ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Cyber Threat Detection and Mitigation

Course Summary

Description

Network Signature Development Understood.

Cyber threats are increasing at an alarming rate every year and the ability for organizations to defend against full-scale, distributed attacks quickly and effectively has become much more difficult. An Intrusion Detection system affords security administrators the ability to automate the process of identifying attacks amongst the thousands of TCP and UDP conversations on their network, provided the IDS signatures are well-written.

Taught by leaders in network defense who work in the computer security industry, this course demonstrates how to defend large scale network infrastructure by building and maintaining intrusion detection systems and mastering advanced signature writing techniques. With Intrusion Detection Systems and trained network security auditors, organizations have a reliable means to prioritize and isolate the most critical threats in real time.

On the fifth day of class, students are given several packet captures containing a variety of scanning and exploitation techniques. They are tasked with identifying the significant elements of the attack and translating them into IDS signatures. Finally, they are tasked with tuning those signatures to reduce false positives and limit excessive events.

Objectives

After taking this course, students will be able to understand:

- IDS Types and Features
- Sensor Placement
- Sensor Configuration
- Signature Writing Basics
- IDS Evasion Techniques
- TCP and UDP Conversation Reassembly
- Signature Tuning
- Sensor Tuning
- Event Filtering and Post Detection Event Analysis
- Attacks on IDS Sensors and Mitigation Techniques

Topics

- Intrusions (Types and Methodologies)
- Common Threats
- Intrusion Detection Systems In Depth
- Introduction to Snort
- Snort Configuration and Variables
- Snort Output
- Output Plugins
- Signature Writing
- Snort Rule Options
- Detect Offset Pointer
- Doe Content Modifiers
- Doe Rule Options
- Snort Packet Header Rule Options
- Pre-Processors
- Post Detection Rules
- Effective Rule Writing
- Perl compatible regular expressions (PCRE)
- Tracking State across Sessions
- Group Exercise
- Student Practical Demonstration

Cyber Threat Detection and Mitigation

Course Summary (cont'd)

Audience

This course is designed for:

- Incident Responders who need to understand and react to IDS alerts
- Network Defenders seeking to automate threat detection
- Security Managers who desire to improve their defensive model
- IDS administrators who wish to improve their signature writing skills
- Security Operations Center Staff seeking to automate traffic analysis
- Penetration Testers looking to reduce their network visibility

Prerequisites

Before taking this course, students should have the following skills and experience:

- A firm understanding of TCP/IP
- Network+ or equivalent knowledge or background
- Both the Network Traffic Analysis course and the Malicious Network Traffic Analysis course are recommended prior to attending.

Duration

Five days