Taller Seguridad Informática- El Lado Oscuro De La Red

technologyINT
Ciberseguridad & Computo Forense

Ver 2.6

Objetivo General

El Taller de Seguridad informática brinda un amplio conocimiento y práctica real en equipos de las más actuales herramientas y técnicas de ataque y defensa, permitiéndonos consecuentemente actuar profesionalmente sobre el tema. Tiene un enfoque totalmente práctico basado en distintos tipos de ataques y sobre diversos entornos.

Tobe Security una empresa israelí de seguridad informática, forma desde hace más de 19 años a nivel internacional a los más importantes líderes del sector de seguridad de la información, mediante programas de alcance mundial con visión estratégica de las últimas tendencias del mercado, ahora se une a technologyINT para transmitir ese conocimiento tan importante para los equipos responsables de la seguridad lógica de las organizaciones.

Usted obtendrá los conocimientos teóricos, una visión estratégica, y aplicación practica, con los cuales profesionales especializados trabajan en el campo de la seguridad informática de los más altos niveles de complejidad a nivel internacional.

El enfoque de los contenidos estará en constante correlación con los estándares internacionales de seguridad informática.

Capacitar a los profesionales de Seguridad Informática en tecnologías y herramientas de implementación y control de medidas de seguridad de la información en concordancia con estándares internacionales.

01. Seguridad de las redes

- Composición de una red de información.
- Políticas de seguridad.
- Topología de una red segura.
- Vulnerabilidades y consideraciones de seguridad para cada componente de una red.
- Social Engineering (Ingeniería social).
- Registro de auditoria/Administración de los Logs.
- Seguridad de Servidores Web/Medidas de seguridad en un servidor web.
- Security in Depth (seguridad en etapas).
- Control de accesos.

02. Seguridad en Routers/Switches

- Hardening.
- Metodologías y herramientas para atacar Switches/Routers.
- Arp poisoning.
- VLANs.
- Mac Lucking.
- NAC 802.1X.
- Detección de posibles fallas en seguridad.

03. Seguridad de las redes

- Principales tipos de Firewalls.
- Amenazas de códigos maliciosos.
- Cómo crear una base de reglas Robusta y eficiente.
- Problemas con Firewalls.
- Firewalls de Open Source.
- High Availability /Load Sharing- Redundancia.
- Leer y entender los logs del Firewall para detectar intrusiones.

04. IDS/IPS-Best practice

- Principales tipos de IPS/IDS.
- Dónde colocar IPS/IDS en la red.
- Maneras en que los hackers atacan redes protegidas por IDS/IPS.
- Estrategia para evitar falsos positivos/falsos negativos.
- Cómo configurar nuestros IDS/IPS para evitar ataques de Hackers.

05. Seguridad en servidores Windows

- Métodos para armar un servidor seguro.
- Hardening.
- Seguridad hasta el nivel de la aplicación.
- Cómo saber si un hacker penetro servidores de la organización.
- Manejo de parches y Service Packs.
- Cifrado de datos.
- Protección de archivos y carpetas.

06. Arquitectura de red segura

- Autenticación.
- Cómo evitar un único punto de falla.
- Biometría.
- SSL.
- Firmas Digitales.
- BCP/DRP Plan de contingencia.
- VPN.
- Rastreos locales.
- Cloud Computing/Computación en la nube.
- DLP/Fuga de información.
- Dos Factores autenticación.
- Protección contra ataques con Triggers (Bombas lógicas).

07. Seguridad en Wireless

- Diferentes algoritmos.
- Hardening de Access points y red inalámbrica.
- Penetration Test en una red wireless.

08. Ethical Hacking/Penetration Test

- Herramientas .
- Auditorias de seguridad.
- Diferencia entre auditoria y Penetration Tests.
- Diferencias entre un Penetration Test interno y externo.

09. Google Hacking para penetration Testers

Numero de horas:

20 horas

Modalidad:

Online con presencia continua del instructor.

¿A quién esta dirigido?

Personal del departamento de Sistemas, Programación, Infraestructura tecnológica, soportes de tecnología, redes, seguridad informática, personal responsable de la configuración del hardware y software de seguridad de la información. El Nivel de este curso es Intermedio-Avanzado.

Al finalizar este curso los participantes podrán tener conocimientos de los diferentes dominios:

1. Seguridad y gestión de riegos.
2. Seguridad de activos.
3. Arquitectura de seguridad e ingeniería.
4. Comunicación y seguridad de red.
5. Evaluación de seguridad y pruebas.
6. Operaciones de seguridad.
7. Seguridad de desarrollo de software.
8. Al hacer este curso podrás aprender implementar controles de seguridad correctos en la red.

Quorum:

Cupo limitado

Horario:

9:00 AM a 6:00 PM
Miércoles 9, Jueves 10 y Viernes 11 de Marzo.

Fecha de inicio:

9 de Marzo del 2022

Cuentas para hacer pagos:

INTEGRATION CONSULTING TECHNOLOGYINT
Cuenta en dolares: Ahorros, Swift BPDODOSX, Banco Popular Dominicano #8137766812
Cuenta en Pesos Dominicanos: Corriente, Banco Popular Dominicano #778607648

Esto incluye:

Certificado de participación
Herramientas proporcionadas por el instructor

Inversión:

Organizaciones	**US$ 650.00**
Profesionales	**US$ 350.00**
Empleados Sector Publico, Maestros y ONG	**US$ 175.00**
Estudiantes de grado	**US$ 100.00**

Mr. Juan Baby (CISSP – CCNA – CCSA - MCSE – SCSA - CEH)

Especialista israelí en seguridad informática, con 13 años de experiencia en sólidas técnicas de Penetration Tests, habilidades y métodos de operaciones. Tiene una amplia formación en tecnologías de seguridad, entre otras: IDS/IPS, Firewalls, Application Security, Buffer Overflows, Microsoft Security, Linux Security, IDS Evasion Attacks, Assesment Services y Penetration Tests.

Mr. Baby tiene las siguientes certificaciones: en Check Point System Administrator (CCSA), Microsoft Certified System Engineer (MCSE), Cisco Certified Network Administrator (CCNA), Sun Certified System administrator (SCSA) y ISC2 Certified Information Systems Security Professional (CISSP) y CEH (Certified Ethical Hacker).

Más información

informacion@technologyint.net
Rep. Dominicana: +1 (809) 685 8883
Orlando, Florida: +1 (321) 310 1830

Enlace de registro:

www.forms.gle/2NUDnJUBtWaJ7Tmp6

technologyINT
Ciberseguridad & Computo Forense