Hacking y seguridad, nivel 1

Curso práctico de 5 días - 35h
Ref.: HAC - Precio 2024: 2 470€ sin IVA

Este curso avanzado le enseñará las técnicas necesarias para medir el nivel de seguridad de su sistema de información. Tras estos ataques, aprenderá a activar la respuesta adecuada y a elevar el nivel de seguridad de su red.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Comprender las técnicas de los piratas informáticos y poder contrarrestar sus ataques

Medir el nivel de seguridad de su Sistema de Información

Realizar una prueba de intrusión

Definir el impacto y el alcance de una vulnerabilidad

PROGRAMA

última actualización: 01/2023

1) Hacking y seguridad

- Formas de ataques, modos de operar, actores, problemas.
- Auditorías y pruebas de intrusión, lugar en un SGSI.

2) Interceptar, analizar, inyectar en la red

- Anatomía de un paquete, tcpdump, Wireshark y tshark.
- Secuestro e interceptación de comunicaciones (ataque de intermediario, ataques de VLAN, señuelos).
- Paquetes: Interceptación, lectura/análisis a partir de un pcap, extracción de datos útiles, representaciones gráficas.
- Scapy: arquitectura, capacidades, utilización.

Trabajo práctico : Escuchar la red con programas interceptores (sniffers). Construir un miniinterceptor de paquetes en C. Utilizar scapy (línea de comandos, script de python): inyecciones, interceptación, lectura de pcap, escaneo, DoS y MitM.

3) Reconocimiento, escaneo y enumeración

- Recogida de información, lectura en caliente, explotación de la red oscura e ingeniería social.
- Reconocimiento de servicios, sistemas, topologías y arquitecturas.
- Tipos de escaneos, detección de filtros, firewalking y fuzzing.
- El camuflaje por suplantación y rebote, la identificación de rutas con traceroute y enrutamiento de origen.
- Evasión de IDS e IPS: fragmentaciones, canales encubiertos.
- Nmap: escaneo y exportación de resultados, opciones.
- Otros escáneres: Nessus y OpenVAS.

Trabajo práctico : Uso de la herramienta nmap, escritura de un script NSE en LUA. Detección del filtrado.

4) Ataques a la web

- OWASP: organización, capítulos, Top10, manuales y herramientas.
- Descubrimiento de infraestructuras y tecnologías asociadas, puntos fuertes y débiles.

PARTICIPANTES

Responsables y arquitectos de seguridad. Técnicos y administradores de sistemas y redes.

REQUISITOS PREVIOS

Buenos conocimientos sobre seguridad SI, redes, sistemas (en particular Linux) y programación. O conocimientos equivalentes a los del curso «Seguridad de sistemas y redes, nivel 1» (ref. FRW).

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- En el cliente: clickjacking (secuestro de clic), CSRF, robo de cookies, XSS y componentes (flash, java). Nuevos vectores.
- En el servidor: autenticación, robo de sesión, inyecciones (SQL, LDAP, archivos y comandos).
- Inclusión de archivos locales y remotos, ataques y vectores criptográficos.
- Evasión y elusión de protecciones: ejemplo de las técnicas de elusión de WAF.
- Herramientas Burp Suite, ZAP, Sqlmap y BeEF.

Trabajo práctico : Implementación de diferentes ataques web en condiciones reales en el servidor y el cliente.

5) Ataques de aplicación y posexplotación

- Ataque a las autentificaciones de Microsoft, PassTheHash.
- De C a ensamblador y a código máquina. Shellcodes.
- Codificación de shellcodes y eliminación de NULL bytes.
- Rootkits. Explotación de procesos: Desbordamiento de búfer, programación orientada al retorno (ROP) y referencias colgantes.
- Protecciones y soluciones: Bandera GS, ASLR, PIE, RELRO, Safe SEH y DEP. Shellcodes con direcciones codificadas/LSD.
- Metasploit: arquitectura, funcionalidades, interfaces, espacios de trabajo, escritura de programas intrusos (exploits) y generación de shellcodes.

Trabajo práctico : Metasploit: explotación y utilización de la base de datos. Msfvenom: generación de Shellcodes y captura de archivos. Desbordamiento de búfer en Windows o Linux y explotación con shellcode Meterpreter.

FECHAS

Contacto