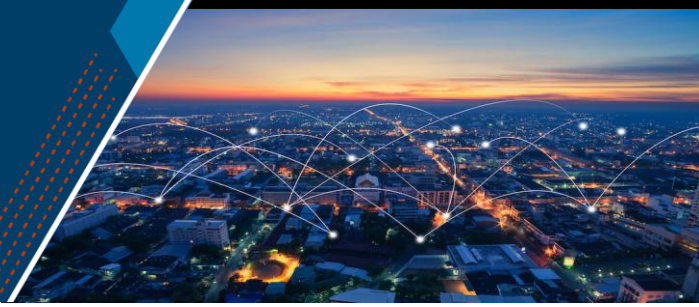
SYSTEMS SECURITY ANALYSIS PATHWAY



SYSTEMS SECURITY ANALYSIS PATHWAY

The **Systems Security Analysis Pathway** is a comprehensive 4-week, instructor-led cybersecurity training course designed to develop expertise in systems security analysis and protection. Starting with foundational security principles, participants progress through operating system hardening, network security, and application protection while gaining hands-on experience with industry-standard tools. The course emphasizes practical application through vulnerability scanning, firewall configuration, and intrusion detection across various environments. By course completion, students gain introductory skills to design and implement comprehensive security assessment strategies, execute full-scale vulnerability assessments, and effectively communicate findings through professional documentation.

KEY LEARNING OUTCOMES

- Set up and configure secure virtual environments for cybersecurity testing
- Implement system hardening techniques across Windows and Linux systems
- Identify and exploit common web application vulnerabilities
- Assess cloud infrastructure for security vulnerabilities

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- Systems Security Analyst
- Security Engineer
- IT Security Specialist
- Infrastructure Security Analyst
- Security Operations Analyst
- Network Security Engineer
- Application Security Analyst
- Cloud Security Engineer

PATHWAY METRICS

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

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: ENTRY-LEVEL CYBERSECURITY PROFESSIONAL

Participants should have a solid foundational understanding of basic IT and cybersecurity principles. Prior hands-on experience with system security tools or frameworks may be beneficial but is not required. The course is designed to build on foundational knowledge and introduce increasingly complex concepts and practical applications.

Although this course is open to entry-level professionals, it includes hands-on practice, lab exercises, and real-world simulations, offering more advanced professionals the opportunity to further refine their skills and core competencies in practical scenarios.

TARGET AUDIENCE

This pathway is designed for individuals who want to build or strengthen their foundational skills in cybersecurity with a focus on systems security analysis. It is especially suited for:

- Aspiring cybersecurity analysts and entry-level security practitioners
- IT personnel expanding into security-focused roles
- Students or recent grads with a technical background looking to specialize in system security
- Government staff supporting system administration, risk management, or compliance activities

RECOMMENDED PREREQUISITES:

While the prerequisites listed are recommended to help you successfully complete the course, they are not mandatory. If you are confident in your skills and capabilities and can dedicate the time needed to fully engage in the training material, we encourage you to apply. 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 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 protocols like Transmission Control Protocol/ Internet Protocol (TCP/IP) and Hypertext Transfer Protocol (HTTP). *No prior exposure to packet analysis, protocol vulnerabilities, or secure network design is needed.*
- 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

SYSTEM SECURITY ANALYSIS COURSE OUTLINE

Week 1: Fundamentals of Systems Security Analysis: *A comprehensive introduction to systems security fundamentals, combining theoretical concepts with practical experience in threat modeling, risk assessment, and vulnerability scanning through hands-on labs with industry-standard tools.*

Week 1 Learning Outcomes:

- Set up and configure secure virtual environments for cybersecurity testing
- Explain core cybersecurity concepts including the CIA triad and security principles
- Apply threat modeling methodologies including STRIDE framework and attack trees
- Perform foundational risk assessments using standard frameworks
- Execute basic vulnerability scans using industry tools
- Understand and apply security standards including ISO 27001 and NIST SP 800-53
- Map compliance requirements to security controls
- Create basic security documentation and audit preparations

Week 2: Operating System and Network Security Analysis: *An intensive exploration of operating system and network security analysis, focusing on system hardening, security controls, and infrastructure protection through practical implementation exercises.*

Week 2 Learning Outcomes:

- Evaluate and implement OS security mechanisms across Windows and Linux systems
- Analyze Windows security architecture including Active Directory and Group Policies
- Configure Linux security features including SELinux, AppArmor, and SSH hardening
- Identify and mitigate common OS vulnerabilities including privilege escalation
- Assess network protocol security and TCP/IP security implications
- Identify and defend against common network attacks (MITM, ARP spoofing, DDoS)
- Implement defense-in-depth strategies with multi-layered security controls
- Configure and manage IDS/IPS systems using signature and anomaly-based detection
- Develop secure configuration management and patch management strategies
- Utilize security monitoring tools including SIEM for real-time threat detection

Week 3: Application and Web Security Analysis: *A practical immersion in application and web security analysis, incorporating OWASP standards and secure development practices through hands-on testing and vulnerability assessment.*

Week 3 Learning Outcomes:

- Identify and exploit common web vulnerabilities (SQL injection, XSS, CSRF, SSRF, IDOR)
- Analyze and mitigate OWASP Top 10 security risks
- Implement secure coding practices to prevent vulnerabilities
- Integrate threat modeling into the SDLC process
- Apply DevSecOps and CI/CD security best practices
- Compare and secure REST vs GraphQL API architectures
- Configure OAuth2, OpenID Connect, and JWT authentication mechanisms
- Implement API gateway security controls and rate limiting
- Perform web application penetration testing using Burp Suite and OWASP ZAP
- Execute both automated and manual security testing methodologies

Week 4: Advanced Topics and CompTIA Security+ Preparation: *Comprehensive preparation for CompTIA Security+ certification, focusing on fundamental security concepts, controls, and cryptographic solutions through review sessions*

and practice exams.

Week 4 Learning Outcomes:

- Compare and contrast various types of security controls
- Summarize fundamental security concepts for certification readiness
- Explain the importance of change management processes and security impact
- Apply appropriate cryptographic solutions to security scenarios
- Master CompTIA Security+ exam objectives and domains
- Complete practice questions and certification-focused labs
- Demonstrate proficiency in security control implementation