

IDS OPERATOR SERIES: INTRUSION ANALYSTS COURSE

Summary:

By the end of this course, the student will be certified in the current threats facing today's networks, know how to identify true signs of trespass, make informed decisions about IDS technologies, and know how to separate fact from fiction in vendor claims. The purpose of this course is to introduce the student to the world of exploits and attack recognition. Unlike other courses which walk the student through a few attack and analysis examples, this course takes a hands-on approach to analyzing current methodologies for exploiting systems in addition to the reasons why these techniques are being employed by attackers. Additionally, we will closely examine the technologies behind IDSes which allow security personal to detect and respond to these events.

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

- 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: Trends in Vulnerabilities, Exploits, and IDSs

- Introduction and Backgrounds
- Vulnerability and Exploit Trends - What You Will be Facing More of as an IDS Analyst and Why
 - The evolution of opportunities available to hackers
 - Evolution of services and protocols being targeted
 - Evolution of methods for accessing data
 - *DEMO*
 - Attacks of enthusiasm
 - Motivations for vulnerability research

- Motivations for target selection
 - Trends in disclosure and dissemination of exploits
 - Threats to attackers
 - The impact of security personnel on attackers
 - *DEMO*
- Survey of Methods for Performing Intrusion Detection
 - Engines for Network-Based Technologies
 - Pattern Matching
 - Protocol Decoding
 - Anomaly
 - Overview of Host-Based IDS/IPS
 - User-land detection versus kernel-space detection/prevention

Day Two: Attack Analysis

- Exploit Analysis
 - The attack cycle
- Compromise Analysis
 - *LAB*
- Custom Applications in Government and Enterprises
 - *LAB*
- IDS Signature Analysis
 - Open vs. Closed
 - Languages
 - *LAB*
- IDS Event Analysis
- [False Positive] Attack Analysis
 - *Lab*

Day Three: Complex Analysis of Exploits and Methods to Avoid Detection

- Layer Two
 - ARP attacks and their impact
 - Network Infrastructure
 - Hijacking
- Layer Three
 - IP attacks
 - Impacts on hosts
 - Fingerprinting
 - IP Obfuscations
 - Formatting

- Overlapping
 - Data Insertion
 - *DEMO*
- Layer Four
 - TCP attacks
 - Impacts on hosts
 - Fingerprinting
 - TCP Obfuscations
 - Overlapping
 - Data Insertion
 - UDP Obfuscations
- Application Layer
 - Application Input Validation
 - *DEMO* SQL Injection
 - Encoding/Decoding
 - *DEMO* HTTP Encoding
 - Examples of application protocol obfuscations
 - Overflows
 - How they work, what they do
 - *DEMO* Samba (or more current)
 - Obfuscations for overflows
 - Compromises
 - Examples of activity to look for
 - *DEMO*

Day Four: Advanced IDS Concepts

- Planning for Deployments
 - Topologies
 - Designs
 - Staff
- Available Products
- Testing
 - Management
 - Forensics/Analysis
 - Reporting
 - Testing Consortiums
- Overview of Legal Issues Relevant to IDS
- Introduction to Incident Response
- Introduction to Incident Analysis and Containment
 - *LAB* Analysis of a possibly compromised machine

Test for Class Certification