Certified Red Team Professional (CRTP) Training

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

Hands-on Exercises on the following 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 simulates 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