CBHE
CÁMARA BOLIVIANA DE HIDROCARBUROS Y ENERGÍA

Integrando energías!

TALLER DE SEGURIDAD INFORMÁTICA
EL LADO OSCURO DE LA RED

CONTENIDO

1. 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/Administracion de los Logs
Seguridad de Servidores Web/Medidas de seguridad en un servidor web
Security in Depth (seguridad en etapas)
Control de accesos

2. 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

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

4. 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

5. 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 Á

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

7. Seguridad en Wireless
Diferentes algoritmos
Hardening de Access points y red inalámbrica
Penetration Test en una red wireless

8. Ethical Hacking/Penetration Test
Herramientas
Auditorias de seguridad
Diferencia entre auditoria y Penetration Tests
Diferencias entre un Penetration Test interno y externo

9. Google Hacking para penetration testers

OBJETIVO:

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

Tobe Security una empresa israelí de seguridad informática forma desde hace más de 19 años a nivel internacional a los mas importantes líderes del sector de seguridad de la información, mediante programas de alcance mundial con visión estratégica de las últimas tendencias del mercado.

AGENDA:

Fechas: del 29 al 31 de octubre 2018

Duración: dos días y medio

Carga Horaria: 20 horas

Horario: de 08:00 a 18:00

Lugar: Auditorio CBHE
Av. Radial 17 y 1/2 y 6to Anillo
Santa Cruz - Bolivia

INCLUYE:

- Impuestos de Ley.
- Certificado de participación emitido por la CBHE.
- Material impreso , material digital.
- Refrigerios mañana y tarde.

INSTRUCTOR: Mr. JUAN BABY

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. certificaciones: 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).

Contacto e información: Diego de la Torre C.
E-mail: diego@cbhe.org.bo
Teléfono: (591)3-3538799
WhatsApp: (591) 79891193

CBHE
CAPACITACIÓN