ADVERSARIAL THREAT MODELING AND EMULATION COURSE

The Adversarial Threat Modeling and Emulation course is an intense, hands-on course that takes students through each stage of offensive operations methodologies using tradecraft, stealth and detection avoidance as the key principals. Students will gain proficiency with open-source penetration tools and learn techniques in vulnerability scanning, remote and client-side exploitation, and advanced post-exploitation techniques targeting both Windows and UNIX based operating systems. Students will utilize a wide range of advanced exploitation techniques to gain remote execution on multiple platforms ranging from Ubuntu to Windows 10. The course culminates with a comprehensive, challenging Capture-the-Flag competition. The exercise is a scenario-based challenge that engages the students in a friendly competition between two teams to capture multiple flags implanted throughout the network and solve various challenges and tasks. Techniques used will cover the gamut from scanning, network exploitation, and backdoor installation to artifact recovery and forensics.

CHIRON METHODOLOGY DOMAIN

CYBER THREAT EMULATION PROFESSIONAL™ (CTEP)™

DURATION

5 DAYS

RECOMMENDED PRE-REQUISITES

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

ADVERSARIAL THREAT MODELING AND EMULATION COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understanding of exploitation concepts and methodology
- Understanding of operational tradecraft, and the benefits of stealth
- Understanding of how an attack platform is utilized
- Demonstrate the ability to survey a Linux host and vet processes.
- Understanding of Windows operating system components and how they relate to Network Exploitation techniques
- Demonstrate the ability to survey a Windows host and vet both processes and services for potential malware or other actors

OUTLINE

- Orientation
  - Introductions
- Introduction to the Exploitation Methodology
  - Overview of exploitation methodology
  - Introduction to tradecraft
- Getting to know your attack platform
  - Attack platform overview
  - Metasploit basics
- Linux Practical Exercise
  - Survey a host and conduct process investigation
- Windows Fundamentals
  - Overview of windows components
  - Registry fundamentals
- Windows Practical Exercise
  - Survey a host to conduct process and service investigation

DAY 2:

LEARNING OBJECTIVES

- Understanding of how open source intelligence collection drives network exploitation planning and actions
- Understanding of external scanning techniques and procedures
- Determining which exploit is best to use for specific situations
- Understanding of various backdoor types, and when each is appropriate to use
- Attacking web vulnerabilities on Linux based systems
- Understanding the proper techniques used to escalate privileges on Linux based systems.

OUTLINE

- External scanning & OSINT
  - Open Source collection
  - External network scanning tactics
- Exploit Selection
  - Identifying target and scenario
  - Determining the best exploit for the situation
- Payloads & Backdoors
  - Payload basics
  - Backdoor fundamentals
- Linux Web Exploitation
  - Web exploitation fundamentals
  - Drupal exploitation
  - Cleanup techniques
- Linux Privilege Exploitation
  - Overview of the types of escalation used
  - Techniques for determining the best exploit to use
  - Taking advantage of misconfigurations
- Linux Persistence
  - Overview of implant types
  - Techniques to blend persistence with normal system files and configuration

ADVERSARIAL THREAT MODELING AND EMULATION COURSE

COURSE SCHEDULE

DAY 3:

LEARNING OBJECTIVES

- Understanding of Secure Shell, and how it can be used for lateral movement
- Understanding of browser exploitation techniques and iframes
- Understanding of Windows privilege levels and escalation concepts
- Understanding of how persistent access can be gained on windows hosts
- Understanding of internal scanning concepts, and how they differ from external
- Demonstrate the ability to gain remote code execution on multiple Windows kernel versions

OUTLINE

- SSH Masquerades
  - SSH basics
  - Leveraging SSH for lateral movement
- Client Side Exploitation
  - Overview of Client side exploits
  - iframes
- Windows Privilege Escalation
  - Windows privilege escalation concepts
  - Windows privilege escalation techniques
- Windows Persistence
  - Meterpreter built-in techniques
  - Manual Windows persistence techniques
- Internal Scanning
  - Internal vs. external scanning
  - Windows scanning
  - Unix scanning
- Remote Exploits
  - Kernel 5 exploits
  - Kernel 6 exploits
  - Cleanup techniques

DAY 4:

LEARNING OBJECTIVES

- Knowledge of the principals of domain trusts
- Demonstrate the ability to exploit domain trusts to move laterally through a network using native functionality
- Demonstrate the ability to decode executable binaries to allow them to be transferred across Terminal Services Connections
- Understanding of how windows stores both passwords and password hashes
- Demonstrate the ability to move laterally across a network without credentials, using only hashes.
- Understanding of why and how pivoting us used to navigate across multiple networks
- Demonstrate the ability to apply all the scanning, enumeration, and mapping techniques learned during the course in a simulated target environment

OUTLINE

- Techniques I – Net Use & Power Use
  - Masquerade basics
  - Windows 7 net use masquerade
  - Windows 10 net use masquerade
  - PowerShell Masquerade
  - Advanced masquerade techniques
- Techniques II – Binary Decode
  - Using PowerShell to manipulate hosts via RDP
  - 64-bit binary decode technique
- Techniques III – Pass the Hash
  - Mimikatz
- Pivoting & Redirection
  - Principals of redirection
  - Redirection through multiple networks

DAY 5:

LEARNING OBJECTIVES

- Culmination Exercise

OUTLINE

- Scanning, Enumeration, and mapping
- Exploitation and collection