Cyber Technical Operators Course Syllabus (CyTOC)

This 40-hour, five (5) day course teaches cyber operators how to apply cyber threat intelligence, analyze adversarial cyber key terrain, and employ common tactics in support of Red Team operations and threat hunting missions using open-source and commercial tools. This course is designed to expose cyber operators to offensive methodologies, common tool kits, and analytic techniques used to support Red Team and threat hunting objectives.

Through hands-on exercises and team collaboration, CyTOC students will explore use-cases from around the world to practice effective tradecraft and be prepared to operate immediately.

Contact Information

Contact: 443-620-TEAM (8326) Option #2 **or** training@teamworxsecurity.com

Course Description and Course Goals

- Introduction and hands on application of offensive methodologies
- Introduction and hands on application of basic threat hunting techniques
- Understanding of Cyber Threat Intelligence (CTI) and application to Red Team and threat hunting missions
- Identify and explain adversarial cyber key terrain (KT-C)
- Application of Red Team tactics and techniques
- Ability to communicate actions taken into written report or verbal discussion
- Ability to translate written instructions into Red Team or threat hunt actions

Module 1

- Exposure to Key Terrain Cyber and how to use targeting methods against it
- Exposure to Cyber Threat Intelligence (CTI) methodologies
- Understanding and application of OSINT techniques
- Review of intelligence oversight
- Exposure to and application of CTI and OSINT tooling

Module 2

- Review of red cell rules of engagement
- Understanding of offensive methodologies and tradecraft
- Practical application of offensive methodologies and tradecraft
- Understanding of OCO tooling an infrastructure
- Practical application and appropriate use of OCO tools
- Exposure to vulnerability research
- Exposure to technical assessments
- Practical application to vulnerability research and assessment tools

Module 3

- Exposure hashing and hash tooling
- Understanding of common encoding types
- Understanding of tactical scripting methodologies
- Practical application of Python basics
- Practical application of PowerShell basics
- Exposure to Nishang and Shell Script basics

Module 4

- Practical application in automating target enumeration
- Understanding the concept of overcoming target restrictions
- Exposure to active exploitation techniques
- Practical application of network penetration testing
- Understanding of Command and Control mechanisms during active exploitation
- Exposure to cloud and wireless penetration testing
- Understanding of physical penetration testing concepts
- Understanding and application of fuzzing

Module 5

- Practical application of exploitation development
- Understanding of analysis and production
- Practical application of reconnaissance, exploitation, and reporting
- Show positive knowledge transference through capstone exercise

Students will Need

A computer with internet access. Students are welcome to bring any other note taking materials they wish. (some handouts will be provided)

Grading

This course is based on participation within daily discussions and group activities. Students **MUST** be present to do so.

Course Schedule

Course schedules can vary based on customer needs.

Five (5) Day Course Schedule Expectations:

- Daily start time will be 0900 (9 a.m.)
- Daily end time will be between 1600 (4 p.m.) and 1730 (5:30 p.m.)
- Daily lunch break time will be between 1130 to 1300 (1:00 p.m.)
- Daily schedule may flex based on how quickly students are understanding concepts and questions.