



Curso Gestión en Seguridad Informática y Hacking de Sistemas I

MODULO 1

Métodos de Rastreo y Análisis de objetivos utilizados por los intrusos maliciosos desde Internet.

Los asistentes conocerán y practicarán con los métodos y técnicas utilizadas cuando un intruso malicioso planea comprometer los servicios cara a Internet de una empresa. Utilizarán técnicas de rastreo, enumeración y escaneos de puertos que permiten definir un vector de ataque desde Internet hacia sistemas conectados a esta. Además obtendrán la base de conocimientos técnicos necesarios para comprender el funcionamiento de las distintas técnicas.

BREVE INTRODUCCIÓN Y CONCEPTOS PREVIOS

INTRODUCCIÓN Y CONCEPTOS PREVIOS

· ¿Qué es la seguridad informática? · ¿Por qué es necesaria la seguridad informática en la organización? · Campos de acción de la seguridad informática. · Programas malignos y tipos de intrusos. · Tipos de protección. · Seguridad de los sistemas operativos. · Seguridad en redes. · Herramientas de seguridad informática.

· La utilización de sitios Web indispensables para trabajar en seguridad informática.

Conceptos imprescindibles y el protocolo TCP/IP

- Introducción
- Capas de red
- Dirección IP
- Intranet
- Extranet
- Internet
- Mascara de subred
- Protocolo IP
- Protocolo ICMP
- Encaminamiento
- Capa de transporte
- Puertos
- Protocolo UDP
- Protocolo TCP
- Nombre de dominio

Problemas de seguridad en las empresas

- Casos documentados de ataques.
- Los nuevos caminos del crimen en Internet.
- Tipos de Ataque que comprometen la seguridad global de la organización.

Técnicas de Rastreo y Exploración

- ¿Qué es seguir el rastro a un objetivo?
- Seguir el rastro en Internet.
- Determinación del ámbito de actividades de la víctima.
- Enumeración de la red.
- Interrogaciones DNS.
- Reconocimiento de la red y su topología previo al ataque.
- Ejercicios prácticos de rastreo.
- Interpretación de resultados y fisuras.
- Contramedidas a adoptar ante las fisuras.

Exploración del objetivo

- Barridos ping.
- Consultas ICMP.
- Exploración de puertos.
- Tipos de escaneos a realizar sobre el objetivo.
- Detección del sistema operativo, versiones y servicios en ejecución.
- Ejercicios prácticos y de análisis.
- Interpretación de resultados y fisuras.
- Medidas a adoptar ante las fisuras.
- Herramientas automáticas de descubrimiento y contramedidas

TÉCNICAS DE HACKING CONTRA LOS SISTEMAS Y CONTRAMEDIDAS

- Introducción
- Firewalls y routers
- Técnicas de firewalking (atravesar cortafuegos)
- Métodos para engañar a los ficheros .log en la ofensiva.
- Como los intrusos se hacen invisibles en Internet.
- Técnicas de suplantación de IP atacantes en Internet (looping spoofing ip)
- Medidas a implementar de prevención.

MODULO 2

Metodología de la intrusión no autorizada a sistemas:"Comprometiendo y atacando sistemas"

En este modulo los asistentes aprenderán y realizaran técnicas intrusivas que los asaltantes realizan sobre sistemas y servicios. Descubrirán herramientas que permiten el acceso no autorizado, así como contramedidas para su utilización contra los sistemas de

su empresa o su institución. Descubrirán como se implantan puertas traseras en sistemas y como los intrusos desactivan los sistemas de seguridad en muchas ocasiones.

TÉCNICAS DE HACKING CONTRA LOS SISTEMAS

- Obtención de exploits (el problema buffer overflow).
- Introducción a los escaneadores de vulnerabilidades.
- Compilación y utilización de exploits sobre vulnerabilidades.
- Shells reversas y directas.
- Ataques distribuidos desde Internet contra usuarios o empresas.
- Entrando en los sistemas y la escalada de privilegios.
- Detección de la utilización de exploits contra nuestra red.
- Métodos de descarga de herramientas de prospección en el servidor comprometido
- Anulando la efectividad de los antivirus (generación de herramientas indetectables)
 - Como se recaba información una vez en los sistemas.
- Medidas de seguridad a implementar.
- Alteración, falsificación e intoxicación de ficheros .log.
- Establecimiento de puertas traseras (backdoors).
- Metodología para la detección de puertas traseras.
- Práctica paso a paso de asalto en laboratorio de testing.

ENUMERACIÓN

- Enumeración Windows NT/2000/2003
- Buscando Usuarios validos y recursos accesibles.
- Ataques contra contraseñas

MODULO 3

Auditorias de vulnerabilidades. Fortalecimiento de las medidas de la Intranet. Monitorización de redes en segmentos críticos.

En este modulo los asistentes aprenderán métodos de endurecimiento de servicios y ordenadores. Utilizaran herramientas de auditoría a sistemas que permiten mantener bajo control la seguridad en la organización. Descubrirán técnicas de cracking y auditoria de ficheros de contraseñas. Además de monitorizar determinados segmento de red críticos o que requieren mayor supervisión

INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE

SERVIDORES CONFIABLES.

- Introducción.
- Vulnerabilidades básicas tras la instalación del sistema.
- Vulnerabilidades en los servicios del sistema.
- Montar la seguridad.
- Mantenimiento y actualizaciones de las medidas de seguridad.
- Scaneadores de vulnerabilidades en redes de ordenadores.

- Uso de los scanners de vulnerabilidades
- Auditorías periódicas de seguridad y análisis de resultados.

AUDITORIA SOBRE POLÍTICAS DE USUARIOS Y CONTRASEÑAS

- Análisis del problema en la organización.
- Métodos de descifrado y ruptura de contraseñas.
- Herramientas para la auditoría de contraseñas.
- Herramientas para ruptura de contraseñas y métodos de cracking de contraseñas
- Implementación de políticas confiables

HERRAMIENTAS PARA AUDITORAR LA SEGURIDAD DE LA RED DE LA EMPRESA Y MONITORIZADORES DE TRÁFICO

- Configuración de las plantillas de auditoría internas y externas.
- Práctica realización de auditorías sobre sistemas internos.
- Práctica realización de auditorías sobre sistemas cara a Internet.
- Generación de informes.
- Introducción a Sniffers.
- Instalación y uso de Sniffers.
- Configuración de filtros de monitorización.
- Análisis y monitorización de segmentos críticos de red.
- Interpretación de los paquetes monitorizados.

Características de los módulos:

HERRAMIENTAS DE CONTRAMEDIDAS Y HACKING QUE SE UTILIZAN DURANTE LOS MODULOS IMPARTIDOS.

- Herramientas on line.
- Herramientas de exploración.
- Herramientas de enumeración.
- Herramientas de footprinting (rastreado).
- Herramientas para conseguir accesos.
- Herramientas de penetración y puertas traseras.
- Ocultación de huellas.
- Herramientas de auditoría de redes y ordenadores.