SEC503.1: Fundamentals of Traffic Analysis: Part I

Concepts of TCP/IP
• Why is it necessary to understand packet headers and data?
• TCP/IP communications model
• Data encapsulation/de-encapsulation
• Discussion of bits, bytes, binary, and hex
Introduction to Wireshark
• Navigating around Wireshark
• Examination of Wireshark statistics
• Stream reassembly
• Finding content in packets
Network Access/Link Layer: Layer 2
• Introduction to 802.x link layer
• Address resolution protocol
• ARP spoofing
IP Layer: Layer 3
IPv4
• Examination of fields in theory and practice
• Checksums and their importance, especially for an IDS/IPS
• Fragmentation: IP header fields involved in fragmentation, composition of the fragments, fragmentation attacks
IPv6
• Comparison with IPv4
• IPv6 addresses
• Neighbor discovery protocol
• Extension headers
• IPv6 in transition

SEC503.2: Fundamentals of Traffic Analysis: Part II

Wireshark Display Filters

• Examination of some of the many ways that Wireshark facilitates creating display filters
• Composition of display filters
Writing BPF Filters
• The ubiquity of BPF and utility of filters
• Format of BPF filters
• Use of bit masking
TCP
• Examination of fields in theory and practice
• Packet dissection
• Checksums
• Normal and abnormal TCP stimulus and response

• Importance of TCP reassembly for IDS/IPS

UDP

• Examination of fields in theory and practice
• UDP stimulus and response

ICMP

• Examination of fields in theory and practice
• When ICMP messages should not be sent
• Use in mapping and reconnaissance
• Normal ICMP
• Malicious ICMP

Real-World Analysis -- Command Line Tools

• Regular Expressions fundamentals
• Rapid processing using command line tools
• Rapid identification of events of interest

SEC503.3: Signature Based Detection

Scapy

• Packet crafting and analysis using Scapy
• Writing a packet(s) to the network or a pcap file
• Reading a packet(s) from the network or from a pcap file
• Practical Scapy uses for network analysis and network defenders

Advanced Wireshark

• Exporting web objects
• Extracting arbitrary application content
• Wireshark investigation of an incident
• Practical Wireshark uses for analyzing SMB protocol activity
• Tshark

Detection Methods for Application Protocols

• Pattern matching, protocol decode, and anomaly detection challenges

DNS

• DNS architecture and function
• Caching
• DNSSEC
• Malicious DNS, including cache poisoning

Microsoft Protocols

• SMB/CIFS
• MSRPC
• Detection challenges
• Practical Wireshark application

Modern HTTP and TLS

• Protocol format
• Why and how this protocol is evolving
• Detection challenges

SMTP

• Protocol format
• STARTTLS

• Sample of attacks
• Detection challenges

IDS/IPS Evasion Theory

• Theory and implications of evasions at different protocol layers
• Sampling of evasions
• Necessity for target-based detection

Identifying Traffic of Interest

• Finding anomalous application data within large packet repositories
• Extraction of relevant records
• Application research and analysis
• Hands-on exercises after each major topic that offer students the opportunity to reinforce what they just learned.

SEC503.4: Anomalies and Behaviors

Network Architecture

• Instrumenting the network for traffic collection
• IDS/IPS deployment strategies
• Hardware to capture traffic

Introduction to IDS/IPS Analysis

• Function of an IDS
• The analyst's role in detection
• Flow process for Snort and Bro
• Similarities and differences between Snort and Bro

Snort

• Introduction to Snort
• Running Snort
• Writing Snort rules
• Solutions for dealing with false negatives and positives
• Tips for writing efficient rules

Zeek

• Introduction to Zeek
• Zeek Operational modes
• Zeek output logs and how to use them
• Practical threat analysis
• Zeek scripting
• Using Zeek to monitor and correlate related behaviors
• Hands-on exercises, one after each major topic, offer students the opportunity to reinforce what they just learned.

SEC503.5: Modern and Future Monitoring: Forensics, Analytics, and Machine Learning

Introduction to Network Forensics Analysis

• Theory of network forensics analysis
• Phases of exploitation
• Data-driven analysis vs. Alert-driven analysis
• Hypothesis-driven visualization

Using Network Flow Records

• NetFlow and IPFIX metadata analysis
• Using SiLK to find events of interest
• Identification of lateral movement via NetFlow data

Examining Command and Control Traffic

• Introduction to command and control traffic
• TLS interception and analysis
• TLS profiling
• Covert DNS C2 channels: dnscat2 and Ionic
• Other covert tunneling, including The Onion Router (TOR)

Analysis of Large pcaps

• The challenge of analyzing large pcaps
• Students analyze three separate incident scenarios.

SEC503.6: IDS Capstone Challenge