CENTER FOR CYBER SECURITY TRAINING

Physical Penetration Testing - Covert Methods of Entry for Enterprise

Abstract

The Covert Methods of Entry for Enterprise course is an intensive, comprehensive 5-day class focusing on entry into secure commercial facilities. Although this class is comprised of over 70% hands-on instruction, participants are not required to have any previous physical security knowledge to enroll in this course.

Throughout the week, the class will cover an assortment of entry techniques and tools, including many methods of varying difficulties. To help develop their skillset, participants will receive one-on-one instruction from the foremost authorities within the industry for covert entry. The culminating task will challenge students to apply their newfound knowledge as they maneuver their way through a set of various real-world scenarios. Students who demonstrate proficiency in executing an advanced attack chain throughout this culminating challenge will obtain a Certificate of Completion.

Following successful completion of the course, each student will be equipped with the skills and tools necessary to identify and exploit defects in commercial physical security architecture.

Each student will be issued a professional covert entry toolkit to be used for the duration of the course. The issued toolkit is the students' to keep.

Learning Objectives

- Introduction to Locks
- Lock Picking
- Advanced Lock Bumping
- Lock Decoding
- Key Decoding
- Key Impressioning
- Key Mold and Cast Techniques

- Master Key Privilege Escalation
- Lock Bypass Methods
- Lock Cylinder Forensics
- Bypassing of Electronic Access Controls
- RFID Cloning / Replay / Bypass
- Alarm Sensor Bypass
- Construction of Field Expedient Tools
- Facility / Site Recon
- Physical > Digital > Social Attack Chain

Target Audience

For companies wishing to expand the scope of their internal security staff's abilities and responsibilities

Course Outline

- **Introduction**
- **Overt, Covert, and Surreptitious Entry**
- **How Lock Cylinders Work**
- **Post Exploitation Phases**
- **Anatomy of a Lock**
- **Introductory Manipulation**
    - Hands-On Lab
- **Rapid-Entry Manipulation**
    - Hands-On Lab
- **Non-Traditional Mechanisms**
- **Desk Locks & Document Storage**
    - Hands-On Lab
- **Special-Purpose Locks**
- **Lock & Key Decoding**
    - Hands-On Lab
- **Key-Cutting**
    - Hands-On Lab
- **Covert Bypass Methods**

    - Padlocks
    - Commercial Locks
    - Residential Locks
    - Hands-On Lab
- **Key Molding and Casting**
    - Hands-On Lab
- **Key Impressioning**
    - Hands-On Lab
- **Abusing Fire Code**
- **Other Bypass Tools**
    - Hands-On Lab
- **Elevator Security**
- **Attacking Master Key Systems**
    - Hands-On Lab
- **Electronic Access Control Basics**
- **RFID Credentials**
    - Hands-On Lab
- **Magnetic Locks**
    - Hands-On Lab
- **Adams Rite Solenoids**
    - Hands-On Lab
- **Electrified Strikes**
- **Magnetic Sensors**
    - Hands-On Lab
- **Request-to-Exit Devices**
    - Hands-On Lab
- **Telephony Access Control Systems**
- **Passive Recon**
    - Hands-On Lab
- **Active Recon**
    - Hands-On Lab

- **Keyed-Alike Systems**
    - Hands-On Lab
- **Interactive CMoE Thought Process**
- **Lock Forensics**
    - Hands-On Lab
- **Default Codes and Methods**
    - Hands-On Lab
- **Field Expedient Tools**
    - Hands-On Lab
- **Photographic Key Duplication**
    - Hands-On Lab
- **Locksmith Software and Tools**
- **Connecting the Dots**
- **Practical Proficiency Test**
- **Wrap-Up**

REQUIREMENTS

Students Knowledge Pre-Requisites:

Even individuals with absolutely zero experience in covert entry will gain a strong understanding of how such techniques work and will be opening all of the most popular locks in use today in short order.