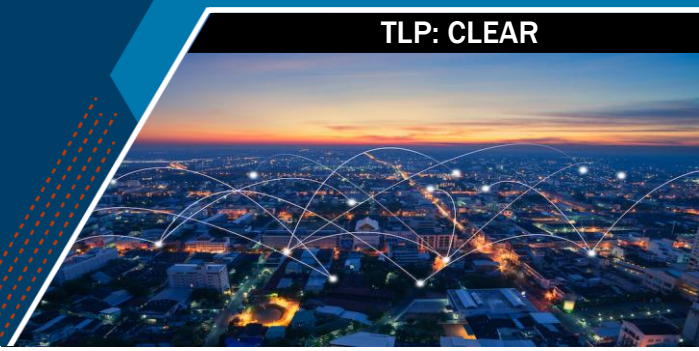
VULNERABILITY ANALYSIS PATHWAY



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+

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 vulnerability analysis, combining theoretical knowledge with hands-on experience in security concepts, vulnerability types, and scanning tools through practical lab environments.*

Week 1 Learning Outcomes:

- Explain core cybersecurity principles and vulnerability analysis concepts
- Identify and categorize different types of vulnerabilities (software, network, web application)
- Understand common vulnerability patterns and attack vectors
- Describe the vulnerability lifecycle including discovery, disclosure, and patch management
- Configure and utilize both open-source and commercial vulnerability scanning tools
- Execute complete vulnerability scans and interpret results
- Generate professional vulnerability assessment reports
- Apply vulnerability tracking methodologies

Week 2: The System Sentinel: *Advanced training in network and system vulnerability analysis, focusing on protocol vulnerabilities, operating system security, and risk assessment through hands-on labs and real-world scenarios.*

Week 2 Learning Outcomes:

- Analyze network protocol vulnerabilities and TCP/IP security issues
- Identify and exploit common network attack vectors
- Perform protocol analysis using industry-standard methods
- Assess operating system vulnerabilities across Windows and Linux platforms
- Implement OS hardening techniques to mitigate vulnerabilities
- Identify and remediate system misconfigurations and security baseline deviations
- Apply CVSS scoring system to evaluate vulnerability severity
- Utilize vulnerability metrics for risk assessment and prioritization
- Conduct comprehensive network and system vulnerability assessments

Week 3: The Web Warrior: *Comprehensive web application and cloud security analysis, incorporating OWASP methodologies and cloud-specific vulnerabilities through practical testing and assessment exercises.*

Week 3 Learning Outcomes:

- Analyze and exploit OWASP Top 10 vulnerabilities
- Perform web application architecture and attack surface analysis
- Identify and test entry points in web applications
- Detect and exploit client-side vulnerabilities including XSS
- Identify and exploit server-side vulnerabilities including SQL injection
- Conduct cloud penetration testing following shared responsibility models
- Assess cloud-specific vulnerabilities and security controls
- Execute comprehensive web application security assessments
- Document and report web and cloud vulnerability findings

Week 4: CompTIA CySA+ Certification Preparation *Intensive certification preparation focusing on CompTIA CySA+ objectives through practice exams, labs, and comprehensive review of vulnerability analysis concepts.*

Week 4 Learning Outcomes:

- Master CompTIA CySA+ exam objectives and domains
- Apply vulnerability analysis concepts to certification scenarios
- Complete practice exams and identify knowledge gaps

- Execute hands-on labs aligned with CySA+ requirements
- Synthesize vulnerability analysis best practices
- Demonstrate proficiency in all course concepts through final assessment
- Develop effective study strategies for certification success