CERTIFIED RED TEAM PROFESSIONAL

CRTP

Duration: 5 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

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.

OBJECTIVES

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.

- 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 MITRE ATT&CK Framework and able to identify attacker techniques, tactics, and procedures (TTP) to investigate indicators of compromise (IOCs) and provide automated / manual responses to eliminate the attack/incident
- 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.
- 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.

PREREQUISITES

- 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

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

COURSE CONTENTS

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

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

- Microsoft Windows Server exploitation with persistence

GemRain Consulting Sdn Bhd.
33-5.6, Block C, Jaya One, Jalan Profesor Diraja Ungku Aziz, 46200 Petaling Jaya, Selangor, Malaysia
Contact: (+60)3 7931 3036 | (+60)12 613 3667 | Email: enquiry@gemrain.net | Website: www.gemrain.net

- 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
- Host Exploitation on Windows and Linux Operation systems

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