Network Intrusion Analysis (Hands on)

TCP/IP protocol suite is the core of the Internet and it is vital to understand how it works together, its strengths and weaknesses and how it can be used to detect and analyze malicious traffic used to bypass your organization's security infrastructure.

To better understand this complex suite of protocols, IPSS has developed a course that walks the student through TCP/IP and also provides hands on exercises to help understand how TCP/IP suite of protocols and services interact together. This is done using real and simulated traffic of actual attacks and exploits used to compromise a host or network.

This course address some of the Government of Canada Operational Security Standard: Management Information Technology Security (MITS)[1] specifically items 15, 16.4.2, 16.4.6, 16.4.11, 17 and 18.

Course Objectives

The purpose of this course is to help IT professionals develop an in-depth understanding of TCP/IP. The course was put together to take the student from the basics of networking to the more complex inner working of TCP/IP, including;

1. A detailed understanding of IPv4 headers and traffic structure;
2. Introduction to IPv6;
3. Analyze and profile benign and malicious traffic through hands-on exercises;
4. Learn how to use tcpdump/windump and write libpcap filters to view and extract information;
5. Learn how to do network traffic forensics including how to use Wireshark to carve files from data collected in pcap files;
6. Basic malware analysis using some simple tools;
7. Learn how to install, configure and write signatures for Snort IDS using the Snort IDS with Sguil freeware sensor from http://handlers.dshield.org/gbruneau/
8. Learn to use the various tools built-in Sguil (sancp network profiler, p0f, tcpflow, httpry, PADS, Wireshark) to analyze suspicious traffic.
9. Several hand-on exercises to gain a better understanding of the material

This course uses a combination of theory and appropriate hands-on technical exercises. PC's and software are provided for each student.

[1] http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

A sample of the course content is provided below:

Understanding TCP/IP

i. IPv4 and IPv6 TCP/IP Overview

- Understanding Binary, Decimal and Hexadecimal number systems (with exercises)
- What is IPv4 and IPv6 as it relate to TCP/IP?
- Internet Protocol Functions
- OSI Model
- Detailed understanding of IP
- An in-depth look at IP, TCP, UDP, and ICMP
- Sample outputs of each protocols using tcpdump examples
- Exercises: Using tcpdump/windump to reinforce material

Profiling and Analysis of Malicious Activity

i. Using various Network Traffic Forensic Analysis Tools and Techniques

- tcpdump and ngrep basics
- Understanding tcpdump and ngrep options
- tcpdump and ngrep examples
- Berkley Packet Filters and examples (BPF)
- Carving files from pcap
    - Carving emails attachments
    - Files transfer from site/server download
    - Files type analysis

ii. Profiling traffic

- Attacker methodology
- Reconnaissance and scanning
- Identifying Malicious code
- Defenses and countermeasures
- Computer attack examples
- Using Netflow to monitor traffic and services
- Exploits;
    - DOS
    - DDOS
    - Buffer Overflow
    - SQL Injection
    - Rootkits

iii. Introduction to DNS Sinkhole

- Teach the basic theory on DNS Sinkhole
- Learn how a DNS Sinkhole can be used to detect and/or prevent clients from contacting known malicious sites such as bot controllers
- Collecting and storing all DNS queries with PassiveDNS (with DNS Sinkhole or Sguil)
- ISO available at: http://handlers.dshield.org/gbruneau/

iV Packet and Network Traffic Forensic Analysis Tools Overview

- Exercises: Hands on exercises using tcpdump and ngrep
- Exercises: Wireshark exercises
- Exercises: Malware analysis with ancillary tools

- Exercises: NTFA with freeware tools
- Exercise: Regular Expression (Regex) search and reporting

Introduction to Snort as an Intrusion Detection Sensor

i. Snort IDS with Sguil Console

a. IDS/IPS overview and placement

b. Snort overview

c. Sguil 0.8.0 overview

d. Installation

- Installation of the database server and the sensor
- Installation and configuration of Sguil 0.8.0 on the database and the sensor including the post installation tasks

e. Webmin for sensor and server management

- Web management via SSL
- Management of MySQL
- Management of the Snort rules

f. Introduction to SQueRT – A Simple Query and Report Tool

- Review of SQueRT console to monitor Sguil events

g. Introduction to Sagan – Realtime Log Analysis & Correlation Engine

- Review Sagan rule structure
- Monitoring Sagan events via Sguil and SQueRT

h. Introduction to NfSen – Netflow Sensor

- Review NfSen basic configuration
- Using softflowd to collect netflow data seen by Snort IDS sensor

i. Introduction to Snort signatures

- Snort as a NIDS
- Rule update with Oinkmaster
- Snort rule structures

- Some of the most common options
- How to optimize Snort IDS rules (best to worse rules)

j. IDS exercises with Sguil console

- Exercise: Writing and testing rules
- Exercise: Traffic analysis using Sguil console

k. Technical exercises using the tools learned during the course