Temario del curso: Auditorías de Seguridad.

Duración: 24 horas.
Público: administradores de sistemas.
Objetivo: Proporcionar conocimientos sólidos para la realización de auditorías de seguridad, tanto internas como externas.

Temario

1. Introducción:
   Penetration Test.
   Diagnóstico o evaluación de Seguridad.
   Auditoría de seguridad.
   - Definición del alcance del proyecto.
   - Penetration Test o evaluación Externo e Interno.
   - Penetration Test vía Internet.
   - Duración del proyecto.
   - Objetivos del proyecto.
2. Pasos para realizar un Penetration Test o evaluación
   Definición del alcance.
   Definición de la metodología a utilizar.
   Aplicación de la metodología.
   Evaluación de los resultados obtenidos.
   Corrección de los expuestos detectados.
3. Metodologías y Estándares en proyectos de Penetration Testing:
   OSSTMM (Open Source Security Testing Methodology Manual.)
   Metodología de Penetration Test o evaluación de Seguridad.:
   - Descubrimiento.
   - Exploración.
   - Evaluación.
   - Intrusión.
4. Fase de Descubrimiento
   Recolección de información.
   Descubriendo la red.
   Fuentes de información en Internet.
   Dirección física.
   Detección de Redes WiFi.
   Números telefónicos.
   Nombres de personas y cuentas de correo electrónico.

Rango de direcciones IP.
Información de prensa sobre el lugar.
Análisis de las páginas Web Institucionales y/o Intranet Corporativa.
Evaluación del código fuente.

5. Fase de Exploración:
   - Scanning telefónico.
   - Detección de hosts activos.
   - Detección y Análisis de servicios activos
   - Detección remota de sistemas operativos.
   - Determinación de mecanismos de encripción en redes Wi-Fi.
   - Relevamiento de aplicaciones Web.
6. Fase de Evaluación:
   - Detección de vulnerabilidades en forma remota.
   - Herramientas de detección de vulnerabilidades.
   - Testing de seguridad en Routers / Firewalls/ Dispositivos de Comunicaciones
   - Testing de seguridad de un servidor UNIX.
   - Testing de seguridad de un servidor Windows NT/2000.
   - Testing de seguridad de un servidor Novell.
   - Testing de eficacia de Sistemas de Detección de Intrusiones.
   - Testing de seguridad de una Base de Datos.
   - Testing de seguridad de aplicaciones Web.
7. Fase de Intrusión:
   - Planificación de la intrusión.
   - Utilización de ingeniería social para obtención de información.
   - Explotación de las vulnerabilidades detectadas.
   - Acceso vía módems o accesos remotos detectados.
   - Intrusiones vía web.
   - Escalada de privilegios.
   - Combinación de vulnerabilidades para elevar el control.
   - Acceso a información interna.
   - Generación de evidencia de expuestos detectados.
8. Evaluación y corrección:
   - Evaluación de los resultados obtenidos.
   - Determinación de niveles de riesgo.
   - Propuesta de soluciones de seguridad.
   - Corrección de las vulnerabilidades detectadas.