FORTRA

DATASHEET (OFFENSIVE SECURITY)

Red Team Operations Training I

Author: Daniel Duggan

Levels: Practitioner

Study time: 20 hours

Certifications: Red Team Operator

ZERO POINT SECURITY

This Red Team Ops I training course, created by Zero-Point Security, provides you with the knowledge and skills necessary to excel in performing adversary simulation and emulation exercises with Cobalt Strike.

Training Content

1. Getting Started

- Welcome
- Introduction to Red Teaming
- Adversary Emulation vs Simulation
- The Attack Lifecycle
- Engagement Planning

2. Law & Compliance

- Introduction
- Computer Misuse Act
- Human Rights Act
- Data Protection Act & GDPR
- Sector Legislation

3. Malware Essentials

- Introduction
- Processes
- Process Injection
- .NET & P/Invoke

4. Cobalt Strike Primer

- Introduction
- Listener Management
- Beacon Payloads
- Interacting with Beacon
- Cobalt Strike Lab

5. Defense Evasion

- Introduction
- Compiled Artifacts
- Artifact Kit Demo
- Script Artifacts
- Beacon Memory
- Beacon Command Behavior
- Blending Post-ex
- Command-Line Detections
- Defense Evasion Lab

6. Initial Access

- Introduction
- Payloads
- Droppers
- Triggers
- Containers
- Delivery
- Initial Access Demo
- Initial Access Lab

7. Persistence

- Introduction
- Boot & Logon Autostart
- Logon Script
- PowerShell Profile
- Scheduled Task
- COM Hijacking
- Persistence Demo
- Persistence Lab

8. Post-Exploitation

- Introduction
- Session Passing
- File System
- Downloading Files
- Processes
- Keylogger
- Clipboard
- Registry
- Screenshots
- VNC
- Execution Commands
- Executing Custom Tools

9. Privilege Escalation

- Introduction
- Path Interception
- Weak Service Permissions
- DLL Search Order Hijacking
- Software Vulnerabilities
- User Account Control
- Privilege Escalation Demo
- Privilege Escalation Lab

10. Elevated Persistence

- Introduction
- Scheduled Task
- Windows Service
- Windows Management Instrumentation
- Elevated Persistence Demo
- Elevated Persistence Lab

11. Credential Access

- Introduction
- Credentials from Web Browsers
- Windows Credential Manager
- OS Credential Dumping
- Kerberos Tickets
- Credential Access Challenge
- Credential Access Solution

12. User Impersonation

- Introduction
- Token Impersonation
- Pass the Hash
- Pass the Ticket
- Process Injection
- User Impersonation Demo
- User Impersonation Lab

13. Discovery

- Introduction
- Lightweight Directory Access Protocol
- BOFHound
- Discovery Demo
- Discovery Lab

14. Lateral Movement

- Introduction
- Windows Remote Management
- PsExec
- Custom Techniques
- Leveraging LOLBAS
- Security Logon Types
- Lateral Movement Demo
- Lateral Movement Lab

15. Pivoting

- Introduction
- SOCKS Proxies
- SOCKS Demo
- SOCKS Lab
- Reverse Port Forwards

16. Kerberos

- Introduction
- Unconstrained Delegation
- Unconstrained Delegation Demo
- Unconstrained Delegation Lab
- Constrained Delegation
- Constrained Delegation Demo
- Constrained Delegation Lab
- Service Name Substitution
- Service Name Substitution Demo
- Service Name Substitution Lab
- S4U2self Computer Takeover
- S4U2self Demo
- S4U2self Lab
- Resource-Based Constrained Delegation
- Resource-Based Constrained Delegation Demo
- Resource-Based Constrained Delegation Lab
- Lateral Movement Services
- Kerberos Challenge

17. Microsoft SQL Server

- Introduction
- Code Execution
- Linked Servers
- Privilege Escalation
- SQL Server Demo
- SQL Server Lab

18. Domain Dominance

- Introduction
- DCSync
- Ticket Forgery
- DPAPI Backup Keys

19. Active Directory Certificate Services

- Introduction
- ESC1 - Misconfigured 'Client Authentication' Templates
- ESC1 Demo
- ESC1 Lab
- ESC3 - Misconfigured 'Certificate Request Agent' Templates
- ESC2 - Misconfigured 'Any Purpose' Templates
- ESC4 - Certificate Template Access Control
- ESC8 - NTLM Relay to ADCS HTTP Endpoints
- ESC8 Demo
- ESC8 Lab
- DPERSIST1 - Golden Certificates
- DPERSIST1 Demo
- DPERSIST1 Lab

20. Forest & Domain Trusts

- Introduction
- Inter-Realm Tickets
- Parent-Child Trusts
- Parent-Child Trust Demo
- Parent-Child Trust Lab
- Inbound Trusts
- Inbound Trust Demo
- Inbound Trust Lab
- Outbound Trusts
- Outbound Trust Demo
- Outbound Trust Lab

21. AppLocker

- Introduction
- Enumeration
- Bypasses
- AppLocker Challenge

22. Reporting

- Reporting

23. Course Completion

- Course Evaluation 3 questions
- Certificate of Course Completion

24. Final Exam

- Exam Information - READ THIS FIRST 04:21
- Red Team Operator Exam
- Red Team Operator Certificate

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.