Fundamentos de Test de Intrusión

Un test de intrusión o test de penetración consiste en una serie de pruebas ofensivas contra los mecanismos defensivos del entorno que se analiza. Este test cubre todos los aspectos desde dispositivos físicos y digitales hasta análisis del factor humano mediante el uso de ingeniería social. El objetivo de estas pruebas es veridicar cual es el comporamiento de los mecanismos defensivos en situaciones extremas para detectar vulnerabilidades. También se identifican faltas de controles y prechas de seguridad que puede haber entre la información crítica y los controles existentes.

- Un test de penetración recrea las acciones ofensivasx de un agente hostial para identificar vulnerabilidades
- Los resultados obtendios se utilizan para generar la documentación con los detalles de la auditoría.

Tipos de hackers por motivación

- White hat o Hacker Ético: Trabajan para empresas como especialistas de seguridad que buscan agujeros de seguridad.
- Black Hat Hacker: Tienen motivaciones personales o financieras, también pueden estar involucrados en espionaje o cibercrimen.
- Gray Hat Hacker: Mezcla de white hacker y Black Hacker. Buscan vulnerabilidades en un sistema sin permiso del propietario.

Tipos de Hackers

- Cracker: Hackers de tipo black hat que entran en sistemas vulnerables y provocan daños. También pueden ser los que diseñan programas para romper la seguridad de software o hardware.
- Script Kiddies: Utilizan programas escritos por otros para penetrar los sistemas ya que tienen poco conocimiento sobre el funcionamiento del software.
- Newbie: Principiante en busca de información sobre hacking
- Lammer: El que se cree hacker pero no tiene los conocimientos ni lógica para comprender que está haciendo.

Conceptos

- Vulnerabilidades: Debilidad que podría lelvar un fallo de seguridad. Clasificadas por el CWE, NVD y OWASP
- Ataques: Explotación de vulnerabilidades que puede provocar una interrupción del servicio, intercepción de datos, modificación del sistema o comprometer los datos de un sistema.
- Amenazas: Amenazas identificadas por las que puede estar afectada una infraestructura empresarial.
- Vector de ataque: ruta o medio uitilizado para realizar el ataque, permite al atacante explotar o tomar ventaja de vulnerbilidades o debilidades del sistema.

Auditorías de pentesting

Las auditorías de pentesting pueden ser clasificadas por según la información que proporciona la organización auditada:

- White Box: Se cuenta con información detallada
- Grey Box: Se cuenta con información parcial de la organización
- Black Box: No hay información sobre la organización

Fases de una auditoría de pentesting

1. **Reconocimiento**: Se definen objetivos y se recopila toda la información posible que será usanda durante las siguientes fases.
    1. **FootPrinting**: Recogida de datos o información que se lleva a cabo en medios o fuentes de acceso público. Se suelen usar las siguientes herramientas:
        1. Shodan
        2. NameCHK
        3. Google / Bing Hacking
    2. **Fingerprinting**: Se recaba información sobre la topología, direcciones y nombres a diferentes niveles, puertos, versiones del software, parches del sistema operativo, vulnerabilidades...
2. **Enumeración**: Se buscan posibles vectores de ataque usando los datos obtenidos en el reconocimiento. Se escanean puertos y servicios.
3. **Acceso**: Se realiza el acceso al sistema mediante la explotación de las vulnerabilidades detectadas.
4. **Mantenimiento** de acceso: Se busca una manera de preservar el acceso a los sistemas comprometidos.

Tipos de equipos de pentesting

- Blue Team: Defensivo, tiene como objetivo detectar, bloquear y prevenir ataques
- Red Team: Ofensivo, tiene como objetivo escanear, detectar y explotar vulnerabildiades.
- Purple Team: Mixto

From:
http://www.knoppia.net/ - **Knoppia**

Permanent link:
http://www.knoppia.net/doku.php?id=master_cs:int:tm1v2

Last update: **2026/05/17 21:51**