CNO ATTACK AND DEFEND COURSE

This rigorous, hands-on course is designed to take students through a wide variety of topics relevant to operationally-focused cyber missions within the offensive and defensive arena. This course focuses heavily on deep packet inspection, statistical flow record analysis, post-exploitation forensics, intrusion detection, network tunneling, and malware network behavior. Extensive network analysis is conducted throughout each stage of the hacker methodology to include packet capturing of scanning, service enumeration, exploitation, man-in-the-middle techniques, and tunneling. Deep packet inspection is performed on the newest remote and client-side exploits and C&C communications. Forensic analysis using IDS logging and network signatures are used to find, preserve, and extract evidence of intrusion. Students will gain an extensive understanding of each packet transmitted on the wire from the very first scan, up to and after successful (or unsuccessful) compromise of the remote system using a variety of tools to include but not limited to Wireshark, Snort, BRO, Security Onion, and Metasploit. During the course, students will learn exploitation skills, both remote and client-side attacks, through extensive hands-on exercises. A 2-day intense culmination exercise designed to replicate real-world operational challenges in both offensive and defensive space reinforces topics taught throughout the course.

CHIRON METHODOLOGY DOMAIN

DISCOVERY AND COUNTER-INFILTRATION PROFESSIONAL™ (DCIP)™

DURATION
5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with network sniffing tools (Wireshark, tcpdump, tshark)
- Familiarity with VMware Player or Workstation
- Exposure to Metasploit Framework

CNO ATTACK AND DEFEND COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understand networking infrastructure components, terminology, and definitions
- Understand networking protocols
- Understand packet analysis

OUTLINE

- Orientation & introductions
- Network components
  - Hubs
  - Switches
  - Routers
  - Proxies
  - Firewalls
- Examination of network protocols
  - Ethernet/802.3
  - Internet protocol (IP)
  - Transmission control protocol (TCP)/user datagram protocol (UDP)
  - Internet control message protocol (ICMP)
  - Address resolution protocol (ARP)
    - Identify man in the middle (MiTM) attacks
    - Mitigation: port security, dhcp snooping, dynamic arp inspection
  - Domain name system (DNS)
  - Transport layer security (TLS/SSL)
  - Hypertext transfer protocol (HTTP)
  - Dynamic host configuration protocol (DHCP)
  - Stream control protocol (SCTP)
- Packet analysis
  - Wireshark overview
  - Resessionizing TCP connections
  - Data reduction with filters
  - Data reduction with tshark

DAY 2:

LEARNING OBJECTIVES

- Understand networking protocols
- Understand packet carving
- Understand passive operating system (OS) fingerprinting

OUTLINE

- Examination of network protocols
  - Domain name system (DNS)
  - Transport layer security (TLS/SSL)
    - Completely broken?
  - Hypertext transfer protocol (HTTP)
  - Dynamic host configuration protocol (DHCP)
  - Stream control protocol (SCTP)
- Object carving from network traffic
  - Hypertext transfer protocol (HTTP)
  - Server message block (SMB)
  - File transfer protocol (FTP)
- Passive OS fingerprinting
  - IP/TCP characteristics

CNO ATTACK AND DEFEND COURSE

COURSE SCHEDULE

DAY 3:

LEARNING OBJECTIVES

- Overview of network security monitoring
- Understand Snort IDS
- Understand Security Onion distribution
- Identify Snort alerts

OUTLINE

- Network security monitoring
  - Intrusion detection explained
  - Overview of Security Onion features
    - Snort
    - Bro
    - ELSA
    - Sguil
    - Squert
- Writing Snort rules
- Indentify anomalous traffic
  - Scanning
  - Remote exploits
- Indentify anomalous traffic - walkthrough
  - Recognize Snort alert
  - Carve malicious executable from network traffic
  - Analyze malicious executable for clues
  - Submit malicious executable for signature identification
  - Analyze host communication
  - Analyze host memory using Volatility
  - Identify attacker activity
  - Establish malicious activity timeline

DAY 4:

LEARNING OBJECTIVES

- Understand personal security product avoidance
- Demonstrate the ability to apply all the concepts and techniques learned during the course in a simulated target environment

OUTLINE

- Malware identification
  - Signature based
  - Heuristics based
- Building payloads to avoid detection
  - Veil framework
- CULEX

DAY 5:

LEARNING OBJECTIVES

- Demonstrate the ability to apply all the concepts and techniques learned during the course in a simulated target environment

OUTLINE

- CULEX