CMHE – Certificado MILE-SEC Hacking Ético

Temario

- Hacking Ético, Pruebas de Penetración, Red Teaming
- Tipos de Hacking Ético y Pruebas de Penetración
- Metodologías Libres
- Infraestructura y Laboratorio de Pruebas
- Reglas del Contrato, Alcance y Reporte
- Reconocimiento
- Consultas Whois y Consultar DNS
- Búsqueda en Sitios Web
- Análisis de Metadatos en Documentos
- Encontrar Vulnerabilidades en Motores de Búsqueda
- Recon-NG
- Reconocimiento con Maltego
- Shodan
- Objetivos y Tipos de Escaneo
- Consejos Generales para el Escaneo
- Sniffing y Trazado de la Red
- Escaneo de Puertos
- Nmap y Soporte para IPv6
- Reconocimiento Activo del Sistema Operativo
- Escaneo de Versión
- Manipular Paquetes con Scapy
- Métodos para Descubrir Vulnerabilidades
- Nmap Scipting Engine
- Nessus Essentials
- Enumerar Usuarios
- Explotación
- Categorías de Exploits
- Metasploit Framework
- Paylodas en Metasploit Framework
- Meterpreter
- Tácticas y Perspectivas para Evadir Antivirus
- Herramientas para la Evasión de Antivirus
- Base de Datos de Metasploit Framework
- Actividades de Explotación Posterior
- Shell de Comandos y. Acceso Terminal
- PowerShell para Hacking Ético
- Acciones utilizando PowerShell
- Consejos para Atacar Contraseñas
- Bloqueo de Cuentas en Windows
- THC-Hydra
- Representación de Contraseñas en Windows
- John The Ripper
- Ataques con Tablas Arco Iris
- Ataques Pass-The-Hash

Presentación

Como profesionales en ciberseguridad, se tiene la responsabilidad de encontrar y entender los riesgos de seguridad existentes en las organizaciones; para posteriormente trabajar de manera diligente en su mitigación; antes de estos riesgos sean aprovechados por los ciberatacantes. Este curso abarca las herramientas, técnicas, y metodologías para realizar pruebas de penetración contra redes y sistemas, preparándolo para realizar etapa por etapa pruebas de penetración y hacking ético. Todas las organizaciones necesitan profesionales experimentados en ciberseguridad, quienes estén en la capacidad de encontrar diversos tipos de vulnerabilidades, para así poder mitigar sus efectos. Este curso está específicamente diseñado desde esta perspectiva, siendo realizado con una gran cantidad de ejemplos y demostraciones prácticas.

CMHE
CERTIFICADO MILE-SEC
HACKING ÉTICO

Objetivos

Este curso está diseñado para enseñar a realizar pruebas de penetración de principio a fin. Exponiendo la manera de realizar un reconocimiento detallado analizado la infraestructura en evaluación, mediante la recopilación de información públicamente disponible, motores de búsqueda, redes sociales, y otras fuentes. Luego se realizan diversos tipos de escaneo en red, utilizando las herramientas más adecuadas y definiendo las mejores configuraciones. Se exponen los principales métodos para explotar los sistemas, para consecuentemente ganar acceso y estar en la capacidad de medir el riesgo real para la organización. También se exponen temas relacionados con la etapa posterior a la explotación y ataques a contraseñas. Todos los ejemplos y demostraciones prácticas se desarrollan en un entorno de laboratorio controlado, utilizando máquinas virtuales diseñadas específicamente para este propósito.