WIRELESS EXPLOITATION AND ATTACK COURSE

Wireless Exploitation and Attack is an intense, hands-on course that takes students through the most common and current techniques for gaining access to a wireless network. Students will gain proficiency with open-source wireless attack tools and methodology. Subject matter includes everything from learning the foundations of 802.11 technology to the most advanced ways to circumvent wireless defense practices. Each student will learn the latest exploits and use the most effective tools to perform such techniques as secure man-in-the-middle attacks through wireless hotspot impersonations, exploiting weaknesses in Wi-Fi Protected Setup, and how to correctly secure networks using properly configured enterprise-grade authentication.

CHIRON METHODOLOGY DOMAIN

CYBER THREAT EMULATION PROFESSIONAL™ (CTEP)™

DURATION

5 DAYS

RECOMMENDED PRE-REQUISITES

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

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

WIRELESS EXPLOITATION AND ATTACK COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understand hacker methodology
- Understand WLAN components, terminology, and definitions
- Ability to characterize 802.11 networks
- Demonstrate ways to utilize monitor mode

OUTLINE

- Orientation & introductions
- Hacker methodology
  - Footprinting
  - Scanning
  - Exploitation
  - Privilege escalation
  - Post-exploitation
- Introduction to 802.11 and RF Basics
  - Review of current IEEE 802.11 standards, ad hoc vs. infrastructure modes
  - Examination of RF spectrum usage
    - Regulatory Domains
    - 2.4/5GHz, channels, overlap, interference
  - Physical WLAN components and how they connect
  - WLAN terminology

DAY 2:

LEARNING OBJECTIVES

- Ability to examine key 802.11 packets
- Configure a wireless attack/ survey platform
- Understand the importance of hardware selection

OUTLINE

- Examination of 802.11 packets in detail
  - Post-exploitation Breakdown of an 802.11 frame
  - Different WLAN frame types
- Control, Management, Data
  - Capture connection setup and established data transfers
  - Examining packet captures in Wireshark
    - Using common display filters
  - Analyzing client probe requests and access point beacons/probe responses
  - Determination of AP capabilities from passive collection
  - Review of the hidden node problem and its solution (RTS/CTS)
- Building a wireless attack/survey platform
  - Setting up an access point for testing
  - Configuring wireless interfaces
    - Command-line usage
    - Create a monitor mode interface
  - Antenna selection
    - Power/gain, band, drivers patched for injection, type
  - Progressive target identification

WIRELESS EXPLOITATION AND ATTACK COURSE

COURSE SCHEDULE

DAY 3:

LEARNING OBJECTIVES

- Perform passive network detection
- Understand Wardriving/Geolocation techniques
- Ability to reveal hidden networks
- Enable 802.11 decryption
- Identify security implementation flaws in 802.11 networks
- Ability to bypass Wired Equivalent Privacy (WEP) encryption

OUTLINE

- Scanning and enumeration techniques
  - Comparison of features
    - inSSIDer, Kismet, and the aircrack-ng suite
  - Reveal hidden SSIDs through client deauthentication
  - Analysis of client and AP MAC addresses (IEEE OUI lookup)
  - Wardriving/Geospatial Integration
    - Examples of wardriving activities
  - Plotting WLAN AP locations in Google Earth
    - Using third-party sites such as Wigle.net for AP geolocation
- Wired Equivalent Privacy (WEP)
  - Implementation and flaws
    - Keystream and Implementation Vectors and weaknesses
  - Using attacks against a client-less WLAN
    - Korek Chop-Chop or Fragmentation
  - Attacking cryptographically weak IVs (FMS, PTW) for key recovery
  - Revisiting Verizon FiOS implementation failures

DAY 4:

LEARNING OBJECTIVES

- Demonstrate knowledge of the WPA (2) 4-way Handshake
- Ability to bypass Shared Authentication, WEP, and WPA(2)-PSK
- Enable 802.11 decryption
- Knowledge of WLAN defensive measures
- Demonstrate knowledge of Enterprise-Grade WLAN attacks and defense practices

OUTLINE

- Wi-Fi Protected Access (WPA/WPA2)
  - 4-way Handshake
    - Composition and significance
    - Collection
  - Brute force and dictionary attacks
  - Pre-computed hashes (rainbow tables)
  - Speeding up WPA cracking using video card GPUs
  - Improved protection with 802.11w Protected Management Frames
  - Attacking Wi-Fi Protected Setup (WPS) PIN
- WLAN Decryption
- Implementing WLAN defensive measures
  - Proper, strong SSID and passphrase selection
  - Hidden SSIDs and client authentication/association process
  - Using a Wireless IDS for identification of attacks and rogue access points
  - How to protect a WLAN from packet replays and other attacks
- Enterprise
  - WPA-Enterprise configuration
  - Configuring a freeRADIUS-WPE server for improved WLAN authentication
  - Using ASLEAP to actively recover LEAP/PPTP passwords

WIRELESS EXPLOITATION AND ATTACK COURSE

COURSE SCHEDULE

DAY 5:	LEARNING OBJECTIVES	OUTLINE
	➶ Demonstrate knowledge of advanced Man-In-The-Middle (MITM) techniques ➶ Ability to identify host file system artifacts and WLAN profile data ➶ Perform basic host and port scanning techniques ➶ Demonstrate basic use of an exploitation framework	➤ Advanced Man-In-The-Middle (MITM) techniques » Scenarios for creating fake APs; impersonating wireless hotspots » Session hijacking, DNS spoofing, and rerouting a victim's traffic » Violating the user's trust of HTTPS and SSL » Identifying Browser Vulnerabilities ➤ Introduction to scanning and enumeration » Discovery Scanning » Operating System fingerprinting ➤ Introduction to exploitation » Vulnerability discovery » Reverse vs. Bind Shells