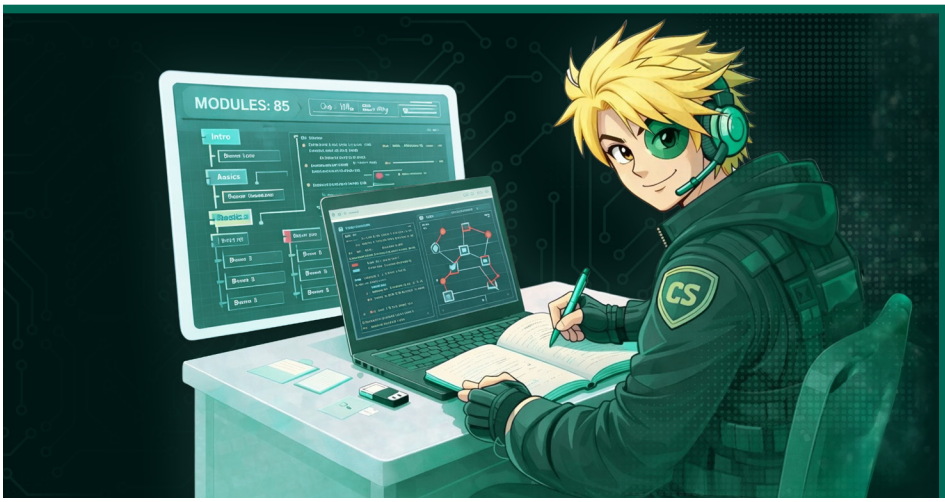
FORTRA

DATASHEET (OFFENSIVE SECURITY)

Cobalt Strike Certified Operator Training I (CSCO I)



85 lessons

Hands-on Labs: The curriculum is reinforced with a series of interactive labs designed to solidify core concepts at your own pace, providing a realistic learning experience.

Format: Self-paced, online

Cobalt Strike Certified Operator Training I (CSCO I) is a collaboration between Zero Point Security and Cobalt Strike, designed to provide a hands-on, detailed introduction to Cobalt Strike.

Through direct application of the framework, you will gain experience in everything from initial setup and basic command usage to advanced post-exploitation, bypassing network filters, and customizing the tool's behavior. The focus is on building practical skills that can be immediately applied in a professional environment.

Training Content

This module-based tour of the Cobalt Strike framework covers the entire lifecycle of a red team engagement through written explanations, graphics, and videos.

1. Getting Started

Dive into the methodology for red teaming and adversary simulation.

- Introduction to Red Teaming
- Adversary Emulation vs. Simulation
- The Attack Lifecycle

2. Initial Setup

Master the fundamental command-line interface for the framework.

- First Time Setup
- Client Tour
- Command Basics
- Getting to Know the Cobalt Strike Client
- Aggressor Script
- Home Lab

3. Command and Control (C2)

Learn to use various types of Beacons.

- HTTP/HTTPS
- DNS Beacons
- Stealthy Network Comms with DNS over HTTPS Beacon
- DNS over HTTPS Beacons
- TCP and SMB Beacons
- External C2

4. Code Execution

Understand Cobalt Strike payload generation and execution.

- Reflective Loading
- Staged vs. Stageless Payloads
- Payload Guardrails
- Resource Kit
- Artifact Kit
- Custom Payloads
- Cobalt Strike's Built-In Web Server

5. Post-Exploitation

Develop proficiency with post-exploitation commands.

- Command Behavior
- File System & File Browser
- Processes & Process Browser
- Keylogger & Clipboard
- Registry
- Screenshots
- VNC
- Domain Reconnaissance
- Execution Commands
- Executing Custom Tools
- Beacon Object Files (BOFs)
- Beacon Data Store

6. Privilege Escalation

- Learn about the built-in options and techniques Cobalt Strike offers for elevating privileges.
- UAC Bypasses
- Get SYSTEM

7. Credentials and Lateral Movement

Discover how Cobalt Strike leverages built-in Windows authentication technologies to remotely authenticate to other targets and get administrative access to move laterally across a network.

- Credential Access
- Credentials Model
- User Impersonation
- Lateral Movement

8. Bypassing Network Filtering

Get an overview of techniques for bypassing network restrictions.

- SOCKS Proxy
- Reverse Port Forward
- Pivot Listeners

9. Malleable C2

Customize Beacon's indicators and behaviors to transform the appearance of Beacon's network traffic to appear legitimate or benign.

- Customizing HTTP Traffic
- Customizing DNS Traffic
- Profile Variants
- Host Profiles
- HTTPS Certificates
- Code Signing

10. Malleable C2 (Beacon)

Configure Beacon's default reflective loading process to make it emulate a known threat or bypass AV and EDR signatures.

- Beacon's Reflective Loader
- Beacon's Runtime Behavior
- Controlling Post Exploitation
- Malleable Profile Configuration

11. Extending Cobalt Strike

Learn to extend the framework with Aggressor Script to create additional functionality to tailor engagements to each specific environment.

- Aggressor Functions
- Custom Elevators
- Custom Lateral Movement
- Custom Dialogs
- Command Callbacks

12. Reporting

Find out about how the raw data logs from engagements can be transformed into reports detailing activity, hosts, indicators of compromise, and more.

- Reporting
- Custom Report Templates

BUY NOW

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.