FORTRA®

DATASHEET (OFFENSIVE SECURITY)

BOF Development & Tradecraft

Author: Alex Reid

Levels: Registered

Study time: 5 hours

ZERO POINT SECURITY

This BOF Development & Tradecraft course, created by Alex Reid and Zero-Point Security, teaches how to write and unit test Beacon Object Files (BOFs) for use in Cobalt Strike and other C2 frameworks.

Training Content

Getting Started

- Welcome
- Author's Note
- Software Requirements
- Windows Environmen Setup
- Linux Environment Setup
- Resources

Introduction to BOF Development

- Background and Basics
- Windows API
- COFFLoader
- BOF Development on Linux
- BOF Development on Windows
- Aggressor Scripting

Practical 1: Ransomware Simulator

- Introduction
- Initial Setup
- Finding the Desktop folder
- Code Download
- Changing the Wallpaper and Leaving the Ransom Note
- Code Download
- Renaming Files
- Code Download
- Aggressor Script
- Code Download
- Closing

Practical 2: Iscsipl.exe UAC Bypass

- Introduction
- Initial Setup
- Code Review, Testing, and Analysis
- Initial Port of Code
- Code Download
- Replacing Resource Functionality
- Code Download
- Offensive Tradecraft
- Code Download
- Code Cleanup
- Code Download
- Aggressor Script
- Code Download
- Closing
- Resources

Practical 3: TGT Auto-Harvester

- Introduction
- Initial Setup
- Introduction to Stardust
- Calling Beacon APIs from Stardust
- Code Download
- Monitoring for New Logins
- Code Download
- Dumping TGTs Automagically
- Code Download
- Patching BOF Arguments
- Code Download
- Teardown and Cleanup
- Code Download
- Aggressor Script
- Code Download
- Dancing with Sleep Mask
- Code Download
- Closing
- Resources

Update 1: BOFPatcher

- Background
- Design Process
- Code Download

Course Completion

- Course Evaluation (3 questions)
- Certificate of Course Completion

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.

