Certified Professional Ethical Hacker

Código: CPEH-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas

PEH es desarrollado por manos expertas en metodologías de Prueba de Penetración utilizadas por un grupo de consultores en vulnerabilidades internacionales.

El curso PEH presenta información sobre las últimas vulnerabilidades y defensas. Este curso también reafirma las habilidades de negocio necesarias para identificar oportunidades de protección, justificar actividades de pruebas y optimizar los controles de seguridad apropiados para las necesidades de cada negocio, con la finalidad de reducir riesgos de negocio. Nuestros cursos van más allá de simplemente enseñar a “Hackear”. Nuestros cursos son desarrollados basándose en principios y metodología usados por hackers maliciosos, pero enfocados en pruebas de penetración profesional y asegurando los activos de información.

Este es un curso intensivo con metodología “hands on” que se enfoca en el modelo de Pruebas de Penetración. En él encontrará las herramientas y métodos más recientes para Pruebas de Penetración. Los laboratorios cambian semanalmente conforme nuevos métodos aparecen. Utilizará muchas y variadas herramientas GUI para línea de comando. Como el trabajo es a través de estructuras de ataque, cubrimos herramientas de sistemas Windows y Linux

AUDIENCIA

Este curso está dirigido a:

- Propietarios de sistemas de información.
- Oficiales de seguridad.
- Ethical Hackers.
- Propietarios de información.
- Probadores de penetración.
- Propietarios y administradores del sistema.
- Ingenieros de seguridad cibernética.

PRE REQUISITOS

- Un mínimo de 12 meses de experiencia en tecnologías de red.
- Buen conocimiento de TCP/IP.
- Conocimiento en hardware.

- Conocimiento de paquetería Microsoft.
- Network+, Microsoft Security+.
- Conocimiento deseable en Linux, no es indispensable.

OBJETIVOS

- Los estudiantes que tomen el curso Certified Professional Ethical Hacker habrán obtenido conocimiento real del mundo de la seguridad que los hará capaces de reconocer vulnerabilidades, exponer debilidades de sistemas y ayudar a protegerlos de las amenazas.
- Los estudiantes aprenderán el arte del Hackeo Ético, pero con enfoque profesional (Penetration Testing). Una vez completado, el estudiante será capaz de tomar el examen CPEH de manera competente.

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.
- El curso lo prepara para la certificación internacional **Mile2 c)PEH**.

CONTENIDO

1. FUNDAMENTOS DE SEGURIDAD Y CONTROLES DE ACCESO

1.1. INFORMACIÓN GENERAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN
1.2. AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN Y VECTORES DE ATAQUE
1.3. CONCEPTOS DE HACKING
1.4. CONCEPTOS DE HACKING ÉTICO
1.5. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN
1.6. CONCEPTOS DE PRUEBAS DE PENETRACIÓN
1.7. LEYES Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

2. PROTOCOLOS

2.1. PROTOCOLOS DE DIRECCIONAMIENTO
2.2. PROTOCOLOS DE DIRECCIONAMIENTO INTERIOR Y EXTERIOR
2.3. PROTOCOLO DE PASARELA DE FRONTERAS (BGP)
2.4. IP VERSIÓN 6
2.5. CAMPOS DE CABECERA TCP Y ESTABLECIMIENTO DE CONEXIÓN
2.6. DIRECCIONAMIENTO IP Y DIRECCIONAMIENTO
2.7. SUBREDES IP
2.8. NÚMEROS DE TCP, UDP Y PUERTO
2.9. GUÍA PRÁCTICA DE DIRECCIONAMIENTO

3. CRIPTOGRAFÍA

3.1. CONCEPTOS DE CRIPTOGRAFÍA
3.2. ALGORITMOS DE CIFRADO
3.3. HERRAMIENTAS DE CRIPTOGRAFÍA

3.4. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
3.5. CIFRADO DE CORREO ELECTRÓNICO
3.6. CIFRADO DE DISCO
3.7. CRIPTOANÁLISIS
3.8. CONTRAMEDIDAS

4. POR QUÉ EVALUACIONES DE VULNERABILIDAD

4.1. CONCEPTOS DE EXPLORACIÓN DE VULNERABILIDADES
4.2. TIPOS DE VULNERABILIDADES EN SITIOS WEB
4.3. BYPASS DE AUTENTICACIÓN DE INYECCIÓN DE SQL
4.4. ERROR DE INYECCIÓN DE SQL BASADO
4.5. SQLMAP
4.6. SCRIPT ENTRE SITIOS
4.7. VULNERABILIDAD DE CARGA DE ARCHIVOS

5. HERRAMIENTAS DE HERRAMIENTAS DE ANÁLISIS DE RED

5.1. INTRODUCCIÓN A LA HERRAMIENTA NMAP
5.2. EXPLORACIÓN DE PUERTOS
5.3. USO DE SCRIPTS EN NMAP
5.4. ANÁLISIS DE RED UTILIZANDO WIRESHARK
5.5. HERRAMIENTAS DE ANÁLISIS DE RED- CASOS PRÁCTICOS

6. ANÁLISIS DE RESULTADOS E INFORMES

6.1. ¿QUÉ ES LA RECOPILACIÓN DE INFORMACIÓN?
6.2. DESCARGA DE SITIOS CON HTTRACK
6.3. DETECCIÓN DE PUERTOS
6.4. DETECCIÓN DE SUBDOMINIOS
6.5. DETECCIÓN DE SUBDOMINIOS ONLINE
6.6. ANÁLISIS DE CONSULTAS WHOIS
6.7. REVERSE IP LOOKUP

7. RECONOCIMIENTO, ENUMERACIÓN Y ESCANEADO

7.1. CONCEPTOS DE ENUMERACIÓN
7.2. TÉCNICAS DE OSINT Y ENUMERACIÓN PASIVA
7.3. ESCÁNERES DE PUERTOS
7.4. BARRIDO DE PING
7.5. ESCÁNERES ICMP (PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET)
7.6. BÚSQUEDA DE METADATOS EN DOCUMENTOS PÚBLICOS
7.7. ENUMERACIÓN PASIVA A TRAVÉS DE COMMAND LINE INTERFAZ (CLI)
7.8. BUSCADORES IOT (SHODAN)
7.9. HERRAMIENTAS ALL IN ONE PARA LA AUTOMATIZACIÓN
7.10. EL MUNDO DE LAS APIS PARA LA AUTOMATIZACIÓN
7.11. DESCRIPCIÓN GENERAL DE ESCANEO DE RED

7.12. ANALIZAR EN BUSCA DE VULNERABILIDAD

8. PENTESTING

8.1. ¿QUÉ ES Y QUÉ NO ES UNA PENTESTING?
8.2. TIPOS DE PENTESTING. FASE PRE-ATAQUE
8.3. PRÁCTICA: BUSCANDO SECRETOS EN REPOSITORIOS GIT
8.4. INTRODUCCIÓN AL ESCANEO DE REDES
8.5. PRÁCTICA: ESCANEO DE REDES CON NMAP
8.6. FASE DE ATAQUE. TESTING DE APLICACIONES WEB CON BURP SUITE
8.7. PRÁCTICA: EXPLOTANDO VULNERABILIDADES EN METASPLOITABLE
8.8. FASE POST - ATAQUE. METODOLOGÍAS

9. MANTENER EL ACCESO

9.1. BACKDOOR (PUERTAS TRASERAS)
9.2. TROJANS (TROYANOS)
9.3. SHELL O SHELL INVERSA
9.4. CUENTAS DE ALTOS PRIVILEGIOS COMO CUENTAS DE ADMINISTRADOR O DE SYSTEM
9.5. TUNNELING, ROOTKITS, KEYLOGGERS, SPYWARE

10. ATAQUES DE SEGURIDAD DE INFORMACIÓN

10.1. CRAQUEO DE CONTRASEÑA
10.2. ATAQUE DE PHISHING
10.3. MALWARE
10.4. ESTEGANOGRAFÍA
10.5. BIOMETRÍA
10.6. ATAQUES BASADOS EN RED
10.7. SEGURIDAD DE DNS Y CORREO ELECTRÓNICO

11. MALWARE

11.1. MALWARE Y ANÁLISIS ESTÁTICO DE MALWARE
11.2. MALWARE Y ANÁLISIS DINÁMICO DE MALWARE
11.3. SNIFFING Y CÓMO REALIZAR UN ATAQUE MAN IN THE MIDDLE AUTOMÁTICO
11.4. SNIFFING Y CÓMO REALIZAR UN ATAQUE MAN IN THE MIDDLE MANUAL
11.5. DENEGACIÓN DE SERVICIO. ATAQUE DOS CON LOIC Y HOIC
11.6. INGENIERÍA SOCIAL

12. DESBORDAMIENTO DE BÚFER

12.1. ¿QUÉ ES UN DESBORDAMIENTO DE BUFFER?
12.2. TIPOS Y CAUSAS
12.3. LENGUAJES DE PROGRAMACIÓN MÁS VULNERABLES
12.4. ¿QUÉ SUCEDE CUANDO SE PRODUCE?
12.5. EJECUCIÓN DE CÓDIGO ARBITRARIO Y ESCALADA DE PRIVILEGIOS
12.6. DENEGACIÓN DE SERVICIO (DOS)

17.1. PRINICIPALES TIPOS DE ATAQUE DOS

17.2. ATAQUE DE INUNDACIÓN DE BUFFER (BUFFER OVERFLOW)

17.3. ATAQUE DE INUNDACIÓN DE SYN (SYN FLOOD)

17.4. ATAQUE TEARDROP

17.5. ATAQUE DE INUNDACIÓN ICMP

17.6. ATAQUE SMURF

17.7. CONTRAMEDIDAS

BENEFICIOS

- Al finalizar el curso, el estudiante podrá demostrar sus conocimientos adquiridos en el examen de certificación internacional **Certified Profesional Ethical Hacker**.