Honeywell Academy

CYBERSECURITY: PROFESSIONAL – OT– INDUSTRIAL PENETRATION TESTING FUNDAMENTALS

COURSE OVERVIEW

Course number: HCCP-OT2102
Course duration: 2 Days

Prerequisite courses: None

Required Skills: Basic Understanding of Cybersecurity concepts, Windows and Linux OS Network protocols.

Companies are confronted with a multitude of cybersecurity threats and vulnerabilities, with the attack surface continually expanding. Bad actors are constantly searching for new ways to compromise networks, and no one can be completely safe. Penetration testing provides an avenue for IT professionals to think and act like threat actors, using the same tools and techniques hackers use to find vulnerabilities and mitigate them before an actual attack occurs.

This course is specifically designed for IT professionals who want to get started on a pen testing path. This course provides an in depth understanding of the most common attacks, tools, and techniques attackers use. Training includes lecture time to learn the mindset of an attacker and hands-on labs in our dedicated testing environment so students can use the tools that hackers use in a safe and secure manner.

This course is intended for individuals in roles such as cybersecurity engineers, plant managers, asset owners, and cybersecurity personnel entrusted with security governance, and any IT professional with an interest in learning an attacker's mindset.

COURSE DELIVERY OPTIONS

- Asynchronous Training (AT)
  - ➢ Self-paced with 10 days to complete
- Instructor-Led Training (ILT)
- Virtual Instructor-Led Training (VILT)

COURSE OBJECTIVES

Key Concepts

- Key Principles and Concepts
  - Structure
  - Legal Considerations
- Penetration Testing Framework (PTES)
  - Methodology
- Scoping, Goals, and Rules of Engagement
  - Collaborate with customer on what is and is not allowed
- Linux OS
  - Command basics
  - Difference between Windows and Linux
  - Pentester's OS of choice
- Enumeration
  - Types
  - Process
  - Tools and techniques
- Vulnerability Analysis
  - Environment specific considerations
- Exploitation
  - Definition
  - Tools and techniques
  - Safety Precautions
- Post-Exploitation
  - Tools and techniques
  - Process
- Post-engagement clean-up
  - Legal
  - Special considerations
- Reporting
  - Create a detailed report
  - Data Protection at rest and in motion

Honeywell