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 has content that attempts to address some of the content included in Government of Canada Cyber Security Event Management Plan
Specifically: Government Security Management in Appendix G

- Departmental security event management practices
- Security event reporting
- Security in emergency and increased threat situations
- Administrative investigations of security events
- Post-event analysis
- Security event records

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 and write libpcap filters to view and extract information;
5. Learn the basic use of Windows 10 pktmon packet capture tool
6. Learn how to do network traffic forensics including how to use Wireshark to carve files from data collected in pcap traffic;
7. Basic malware analysis using some simple tools;
8. Introduction to Snort/Suricata signatures: Learn how to write, test and run Snort/Suricata signatures
9. Learn to use the basic functions of tools such as: CyberChef, tcpflow, httpry, Wireshark, tshark, etc to analyze and collect traffic.
10. 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.

A sample of the course content is provided below:

Understanding TCP/IP Suite of Protocols

i. IPv4 and IPv6 TCP/IP Overview

- Basic understanding of Binary, Decimal and Hexadecimal number systems (with exercises)
- In-depth look at IPv4
- Introduction to IPv6
- Internet Protocol Functions
- OSI Model
- Detailed understanding of IP
- An in-depth look at IP, TCP, UDP, and ICMP
- Sample outputs of each protocols represented with tcpdump examples
- Exercises: With tcpdump to gain an understanding of the TCP/IP headers

Profiling and Analysis of Malicious Activity

i. Using various Network Traffic Forensic Analysis Tools and Techniques

- Using and understanding various analysis tools
- tcpdump, pktmon, Wireshark, httpry, Bro, Elastic Stack and much more
- Berkley Packet Filters and examples (BPF)
- File recovery from pcap files using various carving methods
    - Carving emails attachments
    - Files transfer from site/server download
    - Files type analysis
- Introduction to Regular Expressions
- Introduction to RSA Security Analytics including NetWitness Investigator

ii Packet and Network Traffic Forensic Analysis Tools Overview

- Exercises: Hands on exercises using tcpdump, Bro, etc
- Exercises: Wireshark exercises
- Exercises: Malware analysis with ancillary tools
- Exercises: NTFA with freeware tools
- Exercise: Introduction to RSA NetWitness and NetWitness Investigator
- Exercise: Regular Expression (Regex) search and reporting

iii. Profiling traffic

- Threat Hunting Methodology
- Six steps of Incident Response
- Attacker methodology
- Reconnaissance and scanning
- Identifying Malicious code
- Defenses and countermeasures
- Various attack examples
- Network visualization theory and analysis using link graph
- Using Netflow to monitor traffic and services
- Exploits;
    - DOS
    - DDOS
    - Buffer Overflow
    - SQL Injection
    - Rootkits

Defending a Network with a Sinkhole, ELK, Suricata & Snort

iV. Introduction to DNS Sinkhole

- 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
- Additional information available at: http://handlers.dshield.org/gbruneau/

This section provides an overview on host/network monitoring and architecture designs with some examples to place network appliances to defend a network.

Introduction to rockNSM (Elastic Stack, Suricata & Bro)

Snort & Suricata Overview and Placement

a. Introduction to Netflow

• In class discussion about the benefits of collecting netflow data
• Configuring and using softflowd to collect network flow data with ELK

b. Introduction to Snort/Suricata signatures

• Snort/Suricata as a NIDS/NIPS
• Rule management
• Rule structures
• Some of the most common options
• How to optimize IDS rules (best to worse rules)

c. Rule writing exercises

• Exercise: Writing and testing rules

d. Final Team Exercises: This last series of exercises using the tools learned during the course

• Exercise: The students are encouraged to use all the tools they learned and mastered during this course. The students are divided into teams to complete a series of challenge exercises (supplied pcaps).