¿Qué es una prueba de penetración?

Antes de analizar los marcos y metodologías de pruebas de penetración más populares que puede utilizar para realizar una evaluación, definamos qué es una prueba de penetración.

Una prueba de penetración es un ciberataque simulado diseñado para identificar vulnerabilidades dentro de una red, sistema o aplicación informática que un atacante puede explotar para obtener acceso no autorizado. Su objetivo principal es proporcionar una evaluación integral que descubra vulnerabilidades y controles de seguridad mal configurados o faltantes que un hacker podría explotar en el mundo real.

Proporcionan al equipo azul información sobre las brechas de seguridad que deben priorizar y, a menudo, son requisitos de cumplimiento establecidos por los organismos reguladores.

Marcos y metodologías

Ahora que sabemos qué es un pentest, veamos los marcos y metodologías que utilizan los profesionales de seguridad para realizarlos.

Existen innumerables metodologías de pruebas de penetración. Sin embargo, muchas de ellas son muy similares y solo tienen diferencias sutiles. Estas diferencias surgen del tipo de prueba de penetración que se realiza. Por ejemplo, algunas metodologías se centran en probar aplicaciones web, mientras que otras están diseñadas para pruebas de penetración en redes. A continuación, se muestran algunos de los marcos y metodologías más populares que se utilizan comúnmente en la actualidad.

Proyecto de seguridad de aplicaciones web abiertas

El Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) es una organización sin fines de lucro que ofrece una **guía integral de pruebas para aplicaciones web** . Esta guía ofrece un enfoque sistemático para evaluar la seguridad de las aplicaciones web. Incluye listas de verificación, ejemplos para ayudar a los evaluadores y herramientas adicionales que mejoran la eficiencia de una prueba.

OWASP tiene otros proyectos destacados que puedes usar libremente. Entre ellos se incluyen:

- Proyecto OWASP Top Ten : una lista de los riesgos de seguridad de aplicaciones web más críticos. Puede aprender a utilizar este proyecto en Cómo utilizar el OWASP Top 10 para pruebas de penetración de aplicaciones web .
- OWASP ZAP (Zed Attack Proxy): un escáner de seguridad de aplicaciones web de código abierto.
- Modelo de madurez de garantía de software (SAMM) de OWASP: directrices y mejores prácticas para escribir código seguro.
- Seguridad de aplicaciones móviles OWASP : una guía de pruebas para aplicaciones móviles.
- OWASP Juice Shop : una aplicación web deliberadamente vulnerable para capacitación práctica en seguridad.

Estándar de ejecución de pruebas de penetración

El estándar de ejecución de pruebas de penetración (PTES) es un marco que proporciona un lenguaje y un alcance comunes para realizar pruebas de penetración. Fue desarrollado por profesionales de seguridad de la información de diversas industrias para establecer un enfoque estandarizado y garantizar la coherencia al realizar pruebas de penetración.

Incluye siete fases que lo guiarán a través del proceso de pentesting:

- **Interacciones previas al compromiso** : discutir el alcance, los objetivos y las reglas de la prueba de penetración.
- **Recopilación de información** : recopilación de inteligencia sobre el sistema u organización objetivo.
- **Modelado de amenazas** : análisis de la inteligencia recopilada para identificar amenazas y riesgos potenciales.
- **Análisis de vulnerabilidad** : evaluación del sistema de destino en busca de vulnerabilidades conocidas.
- **Explotación** : Explotación activa de las vulnerabilidades identificadas.

- **Post explotación** : mantener el acceso, aumentar los privilegios y explotar aún más el sistema o la red objetivo.
- **Informes** : documentar sus hallazgos en un informe para el cliente.

La norma también incluye directrices técnicas para acompañar estas fases, definiendo ciertos procedimientos a seguir durante una prueba de penetración.

Instituto Nacional de Normas y Tecnología Publicación Especial 800-115

La publicación especial 800-115 del Instituto Nacional de Normas y Tecnología (NIST) se describe mejor por su título "Guía técnica para la evaluación y prueba de la seguridad de la información". La publicación proporciona recomendaciones y mejores prácticas para planificar, ejecutar y documentar evaluaciones de seguridad. Hace mucho hincapié en los aspectos técnicos de la evaluación de los controles de seguridad y las vulnerabilidades.

Esta publicación incluye cuatro fases de alto nivel que deben guiar sus pruebas de penetración:

- **Plan** : Definir el alcance, los objetivos y las reglas del trabajo.
- **Descubrir** : Recopilar información y realizar actividades de reconocimiento para comprender el entorno objetivo.
- **Ataque** : Explotar activamente las vulnerabilidades identificadas para probar sistemas y aplicaciones.
- **Informe** : Documente sus hallazgos y comuníqueselos al cliente.

ATT&CK DE INGLETE

Las tácticas, técnicas y conocimientos comunes adversarios (ATT&CK) de MITRE son una base de conocimientos que cataloga las tácticas, técnicas y procedimientos (TTP) conocidos que utilizan los actores de amenazas del mundo real. Estos TTP están organizados en una matriz que modela las diferentes etapas

de un ciberataque. Esta matriz incluye dos componentes principales:

- **Tácticas** : Las fases de alto nivel del ciclo de vida del ataque desde el acceso inicial hasta el comando y control.
- **Técnicas** : Las acciones, métodos o procedimientos específicos que utiliza un adversario para lograr sus objetivos.

Los equipos rojos y los evaluadores de penetración utilizan MITRE ATT&CK para emular ataques del mundo real y evaluar la eficacia de los controles de seguridad de una organización.

MITRE tiene matrices ATT&CK específicas para sistemas de control empresariales, móviles e industriales (ICS).

CompTIA

CompTIA es un proveedor de capacitación en seguridad cibernética que ofrece una certificación de pruebas de penetración independiente del proveedor **Pentest+** . Esta certificación incluye una metodología para evaluar, identificar y probar vulnerabilidades en sistemas y redes.

La metodología consta de cinco objetivos clave:

- **Planificación y alcance** : comprender el alcance del proyecto, los objetivos, los requisitos legales y las reglas del pentest.
- **Recopilación de información y análisis de vulnerabilidades** : recopilación de información sobre la red, los sistemas y las aplicaciones de destino.
- **Ataques y exploits** : realización de ataques a redes, redes inalámbricas, aplicaciones e ingeniería social.
- **Informes y comunicación** : comunique eficazmente los resultados de su prueba de penetración a través de un informe completo.

CEH

El Consejo Internacional de Consultores de Comercio Electrónico (EC-Council) es otro proveedor de formación en seguridad cibernética que ofrece una certificación de pruebas de penetración neuronales de proveedores. Ofrecen el Certificado de Hacker Ético (CEH), que muestra un enfoque estructurado para realizar una prueba de penetración utilizando ocho etapas clave:

- **Permiso** : obtener la autorización adecuada y los permisos legales de un cliente para realizar su prueba de penetración.
- **Reconocimiento** : recopilación de información sobre el sistema u organización objetivo.
- **Escaneo y enumeración** : escaneo y enumeración activos de las redes, sistemas y aplicaciones de su objetivo en busca de posibles vulnerabilidades.
- **Obtener acceso** : explotar vulnerabilidades identificadas para obtener acceso al sistema objetivo.
- **Escalada de privilegios** : obtener mayor acceso o privilegios en el sistema de destino.
- **Mantener el acceso** : utilizar técnicas para establecer acceso persistente al sistema de destino.
- **Cubriendo pistas/Instalando puertas traseras** : eliminando evidencia de tus actividades en el sistema objetivo.
- **Informe** : documentar y comunicar sus hallazgos al cliente.

Los 8 pasos de las pruebas de penetración

Como puedes ver, estos frameworks y metodologías tienen varios componentes en común. Estas similitudes se pueden dividir en ocho pasos que debes realizar al ejecutar cualquier tipo de prueba de penetración. Veamos estos pasos en detalle.

Paso 1: Planificación y preparación

El primer paso es la fase de planificación y preparación. Aquí es donde debe trabajar con su cliente para definir el alcance de la prueba de penetración, los objetivos y metas clave de la

evaluación, un cronograma para la prueba y obtener los permisos legales necesarios para realizar la prueba.

Por lo general, analizará estos requisitos previos en su reunión inicial con el cliente y los ultimará firmando un contrato legal. No debe omitir este paso. Si no planifica adecuadamente su prueba de penetración o no obtiene los permisos adecuados, su prueba de penetración no tendrá éxito.

Paso 2: Reconocimiento

En este paso, recopilará información sobre la organización objetivo mediante técnicas de recopilación de información pasiva (reconocimiento pasivo). Esto implica recopilar información disponible públicamente sobre una organización y sus sistemas. Evita interactuar directamente con el objetivo y activar cualquier detección.

Esta información se suele denominar **inteligencia de fuentes abiertas (OSINT)** e incluye nombres de dominio, direcciones IP, hosts activos, tecnologías utilizadas, información de empleados, documentos internos y posibles vulnerabilidades. Esta información le permitirá saber cuál es el mejor enfoque para atacar al objetivo.

Un método poderoso para realizar OSINT es Google Dorking. Para aprender a dominar esto, lea **Cómo buscar en Google un sitio web específico para hackearlo .**

Herramientas de pruebas de penetración utilizadas durante la fase de reconocimiento:

- Maltego : una herramienta OSINT que representa visualmente la relación de los datos con los objetivos.
- Recon-ng : una herramienta modular capaz de recopilar datos OSINT de varias fuentes utilizando una colección de scripts.
- TheHarvester : una herramienta que puede descubrir subdominios, direcciones de correo electrónico, nombres de usuario y otra información pública relacionada con un objetivo a partir de datos OSINT.

Paso 3: Escaneo y enumeración

Con una lista de objetivos iniciales para atacar, puede comenzar a escanearlos en busca de vulnerabilidades. Esto se conoce como reconocimiento activo e implica interactuar directamente con los sistemas que está atacando mediante el envío de paquetes de red diseñados para obtener una respuesta del sistema objetivo.

Primero, realizará un escaneo de red, en el que escaneará la red del cliente para descubrir los hosts activos y ampliar su lista de objetivos. Luego, puede comenzar a enumerar estos objetivos para determinar qué puertos de red están abiertos y qué servicios están ejecutando estas máquinas. Al descubrir los servicios utilizados, puede identificar posibles vulnerabilidades o controles de seguridad faltantes que puede explotar.

Herramientas de pruebas de penetración utilizadas durante la fase de escaneo y enumeración:

- Nmap : una poderosa herramienta de mapeo de red que le permite descubrir puertos abiertos y servicios que se ejecutan en una máquina de destino.
- PowerView : un script de PowerShell que le permite enumerar entornos de Active Directory.

Paso 4: Evaluación de vulnerabilidad

Una lista de objetivos activos y los servicios que se ejecutan en ellos no necesariamente le indica si son vulnerables a un exploit específico. Para obtener esta información, debe realizar una evaluación de vulnerabilidades.

Esto implica el uso de un escáner de vulnerabilidades automatizado que realiza análisis intensivos en un sistema de destino para identificar vulnerabilidades conocidas en función de cómo responde ese sistema a los paquetes de red que envía. El escáner le proporcionará una lista de vulnerabilidades conocidas, que puede priorizar para probar en función de la gravedad de la vulnerabilidad y el impacto potencial.

Es importante tener en cuenta que un **análisis de vulnerabilidades** es muy ruidoso, ya que genera mucho tráfico en la red del cliente. Es probable que las soluciones de seguridad modernas detecten esta actividad y, si su prioridad es pasar

desapercibido, debe comprobar las vulnerabilidades de forma manual.

Para saber qué escáner de vulnerabilidad utilizar, eche un vistazo a **Los mejores escáneres de vulnerabilidad para Kali Linux .**

Herramientas de pruebas de penetración utilizadas durante la fase de evaluación de vulnerabilidad:

- Nessus : un escáner de vulnerabilidades que escanea más de 75 000 CVE (vulnerabilidades y exposiciones comunes) utilizando varias opciones de configuración y produce automáticamente un informe.
- Metasploit : un marco de pruebas de penetración todo en uno con módulos para recopilación de información, reconocimiento, escaneo, evaluación de vulnerabilidades, explotación y post-explotación.
- Greenbone Vulnerability Manager (anteriormente OpenVAS): una bifurcación de Nessus de código abierto diseñada para atacar objetivos o redes individuales.

Paso 5: Explotación

Una vez que haya identificado vulnerabilidades o controles de seguridad débiles, puede comenzar a intentar explotarlos para obtener acceso inicial a los sistemas de destino. Esto podría implicar explotar aplicaciones, dispositivos de red, sistemas operativos, personas, configuraciones incorrectas o cualquier otra tecnología que sea vulnerable a ataques.

Esta es la etapa que la mayoría de las personas asocian con el hackeo, ya que es la que se popularizó en películas y programas de televisión. Sin embargo, esta etapa no sería posible sin las cuatro etapas anteriores. La recopilación y enumeración de información son las más vitales para realizar este paso con éxito.

Herramientas de pruebas de penetración utilizadas durante la fase de explotación:

- sqlmap : una herramienta de prueba de penetración de código abierto que detecta y explota automáticamente vulnerabilidades de inyección SQL .

- John the Ripper : una herramienta para descifrar contraseñas que permite realizar varios ataques basados en contraseñas para descubrir las credenciales de los usuarios. Puede aprender a utilizar John en esta guía rápida y sencilla .
- Burp Suite : el kit de herramientas de prueba de penetración de aplicaciones web por excelencia para descubrir y explotar vulnerabilidades comunes en aplicaciones web.

Paso 6: Post-explotación

Una vez que haya explotado un sistema objetivo y haya obtenido acceso inicial, puede comenzar a realizar actividades posteriores a la explotación. Estas incluyen: recopilar información adicional sobre el sistema y la red interna, **aumentar sus privilegios** para tener un mayor control del sistema comprometido y configurar mecanismos de persistencia para mantener el acceso.

Estas actividades iniciales de postexplotación le permiten utilizar la máquina comprometida como punto de pivote para realizar movimientos laterales y comprometer otros sistemas en la red interna.

Esta etapa finaliza cuando se recopilan pruebas de que se han alcanzado los objetivos de la prueba de penetración, como acceder a un sistema sensible o robar cierta información. En este punto, se deben limpiar todos los archivos que se hayan dejado atrás, cambiar las configuraciones que se hayan modificado y eliminar todos los mecanismos de persistencia que se hayan instalado. Es necesario devolver los sistemas que se han visto comprometidos al estado en el que se encontraban.

Herramientas de pruebas de penetración utilizadas durante la fase de post-explotación:

- **BloodHound** : una herramienta que utiliza la teoría de grafos para revelar relaciones en un entorno de Active Directory que puedes explotar una vez que hayas obtenido acceso inicial.
- **Responder** : una herramienta proxy de interceptación que permite envenenar LLMNR, NBT-NS y MDNS para secuestrar

credenciales y hashes. Se utiliza ampliamente en ataques de transferencia de hash .

- Cinturón de seguridad : herramienta AC# que se puede utilizar para enumerar las vulnerabilidades del sistema ante ataques de escalada de privilegios.
- **Mimikatz** : una conocida herramienta de recolección de credenciales que puede extraer información confidencial de máquinas Windows, incluidos hashes de contraseñas y tickets Kerberos.

Paso 7: Informes

Una vez que se hayan completado las etapas técnicas de su prueba de penetración, deberá crear un informe que detalle todas las vulnerabilidades que descubrió, las explotaciones exitosas que realizó y todos los riesgos de seguridad potenciales que descubrió durante la prueba.

También es importante destacar el impacto de las vulnerabilidades que descubrió y cómo el cliente puede remediarlas o mitigarlas en el futuro. El objetivo de una prueba de penetración es proporcionar al cliente información útil sobre cómo proteger mejor su infraestructura de TI. Para ello, debe proporcionar recomendaciones claras y concisas que permitan al cliente mejorar su postura de seguridad.

Herramientas de pruebas de penetración utilizadas durante la fase de informes:

- Dradis : una plataforma de código abierto que se puede utilizar para generar y gestionar informes de pruebas de penetración.
- Faraday : una herramienta colaborativa de informes de pruebas de penetración que permite a los equipos compartir hallazgos y generar informes de pruebas de penetración utilizando plantillas personalizadas.

Paso 8: Remediación y seguimiento

La fase final de una prueba de penetración implica hacer un seguimiento con el cliente. Esto suele hacerse mediante una sesión informativa en la que el evaluador de penetración

analizará el resultado de la evaluación con el cliente y responderá a cualquier pregunta o inquietud.

Esta fase también puede incluir la colaboración con el cliente para desarrollar un plan para remediar las vulnerabilidades descubiertas o volver a probar los sistemas del cliente para verificar que las vulnerabilidades se hayan remediado eficazmente.

Conclusión

Las pruebas de penetración implican la realización de un ciberataque simulado para identificar vulnerabilidades y controles de seguridad débiles dentro de la infraestructura de TI de un cliente. Proporcionan a los clientes una evaluación integral de su postura de ciberseguridad y ofrecen recomendaciones para mejorarla.