CMKL – Certificado MILE-SEC Kali Linux

Temario

- Configurar un Laboratorio Virtual
- Introducción a Kali Linux
- Bases de Programación y Scripting con Bash y Python
- Utilizando Metasploit Framework
- Payloads y Tipos de Shells
- Configurar Manualmente un Payload
- Utilizar Módulos Auxiliares
- Captura de Información
- Captura OSINT
- Escaneo de Puertos
- Encontrar Vulnerabilidades
- Nessus
- Nmap Scripting Engine NSE
- Módulos para el Escaneo en Metasploit
- Escaneo de Aplicaciones Web y Análisis Manual
- Captura de Tráfico
- Wireshark
- Envenenamiento del Cache ARP
- Envenenamiento del Cache DNS
- Ataques SSL
- Explotación Remota
- Explotación a WebDAV y PhpMyAdmin
- Descargar Archivos Sensibles
- Explotar Aplicaciones Web de Terceros, Servicios Comprometidos, Recursos Compartidos NFS.
- Ataques en Línea de Contraseñas
- Ataques Fuera de Línea de Contraseñas
- Explotación del Lado del Cliente
- Evadiendo Filtros con Payloads de Metasploit
- Ataques para el Lado del Cliente
- Ingeniería Social
- Social Engineer Toolkit SET
- Ataques Web
- Evadir Antivirus
- Como Funcionan los Antivirus
- Evadiendo un Programa Antivirus
- Post Explotación
- Meterpreter
- Scripts de Meterpreter
- Módulos de Post Explotación en Metasploit
- Escalado de Privilegios Locales
- Captura de Información Local
- Movimiento Lateral
- Pivoting
- Persistencia

Presentación

Kali Linux es una distribución basada en el sistema operativo GNU/Linux Debian, diseñada específicamente para realizar auditorias de seguridad y pruebas de penetración avanzadas. Proporciona herramientas, configuraciones, y automatizaciones comunes las cuales permiten centrarse en el trabajo a realizar, y no en la actividad circundante. Kali Linux contiene cientos de herramientas destinadas a las más diversas tareas correspondientes a seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux incluye más de 600 herramientas para pruebas de penetración, es libre, tiene un árbol GIT open source, cumple con FHS, tiene un amplio soporte para dispositivos inalámbricos, incluye un kernel parchado para inyección, es desarrollado en un entorno seguro, sus repositorios y paquetes están firmados con GPG, tiene soporte para múltiples lenguajes, incluye soporte para ARMEL, y ARMHF, además de ser completamente personalizable.

CMKL
CERTIFICADO MILE-SEC
KALI LINUX

Objetivos

Este curso proporciona una gran cantidad de conocimientos para iniciarse en el área del Hacking Ético y Pruebas de Penetración, además de ser una guía práctica para la utilización de las herramientas más populares durante la realización Auditorias de Seguridad, ejercicios de Red Team, y Bug Bounty. Así mismo este curso proporciona conocimientos sobre diversos aspectos de Kali Linux, conceptos sobre programación, metasploit framework, captura de información, búsqueda de vulnerabilidades, técnicas para la captura de tráfico, explotación de vulnerabilidades, técnicas manuales de explotación, ataques a contraseñas, ataques para el lado del cliente, ingeniería social, técnicas para evadir antivirus y técnicas posteriores a la explotación.