Certified Incident Handling Engineer

Duration: 5 Days | Language: English

Course Delivery: Classroom

Course Overview

The Certified Incident Handling Engineer vendor neutral certification is designed to help Incident Handlers, System Administrators, and any General Security Engineers understand how to plan, create and utilize their systems in order to prevent, detect and respond to attacks.

In this in-depth training, students will learn step-by-step approaches used by hackers globally, the latest attack vectors and how to safeguard against them, Incident Handling procedures (including developing the process from start to finish and establishing your Incident Handling team), strategies for each type of attack, recovering from attacks and much more.

Furthermore, students will enjoy numerous hands-on laboratory exercises that focus on topics, such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, malware and using Netcat plus several additional scenarios for both Windows and Linux systems.

BENEFITS OF THIS COURSE

Graduates of the mile2 Certified Incident Handling Engineer training obtain real world security knowledge that enables them to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats. This course covers the same objectives as the SANS® Security 504 training and prepares students for the GCIH® and CIHE certifications

Prerequisites:

- A minimum of 12 months' experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Basic Knowledge of Linux is essential

EXAM INFORMATION

The **Certified Incident Handling Engineer** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple-choice questions.

Course Outline

Introduction

Lab Resources

Knowing your way around VMware Player.

Module One - Attacks Under the Microscope

Lab objectives

Wireshark

Why Wireshark?

Running Wireshark

Starting Wireshark

User interface

Filters

Netstat

Command

Options

Examples

Netcat

Cyber Attacks

Understanding the hacking methodology

IP Space Scanning

Port Scanning

Network Based Attacks

Web Application Based Attacks

Host Based Attacks

Module Two - Ticketing System

Introduction

Ticketing System Components

Tickets:

Queues:

System Functionality

System login

Ticket Creation

Ticket Correspondence

Ticket Priority Escalation

Ticket Assignment

Request Tracker for Incident Response - RTIR

Normal user role:

Incident Handling Role:

Viewing unlinked Incident Reports:

Create an Incident

Linking Incident Reports to an incident:

Starting an Investigation

Module Three Lab - SysInternals Suite

Introduction

Getting Sysinternals.

Usage Guide

Process Explorer

Process Monitor

Autoruns

PsTools

Disk Utilities

Security Utilities

Network and Communication utilities.

First Response Lab Scenario

Module Four Lab - Examine System Active Processes and Running Services

Examine Startup Folders

The Local Registry

The IOC Finder – Collect

IOC Finder – Generate Report

Malware Removal

Final Scenario - 4 hour