simulado en una prueba de penetración implica el uso de las mismas herramientas y técnicas que los actores maliciosos con el fin de imitar un ataque en la vida real. Dado que una prueba de penetración es un ataque autorizado, se considera una forma de hacking ético. A diferencia de una evaluación de vulnerabilidades que encuentra puntos débiles en la Seguridad de un sistema, una prueba de penetración explota esos puntos débiles para determinar las consecuencias potenciales si el sistema se rompe o es penetrado por un agente de amenaza.

Por ejemplo, el Equipo de ciberseguridad de una empresa financiera podría simular un ataque a su aplicación bancaria para determinar si existen puntos débiles que permitirían a un atacante robar información de sus clientes o transferir fondos ilegalmente. Si la prueba de penetración descubre errores de configuración, el Equipo puede abordarlos y mejorar la Seguridad general de la aplicación.

Nota: Las organizaciones reguladas por PCI DSS, HIPAA o GDPR deben realizar pruebas de penetración de forma rutinaria para mantener los Estándares de cumplimiento.

Aprender de perspectivas variadas

Estos ataques autorizados son realizados por pen testers expertos en programación y arquitectura de redes. Dependiendo de sus objetivos, las organizaciones pueden utilizar algunos enfoques diferentes para las pruebas de penetración:

- Las pruebas del Equipo Rojo *simulan* ataques para identificar vulnerabilidades en sistemas, redes o aplicaciones.
- Las pruebas del equipo azul se centran en la *defensa y la Respuesta ante incidentes* para validar los sistemas de Seguridad existentes en una organización.
- Las pruebas del equipo púrpura son *colaborativas* y se centran en mejorar la postura de seguridad de la organización combinando elementos de los ejercicios de los equipos rojo y azul.

Las Pruebas de penetración de los equipos rojos suelen ser realizadas por "pen testers" independientes contratados para evaluar los sistemas internos. Aunque los equipos de ciberseguridad también pueden contar con sus propios expertos en pruebas de penetración. Independientemente del enfoque, los expertos en pruebas de penetración deben tomar una decisión importante antes de simular un ataque: *¿Cuánto acceso e Información necesito?*

Estrategias de pruebas de penetración

Existen tres estrategias comunes de pruebas de penetración:

- Las pruebas de caja abierta son aquellas en las que el evaluador tiene el mismo acceso privilegiado que tendría un desarrollador interno a información como la arquitectura del sistema, el flujo de datos y los diagramas de red. Esta estrategia recibe varios nombres diferentes, como pruebas de penetración internas, de pleno conocimiento, de caja blanca y de caja clara.
- Las pruebas de cajacerrada son aquellas en las que el probador tiene poco o ningún acceso a los sistemas internos, algo similar a lo que haría un hacker malintencionado. Esta estrategia se conoce a veces como pruebas de penetración externas, de caja negra o de conocimiento cero.

- Las pruebas de conocimientos parciales se producen cuando la persona que realiza las pruebas tiene acceso y conocimientos limitados de un sistema interno; por ejemplo, un representante de atención al cliente. Esta estrategia también se conoce como pruebas de caja gris.

Las pruebas de caja cerrada tienden a producir las simulaciones más exactas de un ataque en el mundo real. No obstante, cada estrategia produce resultados valiosos al demostrar cómo un atacante podría infiltrarse en un sistema y a qué información podría acceder.

Convertirse en un probador de penetración

Los probadores de penetración están muy demandados en el campo de la ciberseguridad, en rápido crecimiento. Todas las habilidades que está aprendiendo en este Programa pueden ayudarle a avanzar hacia una carrera en pruebas de penetración:

- Seguridad de redes y aplicaciones
- Experiencia con sistemas operativos, como Linux
- Análisis de vulnerabilidad y Modelado de amenazas
- Herramientas de Detección y respuesta
- Lenguajes de programación, como Python y BASH
- Habilidades de comunicación

Los conocimientos de programación son muy útiles en las pruebas de penetración porque a menudo se realizan en software y sistemas informáticos. Con suficiente práctica y dedicación, los profesionales de la ciberseguridad de cualquier nivel pueden desarrollar las habilidades necesarias para ser un "pen tester".

Programas de Recompensas por errores

Las organizaciones suelen llevar a cabo programas de recompensas por errores que ofrecen a los pen testers autónomos recompensas económicas por encontrar y notificar vulnerabilidades en sus productos. Las Recompensas por errores son

grandes oportunidades para que los profesionales de la Seguridad aficionados participen y hagan crecer sus habilidades.

Consejo profesional: [HackerOne](#) es una comunidad de hackers éticos en la que puede encontrar Recompensas por errores activas en las que participar.

Puntos clave

Un Riesgo importante para las organizaciones son los hackers malintencionados que irrumpen en sus sistemas. Las pruebas de penetración son otra forma que tienen las organizaciones de asegurar sus sistemas. Los Equipos de Seguridad utilizan estos ataques simulados para hacerse una idea más clara de los puntos débiles de sus defensas. Hay una necesidad creciente de profesionales especializados en Seguridad en este campo. Incluso si empieza ayudando en estas actividades, hay muchas oportunidades para crecer y aprender las habilidades necesarias para ser un "pen tester".

Resumen Esquemático: Pruebas de Penetración

¿Qué es una prueba de penetración?

- **Definición:** Ataque simulado y autorizado para identificar y explotar vulnerabilidades.
 - **Objetivo:** Evaluar la **eficacia real** de las defensas informáticas imitando un ataque real.
 - **Diferencia con evaluación de vulnerabilidades:**
 - Evaluación: **Detecta** debilidades.
 - Pen Test: **Explota** debilidades para ver consecuencias.
-




Ejemplo práctico

- Una entidad financiera prueba su app bancaria simulando un ataque para descubrir:
 - Si se puede robar información.
 - Si es posible transferir dinero ilegalmente.
-

Cumplimiento normativo




- Obligatorias en empresas bajo regulaciones como:
 - **PCI DSS**
 - **HIPAA**
 - **GDPR**
-

Tipos de enfoques según los equipos

Tipo de equipo	Función principal
 Equipo Rojo	Simula ataques para detectar vulnerabilidades.
 Equipo Azul	Defiende y responde a incidentes.
 Equipo Púrpura	Colabora y mezcla tácticas del rojo y azul.

Los Pen Testers pueden ser internos o externos (freelance).

Estrategias de Pen Testing

Estrategia	También conocida como	Acceso del atacante simulado
 Caja blanca / abierta	Interna / de pleno conocimiento	Acceso completo al sistema.
 Caja negra / cerrada	Externa / conocimiento cero	Sin acceso ni información previa.
 Caja gris / conocimiento parcial	–	Acceso limitado (como un empleado).

 Las pruebas de **caja negra** son las más realistas.

¿Cómo convertirse en Pen Tester?

Habilidades clave:

- Seguridad de redes y aplicaciones.
- Sistemas operativos (Linux, principalmente).
- Modelado de amenazas y análisis de vulnerabilidades.
- Manejo de herramientas: escáneres, EDR, etc.
- Programación: **Python**, **Bash**.
- Comunicación técnica (informes claros).

Programas de Recompensas por Errores ("Bug Bounties")

- **Qué son:** Plataformas donde se paga a hackers éticos por encontrar fallos.
- **Ejemplo destacado:** [HackerOne](#)
- **Ventaja:** Aprendizaje práctico + recompensas económicas.

Puntos Clave Finales

- Las pruebas de penetración son una defensa **activa y ofensiva**.
- Simulan ataques reales para **validar la seguridad**.
- Son una carrera profesional en auge en el campo de la ciberseguridad.
- Cualquier estudiante motivado puede especializarse en esta disciplina con práctica y dedicación.