

IDS OPERATOR SERIES: DETECTING AND MANAGING INTRUSIONS WITH DRAGON

Summary:

By the end of this course, the student will be certified to plan for an IDS deployment, install, configure and manage a Dragon IDS network. The student will also understand how to begin a forensic examination of events, analyze false positives, tune sensors for better performance and alerting, and the basics of incidence response and forensics. As this is a technical class, many of the lessons are delivered in hands-on labs and instructor lead demos. A basic understanding of navigating in a Unix environment is required.

The class ends with a challenging take-home test that is sent back to be graded by the instructor. If passed, the student is presented with a certificate of success.

(Optional) PRE-Day One – Examining Internet Protocols and IDSs

- Review of IP Protocols
- Review of Major Internet Application Protocols
- Analyzing network Traffic with a Sniffer
 - *LAB*
- Comparing IDS to Other Network Security Technologies
- Introduction to the Strengths and Weaknesses of IDS

Day One - Analysis of IDS Technologies and Dragon

- Introductions and Backgrounds
- Survey of Methods for Performing Intrusion Detection
 - Engines for Network-Based Technologies
 - Pattern Matching
 - Protocol Decoding
 - Anomaly
 - Host-Based
 - User-land detection versus kernel-space detection/prevention

- Comparing Host versus Network Intrusion Detection
- Analyzing Dragon's Methodologies for Detecting Intrusions and Comparing it to Other IDSes on the Market
 - Attack and Compromise *DEMO*
- The Dragon System Architecture

Day Two – Installing and Basic Configuration

- Overview of Different Installation Scenarios and Options
 - Design Considerations
- Installing a Multi-Tier Architecture
 - *LAB* installing Dragon's components
- Overview of the Dragon GUI
- Managing the Server
 - *LAB* updating signatures
- Examining the Signature Structure
- Lower-Layer Attacks
 - Introducing the dragon.net file
 - Attacks
 - Obfuscations

Day Three – Attack Analysis

- Exploit Analysis
 - The attack cycle
- Compromise Analysis
 - *LAB*
- Custom Applications in government and enterprises
 - *LAB*
- Dragon Signature Analysis
 - *DEMO*
 - *LAB*
- Event Analysis in the Dragon Real-Time Console
 - *DEMO*
- [False Positive] Attack Analysis
 - *Lab*

Day Four – Tuning and Configuration of Dragon

- Review and Additional Analysis of dragon.net
 - Performance tuning
 - Examination of keywords on performance
 - Detection tuning
 - Examination of Dragon's abilities to compensate for attacker methodologies
 - Fine-tuning
 - Tuning based on scenarios
 - Tuning *LAB*
- Introduction to Incident Response
- Introduction to Incident Analysis and Containment
 - *LAB* Analysis of a possibly compromised machine

Test for Class Certification