ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Malicious Network Traffic Analysis

Course Summary

Description

Uncover system intrusions by identifying malicious network activity. There are a tremendous amount of network-based attacks taking place and that number is increasing rapidly. You can't defend against these lethal network attacks if you don't know about them or if you've never seen they look like at the packet level. This course teaches you how to analyze, detect, and understand all the network-based attacks that we could find being used today in modern network warfare.

From layer two attacks against network devices through complex botnets and specific application vulnerabilities, this class will give you a glimpse of what these attacks looks like. We even show you how to detect attacks using Flow Analysis if you don't have network packets to perform an analysis or if you only have statistical information at your disposal. We'll use the popular protocol analyzer “Wireshark” and session analysis tool “Netwitness” alongside custom tools developed by Focal Point networking experts to show you how to detect these network attacks and be prepared to handle them.

Using the tools, skills, and methodologies taught in Days 1 through 4 of the class, on Day 5, students will uncover and analyze a multi-part network intrusion. In the intrusion capture file, there will be at least 3 Application Layer attacks, 2 Advanced Communications Methods, and a hacker toolkit to discover. Students will have to prepare a report detailing the attack from start to finish, documenting what things the hacker did and what information was leaked, if any.

Objectives

After taking this course, students will be able to:

- Strategic, Tactical and Operational Analysis
- Situational Awareness
- Current Networking Trends in Malware
- IDS / IPS evasion techniques
- Flow Analysis to help identify malicious behavior
- Coordinated Attacks
- Botnets
- Browser Attacks (Javascript, Obfuscation)
- Drive-By-Downloads
- OSI Layer 2,3,4,5,6,7 Attacks
- Social Engineering and Phishing Attacks
- Tunneling and Advanced Tunneling

Topics

- What Constitutes Malicious Traffic
- Network Attack Lifecycle
- OSI Layer Attacks
- Targeted Attack vs. Large Scale Attack
- Network Intrusion Analysis Process
- Analytical Tools of the Trade
- Beginning Phase of Attacks - Recon
- NMAP Port Scans
- Afternoon Labs
- Vulnerability Discovery Phase
- User Layer Attacks
- Application Layer Attacks
- Presentation Layer Attacks
- Session Layer Attacks
- Transport Layer Attacks
- Network Layer Attacks
- Data Link Layer Attacks
- Physical Layer Attacks
- Botnet History and Evolution
- Botnet Architectures and Design
- Malicious Uses
- Botnet Communications
- Bot Evasion and Concealment
- Identification Challenges
- Fast Flux Service Network
- Double Flux Services
- Analysis Techniques
- Black Energy Walkthrough
- Zeus Walkthrough
- Covert Communication Methods
- Network Layer Tunneling
- Transport Layer Tunneling
- Application Layer Tunneling
- Traffic Cloaking
- Student Practical Demonstration

Malicious Network Traffic Analysis

Course Summary (cont'd)

Audience

This course is designed for:

- Threat operation analysts seeking a better understanding of network-based malware and attacks
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious network attacks
- Individuals who want to learn what malicious network activity looks like and how to identify it

Prerequisites

Before taking this course, students should have:

- Knowledge of IPv4 networking protocols is required
- Skills and experience with Wireshark display filtering is required
- Knowledge of RSA Netwitness is recommended
- Attending students should have a thorough understanding of Microsoft Windows
- Python scripting abilities would be beneficial
- CompTIA's Network+ and Security+ certifications would be beneficial but not required

Duration

Five days