

COMPTIA SECURITY + SY0-501

Course Outline

Mod 1 Threats, Attacks, and Vulnerabilities

- 1.1 Introduction
- 1.2 Types Of Malware- Part 1
- 1.3 Types Of Malware- Part 2
- 1.4 Types Of Attacks- Part 1
- 1.5 Types Of Attacks- Part 2
- 1.6 Types Of Attacks- Part 3
- 1.7 Types Of Attacks- Part 4
- 1.8 Types Of Attacks- Part 5
- 1.9 Threat Actors- Part 1
- 1.10 Threat Actors- Part 2
- 1.11 Penetration Testing And Vulnerability Scanning- Part 1
- 1.12 Penetration Testing And Vulnerability Scanning- Part 2
- 1.13 Impact Of Vulnerabilities- Part 1
- 1.14 Impact Of Vulnerabilities- Part 2

Mod 2 Technologies and Tools

- 2.1 Networking Hardware And Software- Part 1
- 2.2 Networking Hardware And Software- Part 2
- 2.3 Networking Hardware And Software- Part 3
- 2.4 Networking Hardware And Software- Part 4
- 2.5 Networking Hardware And Software- Part 5
- 2.6 Networking Hardware And Software- Part 6
- 2.7 Security Assessment- Part 1
- 2.8 Security Assessment- Part 2
- 2.9 Troubleshooting Issues- Part 1
- 2.10 Troubleshooting Issues- Part 2
- 2.11 Securing Mobile Devices- Part 1
- 2.12 Securing Mobile Devices- Part 2
- 2.13 Securing Mobile Devices- Part 3
- 2.14 Securing Mobile Devices- Part 4
- 2.15 Secure Protocols- Part 1
- 2.16 Secure Protocols- Part 2

Mod 3 Architecture and Design

- 3.1 Secure Network Architecture- Part 1
- 3.2 Secure Network Architecture- Part 2
- 3.3 Secure System Designs- Part 1
- 3.4 Secure System Designs- Part 2
- 3.5 Secure Staging Deployment Concepts
- 3.6 Embedded Systems- Part 1
- 3.7 Embedded Systems- Part 2
- 3.8 Application Development And Deployment- Part 1
- 3.9 Application Development And Deployment- Part 2
- 3.10 Application Development And Deployment- Part 3
- 3.11 Physical Security Controls- Part 1
- 3.12 Physical Security Controls- Part 2
- 3.13 Physical Security Controls- Part 3
- 3.14 Cloud Virtualization- Part 1
- 3.15 Cloud Virtualization- Part 2

Mod 4 Identity and Access Management

- 4.1 Identity And Access Management- Part 1
- 4.2 Identity And Access Management- Part 2
- 4.3 Identity And Access Services- Part 1
- 4.4 Identity And Access Services- Part 2
- 4.5 Management Controls- Part 1
- 4.6 Management Controls- Part 2
- 4.7 Account Management Practices- Part 1
- 4.8 Account Management Practices- Part 2
- 4.9 Account Management Practices- Part 3

Mod 5 Risk Management

- 5.1 Organizational Security- Part 1
- 5.2 Organizational Security- Part 2
- 5.3 Business Impact Analysis Concepts- Part 1
- 5.4 Business Impact Analysis Concepts- Part 2
- 5.5 Risk Management- Part 1
- 5.6 Risk Management- Part 2
- 5.7 Incident Response Procedures- Part 1
- 5.8 Incident Response Procedures- Part 2
- 5.9 Forensics- Part 1
- 5.10 Forensics- Part 2
- 5.11 Disaster Recovery- Part 1
- 5.12 Disaster Recovery- Part 2
- 5.13 Types Of Control- Part 1
- 5.14 Types Of Control- Part 2
- 5.15 Data Security And Privacy Practices- Part 1
- 5.16 Data Security And Privacy Practices- Part 2

Mod 6 Cryptography and PKI

- 6.1 Cryptographic Basics- Part 1
- 6.2 Cryptographic Basics- Part 2
- 6.3 Cryptographic Basics- Part 3
- 6.4 Cryptographic Algorithms- Part 1
- 6.5 Cryptographic Algorithms- Part 2
- 6.6 Wireless Security- Part 1
- 6.7 Wireless Security- Part 2
- 6.8 Implementing PKI- Part 1
- 6.9 Implementing PKI- Part 2
- 6.10 Implementing PKI- Part 3
- 6.11 Conclusion

Course Duration: 20 hours 49 minutes