**Engineer**

# Prueba de penetración

Ataque autorizado que muestra qué fallos se pueden explotar

## Qué es

Una prueba de penetración, a menudo abreviada como pentest, es una prueba de seguridad en la que se imitan ataques reales para encontrar formas de eludir las funciones de seguridad de una aplicación, un sistema o una red. La Guía técnica de pruebas y evaluación de la seguridad de la información del NIST, SP 800-115, señala que esto suele implicar lanzar ataques reales contra sistemas y datos reales, con las herramientas y técnicas de los atacantes. La definición más breve de SP 800-53 Rev. 5, el catálogo de controles de seguridad y privacidad del NIST, añade que los evaluadores suelen trabajar con restricciones concretas. Eso distingue una prueba de un ataque: está autorizada, delimitada y acordada por escrito antes de empezar.

Lo que la distingue de otras pruebas de seguridad es el objetivo. Un escáner de vulnerabilidades compara lo que observa con descripciones de fallos conocidos e informa de lo que podría haber. Quien realiza una prueba de penetración intenta aprovechar el fallo. SP 800-115 explica la diferencia con claridad: los escáneres solo comprueban la posible existencia de una vulnerabilidad, mientras que la fase de ataque de una prueba de penetración la explota para confirmar que existe. La mayoría de las pruebas también buscan combinaciones: debilidades de uno o varios sistemas que, juntas, dan más acceso que cada una por separado.

La Guía de pruebas de seguridad web de OWASP (WSTG) señala que la técnica también se conoce como pruebas de caja negra y hacking ético. El equipo prueba desde fuera, sin conocimiento previo del diseño interno del objetivo, y actúa como un atacante, aunque a menudo recibe una o más cuentas de usuario válidas.

Dos decisiones dan forma a cada prueba. La primera es el punto de partida. Una prueba externa empieza fuera de la red con poco más que las direcciones incluidas en el alcance; una interna empieza dentro, normalmente con el acceso de un empleado corriente, e intenta avanzar mediante una escalada de privilegios. La segunda es quién lo sabe. SP 800-115 llama a las pruebas abiertas pruebas de sombrero blanco: se realizan con el conocimiento y consentimiento del personal de TI. Las encubiertas, o pruebas de sombrero negro, se hacen sin que lo sepa el personal de TI, pero con pleno conocimiento y permiso de la alta dirección.

SP 800-115 divide el trabajo en cuatro fases y añade en una nota al pie que esta es una de muchas formas aceptables de agruparlo. En la planificación se acuerdan las reglas, se documenta la aprobación de la dirección y se fijan los objetivos; la prueba propiamente dicha empieza en el descubrimiento. Esta fase reúne información sobre el objetivo, lo escanea y coteja los resultados con bases de datos de vulnerabilidades, como la National Vulnerability Database de Estados Unidos, y con los conocimientos del equipo. La fase de ataque, que la guía llama «el núcleo de toda prueba de penetración», intenta explotar cada posible fallo. Si una explotación abre un acceso nuevo, el equipo vuelve al descubrimiento desde esa nueva posición. La elaboración de informes acompaña a las tres fases y termina con un informe que enumera las vulnerabilidades encontradas, valora su riesgo y explica cómo corregirlas. Otros métodos dividen el mismo trabajo de otra forma: el Penetration Testing Execution Standard (PTES), que la WSTG incluye entre sus metodologías de referencia, utiliza siete fases, desde las interacciones previas al encargo hasta la elaboración de informes.

Utilice el concepto en una decisión

Aplique «¿Qué es una prueba de penetración?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

**Explore nuestros servicios** Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

**1.000 reglas RBAC para servidores Linux** Póngase en contacto →

## Por qué importa

El informe de un escáner es una lista de posibilidades. Algunas no se pueden explotar en su entorno, y un escáner no puede detectar un fallo que nadie ha descrito ni uno que solo aparece al combinar dos debilidades aparentemente

inofensivas. Una prueba de penetración responde a otra pregunta: ¿qué podría hacer realmente un atacante aquí y hasta dónde llegaría? SP 800-115 añade qué más puede mostrar: la resistencia de un sistema a patrones de ataque reales, qué habilidad necesitaría el atacante, qué contramedidas adicionales ayudarían y si los defensores detectan el ataque y responden.

Por eso sus hallazgos tienen peso para quienes nunca leen la salida de un escáner. Un hallazgo que afirma que alguien externo y sin cuenta leyó la tabla de clientes es una prueba, no una probabilidad. SP 800-115 describe las pruebas de penetración como un proceso iterativo que parte de un acceso mínimo para obtener otro mayor. Un buen informe muestra esa cadena paso a paso, de modo que la corrección pueda romperla por el eslabón menos costoso.

Ese mismo realismo las hace costosas y arriesgadas. El NIST señala que requieren mucho trabajo, afirma que exigen gran experiencia y advierte de que los sistemas pueden sufrir daños o quedar inoperativos durante la prueba. Un equipo experimentado reduce ese riesgo, pero nunca puede eliminarlo por completo. Muchas acciones de quienes prueban, como atacar sistemas para comprometerlos, son actividades que las políticas de la propia organización suelen prohibir. Para eso existen las reglas de actuación (ROE): un documento acordado antes de empezar que autoriza al equipo a realizar actividades definidas y nada más.

También es una técnica entre varias, no un veredicto por sí sola. La WSTG observa que muchos equipos hacen de las pruebas de penetración su principal medio para comprobar la seguridad de una aplicación web, y sostiene que no deberían ser ni el control principal ni el único. Las aplicaciones web casi siempre son desarrollos a medida, así que probarlas desde fuera se parece más a investigar que a encontrar fallos conocidos en productos estándar. Además, la prueba llega tarde en el ciclo de desarrollo, cuando el diseño y el código ya están definidos. Si el equipo dispone de la aplicación terminada, pero no de su código fuente, añade la guía, una prueba de penetración sigue siendo claramente mejor que dejarla sin probar.

La frecuencia depende del coste. SP 800-115 sugiere que, dado su elevado coste y posible impacto, puede bastar con probar una vez al año la red y los sistemas de una organización, con escaneos periódicos más ligeros entre pruebas. Algunas normas también lo piden expresamente: la WSTG señala que PCI DSS, el estándar de seguridad de datos del sector de tarjetas de pago, establece su propio requisito de pruebas de penetración, tanto externas como internas.

# Cómo se aplica en la práctica

La mayor parte de una prueba de penetración se decide antes de enviar la primera solicitud. El apéndice B de SP 800-115 ofrece una plantilla de reglas de actuación, con secciones sobre objetivo y alcance, participantes y calendario, comunicación entre las partes y condiciones de interrupción, sistemas incluidos y excluidos, actividades permitidas y prohibidas, tratamiento de los datos de prueba, presentación de resultados y una página de firmas. Una versión reducida para una prueba externa de una tienda web podría ser la siguiente. Se escribió para este artículo, y los nombres y direcciones proceden de los rangos reservados para documentación.

```
REGLAS DE ACTUACIÓN: prueba externa de shop.example.com

Objetivo          Encontrar qué fallos puede explotar alguien externo y hasta
                  dónde permite llegar cada uno.
Objetivos         203.0.113.10 a 203.0.113.20, titularidad comprobada en WHOIS
Exclusiones       203.0.113.15 (proveedor de pagos, sin autorización para
                  probarlo). Todos los servicios de terceros que llama la
                  tienda
Cuentas           Dos cuentas de cliente y una cuenta de soporte
Calendario        3 a 14 de noviembre, 19:00 a 06:00 CET, fuera de las horas de
                  mayor actividad comercial
IP del equipo     Solo 198.51.100.7 y 198.51.100.8
Permitido         Explotar un fallo confirmado para demostrar su impacto; leer
                  datos de las cuentas de prueba; subir un archivo de prueba
                  marcado como tal, que se retira al final
Prohibido         Denegación de servicio; modificar o borrar datos de clientes;
                  ingeniería social; entrada física
Interrumpir       Caída de la tienda en producción, datos de clientes reales
                  visibles o indicios de un intruso real: detenerse y llamar
                  por teléfono al responsable de seguridad
Reanudar          Solo con autorización escrita del responsable de seguridad
Datos de prueba   Sensibles; guardados en los portátiles del equipo de pruebas,
                  eliminados 30 días después del informe final
Informes          Nota diaria de estado; informe final en un plazo de diez días
                  laborables
Firmas            Responsable del equipo de pruebas; responsable máximo de
                  seguridad de la información
```

Cada línea responde a una cuestión planteada en SP 800-115. La guía indica que, antes de empezar, hay que verificar que todas las direcciones públicas de la lista de objetivos pertenecen a la organización y remite para ello a los datos de registro de WHOIS. Sugiere probar un sitio en funcionamiento por la tarde o noche, en vez de en las horas de mayor actividad comercial. Pide las direcciones desde las que trabaja el equipo para que los administradores distingan el tráfico

de prueba de un ataque real. Llama lista de exclusión al listado de sistemas que no se pueden tocar e indica que las reglas deberían incluir criterios para interrumpir la prueba y un proceso para reanudarla. También pregunta qué ocurre si se descubre un intruso real: ¿debe detenerse la prueba y cuándo puede volver a empezar, con autorización de quién? Como mínimo, firman el responsable del equipo de pruebas y la alta dirección, declarando que entienden el alcance y sus límites.

Con estas reglas, la fase de ataque sigue el patrón de inyección SQL que describe la WSTG. Un escaneo de la página de búsqueda de la tienda identifica indicios de un posible fallo. La primera prueba es un error de base de datos al escribir una comilla simple en el campo. Después se envía una entrada preparada que cambia la gramática de la consulta, y solo se confirma el fallo cuando esta devuelve datos que no debería. Si esos datos incluyeran la sesión de la cuenta de soporte, quien realiza la prueba iniciaría sesión como soporte y volvería a investigar desde ahí. El informe mostraría todo el recorrido: un campo sin filtrar, una sesión filtrada y una vista de soporte con acceso a todos los pedidos.

Una prueba así acompaña a otros controles, no los sustituye. La descripción de un programa de escaneo de seguridad continuo, correspondiente al trabajo de la fundadora en NextMariner, detalla el análisis estático, las pruebas dinámicas contra una instancia en funcionamiento y las comprobaciones de dependencias que se ejecutan automáticamente, junto con auditorías de seguridad escritas que incluyen un modelo de amenazas y una evaluación frente a la guía de pruebas de OWASP. La página explica el motivo de combinar ambos: los escáneres encuentran clases de problemas que alguien ya ha descrito, mientras que en el modelo de amenazas se identifican los específicos de una plataforma.

## Dónde surgen los problemas

**Probar sin autorización escrita.** Un «adelante» verbal de un responsable de equipo no cubre los ataques que prohíben las políticas de la empresa ni protege a quienes prueban ni a quienes solicitaron la prueba. Escriba primero las reglas de actuación y haga que las firmen el responsable del equipo de pruebas y la alta dirección antes de enviar tráfico alguno.

**Probar direcciones que no le pertenecen.** Una lista de objetivos copiada de un diagrama antiguo puede incluir direcciones que ahora pertenecen a otros, y las plataformas compartidas sitúan a otros clientes junto al suyo. Compruebe que

todas las direcciones públicas incluidas pertenecen a la organización, como pide SP 800-115, e incluya por su nombre cada servicio de terceros en la lista de exclusión.

**Vender un escaneo como una prueba de penetración.** Un informe de escáner con una portada nueva enumera posibilidades, no pruebas. Pida pruebas de explotación de cada hallazgo: qué se hizo, qué acceso permitió y cuál habría sido el siguiente paso.

**Convertirla en la única prueba de seguridad.** Una sola prueba observa una muestra de los riesgos, en un momento y desde fuera. La WSTG sitúa el modelado de amenazas en el diseño, la revisión de código y el análisis del código fuente durante el desarrollo, y las pruebas de penetración en la fase de pruebas posterior. Realícelos todos y utilice la prueba de penetración para confirmar lo que los controles anteriores no pudieron.

**Empezar sin reglas para detenerse.** Si el equipo interrumpe un servicio en producción o encuentra indicios de un intruso real, y nadie ha acordado quién detiene y quién reanuda la prueba, se improvisa bajo presión. Incluya criterios de interrupción, una cadena de llamadas y un proceso de reanudación en las reglas de actuación.

**Tratar los resultados como datos corrientes.** El informe de una prueba de penetración es un mapa de lo que un adversario podría explotar, y SP 800-115 indica que los resultados deberían tratarse como información sensible. Acuerde cómo se recopilan, envían, guardan y destruyen los hallazgos antes de empezar, y limite quién recibe el informe completo.

**Cerrar hallazgos sin repetir la prueba.** Una corrección puede ser parcial o aplicarse en un lugar distinto del fallo. La WSTG llama pruebas de penetración focalizadas a las que intentan explotar vulnerabilidades encontradas en revisiones anteriores y señala que muestran si los fallos concretos están realmente corregidos en el código desplegado. Repita la explotación original contra cada corrección antes de cerrar el hallazgo.

**Esperar que una prueba encubierta lo encuentre todo.** Según SP 800-115, las pruebas encubiertas examinan el daño que podría causar un adversario; no prueban todos los controles ni encuentran cada vulnerabilidad y suelen entrar

por las debilidades más básicas. Elija una prueba abierta cuando busque cobertura y una encubierta cuando quiera saber si los defensores se dan cuenta.

## Lecturas adicionales

- NIST SP 800-115: Guía técnica de pruebas y evaluación de la seguridad de la información — la guía del NIST para planificar y realizar pruebas de seguridad, con las cuatro fases de una prueba de penetración y una plantilla de reglas de actuación.
- Guía de pruebas de seguridad web de OWASP v4.2: introducción — cómo encajan las pruebas de penetración con la revisión y el análisis del código fuente, y por qué no deberían ser la única técnica.
- OWASP WSTG v4.2: metodologías de pruebas de penetración — una breve descripción de PTES, las orientaciones de PCI DSS, PTF, NIST SP 800-115 y OSSTMM.
- NIST SP 800-53 Rev. 5: Controles de seguridad y privacidad para sistemas de información y organizaciones — el catálogo de controles de seguridad y privacidad del NIST, cuyo control CA-8 trata las pruebas de penetración y sus reglas de actuación.



Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

**Vea cuánto cuesta** Póngase en contacto →

# Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es una prueba de penetración?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

**Explore nuestros servicios**

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/penetration-test/