ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Advanced Network Traffic Analysis

Course Summary

Description

Advanced Network Traffic Analysis will teach students to solve complex challenges in performing traffic analysis. The course focuses on creating baselines, identifying anomalies, and automating analytic processes.

Objectives

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

- Passive Network Reconstruction
- Network Baselines
- Netflow
- Regular Expressions
- Dissector Creation
- TShark
- Python for Network Analysts

Topics

- Automated Research Tools & Advanced Network Concepts
- Automating Analysis with Python
- Blue Team Exercises
- Purple/ HUNT Team Exercises
- Student Practical Demonstration

Audience

This course is designed for security analysts, network security engineers, security managers, information security officers, incident response analysts, and network administrators.

Prerequisites

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

- Knowledge of IPv4 networking protocols is required
- Skill and experience with Wireshark display filtering is required
- Thorough understanding of Microsoft Windows
- Python scripting abilities would be beneficial
- The Network Traffic Analysis course and the Python for Network Defenders course are required prior to attendance.

Duration

Five days

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

... to Your Success!"

Advanced Network Traffic Analysis

Course Outline

I. Automated Research Tools & Advanced Network Concepts
- A. Automated Open Source Research
- B. Maltese, P0F, The Harvester
- C. Advanced Network Concepts
- D. Load Balancing
- E. Network Address Translation
- F. Virtual IP's
- G. Traffic Shaping:
- H. Proxies, VPNs and Tunneling
- I. Afternoon Labs

II. Automating Analysis with Python
- A. Pyreshark Custom Dissectors
- B. Dissector Basics
- C. Data Decoding
- D. Writing Custom Dissectors
- E. SCAPY Basics
- F. Packet Crafting
- G. Custom PCAP Analysis

III. Blue Team Exercises
- A. Advanced Network Mapping
- B. Network Topology Analysis
- C. Securing Networks through Topology Hardening
- D. Large PCAP Analysis
- E. Blue Team Labs

IV. Purple/ HUNT Team Exercises
- A. Network Incident Handling and Reporting
- B. Identifying and Correcting Inaccurate Topology Maps
- C. Botnet Hunting
- D. Creating Dissectors for Botnet Traffic
- E. Discovering Network and Host Compromise
- F. Signs of DNS Highjacking
- G. Identifying Phishing and other Social Engineering Streams
- H. Isolating Network Intrusion Traffic

V. Student Practical Demonstration

Using the tools, skills, and methodologies taught in Days 1 through 4 of the class, students will uncover a multi-part network intrusion. Students will compete in a team-based culmination exercise using their custom scripts and dissectors as well as the advanced skills they learned in class to accurately identify, document, and extract unwanted activities on a network.