

Art of Exploitation: Wiretap Edition



Developing Tomorrow's Security Experts Today.

In continuing our successful effort of providing the best training solution in the area of Computer Network Operations (CNO) and in the field of Network Analysis, TCS Cyber Intelligence Group has developed the "Art of Exploitation Wiretap Edition" curriculum.

The Wiretap Edition follows a methodology for performing network analysis that begins with deploying a sensor and progresses to generating reports. This course is designed heavily with a hands-on practical application to both reinforce the material discussed and evaluate the competency the student has gained from the discussions.

Every technique or process discussed in this course has an associated lab where students will apply what they have learned.

Modules

- Introduction
- Overview
- Anatomy of a Packet
- Post Processing
- Analysis
- Capstone Exercise

Module Descriptions: Wiretap Edition

Suggested Prerequisite Knowledge

- Linux command line experience
- understanding of TCP/IP

Your Established Partner

TCS is a leading provider of software and solutions to customers who require high reliability and security. TCS delivers premier IT and wireless communications solutions to automotive telematics vendors, leading wireless and VoIP carriers around the world, cable MSOs, and US government agencies.

TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401 USA

Toll Free: 1.888.728.8797
Outside US: +1.410.263.7616
www.telecomsys.com

TCS Cyber Intelligence Group - Main Office
1333 Ashton Road
Hanover, MD 21076-3120
phone: 866.356.3535

©2011 TeleCommunications Systems (TCS). All rights reserved. Enabling Convergent Technologies® is a registered trademark of TCS. All other trademarks are the property of their respective companies. Information subject to change without notice. NasdaqGM: TSYS | 100122



Overview

This module will attempt to answer the questions, "Why are we capturing packets?" and "What tools should I use?" We will spend time discussing the types of information an analyst can or cannot obtain from a capture. We will discuss how your mission can affect the what, why, and how of performing packet capturing. We will demonstrate how to determine the best location for your sensor or tap, discuss, and demonstrate various capture tools to include (but not limited to) TCPdump, Wireshark, Tshark, and Snoop. The student will have ample opportunity to develop a capture strategy then configure, install, and deploy a packet-capturing tool. To understand what is truly anomalous, you must first understand what is common. Determining what is common can be achieved through baselining. Module 1 discusses and demonstrates techniques and strategies to perform baselining. Length is approximately 3 hours and includes 3 labs and 1 group exercise.

Anatomy of a Packet

Module 2 covers TCP/IP packet structure. We will completely dissect packets and discuss all the fields and layers as the packet moves up the OSI model. The student will be able to identify the components of a packet both through raw packet captures and hex dumps. Length is approximately 5 hours and includes 7 labs.

Post Processing

Module 3 discusses processing of a packet capture before analysis. These are the methods, tools, and techniques that will be used to narrow the scope or help the analyst find that "needle in the haystack." We will use Snort to generate events, or tipplers, to give the analyst a starting point for further investigation. An overview of Snort and Snort configuration will take place and the student will configure their own version of Snort to generate custom events. We will utilize TCPdump to perform filtering to allow the analyst to isolate the session or communication of interest. We will start the mapping process in this section by loading the capture into a mapping utility and the generated map will be refined and polished in Module 4. Wireshark and Sguil will be used to generate statistics and flow graphs from our capture and we will discuss the cycle of analysis and how the analyst will need to go back and refine their packet capture strategy based off information gained during the

post-processing phase. Length is approximately 8 hours and includes 8 labs.

Analysis

Module 4 is the analysis module and will attempt to "identify what you don't know" and "tie it all together." This module will teach the analyst how to logically and efficiently follow the event from tipper to report. We will discuss and demonstrate how to identify unknown protocols, malformed packets, and malicious intent (intrusions, scans, and malware). The analyst will be taught how to use tools such as Chaosreader and Bro to recreate sessions enabling them to extract binaries and establish intent of communications. The analyst will be shown how to "tie it all together" by correlating events and applying the tools and techniques from previous modules to differentiate between reportable and normal activity. Length is approximately 8 hours and includes 10 labs.

Capstone

The capstone exercise requires the analyst to use the tools and techniques demonstrated during the course. The student will be provided with all the discussed tools and a large capture file. The lab will ask the student to provide as much detail about the activities taking place in the capture to include a detailed network map, network statistics, protocol identification, malicious content, malware, incident reports, and any custom signatures developed during analysis. Length is approximately 8 hours.