CYBER THREAT EMULATION COURSE

The Cyber Threat Emulation Course is focused on the methodologies and processes used by professional "Red" teams in government and corporate spaces. CTE was developed around the behaviors and techniques used by malicious network attackers, while maintaining focus on professional testing, ensuring the integrity and security of information assets. CTE focuses on information gathering, scanning and service enumeration, mapping, remote and local exploitation and reporting. Students will be exposed to and learn advanced penetration testing using advanced persistent threat techniques. CTE perfects the skills needed to effectively identify protection and mitigation strategies and optimize security controls appropriate for the organization.

CHIRON METHODOLOGY DOMAIN

CYBER THREAT EMULATION PROFESSIONAL™ (CTEP)™

DURATION
10 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Exposure to Linux or Unix-based Operating Systems
- Familiarity with network sniffing tools (Wireshark, TCPDUMP. WinDump)

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046

CYBER THREAT EMULATION COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understanding mindset and methodologies of a penetration tester / red team member.
- Awareness of legal issues pertaining to federal network security laws
- Demonstrate the ability to identify the teams and documents involved in planning a red team assessment
- Fundamental knowledge of open source investigation tactics

OUTLINE

- Orientation
  - Introductions
  - Pre-assessment
- Methodology of Penetration Testing and Red Teaming
- Planning and preparing for a Red Team operation
  - Legal aspects
- Customizing your Attack Platform
- Reconnaissance & information gathering
  - Open source tools and techniques

DAY 2:

LEARNING OBJECTIVES

- Deep understanding of active vs passive scanning
- Ability to identify host operating system and services with multiple passive and active tools
- Understanding of tools, techniques and procedures for successfully launching social engineering campaigns
- Knowledge of key concepts regarding types of shellcode and multi-faceted payloads

OUTLINE

- Scanning and enumeration / Vulnerability Assessment
  - Host and network device discovery and scanning
  - Active and passive operating system fingerprinting
  - Service enumeration
  - Application and service mapping
  - Advanced port scanning and packet manipulation
- Social Engineering
- Phishing
- Spear Phishing
- Shellcode and payloads
  - Creating custom payloads
  - Reverse vs. bind shells
  - Multi-faceted payloads
  - Payload encoding and obfuscation
- Netcat and Ncat usage
  - File transfers
  - Scanning and backdoor

DAY 3:

LEARNING OBJECTIVES

- Understanding of normal Linux operating system environment, including processes, threads and memory allocation
- Knowledge Linux process and service management
- Basic understanding of shell scripting

OUTLINE

- Linux command line tactics
  - Network and file system management
  - Processes and Services
- Logging and Accounting
- Introduction to Shell Scripting

CYBER THREAT EMULATION COURSE

COURSE SCHEDULE

DAY 4:

LEARNING OBJECTIVES

- Understanding of normal Windows operating system environment, including processes, threads and memory allocation
- Knowledge of the difference between signature and heuristic based detection and how to remotely identify common commercial security products
- Knowledge of and practice using multiple remote and client side exploits

OUTLINE

- Windows kernels and processes
- Windows Powershell tactics
- Windows registry
- Understanding buffer overflows
- Detecting and avoiding Personal Security Products
- Remote exploitation
  - Windows kernels 5.1-6.3 techniques
- Client-Side attacks
  - Document and PDF exploitation
  - Browser exploitation
  - Iframe attack methods

DAY 5:

LEARNING OBJECTIVES

- Understanding common web application vulnerabilities, ability to identify and attack these vulnerabilities
- Ability to gain access into a network using a web application foothold
- Understanding proper techniques used when attacking a Linux based system

OUTLINE

- Web based attacks
  - XSS in web email clients
  - Command injection vulnerabilities
  - File upload vulnerabilities
  - Local/remote file inclusion
  - SQL injection vulnerabilities
- Implanting web pages for browser hooking
- Linux service exploitation
- SSH masquerading

DAY 6:

LEARNING OBJECTIVES

- Understanding of Active Directory hierarchy and ability to surreptitiously obtain information about domain
- Demonstrate the ability to use common Windows features and services to maneuver through a Windows domain
- Ability to laterally position and execute implants within a Windows domain
- Ability to properly identify and use technique to use to escalate privileges in both Windows and Unix environments
- Properly identifying hardware architecture remotely

OUTLINE

- Windows Active Directory
- Windows authentication
  - Using standard Windows features
  - Windows "Pass-the-Hash"
- Privilege escalation
  - Bypassing user account control
  - Password attacks
  - Password cracking
  - Identifying vulnerable applications
  - Locating errors in Linux configuration files
  - Linux kernel escalation
- 32/64 bit binary decode

COURSE SCHEDULE

DAY 7:

LEARNING OBJECTIVES

- Knowledge of common logging locations of Windows and Linux based systems
- Ability to strategically eliminate suspicious entries from exploitation attempts
- Understand and identifying remote logging techniques used in an enterprise
- Proper deployment of persistence techniques for Windows and Unix systems

OUTLINE

- Covering tracks
  - Cleaning logs
  - Windows event logs
  - Blending in
  - Surveying the target operating environment
- Persistence
  - Beaconing vs. binding implants
  - Windows persistent access
  - Linux backdoors using tools already on target

DAY 8:

LEARNING OBJECTIVES

- Perform 802.11 wireless packet capture, analysis, and injection
- Ability to access 802.11 network security and perform various attacks against each form of encryption
- Demonstrate how to decrypt encrypted wireless data
- Identify Rouge AP, Evil Twin, and other Man in the Middle techniques

OUTLINE

- Building a wireless attack platform
- Wireless traffic collection and analysis
- WEP and WPA exploitation
- Rogue AP / MitM techniques

DAY 9:

LEARNING OBJECTIVES

- Ability to properly survey a host after exploiting on to it
- Ability to enumerate a network once inside the firewall
- Ability to pivot between multiple hosts and understanding of how data flows back out of the network
- Understanding of the risk analysis framework and how to properly identify risk
- Knowledge of reporting guidelines and standards and understanding of how to develop quality deliverables

OUTLINE

- Situational awareness / Maneuvering
  - Injecting Shellcode into memory of a running application
  - Locating and penetrating internal networks
  - Port forwarding, pivoting and redirection
- Risk Assessment and analysis
  - Conducting a risk assessment
  - Identifying threats and vulnerabilities
  - Measure and calculate likelihood and impact
  - Determine risk to organization
- Analysis and reporting
  - Standardized deliverables
  - Executive and technical level requirements

DAY 10:

LEARNING OBJECTIVES

- Understand key reports and deliverables given to a customer
- Ability to perform detailed operational logging when engaged in an assessment
- Implement techniques used throughout class in a practical exercise

OUTLINE

- Validation Exercise (VALEX)
- VALEX Review
- Post-Assessment