Detección de intrusos
Cómo gestionar los incidentes de seguridad

Curso práctico de 4 días - 28h
Ref.: INT - Precio 2025: 2 040€ sin IVA

Esta formación teórica y práctica presenta las técnicas de ataque más avanzadas hasta la fecha y muestra cómo hacerles frente. A partir de ataques realizados contra objetivos identificados (servidores web, clientes, redes, cortafuegos, bases de datos, etc.), los participantes aprenderán a desencadenar la respuesta adecuada (filtrado antitroyanos, filtrado de URL malformadas, detección de spam y detección de intrusiones en tiempo real con sondas IDS).

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Identificar y comprender las técnicas de análisis y detección

Adquirir los conocimientos necesarios para desplegar diferentes herramientas de detección de intrusos.

Implantación de soluciones de prevención y detección de intrusiones

Gestión de un incidente de intrusión

Comprender el marco jurídico

Las arquitecturas seguras y "normalmente" protegidas (cortafuegos multi-DMZ, aplicaciones seguras) serán el blanco de los ataques.

PROGRAMA

última actualización: 02/2024

1) El mundo de la seguridad informática

- Definiciones "oficiales": hacker, piratería informática.
- La comunidad mundial de hackers, los "gurús", los "script kiddies".
- La mentalidad y la cultura hacker.
- Conferencias y grandes sitios de seguridad.

Trabajo práctico : Navegación subterránea. Localice información útil.

2) TCP/IP para cortafuegos y detección de intrusiones

- IP, TCP y UDP desde otro ángulo.
- Centrarse en ARP e ICMP.
- Enrutamiento forzado de paquetes IP (enrutamiento de origen).
- Reglas de fragmentación y reensamblaje IP.
- La necesidad de un filtrado serio.
- Proteger sus servidores: una obligación.
- Contramedidas basadas en la tecnología: de los routers de filtrado a los cortafuegos de inspección de estado; de los proxies a los proxies inversos.
- Una rápida visión general de soluciones y productos.

Trabajo práctico : Visualización y análisis del tráfico clásico. Utilización de diferentes sniffers.

3) Comprender los ataques a TCP/IP

- Suplantación de IP.
- Ataques de denegación de servicio.

PARTICIPANTES

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

REQUISITOS PREVIOS

Buenos conocimientos de redes TCP/IP. Conocimientos básicos de seguridad informática.

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.

- Predicción del número de secuencia TCP.
- Robo de sesión TCP: Hijacking (Hunt, Juggernaut).
- Ataques a SNMP.
- Ataque TCP Spoofing (Mitnick): desmitificación.

Trabajo práctico : Inyección de paquetes fabricados en la red. Uso de herramientas gráficas, Perl, C o scripts dedicados. Secuestro de una conexión telnet.

4) Recopilación de información: el arte del camuflaje

- Búsqueda de rastros: consulta de bases de datos Whois, servidores DNS, motores de búsqueda.
- Identificación del servidor.
- Comprensión del contexto: análisis de resultados, determinación de reglas de filtrado, casos específicos.

Trabajo práctico : Utilización de técnicas no intrusivas para buscar información sobre un objetivo potencial (elegido por los participantes). Utilización de herramientas de exploración de la red.

5) Protección de datos

- Sistemas con contraseñas "claras", contraseñas de desafío, contraseñas cifradas.
- Una actualización sobre la autenticación de Windows.
- Un recordatorio de SSH y SSL (HTTPS).
- Sniffing de una red conmutada: ARP poisoning.
- Ataques a datos cifrados: "Man in the Middle" a SSH y SSL, "Keystoke Analysis" a SSH.
- Detección de sniffer: herramientas y métodos avanzados.
- Ataques con contraseña.

Trabajo práctico : Descifrado y robo de sesiones SSH: ataque "Man in the Middle". Descifrado de contraseñas con LophtCrack (Windows) y John The Ripper (Unix).

6) Detección de troyanos y puertas traseras

- Estado del arte de las puertas traseras en Windows y Unix.
- Instalación de puertas traseras y troyanos.
- Descarga de scripts a los clientes, explotando los fallos del navegador.
- Canales encubiertos: aplicaciones cliente-servidor que utilizan ICMP.
- Ejemplo de comunicación con agentes de denegación de servicio distribuidos.

Trabajo práctico : Análisis de Loki, un cliente-servidor que utiliza ICMP. Acceder a información privada con el navegador.

7) Defender los servicios en línea

- Tomar el control de un servidor: encontrar y explotar vulnerabilidades.
- Ejemplos de creación de puertas traseras y eliminación de rastros.
- ¿Cómo puentear un cortafuegos (netcat y rebotes)?
- Investigación sobre la denegación de servicio.
- Denegación de servicio distribuida (DDoS).
- Ataques de desbordamiento del búfer.
- Explotación de vulnerabilidades en el código fuente. Técnicas similares: "Format String", "Heap Overflow".
- Vulnerabilidades en aplicaciones Web.
- Robo de información de una base de datos.
- RootKits.

Trabajo práctico : Explotación del bug utilizado por el gusano "Código Rojo". Obtención de un shell de root utilizando varios tipos de desbordamiento de búfer. Pruebas de denegación de servicio (Jolt2, Ssping). Utilización de netcat para eludir un cortafuegos. Uso de técnicas de "SQL Injection" para romper la autenticación Web.

8) ¿Cómo se gestiona un incidente?

- Los signos de una intrusión de SI exitosa.
- ¿Qué han conseguido los hackers? ¿Hasta dónde han llegado?

- ¿Cómo reaccionar ante una intrusión exitosa?
- ¿Qué servidores están afectados?
- Encuentra el punto de entrada y llénalo.
- La caja de herramientas de Unix/Windows para encontrar pruebas.
- Limpieza y vuelta a la producción de los servidores comprometidos.

9) Conclusión: ¿cuál es el marco jurídico?

- La respuesta adecuada a los hackers.
- Ley francesa sobre piratería informática.
- El papel del Estado, organismos oficiales.
- ¿Qué podemos esperar de la Office Central de Lutte contre la Criminalité (OCLCTIC)?
- Búsqueda de pruebas y autores.
- ¿Y en un contexto internacional?
- ¿Pruebas intrusivas o hacking domesticado?
- Manténgase dentro de un marco legal, elija el proveedor de servicios, esté seguro del resultado.

FECHAS

Contacto