Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

C0100

Course Interview and Overview

© Defensive Origins LLC C0100.1 – Course Introduction

Instructors

Jordan Drysdale
@Rev10D

Kent Ickler
@Krelkci

© Defensive Origins LLC C0100.2 – Course Introduction

Course Objectives

- Implement Sysmon with the modular configuration
- Configure and launch meaningful audit policies
- Deploy the WEF / WEC model of event collection
- Install and configure WinLogBeat
- The Hunting ELK (HELK) Docker-based Elastic install
- Catch some basic command line execution
- Bonus: Build a Continuous Improvement Purple Team Environment

© Defensive Origins LLC

Course Components

- C0100-1: Course Introduction
- C0300-1: Event Baselines and Sysmon
- C0320-1: Event Handlers and Subscriptions
- C0330-1: Log Shipping and Event Ingests
- C0150-1: Purple Team Lifecycle / Continuous Improvement

- Course Git Repo: https://github.com/DefensiveOrigins/APT06202001

© Defensive Origins LLC

Have everything?

- Lab Environment (Optional!)
- Applied Purple Team Courseware (Git Repo!)

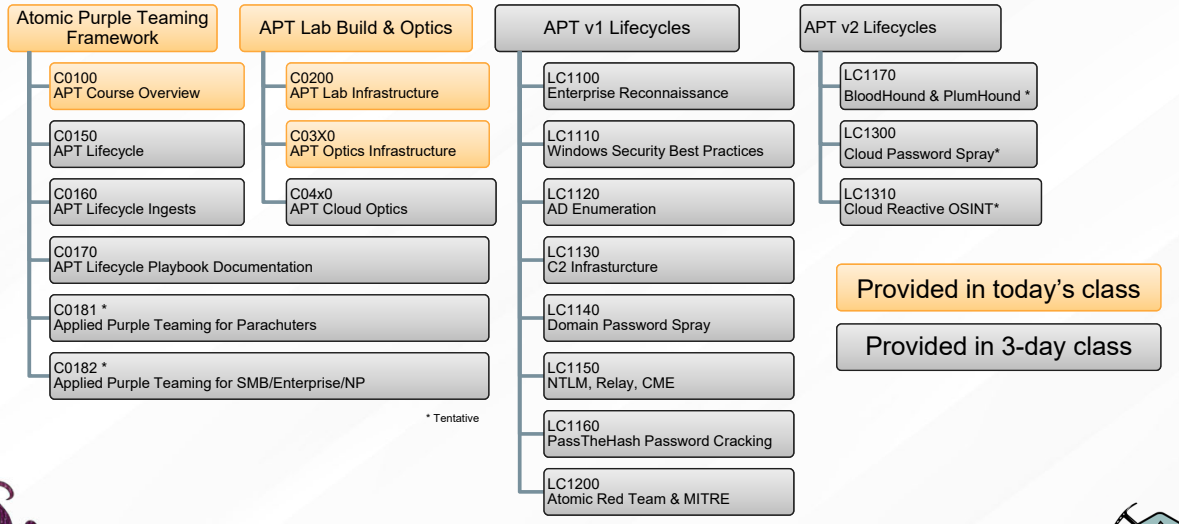
https://github.com/DefensiveOrigins/APT06202001

Course Information

- 4-5 Hours
- Breaks will be announced, approximately hourly.
- Course Git Repo

https://github.com/DefensiveOrigins/APT06202001

Applied Purple Teaming Course Matrix



Applied Purple Teaming Full (3-Day) Course

3 Day Session

- Tue, June 30 – 10:30 a.m. to 5 p.m. EST
- Wed, July 1 – 11:30 a.m. to 5 p.m. EST
- Thu, July 2 – 11:30 a.m. to 5 p.m. EST

Instructors: Kent Ickler & Jordan Drysdale

Price: $395

Scholarships available and will be discussed at the end of todays session.

- Three days of fast-paced interactive learning
- Continuous security hardening framework (Applied Purple Teaming)
- APT for Parachuters, SMB, Enterprise, and NP
- Discussion of Design and implementation network optics and logging
- A Review of Enterprise OSINT Awareness
- Active Directory Best Practices for Securing your Environment
- Interactive Exercises (Labs)
- Plan, Attack, Defend, Hunt, Document Lifecycle-Driven Methodology
- Live-fire attack tactics such as SMB/NTLM Relay, Command and Control, and BloodHound!
- Life hunt-detection methodology using Logstash, Elasticsearch, and Kibana!
- Implementation of continuous security improvement by leveraging MITRE ATT&CK
- Integration of the Atomic Red Team framework in Purple Teaming exercises
- Defensive Origins Hosted Lab Environment
- 6 Months of BHIS AntiSiphon Cyber Range Included!

https://wildwesthackinfest.com/online-training/applied-purple-teaming/