www.cyber2labs.com
Email: info@cyber2labs.com

Intrusion Analysis and Incident Response

Key Reasons to Attend this Course:

- Learn the fundamentals of intrusions
- Examine network traffic for intrusions
- Develop a systematic process for intrusion analysis
- Explore the artifacts of emerging threat attacks
- Establish an incident response lifecycle
- Create a response template for handling basic to advanced attacks
- Process "live" monitored alerts and assess the enterprise threat
- Extract sophisticated malware information from the latest types of attacks

COURSE DESCRIPTION

At Cyber2 Labs we promote the critical need for all cyber security professionals to establish a solid foundation when learning about cyber security. In today's cyber security workforce environment many will learn the higher application level of the network while neglecting the lower levels. Here at Cyber^2 Labs we feel this is a mistake and have developed this course to help the student truly understand malicious attacks, counter the attacks and design the defense needed to protect the network. The student will understand all layers of a network and most importantly how network traffic looks when it is normal and when it is under an attack.

The first step in developing an effective incident response capability is learning the methods of attack that can be used to compromise systems and networks. In this course you will learn the fundamentals of forensics, and how information can be extracted in a forensically sound manner. The course will show the latest types of attacks, and what to look for when these types of attacks are carried out against the enterprise.

Within the course you will learn the characteristics of a number of attacks, and a process to evaluate these attacks for the possibility of an intrusion. The section on intrusion analysis will show the data that can be scavenged after a variety of different types of attacks. These attacks can be from the most basic type all the way through advanced emerging threat attacks. The systematic process you will not only learn, but also practice in the workshop will allow you to analyze virtually all types of intrusions.

Once you have examined the different intrusion methods you will be introduced to an incident response life cycle, and practice implementing it with "live" events and scenarios from actual computer incidents. Each "live" exercise will have a series of events from firewall logs to users calling the help desk, and your task will be to review the information and then using a defined incident response plan determine what is required to be recorded, reported and the required steps to move forward. The incidents will increase in scope and become more challenging as the workshop progresses.

Who Should Attend This

- Cyber Forensic Investigators
- Incident Response/Handler
- Cyber Analyst
- Incident handlers
- Risk Assessment Administrators
- Penetration Testers
- Venerability Assessment Auditors
- System Administrators
- System Engineers
- Firewall Administrators
- Network Managers
- IT Managers
- IT Professionals

DURATION
2 days (9:00 – 5:00)

CERTIFICATION:
A certification of completion will be provided at the end of the training course.

(The main purpose of the course is to build a security skills foundation and prepare the student for work in security, hacking and penetration testing.)

By the time you leave the course you will have seen a multitude of different attack scenarios, and in the end created your own process for responding to potential incidents to an enterprise network architecture.

Course Outline

Module One:

Introduction to Forensics

- Computer Forensics defines
- Traditional forensics
- "Live" system forensics
- Establishing a Forensic Methodology
- Repeatable process

LAB ONE: Forensic Analysis: What were up against?

Module Two:

Intrusion Analysis

- Intrusion Analysis of Network Traffic on Windows and Linux
- Identifying normal vs abnormal traffic
- Determining cause of abnormal traffic
  - Error
  - Malicious
- Recognizing common patterns of network attacks
- Identifying the OS from the network traffic
- Passive fingerprinting characteristics
- Nuances of the TCP/IP stack

LAB: Analyzing basic attacks

- Components of a sophisticated attack
- Deception techniques
- Protocol camouflage
- Encryption and tunnels
- LAB: Analyzing a sophisticated attack
- Components of advanced attacks
- Protocol encapsulation
  - More than one layer 7
- Web attacks
  - Services
  - SQL
  - XSS
  - Access controls

LAB: Analysis of Web Attacks

Module Three:

Introduction to Incident Response

- Security Policy and its role in incident response
- Introduction and overview of computer forensics and incident response
- Planning for incident response: Developing a plan of action
- Incident response life cycle explained

Incident Response Workshop One

Module Four:

Planning a Response to a potential incident

- Search and seizure laws
- What can and cannot you take
- Laws of digital evidence
    - Hearsay
        - Exceptions to the hearsay law
    - Digital evidence references
        - International Journal of Digital Evidence
        - Chief Police Officers Guide

Module Five:

Processing Windows "LIVE" Forensics information to discover malware

- Analyzing volatile data
    - Network connections
    - Ports
    - Processes
    - Memory of processes
    - Open files and handles
    - Routing tables
    - System memory
- Analyzing non-volatile data
    - System version
    - Time and date stamp
    - Registry data
    - Login history
    - Auditing policy
    - Examining the event viewer
    - Logs and using log parser
        - Using log parser
        - Developing powerful queries
            - Basic
            - Advanced

LAB: Windows "LIVE"

Incident Response Workshop Two

Module Six:

Malware Incident Response

Advanced Windows Forensics: Performing low-level internal analysis to identify advanced memory corruptions

- Windows internals
  - System architecture
  - Memory management
  - Cache management
  - Dumps analysis
  - Tools
    - Filemon
    - Regmon
    - Process explorer
    - Process explode
- Windows rootkits
  - Traditional
  - Trojaned files and processes
    - Hooking
    - Man in the middle attack against the descriptor table
      - DKOM
      - Unlinking processes direct in memory

LAB: Malware Analysis

Incident Response Workshop Three

© 2018 Cyber2Labs. All rights reserved. This document is for
Training Requirements, for questions
Please Contact Cyber2Labs.
HTTP://www.cyber2labs.com

For Informational purposes only. Cyber2Labs MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Cyber2Labs logos are Registered Trademarks or trademarks of Cyber2Labs in the United States and/or other countries.