

[View Full Course Details including Latest Schedule Online](#)

PHOENIX TS

# Network Defense Range

**Due to Covid-19 safety restrictions** PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

## Course Overview

The course assumes participants know how to use a computer, and that they're familiar with basic networking and security principles. It does not assume that they've set up basic virtual machines before. Participants will establish the foundation in TCP/IP, this is critical to being able to perform network analysis on a modern enterprise network. Participants will benefit most from this course if they want to learn basic monitoring and analysis tasks, or if they want to augment their understanding of intrusion analysis. Participants will benefit most from this course if they want to learn network analysis tasks, intrusion analysis and incident response. Participants will learn how to recognize and analyze abnormal traffic that could be an attack or an error on the network. Furthermore, the course will add tools to assist in the process of going deeper into analysis. After participants complete this course, they will be able to do the following:

- Identify the required components for a cyber range and build it
- Understand to the lowest level the components and characteristics of TCP/IP
- Apply session analysis techniques to network traffic
- Evaluate IPsec network traffic and understand packet filtering techniques
- List the steps of a hacking methodology
- Perform analysis of hacking techniques and tools
- Understand the components of advanced and sophisticated attacks
- Identify the steps of protocol analysis
- Deploy filters to expedite the analysis of network capture files
- Perform low-level analysis using low-level protocol analysis tools
- Create and customize their own network packets to perform different tasks
- Install, Configure and Tune an Intrusion Detection System
- Deploy analysis tools to assist with network analysis
- Evaluate potential incidents and draft reports of an incident
- List the steps of basic and advanced process analysis



- Understand live memory and the basics of malware analysis
- Explore the concept of leveraging results with different tools

## Course Outline

Module 1: Building a Cyber Range

Module 2: Introduction to Hacking

Module 3: Hacking Analysis Methodology

Module 4: Web Application Hacking

Module 5: Components of Sophisticated Attacks

Module 6: Conducting Protocol Analysis

Module 7: Protocol Analysis One

Module 8: Protocol Analysis Two

Module 9: Protocol Analysis Three

Module 10: Analyzing Basic Attacks

Module 11: Protocol Analysis Tools

Module 12: Advanced Attack Analysis

Module 13: Incident Response

Module 14: Basic Process Analysis

Module 15: Advanced Process Analysis

Module 16: Live Memory Analysis

Module 17: Malware Introduction

Module 18: Malware Analysis 101

Module 19: Leveraging Analysis Results with tools

**Due to Covid-19 safety restrictions** PhoenixTS will temporarily be unable to provide food to our



# PhoenixTS

301-258-8200 | [Sales@PhoenixTS.com](mailto:Sales@PhoenixTS.com) | [www.PhoenixTS.com](http://www.PhoenixTS.com)

students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Starting at **\$1,200**

## ATTENTION

For GSA pricing or Contractor quotes call  
[240.667.7757](tel:240.667.7757)

# GSA



### Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.