TEMARIO DEL CURSO

Ethical Hacking – preparación para el examen CEH (v12)

40 horas

Hacker Ético, proporciona un conocimiento profundo de las fases del hacking ético, los diversos vectores de ataque y las contramedidas preventivas.

A QUIÉN VA DIRIGIDO

- Técnicos de seguridad informática que deseen certificarse para demostrar sus habilidades en hacking ético.
- Nextraining cuenta con instructores certificados, cada uno en su área

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.
Introducción al hacking ético

- Cubre los fundamentos de los temas clave en el mundo de la seguridad de la información, incluyendo los fundamentos del hacking ético, los controles de seguridad de la información, las leyes pertinentes y los procedimientos estándar.

MÓDULO 02.
Huellas y reconocimiento

- Aprenda a utilizar las últimas técnicas y herramientas para llevar a cabo la detección de huellas y el reconocimiento, una fase crítica previa al ataque del proceso de hacking ético.

MÓDULO 03.
Escaneo de redes

- Cubra los fundamentos de los temas clave en el mundo de la seguridad de la información, incluyendo los fundamentos del hacking ético, los controles de seguridad de la información, las leyes pertinentes y los procedimientos estándar.

MÓDULO 04.
Enumeración

- Aprenda varias técnicas de enumeración, como los exploits del Border Gateway Protocol (BGP) y de Network File Sharing (NFS), y las contramedidas asociadas.

MÓDULO 05. **Análisis de vulnerabilidad**	• Aprenda a identificar las brechas de seguridad en la red, la infraestructura de comunicaciones y los sistemas finales de una organización objetivo.
MÓDULO 06. **Hacking de sistemas**	• Conozca las distintas metodologías de hacking de sistemas -incluyendo la esteganografía, los ataques de esteganización y la cobertura de pistas- utilizadas para descubrir las vulnerabilidades del sistema y de la red.
MÓDULO 07. **Amenazas de malware**	• Obtenga una introducción a los diferentes tipos de malware, como troyanos, virus y gusanos, así como la auditoría del sistema para los ataques de malware, el análisis de malware y las contramedidas.
MÓDULO 08. **Sniffing**	• Conozca las técnicas de sniffing de paquetes y cómo utilizarlas para descubrir las vulnerabilidades de la red, así como las contramedidas para defenderse de los ataques de sniffing.
MÓDULO 09. **Ingeniería social**	• Aprenda conceptos y técnicas de ingeniería social, incluyendo cómo identificar intentos de robo, auditar vulnerabilidades a nivel humano y sugerir contramedidas de ingeniería social.
MÓDULO 10. **Denegación de servicio**	• Conozca las diferentes técnicas de ataque de denegación de servicio (DoS) y de denegación de servicio distribuida (DDoS), así como las herramientas utilizadas para auditar un objetivo y diseñar contramedidas y protecciones de DoS y DDoS.
MÓDULO 11. **Secuestro de sesión**	• Comprender las diversas técnicas de secuestro de sesiones utilizadas para descubrir las debilidades de la gestión de sesiones a nivel de red, la autenticación, la autorización y la criptografía, así como las contramedidas asociadas.
MÓDULO 12. **Evadir IDS, Firewalls y Honeypots**	• Conozca las técnicas de evasión de cortafuegos, sistemas de detección de intrusos y honeypots; las herramientas utilizadas para auditar el perímetro de una red en busca de debilidades; y las contramedidas.
MÓDULO 13. **Hackear servidores web**	• Aprenda sobre los ataques a servidores web, incluyendo una metodología de ataque completa utilizada para auditar las vulnerabilidades en las infraestructuras de los servidores web y las contramedidas.

MÓDULO 14.
Hackear aplicaciones web

- Aprenda sobre los ataques a aplicaciones web, incluyendo una metodología completa de hackeo de aplicaciones web utilizada para auditar las vulnerabilidades en las aplicaciones web y las contramedidas.

MÓDULO 15.
Inyección SQL

- Conozca las técnicas de ataque de inyección SQL, las herramientas de detección de inyecciones y las contramedidas para detectar y defenderse de los intentos de inyección SQL.

MÓDULO 16.
Hacking de redes inalámbricas

- Conozca el cifrado inalámbrico, las metodologías y herramientas de pirateo inalámbrico y las herramientas de seguridad Wi-Fi.

MÓDULO 17.
Hackear plataformas móviles

- Conozca los vectores de ataque de las plataformas móviles, los exploits de vulnerabilidad de Android y las directrices y herramientas de seguridad para móviles.

MÓDULO 18.
Hacking de IoT y OT

- Conozca las técnicas de sniffing de paquetes y cómo utilizarlas para descubrir las vulnerabilidades de la red, así como las contramedidas para defenderse de los ataques de sniffing.

MÓDULO 19.
Computación en la nube

- Aprenda diferentes conceptos de computación en la nube, como las tecnologías de contenedores y la computación sin servidores, varias amenazas y ataques basados en la nube, y técnicas y herramientas de seguridad en la nube.

MÓDULO 20.
Criptografía

- En el último módulo, aprenda sobre criptografía y cifrado, infraestructura de clave pública, ataques de criptografía y herramientas de criptoanálisis.