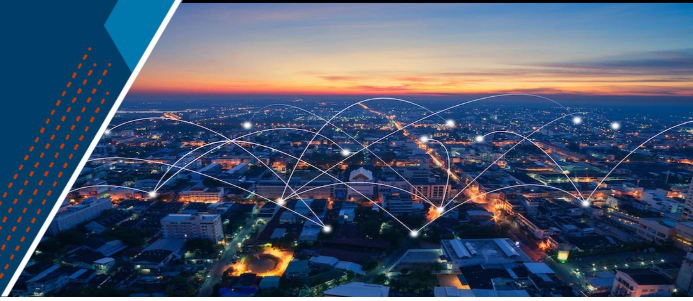
VULNERABILITY ANALYSIS PATHWAY



VULNERABILITY ANALYSIS PATHWAY

The **Vulnerability Analysis Pathway** is a comprehensive 4-week instructor led cybersecurity training course designed to equip IT and cybersecurity professionals with the critical skills needed to identify, assess, and manage vulnerabilities across various digital environments. Starting with foundational concepts, participants progress through hands-on labs and real-world scenarios, mastering key tools and techniques for vulnerability scanning, system assessments, and web application security. By course completion, students develop proficiency in executing comprehensive vulnerability assessments, utilizing industry-standard tools and OWASP methodologies to identify and analyze security weaknesses in both systems and web applications. The course advances through vulnerability chaining, custom script development, and enterprise-level management, teaching students to effectively prioritize risks using vulnerability scoring systems and communicate findings through detailed technical reports. Whether starting out or deepening existing expertise, participants gain practical experience in implementing enterprise-level vulnerability management programs, conducting specialized assessments, and understanding complex attack paths – all essential skills for tackling today's most pressing organizational security challenges.

KEY LEARNING OUTCOMES

- Configure and maintain a secure testing environment for vulnerability analysis
- Conduct comprehensive network vulnerability scans using multiple tools
- Identify and exploit OWASP Top 10 vulnerabilities in a controlled environment
- Develop custom scripts for specialized vulnerability analysis

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- System & Network Administrators
- Cloud Support Engineer
- IT & Security Operations Professionals
- Cybersecurity Incident Responder
- Information Security Specialist
- Vulnerability Management Specialist
- Network Security Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: CompTIA CySA+

This document is marked TLP: CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

PROFICIENCY LEVEL: INTERMEDIATE CYBERSECURITY PROFESSIONAL

Participants should have some technical exposure to basic system and network security concepts and a more robust understanding of foundational IT and cybersecurity principles. The course builds on core competencies and accelerates through complex scenarios and advanced topics within vulnerability analysis and management. A strong foundation in the fundamentals is essential for successfully navigating the course and engaging with the material. This course is not recommended for beginners.

TARGET AUDIENCE

This course is designed for individuals seeking to launch or advance a career in cybersecurity with a specific focus in vulnerability analysis. It is ideal for:

- Aspiring cybersecurity analysts or junior security professionals
- IT professionals transitioning into cybersecurity roles
- Students or recent graduates of cybersecurity or IT programs
- Government personnel currently supporting system hardening, scanning, or compliance operations

RECOMMENDED PREREQUISITES:

While the prerequisites are not mandatory, they are essential for successfully navigating this course. This program is designed for individuals with a more robust understanding of IT and cybersecurity fundamentals—it is not recommended for beginners. If you lack a solid foundation in these areas, the course material may prove too challenging. All Pathway courses are live instructor-led to help facilitate learning and skill development for participants across broad skill levels.

To ensure readiness for the hands-on and technical aspects of the course, participants should ideally have the following exposure and proficiencies prior to enrolling:

- Basic proficiency with computers and operating systems (Windows/Linux), command-line navigation, and general understanding of file systems, folders, and application usage.
- Basic understanding of IT systems, including patch management, software updates, and common misconfigurations. *No prior experience in system hardening, vulnerability scanning, or deep operating systems knowledge is needed.*
- General understanding of networking concepts such as the OSI model (Open Systems Interconnection), IP addressing (Internet Protocol), and network devices like routers, switches, and firewalls.
- Familiarity with basic cybersecurity concepts including the CIA triad (confidentiality, integrity, availability), basic threat types (i.e., malware, phishing), software patching, and high-level understanding on security vulnerabilities.
- Comfort using basic command-line, including directory navigation, file operations, user commands, and introductory scripting capabilities. *No automation or tool-specific experience is required; however, it may be advantageous during training in lab environments*

VULNERABILITY ANALYSIS COURSE OUTLINE

Week 1: The Foundation Scout: *A foundational introduction to essential cybersecurity concepts, focusing on vulnerability analysis through theoretical lectures and hands-on labs, setting the stage for advanced techniques.*

Week 1 Learning Outcomes:

- Configure and maintain a secure testing environment for vulnerability analysis
- Operate basic vulnerability scanning tools and interpret their results
- Understand the fundamental concepts of the vulnerability lifecycle
- Identify and classify different types of vulnerabilities
- Apply basic documentation and reporting practices for vulnerability findings
- Demonstrate understanding of vulnerability scanning tool selection criteria
- Execute basic vulnerability scans in a controlled environment
- Interpret and validate scanning results to eliminate false positives

Week 2: The System Sentinel: *An in-depth exploration of network and system vulnerabilities, emphasizing hands-on experience with CVSS, vulnerability assessments, and the identification, analysis, and documentation of security weaknesses across various platforms and architectures.*

Week 2 Learning Outcomes:

- Conduct comprehensive network vulnerability scans using multiple tools
- Identify and analyze common operating system vulnerabilities
- Apply the CVSS scoring system to prioritize vulnerabilities
- Assess system configurations for security weaknesses
- Perform vulnerability analysis across different operating systems
- Develop network and system vulnerability assessment methodologies
- Create detailed technical reports documenting system vulnerabilities
- Recommend appropriate remediation strategies for identified vulnerabilities

Week 3: The Web Warrior: *An intensive focus on web application vulnerabilities, emphasizing the OWASP Top 10, cloud penetration testing, and hands-on practice with automated and manual testing techniques to identify and exploit common vulnerabilities in traditional and cloud environments*

Week 3 Learning Outcomes:

- Identify and exploit OWASP Top 10 vulnerabilities in a controlled environment
- Perform both automated and manual web application security testing
- Assess cloud-based applications for security vulnerabilities
- Execute client-side and server-side vulnerability analysis
- Develop secure coding recommendations based on findings
- Utilize web application security testing tools effectively
- Create web application security assessment reports
- Design remediation strategies for web application vulnerabilities

Week 4: The Advanced Architect *An advanced exploration of vulnerability analysis and management, focusing on vulnerability chaining, custom script development, and enterprise-level strategies, culminating in a capstone project involving comprehensive end-to-end system vulnerability analysis.*

Week 4 Learning Outcomes:

- Develop custom scripts for specialized vulnerability analysis
- Implement enterprise vulnerability management programs
- Perform vulnerability chaining analysis to identify attack paths

- Create comprehensive vulnerability assessment strategies
- Apply advanced exploitation techniques in a controlled environment
- Design metrics for measuring vulnerability management effectiveness
- Execute end-to-end vulnerability assessments of complex systems
- Present technical findings to various stakeholder groups