CYBER THREAT EMULATION

In Residence
240 hours over 6 weeks

COURSE DESCRIPTION

This course teaches the threat emulation process and provides an in-depth analysis of common cybersecurity vulnerabilities. It also provides students with hands-on threat emulation activities through multiple scenario-based exercises and a hypothetical mission. This course will also provide structural, technical and skill-based content to enhance the student's ability to work within the CTE role and CPT as a whole.

The CTE course encompasses six weeks of instruction and covers the following topics:

- Network Traffic Collection (NTC)
- PowerShell for Responders (PR)
- Tactics, Techniques and Procedures (TTPs)

COURSE OBJECTIVES

After completing this course, students will be able to:

- Explain basic theory, technologies and components that facilitate network data transmission
- Examine network traffic and previously captured data
- Perform a logical and physical assessment of a network to identify potential witness devices and the data they contain
- Assess a network and identify proper placement of a network monitoring sensor
- Configure network data acquisition tools
- Collect and analyze network traffic and system artifacts to identify probing and intrusion techniques
- Examine the capabilities of command line administration
- Express command-line and PowerShell scripting concepts
- Execute commands to accomplish administrative tasks
- Design scripts using branches, loops and functions
- Describe the basics of the Common Information Model (CIM)
- Employ WMIC in accessing WMI objects
- Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
- Analyze threat information
- Develop a Threat Emulation Plan (TEP)

COURSE OBJECTIVES

- Generate mitigative and preemptive recommendations for local defenders
- Develop mission reporting
- Conduct participative operations
- Conduct reconnaissance
- Analyze network logs for offensive and defensive measures
- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)

ASSESSMENTS

Four graded assessments will be administered. No retakes are permitted.

Module and Final Exams

- Open-book format
- Knowledge- and performance-based questions
- Exams require using the Academy's virtual machine-based environments

GRADING CRITERIA

To pass this course, students must meet the following criteria:

- Achieve a score of 70 percent on each exam.
- Achieve a cumulative weighted score of at least 70 percent. Each assessment counts as a specified percentage toward the cumulative weighted score, as shown in the following table.

Assessment	Percent of Total Grade
NTC Final Exam	10%
PR Final Exam	10%
TTPs Module 1 Exam	30%
TTPs Module 2 Exam	50%
Total	**100%**

COURSE SCHEDULE

Week	Activity
1	Pre-course Survey Course Introduction Week 1: Network Traffic Collection (NTC) Module 1 – Introduction to Network Traffic Module 2 – Networks and Witness Devices Module 3 – Assessment and Sensor Placement Module 4 – Capture Module 5 – Analysis NTC Final Exam
2	Week 2: PowerShell for Responders (PR) Module 1 – Introduction to Command-line Administration Module 2 – Pseudocode Module 3 – PowerShell Cmdlets and Syntax Module 4 – Windows Objects Module 5 – WMIC PR Final Exam
3-6	Weeks 3-6: Tactics, Techniques and Procedures (TTPs) Module 1 – CTE Concepts TTPs Module 1 Exam Module 2 – Threat Emulation TTPs Module 2 Exam Post-course Survey