GPPT®

Professional Penetration Tester

Sabemos que la única forma de aprender es haciendo. Por lo mismo todos los laboratorios son con desafíos de hacking en un ambiente en vivo. Con servidores y servicios dentro de nuestro laboratorio de hacking, para que nuestros alumnos tengan una experiencia real.

100% Laboratorio en vivo

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.

GPPT® es un entrenamiento intensivo de hacking y metodologías de seguridad informática.
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.

En el laboratorio podrá obtener un profundo conocimiento de las nuevas técnicas, herramientas y metodologías. Comenzando por explorar el perímetro, descubrir servicios, puertos, direcciones IP y vulnerabilidades asociadas. Escalar privilegios, realizar ataques sobre servidores reales. Por supuesto ninguna red real es atacada, pues nuestro laboratorio esta cerrado únicamente para los alumnos del entrenamiento.
Usted también aprenderá como realizar bypass de Firewalls, sistemas de detección de intrusos (IDS/IPS), como realizar

GPPT® Professional Penetration Tester

bypass de varias soluciones Antivirus, realizar ataques de denegación de servicio (DoS/DDoS), ataques de desbordamiento de buffer (Buffer Overflow), creación de virus e implementación de redes zombies (Botnet).

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.

Acuerdo Legal y NDA

Acuerdo Legal y NDA

GPPT® Professional Penetration Tester es un entrenamiento cuya misión es educar y demostrar las técnicas de hacking solo para propósitos de auditorias de seguridad. Antes de asistir a este entrenamiento se le preguntara por la firma de un acuerdo legal donde los alumnos aceptan no utilizar los nuevos conocimientos adquiridos para propósitos ilegales o ataques maliciosos que puedan comprometer cualquier red o sistema.

No cualquiera puede ser estudiante, los Centros Acreditados de Entrenamiento (ATC) validaran que los postulantes trabajen en compañias legitimas.

Esta es una certificación que reconoce no solo el conocimiento en el uso de técnicas de hacking, sino la practica y experiencia en el mundo real. Siendo un real diferenciador para sus certificados.

AUDIENCIA

Este curso esta dirigido a oficiales de seguridad, auditores, profesionales de seguridad, administradores de sistemas, administradores de redes y cualquier profesional con necesidad de proteger la integridad de su infraestructura tecnológica.

Duración:

5 días de 9AM a 6:30PM (45 horas)

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.

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.

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

"Que el examen sea practico y no teórico, valida toda la certificación"

Abraham Ermann
Auditor Senior, Banco de Chile.

GPPT®

Professional Penetration Tester consiste en 16 módulos base diseñados para obtener una profunda inmersión en Hacking ético y Pentesting.

MÓDULOS G|PPT

- 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

Estado del Arte...

Cada modulo incluye las ultimas técnicas y ataques conocidos, los cuales están diseñados por expertos auditores, ethical hackers y pentesters con mas de 15 años de experiencia.

GPPT®
Professional Penetration Tester

No es solo lo que pueda aprender durante el entrenamiento, sino todo lo que puede hacer. El manual del laboratorio G|PPT® lo guiara paso a paso por técnicas avanzadas de hacking.

¿Qué es lo que aprenderé?

Los alumnos por medio de este entrenamiento intensivo aprenderán los siguientes tópicos:

- Identificación de objetivos, servidores, equipos perimetrales, incluyendo varias formas de identificación de servicios
- Técnicas de escaneo de redes avanzadas, de bypass de firewalls e IDS/IPS
- Búsqueda avanzada de información vía OSINT/Metadatos
- 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 los antivirus con técnicas avanzadas con veil-framework junto a metasploit
- Ataques Client-Side! contra browsers como Internet Explorer, Firefox y Google Chrome para tomar control de equipos cliente con Windows 7 o Windows 8

GPPT® Professional Penetration Tester

- Aprenderá técnicas de hacking "de la vieja escuela" por línea de comandos. Aprenderá comandos de administración de Linux y Windows que podrás usar en auditorias reales

- Como crear virus y malware. Desde algo que desarrollado en clase hasta una red botnet avanzada
  con centro de administración y control (C&C)

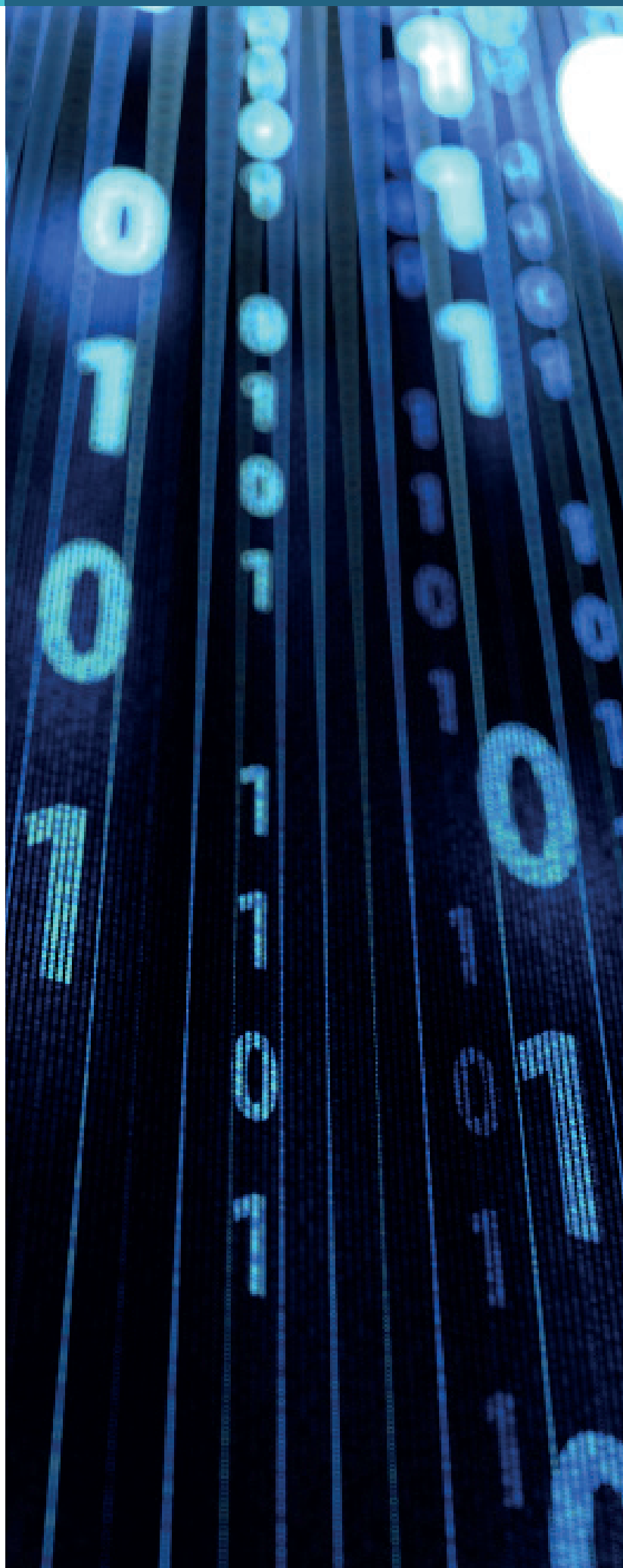
- Auditoria a sitios web donde se iniciara con lo básico de detección de fallos e inyecciones de SQL a Cross-Site Scripting (XSS) hasta como enumerar base de datos por consola a tomar control completo de un servidor Web

- Técnicas avanzadas de bypass de Firewall y sistema de detección de intrusos (IDS/IPS)

- Ataques a redes Wireless donde no solo aprenderá a romper WEP y WPA/WPA2, sino también a crear un dispositivo de ataques wireless a clientes como estaciones de trabajo y smartphones.
- Detección y explotación avanzada de desbordamiento de buffer (Buffer Overflow)
- Ataques de denegación de servicio. Botar una red completa con 1 solo computador y ataques distribuidos (DDoS)

- La metodología G|PPT® esta basado en OSSTMM y OWASP en la cual podrá tener una metodología confiable e internacional para realizar futuras auditorias en clientes.

- Creación de informes de auditoria para clientes. Le entregamos a los alumnos un formato que podrá usar en sus auditorias con clientes



GPPT®
Professional Penetration Tester

GPPT®
Professional Penetration Tester

INCLUYE

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

GLOBALSECURE
ACADEMY