Introduction

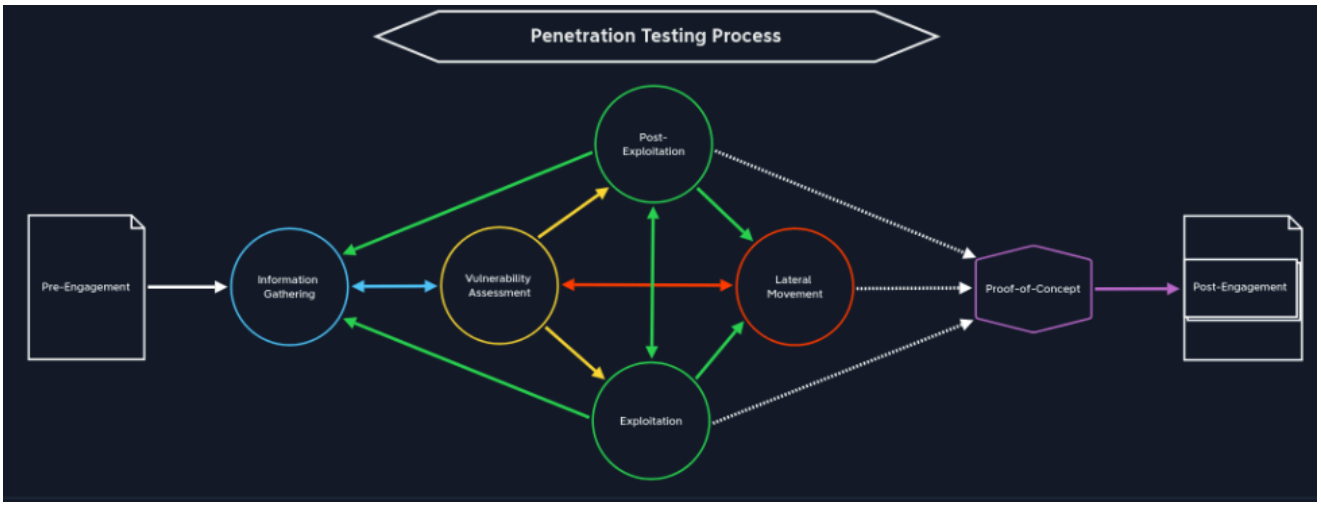
Las pruebas de penetración (pentesting), o hacking ético, consisten en imitar legalmente ciberataques para detectar vulnerabilidades de seguridad en el entorno digital de una empresa. No se trata solo de encontrar debilidades, sino de comprobar la eficacia de las medidas de seguridad actuales, ayudando a las empresas a solucionar problemas antes de que los cibercriminales se aprovechen de ellas.

Definition

Una prueba de penetración es un tipo único de evaluación de seguridad que va más allá del escaneo automatizado y la identificación de vulnerabilidades. Implica intentar explotar las vulnerabilidades descubiertas y obtener acceso no autorizado, elevar privilegios o extraer datos confidenciales. Este enfoque permite a las organizaciones comprender no solo las vulnerabilidades existentes en su infraestructura, sino también cómo podrían aprovecharse y reforzarse en un escenario de ataque real, y cuál sería el impacto.

Las pruebas de penetración abarcan una amplia gama de tareas, entre las que se incluyen:

- **Reconocimiento**: donde los evaluadores recopilan información sobre la organización, el sistema o la red objetivo, como si estuvieran inspeccionando un edificio antes de planificar un asalto.
- **Evaluación de vulnerabilidad**: Utilizan herramientas para detectar puntos débiles, de forma similar a comprobar si hay ventanas o puertas desbloqueadas.
- **Explotación**: Los evaluadores intentan explotar esas debilidades para obtener acceso o control sobre el sistema, de igual manera que un ladrón podría probar esas puertas desbloqueadas.
- **Post-explotación**: Exploran a qué más se puede acceder, mantienen el control y evalúan el impacto de un ataque exitoso, como ver qué tan lejos podría llegar un intruso dentro de un edificio.
- **Informes**: documenta todo, las vulnerabilidades encontradas, los riesgos que plantean y los pasos claros para solucionarlos, de modo que el sistema pueda ser protegido.



Goals of Penetration Testing

1. Identificación de debilidades de seguridad
2. Validación de controles de seguridad
3. Prueba de las capacidades de detección y respuesta
4. Evaluación del impacto en el mundo real
5. Priorizar los esfuerzos de remediación
6. Cumplimiento y diligencia debida
7. Mejorar la conciencia de seguridad
8. Verificación de la gestión de parches
9. Probando nuevas tecnologías
10. Proporcionar una base para las mejoras de seguridad

Types of Penetration Tests

Uno de los métodos de clasificación más frecuentes se basa en la cantidad y el tipo de información proporcionada al evaluador; comúnmente conocido como prueba de caja negra (Black Box), caja blanca (White Box) o caja gris (Grey Box).

Black Box Testing

El equipo comenzó con una prueba de caja negra, simulando un atacante externo **sin conocimiento previo** de los sistemas del banco.

White Box Testing

A continuación, el equipo realizó una prueba de caja blanca con **acceso completo** a la arquitectura de red, el código fuente y las configuraciones del sistema del banco.

Gray Box Testing

Finalmente, se realizó una prueba de caja gris, simulando un escenario en el que un atacante había obtenido **acceso interno limitado**.

Areas and Domains of Testing

Además de estos tres tipos fundamentales de pruebas (caja negra, caja gris y caja blanca), las pruebas de penetración también pueden clasificarse según el entorno o dominio objetivo específico que se evalúa. Este enfoque específico para cada entorno permite una evaluación más enfocada y especializada, donde la prueba de penetración se centra específicamente en abordar los desafíos de seguridad y las vulnerabilidades únicas asociadas con un ecosistema tecnológico o componente de infraestructura en particular.

- Network Infrastructure (Infraestructuras de red)
- Web Applications (Aplicaciones web)
- Mobile Applications (Aplicaciones móviles)
- Cloud Infrastructure (Infraestructuras cloud)
- Physical Security (Seguridad física)
- Wireless Security (Seguridad inalámbrica)
- Software Security (Seguridad de software)

Penetration Test Benefits

- Mejora de la seguridad general
- Cumplimiento normativo y gestión de riesgos
- Mejora de la continuidad del negocio y protección de la reputación
- Validación de los controles de seguridad

Compliance and Penetration Testing

Unión Europea

El **RGPD** exige la realización de pruebas periódicas de las medidas de seguridad, que suelen incluir pruebas de penetración para garantizar el cumplimiento de la protección de datos.

La Directiva **NIS** implica la necesidad de realizar pruebas de penetración para gestionar eficazmente los riesgos de seguridad.

Penetration Testing vs. Vulnerability Assessment

Mientras que las evaluaciones de vulnerabilidades ofrecen una amplia cobertura mediante el análisis y la identificación de problemas de seguridad conocidos, las pruebas de penetración realizan investigaciones específicas y exhaustivas intentando explotar activamente las vulnerabilidades descubiertas o potenciales. Esta diferencia fundamental en el enfoque proporciona información distinta pero complementaria.

Structure of a Penetration Test

1. Pre-Engagement Phase

Es crucial, ya que sienta las bases para toda la prueba de penetración. Durante esta fase, los evaluadores de penetración trabajan en estrecha colaboración con el cliente para comprender sus necesidades, inquietudes y objetivos específicos. Esto incluye definir el alcance de la prueba, establecer plazos y determinar qué sistemas y redes se probarán, normalmente te hacen firmar un **NDA** para que todo quede de forma confidencial.

2. Information Gathering Phase

En esta fase tenemos tanto el reconocimiento de forma activa como pasiva.

- **El reconocimiento pasivo** implica recopilar información sin interactuar directamente con los sistemas objetivo. Esto puede incluir el análisis de registros públicos, la búsqueda en redes sociales, la revisión de sitios web de empresas y el uso de herramientas OSINT (Inteligencia de Fuentes Abiertas). Este enfoque no deja rastro ni supone ningún riesgo para la infraestructura objetivo.
- **El reconocimiento activo**, por otro lado, implica la interacción directa con los sistemas objetivo. Esto incluye actividades como el escaneo de puertos, la enumeración de servicios y la captura de banners. Si bien es más intrusivo, proporciona información técnica detallada sobre el entorno objetivo.

3. Vulnerability Assessment Phase

Durante la fase de evaluación de vulnerabilidades, los evaluadores de penetración analizan la información recopilada para identificar posibles debilidades de seguridad. Esto implica el uso de diversas herramientas de análisis automatizado y técnicas de prueba manuales para descubrir vulnerabilidades en sistemas, aplicaciones e infraestructura de red.

4. Exploitation Phase

La fase de explotación es donde los evaluadores de penetración intentan explotar activamente las vulnerabilidades identificadas en la fase anterior. Esto se hace para demostrar el impacto real de las debilidades de seguridad y determinar lo que un atacante real podría lograr.

5. Post-Exploitation Phase

Una vez obtenido el acceso inicial, comienza la fase de postexplotación. Esta fase incluye actividades como la escalada de privilegios, el movimiento lateral a través de la red, las pruebas de exfiltración de datos y el mantenimiento de la persistencia. El objetivo es comprender el alcance total de lo que un atacante podría lograr tras vulnerar las defensas iniciales.

6. Lateral Movement Phase

Durante el movimiento lateral, los evaluadores emplean diversas técnicas, como la recolección de credenciales, ataques de pass-the-hash y la explotación de protocolos de red para moverse entre sistemas. Esta fase ayuda a demostrar cómo un atacante podría propagarse a través de la infraestructura de red de la organización y acceder a recursos confidenciales.

7. Proof of Concept

La fase de prueba de concepto implica la creación de documentación detallada y evidencia que demuestre cómo se explotaron las vulnerabilidades. Esto incluye el desarrollo de métodos fiables y repetibles para reproducir los problemas de seguridad identificados, lo que ayuda a validar los hallazgos y al equipo técnico del cliente a comprender y corregir las vulnerabilidades.

8. Post-Engagement Phase

La fase de elaboración de informes es crucial, ya que transforma los hallazgos técnicos en información práctica para el cliente. Un informe de pruebas de penetración bien redactado suele incluir un resumen ejecutivo para la gerencia, hallazgos técnicos detallados para el equipo de TI y recomendaciones claras para la remediación.

9. Remediation Support and Retesting

Tras la entrega del informe, muchas pruebas de penetración incluyen un periodo de soporte para la remediación. Durante este periodo, los evaluadores están disponibles

para responder preguntas sobre sus hallazgos y brindar orientación adicional sobre la implementación de correcciones.

Prerequisites for a Penetration Test

- Autorización legal y documentación
- Definición y límites del alcance
- Recopilación de información
- Canales de comunicación y procedimientos de emergencia
- Preparación del entorno de prueba
- Consideraciones sobre copias de seguridad y recuperación
- Documentación e informes
- Responsabilidad profesional y seguros
- Confidencialidad y manejo de datos

Required Skills

1. En primer lugar, los entornos de TI modernos son increíblemente complejos y combinan diversas tecnologías, sistemas y arquitecturas. Aunque algunos afirman que los evaluadores de penetración deben comprender todos estos componentes y sus interacciones para identificar vulnerabilidades eficazmente, esto no es realista. Lo importante, en cambio, es la capacidad de aprender rápidamente comprendiendo cómo estos elementos interactúan. Este enfoque requiere conocimientos fundamentales que abarcan redes, sistemas operativos, tecnologías web y más.
2. En segundo lugar, una prueba de penetración exitosa implica más que solo habilidades técnicas. Los evaluadores deben ser capaces de pensar de forma creativa y original, similar a un atacante, manteniendo al mismo tiempo los límites éticos. También deben ser capaces de comunicar sus hallazgos a las partes interesadas, tanto técnicas como no técnicas, y gestionar proyectos con profesionalidad. Esta combinación de experiencia técnica y habilidades interpersonales es esencial para ofrecer valor a los clientes.
3. En tercer lugar, el panorama de la ciberseguridad está en constante evolución. Surgen nuevas tecnologías, se descubren nuevas vulnerabilidades casi a diario y los métodos de ataque se vuelven más sofisticados. Esto exige que los evaluadores de penetración sean aprendices permanentes capaces de adaptarse y ampliar sus habilidades continuamente.
4. Finalmente, las pruebas de penetración suelen implicar situaciones de alto riesgo donde los errores podrían dañar sistemas críticos o exponer datos confidenciales. El amplio conjunto de habilidades requeridas garantiza que los evaluadores

puedan trabajar de forma competente y segura, a la vez que proporcionan información de seguridad significativa a sus clientes.

Methodologies & Frameworks

La metodología más reconocida en el campo de las pruebas de penetración es el Estándar de Ejecución de Pruebas de Penetración (**PTES**). PTES proporciona un marco que divide el proceso de pruebas de penetración en siete fases distintas: interacciones previas a la interacción, recopilación de inteligencia, modelado de amenazas, análisis de vulnerabilidades, explotación, postexplotación y generación de informes.

La Guía Técnica para las Pruebas y la Evaluación de la Seguridad de la Información (**NIST**) representa un enfoque más formal. Si bien no se trata estrictamente de una metodología de pruebas de penetración, proporciona una valiosa orientación sobre la planificación, la ejecución y las actividades posteriores a las pruebas de seguridad. Este marco es especialmente relevante al trabajar con agencias u organizaciones gubernamentales que siguen las directrices del NIST.

La Guía de Pruebas del Proyecto Abierto de Seguridad de Aplicaciones Web (**OWASP**) es otra metodología ampliamente adoptada que ofrece orientación para las pruebas de seguridad de aplicaciones web. Ofrece un enfoque estructurado en cuatro fases principales: Recopilación de Información, Pruebas de Gestión de Configuración e Implementación, Pruebas de Gestión de Identidad y Pruebas de Autenticación.

El marco de trabajo **MITRE ATT&CK** ha cobrado cada vez mayor importancia en las pruebas de penetración modernas. A diferencia de las metodologías tradicionales, ATT&CK proporciona una base de conocimiento completa sobre las tácticas y técnicas de los adversarios observadas en ataques reales. Los pentesters utilizan este marco para simular escenarios de amenazas realistas y garantizar que sus pruebas cubran todo el espectro de posibles vectores de ataque.