TEMARIO

ETHICAL HACKING

ETHICAL HACKING

DURACIÓN DEL CURSO

30 HRS

Informes: Telf. (01) 640-5805 | Av. Arenales N° 1912 Of. 805 - Lince

AULATEC

FORMACIÓN Y DESARROLLO PROFESIONAL EN T.I.

ETHICAL HACKING

AULATEC
FORMACIÓN Y DESARROLLO PROFESIONAL EN T.I.

MODULO 1 – INTRODUCCION AL ETHICAL HACKING

1. Introducción al Ethical Hacking, Tendencias Actuales. Dónde Apuntan los ataques hoy, Riesgos y Componentes Asociados. Nuevos Riesgos
2. Metodologías de Penetration Testing - Ethical Hacking, Introducción a OSSTM, OWASP, CVSS.
3. Como platear un proyecto y/o servicio de Ethical Hacking, documentación y formatos requeridos.

MODULO 2 – ETHICAL HACKING NETWORKING

1. Footprint y reconocimiento con Google Hacking e Interrogación DNS
2. Escaneo de red redes con Nmap
3. Enumeración de servicios
4. Ataques de password craking a servicios
5. CTF 1: Obteniendo información del objetivo

MODULO 3 - EXPLOITS Y VULNERABILIDADES

1. Trabajando con exploits
2. Introducción a Metasploit como framework de ataque
3. Ataques a sistemas operativos Windows
4. Ataques del lado Cliente
5. Creando ejecutables infectados (Virus), para conseguir control de Windows.

MODULO 4 – ESCANEO DE VULNERABILIDADES

1. Instalación y personalización de Nessus
2. Escaneo de Vulnerabilidades avanzada con Nessus a nivel de Plataforma y aplicaciones
3. Entendiendo reportes de Nesuss, detección de falsos positivos y falsos negativos
4. CTF 2: Detectando y explotando vulnerabilidades de un servidor

MODULO 5 - ETHICAL HACKING A APLICACIONES WEB

1. Introductorio a vulnerabilidades web
2. Uso de proxys de interceptación Burp Suite, ZAP Proxy
3. Explotando vulnerabilidades, en PHP y .NET ASP
4. Ataques a servidores Web con Sql Inyection
5. Explotando vulnerabilidades XSS, LFI, RFI, Upload, SQLI POST, Evacion de Login, HTML inyection, Ataques de fuerza bruta contra formularios de autenticacion, Acceso inseguro de objetos.
6. Ataques de robo de sesión o session hijacking
7. Haciendo un defacement (defaceo) de una página web

MODULO 6 - ETHICAL HACKING DE API, SERVICIOS WEB Y MICROSERVICIOS

1. Introductorio a los servicios web, SOAP, REST
2. Ataques contra servicios web SOAP, SQL Inyection, WSDL Scanning, Web Service SAX Injection.
3. Ataques contra API REST, divulgacion de información, Roptura de acceso, Inyecciones de SQL, debilidad en token JSON, Mongo inyection, API google Hacking.
4. Ataques contra microservicios en contenedores Docker

MODULO 7 - ETHICAL HACKING A APLICACIONES MOVILE

1. Introductorio a las aplicaciones Moviles en Andrioid y iOS
2. Instalación de emulador para aplicaciones Android
3. Análisis, descarga y descompresión de APK
4. Crear archivos .java y analisis de métodos de la aplicación
5. Análisis de dexfiles
6. Capturar credenciales mediante log de la aplicación
7. Análisis de bases de datos SQLITE
8. Análisis de almacenamiento externo
9. Ataques de inyeccion de SQL
10. Captura de paquetes con ZAP Proxy
11. Análisis dinámico de aplicaciones móviles con Frida
12. Envenenamiento de aplicaciones móviles con Metasploit