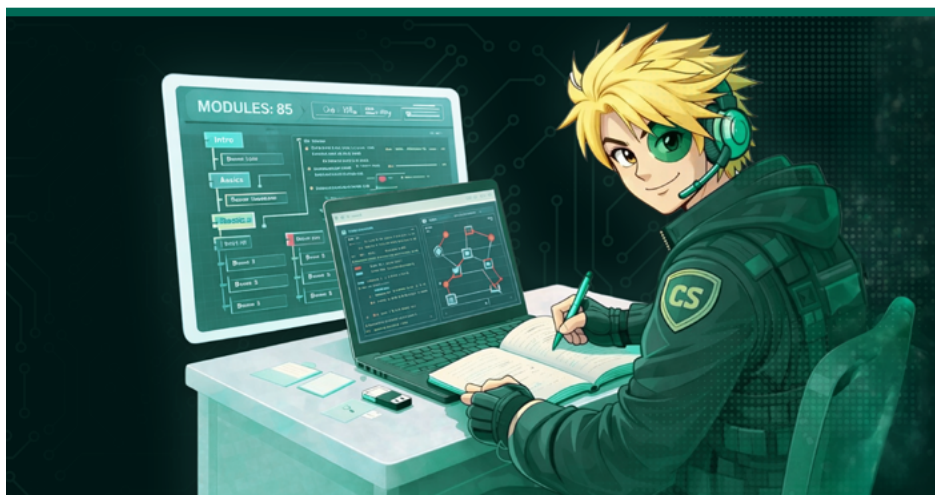




DATASHEET (OFFENSIVE SECURITY)

Cobalt Strike Certified Operator Training I and II Bundle



155 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

Course overview

Cobalt Strike Certified Operator Training I and II, a collaboration between Zero Point Security and Cobalt Strike, provides comprehensive, hands-on training across the full attack chain. Build foundational skills in Cobalt Strike setup, command usage, post-exploitation, network filter bypassing, and customization, then advance to sophisticated payload delivery and evasion techniques using Aggressor Script, User-Defined Reflective Loaders (UDRLs), Sleep Mask, Beacon Gate, and more.

By completing both courses, you will be equipped to confidently operate and tailor Cobalt Strike for professional red team assessments and adversary simulations.

Training Content

Cobalt Strike Certified Operator I (CSCO I)

1. Getting Started

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

2. Initial Setup

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

3. Command and Control (C2)

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

5. Post-Exploitation

- 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

7. Credentials and Lateral Movement

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

9. Malleable C2

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

4. Code Execution

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

6. Privilege Escalation

- UAC Bypasses
- Get SYSTEM

8. Bypassing Network Filtering

- SOCKS Proxy
- Reverse Port Forward
- Pivot Listeners

10. Malleable C2 (Beacon)

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

11. Extending Cobalt Strike

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

12. Reporting

- Reporting
- Custom Report Templates

Cobalt Strike Certified Operator II (CSCO II)

1. Getting Started

- Welcome

2. Aggressor Script

- Introduction
- Sleep 101
- Script Console
- Script Manager
- Aggressor Script Demo
- Aggressor Script Lab

3. Stage 0 Payloads

- Introduction
- AppDomainManager Hijack
- Shellcode Injection
- Payload Delivery
- Stage 0 Demo
- Stage 0 Lab

4. UDRLs

- | | |
|-----------------------------|------------------------------|
| • Introduction | • Integration with Aggressor |
| • PE Review | • Simple Loader Demo |
| • PIC Primer | • Simple Loader Lab |
| • PIC Primer Demo | • PIC Projects |
| • PIC Primer Lab | • Stardust Demo |
| • Loader Fundamentals | • Stardust Lab |
| • Beacon Calling Convention | |

5. Static Evasion

- Obfuscating Beacon at rest
- Bypassing memory scanners

6. Load-Time Evasion

- Introduction
- Export Address Filtering
- Export Address Filtering Demo
- Export Address Filtering Lab
- Module Stomping
- Call Stack Spoofing
- Call Stack Spoofing Demo
- Call Stack Spoofing Lab

7. Built-in Runtime Evasion

- Sleepmask
- Beacon User Data
- Sleepmask Demo
- Sleepmask Lab
- BeaconGate
- BeaconGate Demo
- BeaconGate Lab

8. Custom Runtime Evasion

- Beyond BeaconGate
- IAT Hooking Demo
- IAT Hooking Lab
- Freeing Beacon

9. Postex Evasion

- Introduction
- Reflective DLLs
- Beacon Object Files
- BOF Cocktails Demo
- BOF Cocktails Lab
- Native Commands & Beacon Interpreter

10. Custom Process Injection

- Introduction
- Process Injection Spawn
- Process Injection Explicit
- Process Injection Dialogue

11. UDC2

- Introduction
- UDC2 BOF
- UDC2 Server
- UDC2 Evasion
- UDC2 Demo
- UDC2 Lab

12. Capstone

- Introduction
- Capstone Lab

13. Development Environment

- Introduction
- Environment Setup
- Environment Setup Walkthrough

14. Next Steps

- Course Evaluation — 3 questions
- Certificate of Completion

FORTRA[®]

fortra.com