C)IHE™
CERTIFIED INCIDENT HANDLING ENGINEER

mile2®
CYBER SECURITY CERTIFICATIONS

Certified Incident Handling Engineer

DATOS CLAVE

Nombre del curso:

C)IHE

Duración: 5 días

Pre-requisitos:

- Un mínimo de 12 meses de experiencia en redes
- Conocimientos técnicos de TCP/IP
- Conocimiento de software de Microsoft
- Network+, Microsoft, Security+
- Conocimiento básico de Linux es esencial

Materiales:

- Manual de Estudiante
- Manual de referencia
- Libro de definiciones y conceptos clave de seguridad

Examen de Certificación:

- CIHE - Certified Incident Handling Engineer
- GCIH – GIAC Certified Incident Handler

Track de Certificaciones:

- CPTE - Certified Pen Testing Engineer™
- CPTC - Certified Pen Testing Consultant™
- CDFE - Certified Digital Forensics Examiner™

Puntaje de aprobación: 70%

BENEFICIOS DEL CURSO

Los graduados del curso 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 ataques.

En este profundo entrenamiento, los estudiantes aprenderán paso a paso los enfoques utilizados por los hackers a nivel mundial, ls ultimo's 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 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 seran cpaces 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.

C)IHE™ CERTIFIED INCIDENT HANDLING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

Certified Incident Handling Engineer

OBJETIVOS DE LOS ESCENARIOS DE LABORATORIOS

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

C)IHE™ CERTIFIED INCIDENT HANDLING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

Certified Incident Handling Engineer

MÓDULOS DEL CURSO

Module 1: Introduction

Module 2: Threats, Vulnerabilities, and Exploits

Module 3: Identification and Initial Response

Module 4: RTIR **Module 5:** Preliminary Response

Module 6: Identification and Initial Response

Module 7: Sysinternals **Module 8:** Containment

Module 9: Eradication **Module 10:** Follow-Up

Module 11: Recovery

Module 12: Virtual Machine Security

Module 13: Malware Incident Response

Lab 1: Netcat (Basics of Backdoor Tools)
Lab 2: Exploiting and Pivoting our Attack
Lab 3: Creating a Trojan
Lab 4: Capture FTP Traffic
Lab 5: ARP Cache Poisoning Basics
Lab 6: ARP Cache Poisoning - RDP
Lab 7: Input Manipulation
Lab 8: Shoveling a Shell
Lab 9: Virus Total
Lab 10: Create Malware using SET
Lab 11: The Trojans
Lab 12: Examine System Active Processes and Running Services
Lab 13: Examine Startup Folders
Lab 14: The Local Registry
Lab 15: The IOC Finder – Collect
Lab 16: IOC Finder – Generate Report
Lab 17: Malware Removal

Los cursos de Mile2 están acreditados por NSA CNSS 4011-4016, en Homeland's Security National, NICCS training schedule, preferido por el FBI Nivel 1-3.

CNSS · NIST National Institute of Standards and Technology · NICCS NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES · DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION