C)IHE™
CERTIFIED INCIDENT HANDLING ENGINEER

Certified Incident Handling Engineer™

DATOS CLAVE

Nombre del curso: Certified Incident Handling Engineer

Duración: 5 días

Idioma: Español

Formato: Aula con instructor

Pre-requisitos:

* Un mínimo de 12 meses de experiencia trabajando en tecnología de redes
* Buen conocimiento de TCP/IP
* Conocimiento de paquetería de Microsoft
* Network+, Microsoft, Security+
* Conocimiento básico de Linux

Materiales:

* Cuaderno de Trabajo del Alumno
* Manual de Referencia del Alumno
* Libro de Definiciones y Conceptos Clave de Seguridad

Examen de Certificación:

* CIHE- Certified Incident Handling Engineer™
* GCIH- GIAC Certified Incident Handler™

Track de Certificaciones:

* CIHE- Certified Incident Handling Engineer™
* CPTE - Certified Pen Testing Engineer™
* CPTC - Certified Pen Testing Consultant™
* CDFE - Certified Digital Forensics Examiner™

BENEFICIOS DEL CURSO

Los graduados del curso Certified Incident Handling Engineer de Mile2 obtendrán conocimientos de seguridad mundial que les permita reconocer las vulnerabilidades, explotar las debilidades y ayudar a proteger contra amenazas en los sistemas. Este curso cubre los mismos objetivos que SANS® Security 504 training y prepara al estudiante para las certificaciones GCIH® y CIHE.

DESCRIPCIÓN DEL CURSO

El curso Certified Incident Handling Engineer está diseñado para ayudar a administradores de incidentes, administradores de sistemas e Ingenieros de Seguridad General para entender cómo planificar, crear y utilizar sus sistemas con el fin de prevenir, detectar y responder a los ataques.

En este profundo entrenamiento, los estudiantes aprenderán paso a paso los enfoques utilizados por los hackers a nivel mundial, los últimos vectores de ataque y cómo protegerse contra ellos, procedimientos de gestión de incidentes (incluyendo el desarrollo del proceso de principio a fin y el establecimiento de su equipo de manejo de incidentes), las estrategias para cada tipo de ataque, recuperación de ataques y mucho más.

Además, los estudiantes podrán disfrutar de numerosos ejercicios prácticos de laboratorio que se centran en temas como el reconocimiento y evaluaciones de vulnerabilidad utilizando Nessus, network sniffing, manipulación de aplicaciones web, malware, el uso de Netcast, además de varios escenarios adicionales, tanto para sistemas Windows como Linux.

AL CONCLUIR

Una vez finalizado el curso Certified Incident Handling Engineer, los estudiantes serán capaces de llevar a cabo con seguridad el examen de certificación CIHE (recomendado). Los estudiantes disfrutarán de un curso en profundidad que se actualiza continuamente para mantener e incorporar el cambiante mundo de la seguridad. Este curso ofrece prácticas propias de laboratorio actualizadas al día que han sido investigadas y desarrolladas por líderes profesionales de seguridad de todo el mundo.

CNSS

OBJETIVOS DE LOS ESCENARIOS DE LABORATORIO

Se trata de un curso intensivo de clase práctica centrando la atención en el modelo de prueba Pen, que en lugar de invertir demasiado tiempo instalando 300 herramientas, usted pasará más de 20 horas realizando laboratorios prácticos. Se le enseñarán las herramientas más recientes y los métodos de prueba Pen. Los laboratorios se actualizan semanalmente, en tanto se descubren nuevos métodos. Se utilizarán diferentes herramientas, desde GUI hasta la línea de comando. A medida que trabajamos a través de ataques estructurados, tratamos de cubrir las herramientas actuales, tanto para sistemas Windows como Linux.

DETALLES DE LABORATORIO

- Netcat (Basics of Backdoor Tools)
- Exploiting and Pivoting our Attack
- Creating a Trojan
- Capture FTP Traffic
- ARP Cache Poisoning Basics
- ARP Cache Poisoning - RDP
- Input Manipulation
- Shoveling a Shell
- Virus Total
- Create Malware using SET
- The Trojans
- Examine System Active Processes and Running Services
- Examine Startup Folders
- The Local Registry
- The IOC Finder – Collect
- IOC Finder – Generate Reprot
- Malware Removal

MÓDULOS DEL CURSO

Módulo 1: Introduction
Módulo 2: Threats, Vulnerabilities, and Exploits
Módulo 3: Identification and Initial Response
Módulo 4: RTIR
Módulo 5: Preliminary Response
Módulo 6: Identification and Initial Response
Módulo 7: Sysinternals
Módulo 8: Containment
Módulo 9: Eradication
Módulo 10: Follow-Up
Módulo 11: Recovery
Módulo 12: Virtual Machine Security
Módulo 13: Malware Incident Response