

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

PAI-5. RedTeamPro: Evaluación de la seguridad de la información mediante pruebas de seguridad de una organización pública

Introducción

INSEGUS ha sido contratada para llevar a cabo una evaluación de la seguridad de la información de una determinada organización pública como **Red Team**. El **Red Team** es **un equipo que lleva a cabo simulación de ataques debidamente autorizados usando las tácticas, técnicas y procedimientos (TTP) de los ataques cibernéticos reales**. **MITRE ATT&CK** es una base de datos pública y un marco de referencia que describe las TTP utilizados por adversarios cibernéticos para **poner a prueba** la seguridad de los sistemas de una organización determinada. Por supuesto, para que estas actividades queden dentro de la legalidad vigente **deberían obtenerse las pertinentes autorizaciones por parte de la organización objeto de evaluación**.

El objetivo principal del **Red Team** es **identificar vulnerabilidades y explotaras** de manera realista, tal como lo haría un atacante malicioso. Siguiendo las recomendaciones de NIST 800-115, se pueden utilizar tres tipos de métodos de evaluación: *pruebas, exámenes y entrevistas*. Una **prueba** es el proceso de evaluar uno o más objetivos de evaluación en condiciones específicas para comparar el comportamiento real y el esperado bajo condiciones específicas para comparar el comportamiento real con el esperado.

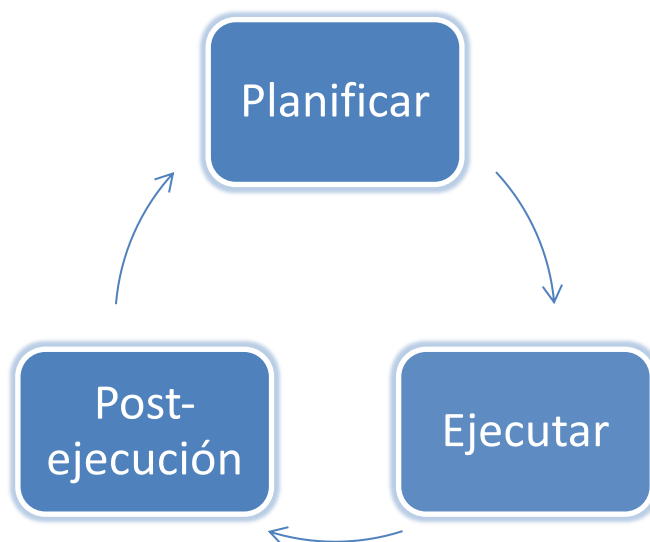


Figura 1: Metodología para la evaluación de la seguridad de la información (NIST 800-115)

En primer lugar, se deberá planificar la evaluación de la seguridad de la información, **esta fase es fundamental para el éxito de la evaluación, en ella se debe recopilar información sobre los activos a evaluar, las amenazas, y los controles de seguridad**. En una segunda fase, se ejecutarán las pruebas de seguridad. Por último, en una fase postejecución se analizan los resultados de las pruebas y se elabora un informe con las conclusiones y recomendaciones



SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

El estándar **NIST 800-115** nos indica que existen diferentes tipos de técnicas para la evaluación requerida:

1. **Técnicas de revisión que permiten un análisis pasivo** de sistemas, aplicaciones, políticas y procedimientos:
 - Revisión de documentación: Para asegurar que las políticas y procedimientos estén actualizados.
 - Revisión de registros (logs): Para detectar actividades inusuales.
 - Revisión de configuraciones del sistema: Para verificar que los sistemas estén configurados de forma segura.
2. **Identificación activos y técnicas de análisis que implican un estudio más profundo** de los sistemas y aplicaciones:
 - Análisis de código fuente: Para identificar vulnerabilidades en el código de las aplicaciones.
 - Análisis de protocolos: Para examinar la comunicación de red en busca de debilidades.
 - Análisis de vulnerabilidades: para identificar debilidades en los sistemas.
3. **Técnicas validación que implican interacciones activas con los sistemas para evaluar su seguridad:**
 - Escaneo de vulnerabilidades: uso de herramientas automatizadas para la detección de vulnerabilidades.
 - Pruebas de aplicaciones web: evaluación de la seguridad de las aplicaciones web en busca de vulnerabilidades como inyecciones SQL, XSS, etc.
 - **Pruebas de penetración (penetration testing):** Para simular ataques reales y evaluar la resistencia de los sistemas.

Los escenarios de las pruebas de penetración deben centrarse en localizar y atacar defectos explotables en el diseño e implementación de una aplicación, sistema o red. **Las pruebas deben reproducir tanto los patrones de ataque más probables y reales** como los más comprometedores, incluidos los peores escenarios, como las acciones maliciosas de los administradores. Dado que un escenario de prueba de penetración puede diseñarse para simular un ataque interno, un ataque externo o ambos, se consideran métodos de prueba de seguridad externos e internos. Si se van a realizar pruebas tanto internas como externas, normalmente se realizan primero las pruebas externas.

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

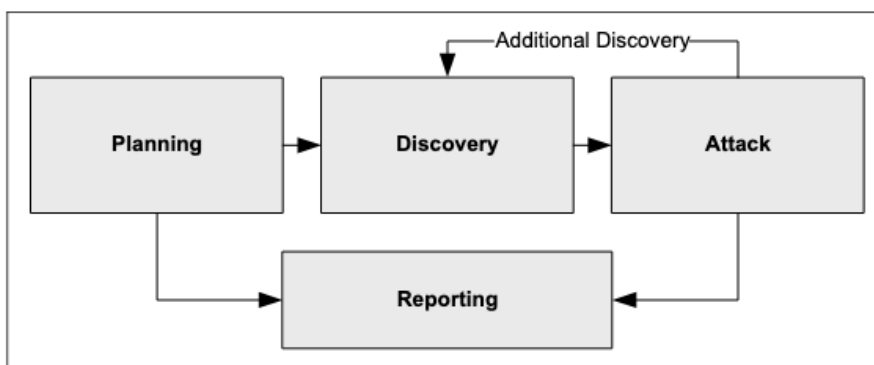


Figura 2: Fases de un penetration testing según NIST 800-115

La prueba de penetración tiene el propósito de generar un informe técnico en el que se ponga de manifiesto la identificación del riesgo, la probabilidad de su ocurrencia, el impacto en la organización y la estimación de su severidad, así como las correspondientes recomendaciones de mitigación de dichos riesgos.

Tipos de pruebas de penetración según el enfoque:

1. **Blackbox:** no se conoce información acerca del sistema objetivo, deberemos de actuar como cualquier ente externo que quiera realizar una penetración en nuestros sistemas de información.
2. **Whitebox:** se posee un conocimiento acerca del sistema objetivo, podremos actuar con conocimiento implícito del sistema que queremos penetrar.

Podríamos definir las fases de una prueba de penetración de la siguiente manera:

1. **Recolección de información (Fingerprinting/Footprinting).** Obtención de información del sistema objetivo, para determinar:
 - a. Servicios activos
 - b. Puertos abiertos
 - c. Mapeo de red
 - d. Sistema operativo

Se suelen usar herramientas como *Nmap*, *Recon-ng*, *Shodan*, *ZoomEye*, *Google Dorks* (<https://www.exploit-db.com/google-hacking-database>), *Maltego*, etc.

2. **Exploración de vulnerabilidades (Vulnerability Scanning):** Test para la identificación y detección de vulnerabilidades, se suelen usar herramientas como, por ejemplo, *Nessus*, *OpenVAS*, *Nikto*, *Qualys*, etc.

Catálogo de herramientas para vulnerability scanning: https://owasp.org/www-community/Vulnerability_Scanning_Tools

3. **Explotación:** Se obtiene el acceso no autorizado a los recursos y/o servicios identificados en el sistema objetivo, se suelen usar herramientas como, por ejemplo *Metasploit*, *SearchSploit*, *Empire*, *Social Engineering Toolkit (SET)*, etc.

Base de datos de exploits: <https://www.exploit-db.com/>
<https://www.rapid7.com/db/>

4. **Escalada de Privilegios:** Con el objetivo de controlar el sistema comprometido. Se suelen usar herramientas como *LinPEAS*/*WinPEAS* para sistemas *Linux* y *Windows*

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

respectivamente, Mimikatz: Herramienta para obtener contraseñas en Windows de la memoria RAM del sistema, etc.

5. **Post-explotación (Post-Exploitation)** Una vez que se ha obtenido acceso al sistema, los pentesters tienen como objetivo mantener el acceso y recopilar toda la información sensible posible, e incluso desplegar un **Command-and-Control**. *Se suelen usar herramientas como Netcat, Empire, PowerSploit, etc.*
6. **Generación de informes técnicos:** Es la parte más importante porque se le indica al usuario qué acciones se han realizado para llevar a cabo el acceso no autorizado y las pruebas. *Las herramientas que se suelen usar son Dradis o Faraday.*

Generación de informe

El informe final o informe técnico es de lo más importante dentro de la evaluación de la seguridad de la información ya que en dicho informe se indica a los clientes las acciones y pruebas que se han realizado, así como se deben incluir información relativa a las técnicas, herramientas, versiones, vulnerabilidades descubiertas etc. y el nivel de gravedad que supone para la organización. Así como las recomendaciones sobre medidas correctoras para mitigar los riesgos de seguridad encontrados.

Aspectos importantes para tener en cuenta a la hora de escribir el informe y de describir las pruebas:

1. Detallar el Plan establecido por el Security para llevar a cabo la Evaluación de la Seguridad de la información de un sistema de la organización pública.
2. Metodología usada, herramientas y TTPs: describir con detalle la metodología usada, así como las tácticas, técnicas y procedimientos usados al detalle, además de las herramientas usadas (marca, producto, versión, etc.). Cualquier resquicio en el procedimiento, las técnicas o tácticas, así como de las herramientas usadas puede usarse para invalidar las pruebas realizadas.
3. Hallazgos y Vulnerabilidades: describir las vulnerabilidades descubiertas y sus características principales (CVE, CVSS, CWE, etc.); describir los componentes afectados (servicios, aplicaciones, configuraciones, etc.); impacto de la vulnerabilidad en el componente; prueba de concepto (incluir alguna evidencia visual de muestra el resultado de dicha vulnerabilidad, por ejemplo, escalado de privilegios); descripción de pasos para reproducir la explotación; sugerencia de mitigación y correcciones.
4. Anexo: Incluir cualquier otro recurso adicional que aporte información respecto a la evaluación de la seguridad de la información realizada.

Los resultados de las pruebas de seguridad pueden utilizarse de las siguientes maneras:

- Como punto de referencia para la adopción de medidas correctivas
- En la definición de las actividades de mitigación para hacer frente a las vulnerabilidades identificadas
- Como punto de referencia para el seguimiento del progreso de una organización en el cumplimiento de los requisitos de seguridad
- Para evaluar el estado de aplicación de los requisitos de seguridad del sistema
- Para realizar análisis de costes y beneficios de las mejoras de la seguridad del sistema.

Objetivos del proyecto

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

Por todo lo anterior, lo que se le propone a los Security Teams es desarrollar un ciclo completo para la evaluación de la seguridad de la información para ello se proponen los siguientes objetivos:

1. **Planificar:**
 - a. Definir un **escenario sobre el que se desarrollarán pruebas de seguridad**.
 - b. **Identificación de los servicios y aplicaciones** sobre los que se desarrollarán las pruebas de seguridad.
 - c. Analizar vulnerabilidades y los controles de seguridad desplegados.
 - d. **Definir las pruebas de seguridad** a realizar.
2. **Ejecutar Explotación, Escalada de Privilegios y Post-explotación:**
 - a. Ejecutar las pruebas e identificar potenciales brechas de seguridad.
 - b. Tomar evidencias de todas las pruebas de seguridad.
3. **Generar informes técnicos de pentesting:**
 - a. Analizar los resultados de las pruebas de seguridad y definir un plan de mitigación.
 - b. Generar un informe técnico tanto del proceso llevado a cabo como los resultados obtenidos en las diferentes tareas de las pruebas de seguridad.

NOTA MUY IMPORTANTE: El mal uso de estas herramientas puede llevar a situaciones de pérdida de la confidencialidad e integridad de la información, interbloqueo, lentitud en la velocidad de conexión e incluso denegación de servicio de las máquinas analizadas y problemas a los usuarios del servicio. Por todo ello **estas herramientas no deben ser utilizadas contra servidores ajenos para los que no se encuentre debidamente autorizado**. El único fin de este proyecto es didáctico, con el objeto de dar a conocer cómo realizar test de penetración y auditorías en seguridad informática de sistemas informáticos propios, y se debe evitar el uso de dichas herramientas para otros fines ilegales o ilícitos.

Normas del entregable

- El plazo de entrega de dicho proyecto finaliza el **día 16 de diciembre a las 23:59 horas**.
- Cada **Security Team** debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado **PA5-ST<NUM>.zip**, que deberá contener al menos los ficheros siguientes:
 - ✓ **Documento: Informe técnico (PDF) que debe contener todas las fases del proceso de evaluación de la seguridad llevado a cabo por el Red Team, detallando resultados de las tareas llevadas a cabo y de las pruebas realizadas (sin límite de páginas).**
 - ✓ **Código fuente de las posibles implementaciones o scripts desarrollados o configuraciones establecidas en herramientas ya disponibles. IMPORTANTE: Entregar los logs y las evidencias de las pruebas realizadas para que todo sea reproducible.**
- Los proyectos entregados fuera del plazo establecido serán considerados inadecuados por el cliente y por tanto entrarán en penalización por cada día de retraso de entrega de 10% del total, hasta agotarse los puntos.