cybertrust

INSPIRANDO CONFIANZA

G|PPT

Professional Penetration Tester

PPT®

Professional Penetration Tester

Introducción

G|PPT® esta diseñado para formar profesionales con habilidades y técnicas de auditoria, hacking Ético y proceso de PenTesting siguiendo metodología abiertas y reconocidas internacionalmente.

El programa tiene foco en las ultimas amenazas, ultimas técnicas y vectores de ataques conocidos. Es un entrenamiento altamente practico, donde los alumnos aprenderán paso a paso como explotar las vulnerabilidades de redes y sistemas complejos.

A diferencia de otros entrenamientos teóricos, este entrenamiento brinda las habilidades practicas para luego de terminado el entrenamiento, poder realizar auditorias reales de seguridad y pentesting de seguridad en clientes.

Los laboratorios son ejecutados sobre la ultima versión de Kali Linux y las ultimas versiones de los distintos sistemas operativos. Incluidos Windows 7, Windows 8, Windows Server 2008 R2, Windows 2012 Server y las ultimas distribuciones Linux.

Es un training 90-95% practico, con múltiples desafíos guiados por el instructor donde el alumno podrá tener un conocimiento en profundidad de las ultimas técnicas de hacking

Objetivos del Curso

- Dominar las ultimas tecnicas de ethical hacking
- Conocer las metodologias OWASP y OSSTMM para realizar procesos de Penetration Testing en clientes o dentro de la propia compañía.
- Dominar metasploit en modo avanzado
- Realizar bypass de Antivirus
- Realizar bypass de IDS-IPS
- Realizar bypass de WAF (Web Application Firewalls)
- Dominar de forma avanzada Kali Linux

Al finalizar el curso cada participante

- Realizar análisis e interceptación de trafico TCP/IP avanzado
- Avanzado análisis de vulnerabilidades de forma manual y con herramientas automáticas
- Elevación de privilegios y ataques a contraseñas contra servicios
- Metasploit desde lo básico hasta lo avanzando. El alumno podrá dominar desde la línea de comandos con hasta la vía grafica con Armitage. También aprenderá como realizar bypass de AV
- Ataques Client-Side! contra browsers como Internet Explorer, Firefox y Google Chrome para tomar control de equipos cliente con Windows 7 o Windows 8

Metodología

Este curso está diseñado para permitir que los participantes aprendan por medio de varios recursos, incluyendo:

- Clases 95% practicas
- Servidores y equipos reales
- Laboratorio con multiples ambientes
- Simulación de Ataques reales (Controlados)

Quienes debieran participar

- Ethical Hackers
- Pentesters
- Auditores
- Gerentes de Riesgo
- Oficiales de Seguridad de la Información
- Oficiales de Cumplimiento
- Administradores de Plataformas
- Administradores de Sistemas
- Administradores de Firewalls y Networking
- Profesionales Tecnicos asociados a TI
- Profesionales interesados en ingresar al creciente y demandante mercado de la seguridad informatica, tanto para trabajar en Chile como en el extranjero.

Contenidos del Programa

- Enumeración y Reconocimiento
- OSINT (Open-Source Intelligence)
- Escaneo de Puertos y Análisis de Trafico
- Análisis de Vulnerabilidades
- Elevación de privilegios y Ataques de Contraseñas
- Metasploit y Post-Explotación
- Ataques al lado del Cliente (Client Side Attacks)
- Pentesting por consola de comandos
- Malware y Botnet
- Ataques a aplicaciones Web
- Bypass de Firewall & IDS/IPS
- Ataques a Redes Wireless
- Explotación de Buffer Overflow en Windows y Linux
- Denegación de Servicio
- Metodología Professional Penetration Tester
- Informe Auditoria de Seguridad

Información general

- Lugar: Apoquindo 4775, oficina 302, Las Condes, Santiago

Incluye

- Kit Alumno Electronico 100% Español
- Manual de Laboratorio 100% Español
- 1 voucher para tomar Examen G|PPT
- Diploma de Asistencia
- 1 Antena Wifi para realizar auditorias

Examen de Certificación

El examen de certificación se realiza en 2 fases, donde primero los alumnos deben pasar un examen con 50 preguntas con múltiples alternativas en 1 hora, la cual se realiza usualmente el ultimo día del curso. Para luego quedar habilitado para tomar el examen practico.

Examen Practico

- El examen practico se realiza conectándose a una red con servidores reales a los cuales se les debe realizar una auditoria de seguridad como se realizaría en un cliente real. El alumno para aprobar debe enviar un informe de auditoria con evidencia del acceso a los servidores. El alumno tiene 24 horas para realizar las pruebas y 24 horas para entregar su informe.

- El ambiente del examen es una replica de una red real con equipos reales como Firewalls, IDS-IPS, WAF, Routers, Multiples Servidores de distintos sistemas operativos y estaciones de trabajo

- Los resultados son revisados por un comité, el cual en 72 horas responderá al alumno para confirmar si aprobó o no su examen.
- El examen de certificación esta 100% en español

Relator

Educación

- Dark-Side Operations: Custom Penetration Testing (BlackHat USA 2015)
- Certificado OPST (OSSTMM Professional Security Tester) ISECOM
- Certificado CEI (EC-Council International Instructor) Único Instructor EC-Council en Chile
- Certificado CEH (Certified Ethical Hacking)
- Certificado CHFI (Computer Hacking Forensic Investigator) EC-Council Solo 9 en Chile
- Certificado ECSP (Certified Secure Programmer)
- Certificado ECSA (Certified Security Analyst)
- Certificado Qualys QCS
- Certificado Auditor Líder ISO 27001

Manuel Moreno
CyberSecurity Partner
CyberTrust

Inspirando confianza en nuestra gente, nuestros clientes y en los mercados

cybertrust
INSPIRANDO CONFIANZA