Tema 6. Seguridad Perimetral

Parte 3. Análisis de seguridad en redes

Tests de intrusión

Seguridad en Sistemas Informáticos

Noviembre-2012

Contenido

Tests de intrusión (I)

¿Qué son?

- Mecanismo de **evaluación** de las medidas de protección de una organización y de los servicios expuestos a Internet.
  - Analizan la efectividad de los **controles de seguridad** implantados en una organización relizando una bateria de **acciones planificadas** que simulan el comportamiento de un atacante.
  - Otros nombres: tests de penetración (*pen testing*), hacking ético (*ethical hacking)*
- **Objetivo:** vulnerar la seguridad de los mecanismos implantados para conseguir accesos no autorizados a la organización, obtener información sensible, interrumpir un servicio,…
  - Dependerá del **alcance** concreto del test realizado
  - Test de penetración != análisis de vulnerabilidades
    - Las vulnerabilidades detectadas se explotan

Tests de intrusión (II)

¿Para qué sirven?

- Conforman un conjunto de actividades destinadas a estimar el estado real de la seguridad de un sistema.
  - Son uno de los posibles métodos y técnicas a usar en las auditorias de seguridad
  - Finalizan con un informe técnico (identificación del riesgo, probabilidad de ocurrencia, impacto en la organización,estimación de su gravedad, recomendaciones)
- Beneficios
  - Encuentran brechas de seguridad no vistas
  - Documentan e informan a la dirección de problemas/amenazas
  - Verificación de configuraciones seguras (en redes y software)
  - Verificación real del cumplimiento de las políticas y medidas de seguridad establecidas

Tipos de tests de intrusión (I)

White box pentest

- Se posee un amplio conocimiento de la organización (estructura, departamentos, responsabilidades) y de la red (topología, dispositivos, SS.OO., bases de datos, IDS, firewalls, ...)
- Se cuenta con colaboración del personal y con acceso a los recursos de la empresa.
- Simula un atacante con conocimiento exhaustivo del sistema
- Análisis interno
  - Desde el punto de vista de un administrador o usuario que cuentan con acceso (privilegiado o no) al sistema
  - Puede ser muy extenso (alcance muy amplio) y minucioso (se dispone de un conocimiento completo)

Tipos de tests de intrusión (II)

Black box pentest

- No hay conocimiento previo de la organización o la red
  - Sólo se dispone de información públicamente accesible
- Pocas personas de la organización saben que esta será atacada.
- Simulación más realista de un ataque auténtico
- Puede ser muy costoso (tiempo [recopilación info.] + personal entrenado)

Grey box pentest (combina los anteriores)

- Usa técnicas de un atacante real (black box) con conocimiento del sistema analizado (white box)

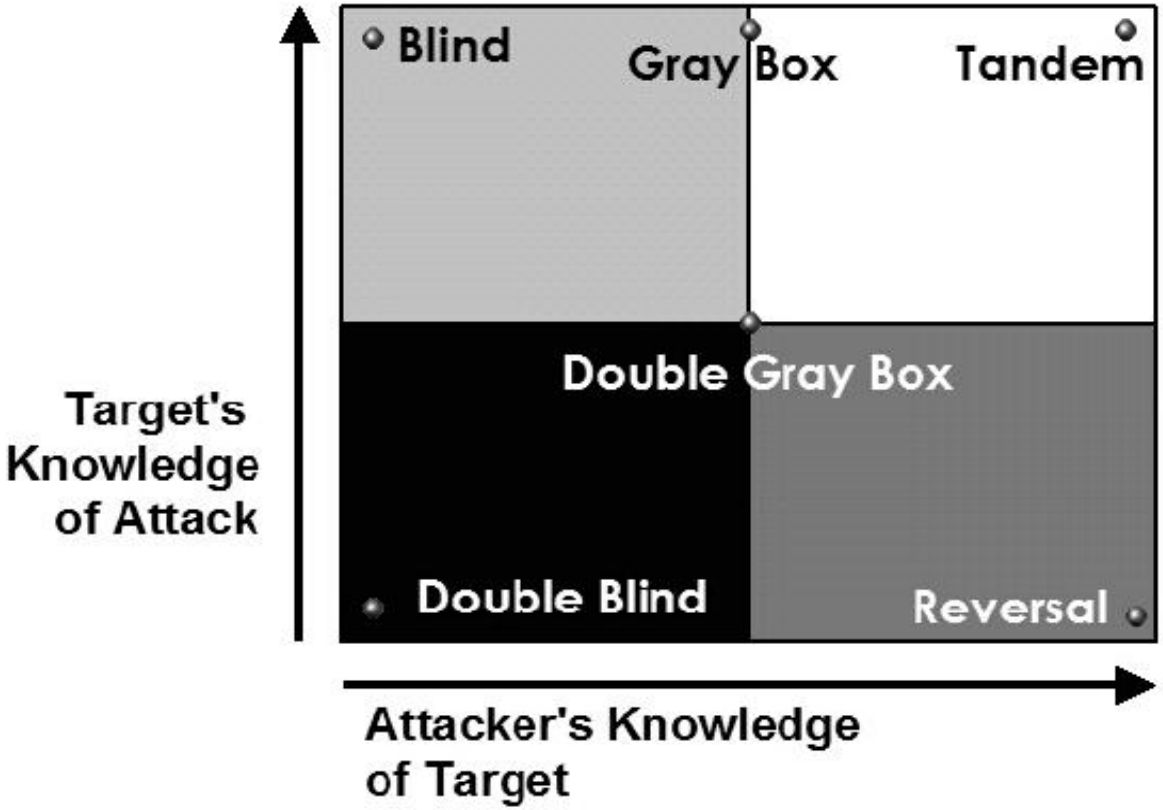
Tests de intrusión específicos

- Servicios/aplicaciones web, bases de datos, wireless, ...
- Las tareas y pasos concretos a seguir varían ligeramente en cada tipo

Tipos de tests de intrusión (III)

Otra visión:

- Conocimiento del atacante *vs* conocimiento del atacado



• Metodologías de Pen Test (I)

Test de penetración supone definir y ejecutar multitud de tareas muy complejas y variadas => necesidad de guias

- Metodologías que definan y organicen los procedimientos a ejecutar para mantener la coherencia en las acciones a realizar

Open Source Security Testing Methodology Manual (OSSTMM)

- Metodología del ISECOM para la realización de evaluaciones de seguridad, incluidos test de penetración
- Metodología Open Source, disponible en http://www.osstmm.org
- Define, organiza y secuencia las tareas y comprobaciones a realizar para analizar 3 aspectos (alcance) de la seguridad:
  - COMMSEC (*communication security*): redes y transferencia de datos
  - PHYSEC (*physical security*): personal y equipos físicos
  - SPECSEC (*spectrum security*): comunicaciones wireless
- Entre esos pasos/tareas/comprobaciones se incluye un marco para la realización de tests de penetración

Metodologías de Pen Test (II)

ISSAF(*Information Systems Security Assessment Framework*)

- Framework del OISSG (*Open Information Systems Security Group*) que define procediemientos de aseguramiento y comprobación de la seguridad incluido *pen testing*
- Web: http://www.oissg.org/

OWASP Testing Guide de OWASP

- Framework del proyecto *Open Web Application Security Project (OWASP)* exclusivamente dedicado a seguridad de aplicaciones web.
- Web: http://www.owasp.org/
- Productos:
  - Guia de desarrollo y testing de aplicaciones web http://www.owasp.org/index.php/OWASP_Guide_Project
    - Define listas de comprobaciones en un test de intrusión web
  - Top 10 de amenazas web http://www.owasp.org/index.php/OWASP_Top_Ten_Project

Fases y tareas típicas

Recopilación de información

- Etapa 1: Rastreo
- Etapa 2: Exploración

Análisis de datos

- Etapa 3: Enumeración

Explotación

- Etapa 4: Acceso
- Etapa 5: Escalada de privilegios
- Etapa 6: Daño
- Etapa 7: Borrado de huellas

Informe final del test

- Informe técnico.
  - Resumen del proceso realizado
  - Clasificación de las vulnerabilidades encontradas y su nivel (alto, medio, bajo)
  - Propuesta de correcciones y sugerencia de buenas prácticas
- Informe ejecutivo.

Fases y tareas típicas (I)

Etapa 1: Rastreo

- Obtener información del sistema/organización/red/máquina bajo análisis
  - Nombres de dominio, direcciones IP, nombres de usuarios, responsables, …
  - Bases de datos públicas: *whois, RIPE, DNS, …*
  - Buscadores
    - Genéricos: *Google hacking, bing hacking, ...*
    - Específicos: Goolag (http://www.goolag.org), KartOO (http://kartoo.org)
  - Herramientas genéricas de gestión de red: *dig, nslookup,...*
  - Herramientas específicas: *FOCA* (análisis metadatos), *Maltego*

Fases y tareas típicas (II)

Etapa 2: Exploración

- Analizar el sistema objetivo para identificar servicios activos, máquinas disponibles, recursos/dispositivos de red (routers, firewalls, ...), sistema operativo, ...
  - Herramientas genéricas de gestión de red: *ping, traceroute,...*
  - Herramientas específicas
    - escáneres de puertos: *nmap, hping3, xprobe, ...*

Fases y tareas típicas (III)

Etapa 3: Enumeración

- Pruebas y tests para identificar recursos específicos y sus características concretas
  - Identificar SS.OO., sus versiones y parches de seguridad (service packs, etc)
  - Versiones concretas de servicios/aplicaciones
  - Cuentas de usuario válidas
  - Herramientas específicas
    - Escáneres puertos e identificadores de servicios: *nmap, xprobe...*
    - Escáneres de vulnerabilidades: *nessus, openvas, …*
    - Escáneres de vuknerabilidades específicos: *w3af (escaner de wulnerabilidades web)*

Fases y tareas típicas (IV)

Etapa 4: Acceso

Obtener un acceso no autorizado o no previsto a alguno/s de los recursos o servicios identificados en el sistema objetivo.

- Rotura de contraseñas
  - Por fuerza bruta, ataques de diccionario (Rainbow tables), prueba de contraseñas por defecto o contrseñas débiles
  - Herramientas: *THC hydra, John the Ripper, Abel and Cain,...*
- Sniffing/escucha de contraseñas o datos sensibles: *wireshark, tcpdump, ettercap, ...*
- Inyección de tráfico: *ettercap, dnsniff, sslsniff, ...*
- Explotación de vulnerabilidades específicas de las versiones concretas de los servicios/recursos identificados.
  - Exploits específicos: http://milw0rm.com
  - Herramientas automatización exploits:*Metasploit, CORE Impact, SAINTexploit*
  - Uso de valores de entrada no previstos
    - *fuzzers*: exploraciones exhaustiva automatizada de los posibles datos de entrada, buscando (a ciegas) situaciones no previstas

Etapa 5: Escalada de privilegios

Obtener control completo del sistema, adquiriendo (y manteniendo) permisos, credenciales y privilegios propios de los administradores.

- **Objetivo:** Validar si para el supuesto atacante sería posible adquirir privilegios que le permitieran ejecutar acciones maliciosas o acceder a datos restringidos.
- Suele requerir incluir código específico en el sistema objetivo (*payload*) que permitan realizar determinadas acciones:
  - Normalmente ofrecen algún tipo de acceso remoto al mismo (habilitan *puertas traseras*):
    - abrir shells del sistema con privilegios (bash), habilitar conexiones de escritorio remoto (VNC),...
- Explotación de vulnerabilidades específicas de las versiones concretas de los servicios/recursos identificados.
  - Exploits específicos: http://milw0rm.com
  - Herramientas automatización exploits: *Metasploit, Core Impact*
  - Puertas traseras: *BackOrifice,LCP 5.0*

Fases y tareas típicas (VI)

Etapa 6: Daño

- Valorar y evaluar la capacidad del atacante que ha “escalado” privilegios de realizar acciones maliciosas que causen daño:
  - Daños posibles:
    - Acceso a datos confidenciales
      - Robo de información
      - Alteración de información: datos protegidos, páginas web, ...
    - Denegación de servicio (DoS)
      - Imposibilitar el acceso o uso de determinados componentes del sistema a sus usuarios legítimos.
    - Extensión del ataque
      - Evaluar la posibilidad de usar el sistema controlado como punto de partida para iniciar ataques a otras parte del propio sistema objetivo o a sistemas ajenos

Fases y tareas típicas (VII)

Etapa 7: Borrado de huellas

- Verificar hasta que punto el potencial atacante tendría capacidad de eliminar el rastro de sus acciones maliciosas y mantener su control del sistema de forma permanente sin ser detectado.
  - **Objetivo:** Eliminación de los registros y logs que contengan información que releve la existencia del ataque y que pudiera ser de utilidad en un análisis forense o una auditoría de seguridad.