CYBERTRONIUM

Certified Red Team Professional (CRTP)

Overview of

Certified RedTeam Professional

As organizations work to keep from becoming the next breach headline, they increasingly look to exercise their defenses through simulation of the sophisticated attackers they face. Organizations that have adopted an “assume breach” mentality understand it's a matter of when - not if - they will be compromised by these adversaries. The best way to test enterprise security operations against advanced threat actors is through application of the adversary mindset - commonly known as red teaming - through exercises that leverage the same tactics, techniques and procedures (TTPs) as real adversaries.

If you’re looking to learn the tradecraft of adversary simulation operations in enterprise environments, sharpen your offensive technical skillset, and understand how to detect modern offensive tradecraft, Certified Red Team Professional (CRTP) is for you.

The course focuses on “offense-in-depth”, the ability to rapidly adapt to defensive mitigations and responses with a variety of offensive tactics and techniques.

CRTP immerses students in a single simulated enterprise environment, with multiple VMs, up-to-date and patched operating systems, and defenses. In keeping with the assumed breach mentality, the course provides detailed attacker tradecraft post initial access, which includes performing host situational awareness and "safety checks", escalation privileges locally, breaking out of the beachhead, performing advanced lateral movement, escalating in Active Directory, performing advanced Kerberos attacks, and achieving red team objectives via data mining and exfiltration.

The course is fast paced and highly intensive, teaching delegates an in-depth methodology and approach while operating as a professional Red Teamer. We not only show delegates how to perform advanced red team tactics, techniques and procedures (TTP’s) but further cover how to run a successful end-to-end engagement with a focus on operational security and risk.

Programme **Outcome**

- Understand the MITRE ATT&CK Framework with details on techniques, tactics, and procedures (TTP) commonly used by threat actors as this can be used as a reference during Red Teaming.
- Understand the core concepts of adversary simulation, command & control, and how to plan an engagement.
- Learn about each stage of the attack lifecycle from initial compromise to full domain takeover, data hunting, and data exfiltration.
- Learn to mimic the offensive hacker mindset and think outside the box and come up with new attack vectors and approaches
- Discover and leverage vulnerabilities towards take over and data breach
- Perform post-exploitation tasks such as host and network reconnaissance, Pivot to n-tiered networks, and establish persistence.
- Perform Active Directory attacks such as kerberoasting, ASREP, abuse unconstrained delegation and exploit insecure ACLs, and move laterally across a Windows estate.
- Perform a comprehensive red team operation penetration test, from reconnaissance to establishing a foothold and maintaining a covert presence.

Target Audience

- **Red Teamers**
- **Bug Bounty Hunters**
- **Security Analysts**
- **Vulnerability Assessors**
- **Penetration Testers**
- **IT Security Professionals**
- **Security Consultants**
- **Blue Team members, Defenders, and Forensic Analyst**
- **Anyone who wants to learn the Offensive side of Cyber Security**

Pre-requisites

- Cybertronium Certified Penetration Tester or other Pentest certifications
  OR A thorough understanding of Penetration Tests and Security Assessments
- Networking Basics
- Understanding & Navigating Different OSes like Windows, Linux
- Prior knowledge on OWASP TOP 10
- Knowledge of Active Directory

"I thoroughly enjoyed the hands-on approach of the class in relation to all the buckets of theory you get online. Trainer was patient and managed to translate complexity to simplicity so easily. Highly recommended, Thanks man! Truly greatly appreciated!

Director,
Credit Claim Bureau

Amazing instructor! I loved the live hands-on approach. I benefited so much from the trainer, and it was insufficient. I need at least 20-30 days with him, full-time. Thank you, a very good course.

Regional Auditor, Inspection Générale

With this hands-on course, I'm able to know better how to protect my organization from Cyber threats. I highly recommend this course.

Head Of Portfolio Management, Investment Company

Hands-On Labs

CRTP is a 100% hands-on training with practical exercises designed to get you be a red team professional from the word, GO!, so you can find and exploit network, active directory and application vulnerabilities in our intuitive virtualized environment configured with popular hacking tools.

Exam

2 Hours Capture the Flag style Hands-on Exam
70% is the passing score
(Minimum 7 Flags to be captured)

Course Duration
5 Days

trainings@cybertronium.com www.cybertronium.com

Course Outline

Module 1
Introduction to Red Teaming and Understanding of Attack DNA

- Introduction to Red teaming
- Role of red team in organizational security programs
- Red team vs. blue team
- Red team assessment phases
- Red teaming methodology
- Planning red team operations
- Attack Lab Infrastructure
- Threat Intelligence: Frameworks, Platforms, and Feeds
- What is MITRE ATT&CK Framework?
- Tactics, Techniques and Procedures (TTP)
- Indicators of Compromise (IoC) and Indicators of Attack (IoA)
- Mapping to ATT&CK from Raw Data : 2 Hands-on Labs on Real world attack logs.

Module 2
Host Exploitation : Windows & Linux

Host Exploitation on Windows and Linux Operation systems with the following red teaming steps and tons of scenario based hands-on exercises:

- Reconnaissance (OSINT)
- Weaponization & Delivery
- Exploitation
- Establishing a backdoor (C&C)
- Installing multiple utilities
- Privilege escalation, lateral movement, and data exfiltration
- Maintaining persistence

35 Hands-on Exercises on the following 4 Real world scenarios without any automated exploitation tools:

- Microsoft Windows Server exploitation with persistence
- Web Application and FTP exploitation together with Linux privilege escalation, brute force, hash cracking, shell injection, process snooping, c&c communication and many more
- Content Management System and LFI Exploitation together with GTFOBins Privilege Escalation, network file share enumerations, c&c communication and many more
- Jenkins Open-Source Server Exploitation together with Windows Privilege Escalation, network traffic pivoting, c&c communication and many more

Module 3
Active Directory Exploitation

Most enterprise networks today are managed using Windows Active Directory and identity based exploitation is the low hanging fruit for hackers to gain access on the servers and to perform lateral movement and exfiltrate data from critical systems as we have seen in many high profile incidents in ASEAN like SingHealth. This module simulate real world attack with a non-admin user account in the domain and how hackers work their way up to become an enterprise admin. The focus is on exploiting the variety of overlooked domain features and not just software vulnerabilities and to establish that a single machine compromise in a AD environment is enough for an entire organisational compromise.

Following 9 Hands-on Lab Cover AD enumeration, trusts mapping, domain privilege escalation, domain persistence, Kerberos based attacks (Golden ticket), ACL issues, SQL server trusts, Defenses and bypasses of defenses:

- LLMNR Poisoning
- SMB Relay with Interact shell
- Gaining Shell
- IPv6 Attacks
- Pass the Hash/Password
- Token Impersonation
- Kerberoasting attack
- Golden Ticket Attack

Check out our other certification courses

CCSP
Certified Cloud Security Professional

CSOC
Certified SOC Analyst

CPT
Certified Penetration Tester

CTIA
Certified Threat Intel Analyst

CSAU
Certified Security Aware User

CSD
Certified Secure Developer