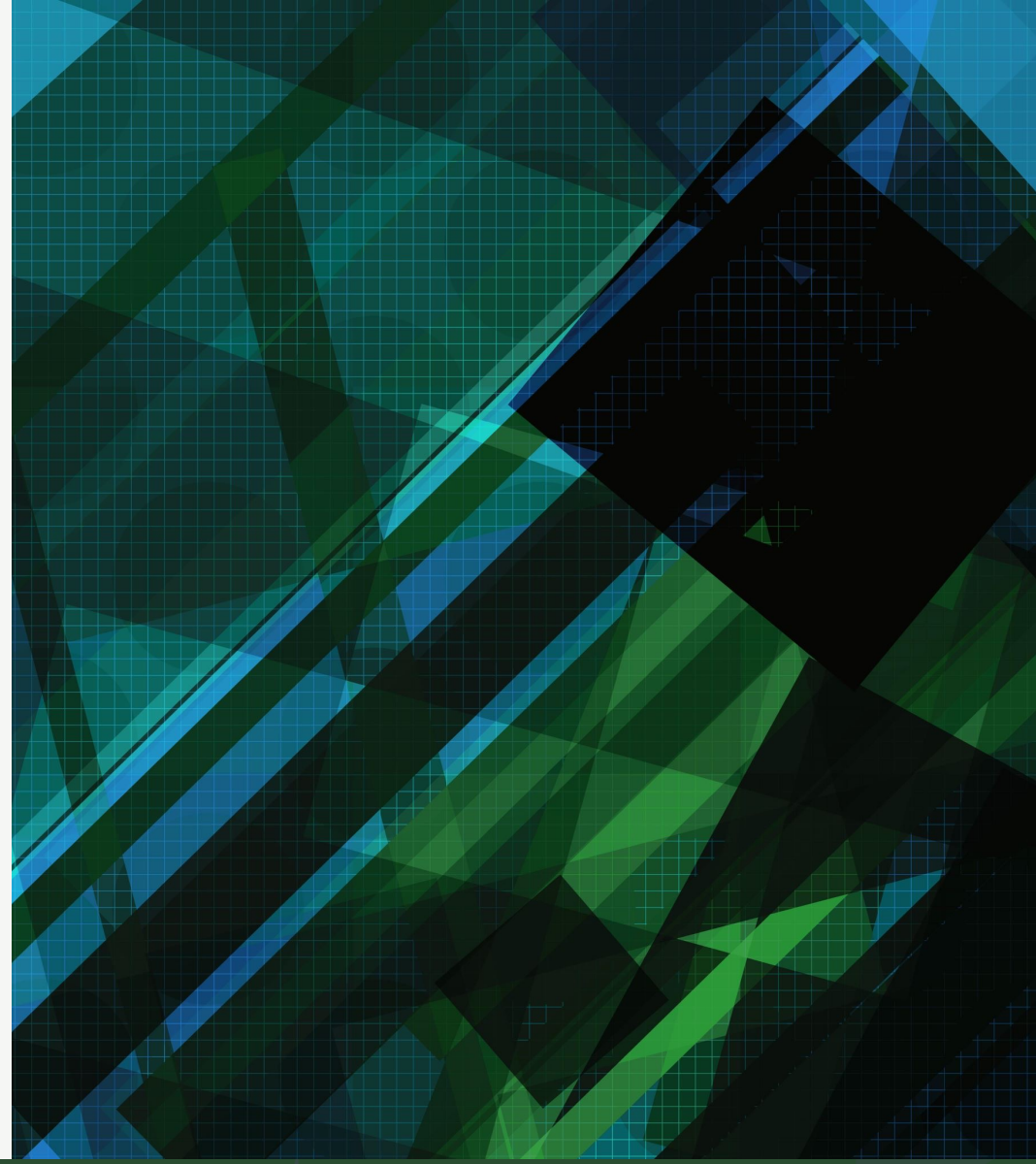
Certified Red Team Operator (CRTO)

Dominic Clark



Who created the CRTO?

- Course created by Zero-Point Security which is ran by Rastamouse.
  - Creator of multiple lab environments on HackTheBox (RastaLabs).
  - Published several widely used tools such as Watson and Tikitorch.
  - Significant contributions to Covenant (C2) among a list of many things I can't fit in here.
  - Recognized within the InfoSec community as a great certificate to have.

What's the CRTO?

- Course and certificate teaching Red Team Tactics
  - Emphasis on learning typical TTPs of a Red Team assessment.
  - Goal of the CRTO is to teach a student core concepts of adversary simulation, command & control, and how to plan a red team engagement.
  - Beginner friendly!

That sounds l33t! What else?

- Lifetime access to course materials!
- Emphasis on learning and utilizing Cobalt Strike (free with the course as of a recent update).
- Learn about each stage of the attack cycle, beginning with OSINT against the ‘dummy’ organization to full domain takeover.
- Take various OPSEC concerns into account.
- Bypass defenses such as Windows Defender, AMSI, and AppLocker.
- 48 Hour Exam (NO REPORT!) – either ☺ or ☹

Before we Proceed..

- Purchased the CRTO in January 2021 and passed the exam in June 2021.
- In August 2021, major updates to course material and labs.
  - Access to Cobalt Strike provided.
  - Private labs instead of shared labs.
  - Splunk provided to hunt for your own indicators.
  - Take the certification without purchasing the course.
- Did I miss out? More on that now.

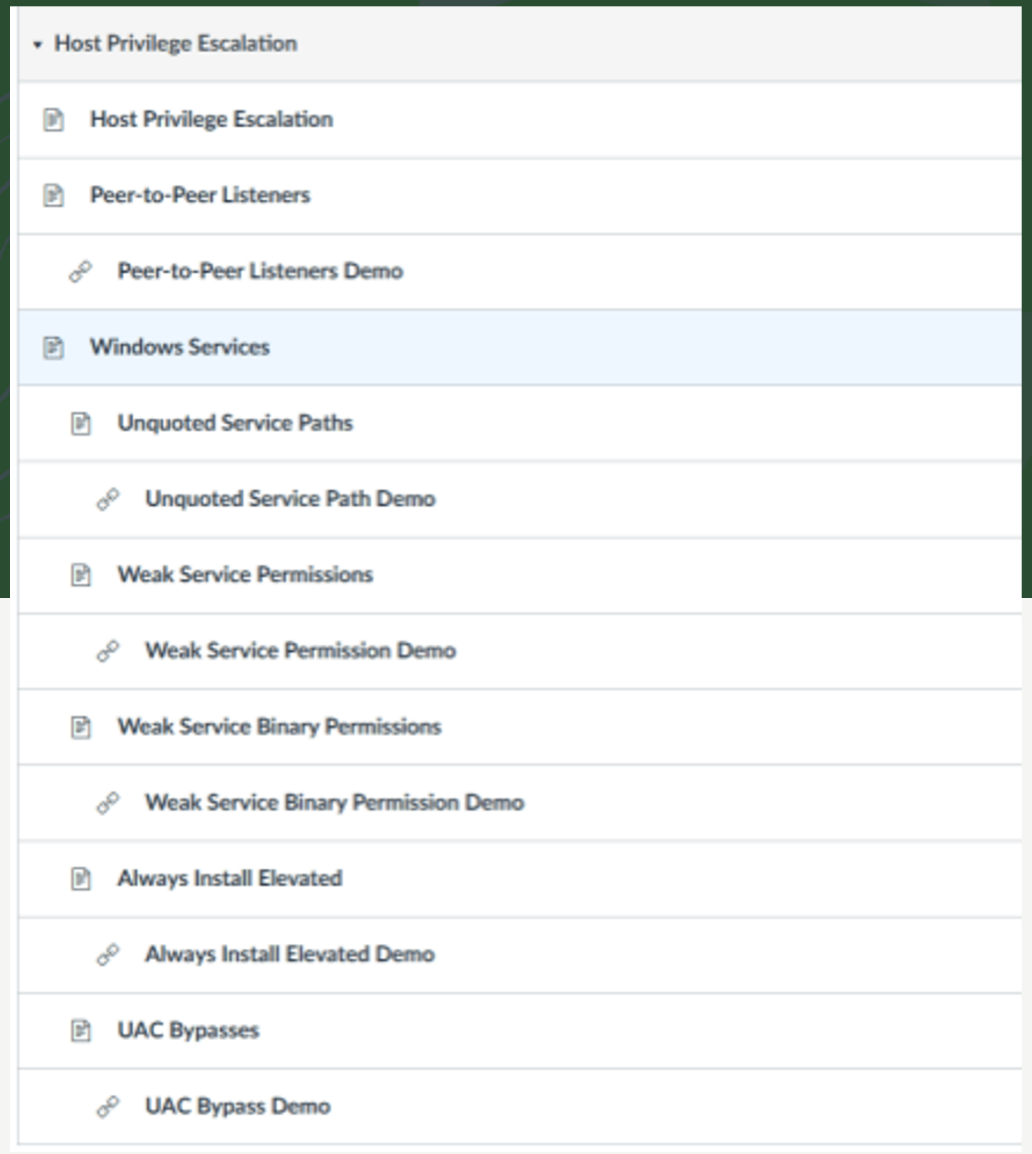
RTO Requirements

- No existing requirements
- Recommendations? Sure.
  - Methodology
  - Knowledge in C#
  - Experience working in Active Directory
  - Experience with a C2 framework will only assist you.
    - And the willingness to wrestle the C2 when needed.
- Course material is more than sufficient to pass the exam.

Modules.. Lots

- Course Introduction
- External Reconnaissance
- Initial Compromise
- Host Reconnaissance
- Host Persistence
- Host Privilege Escalation
- Domain Reconnaissance
- MS SQL Servers
- Lateral Movement
- Impersonation
- Password Cracking
- Session Passing
- Pivoting
- Data Protection API
- Kerberos
- Group Policy
- Domain Dominance
- Forest & Domain Trusts
- LAPS
- Bypassing Defenses
- Data Hunting & Exfil
- Post Engagement
- Extending Cobalt Strike

No.. Really


Host Privilege Escalation
Host Privilege Escalation
Peer-to-Peer Listeners
Peer-to-Peer Listeners Demo
Windows Services
Unquoted Service Paths
Unquoted Service Path Demo
Weak Service Permissions
Weak Service Permission Demo
Weak Service Binary Permissions
Weak Service Binary Permission Demo
Always Install Elevated
Always Install Elevated Demo
UAC Bypasses
UAC Bypass Demo

Attacks

- Password Spraying
- Phishing (HTA and VBA)
- Persistence via Task Scheduler, Startup Folder, etc.
- PowerView, SharpView, ADSearch, BloodHound
- Lateral Movement with PS-Remoting, PSExec, and DCOM
- Pass the Hash, Overpass the Hash, the list goes on!
- Session passing is cool..

Lab Experience

- Extremely realistic labs (Defender, AI, External Presence)
- Hardware and VPN requirements no more!
- Fast and responsive (unlike the OSCP)
- Private! (New)
- You’re getting hands-on experience using the most popular C2 framework for free?
- Back in my day the labs were different..

The Exam

PRACTICAL 48 HOUR
RED TEAM EXERCISE

CAPTURE 3/4 FLAGS

EXAM RESULTS
PROVIDED INSTANTLY

RTO Exam

Awarded to [redacted]outlook.com

Issued on **Jun 8, 2021**

Pass the Red Team Ops exam.

Verified

Last verified by Badgr on **Jan 12, 2022**

Re-verify Badge

Do I Recommend the CRTO?

- Amazing introduction to Red Teaming
- Amazing introduction to Active Directory testing
- Up to date and relevant course materials
- TTP to follow when testing Active Directory
- Hunt your indicators in Splunk?? Whaaat.

A few cons..

- Some sections are a little unpolished (TTP feel)
- Support
- Popularity
- Restrictions on Tooling?