STUDY PLAN
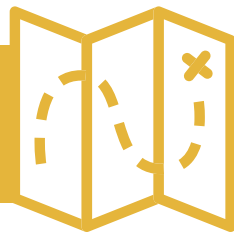
CompTIA Security+ SY0-501

Total Videos: **110**   Time: **23 hrs**

CBTnuggets

Learners use a great variety of strategies to attack their training. Here are some options you can choose from to get the most out of your training experience:

Proceed through all CBT Nuggets video training on double-speed to develop a strong overview of the material; Then proceed through all the training for a second time, taking good notes and focusing on deeper learning.

OR

Proceed through all CBT Nuggets video training, taking good notes and focusing on deep learning on the first pass; Then proceed back through all training a second time, using double-speed when appropriate.

Supplement all video training with book study and practical application of knowledge.

Develop a test environment where new skills can be practiced.

Learn more about how to get all you can out of your practice exam experience from a quick video by Keith Barker ▶

CBT Nuggets offers practice exams as part of your subscription. You can take the practice exams as many times – and as often – as you like! Here are some tips to help you take full advantage of this excellent resource:

⚠ **PLAN TO TAKE THE PRACTICE EXAM 3 TIMES**

FIRST EXAM

Create a baseline against which you can measure your progress with future exams.

Identify areas of weakness in order to direct your training as you move forward.

SECOND EXAM

Measure your progress since your first practice exam! Ask yourself: Are you retaining the information and material you learned at the beginning of your training? Are there areas to which you should return now to ensure your understanding before moving forward?

The results from your second practice exam experience should help you identify areas where you may need to spend extra effort and energy in the training ahead.

THIRD EXAM

Measure your progress against your first two practice exams! Ask yourself: Are you scoring 90% by now? If so, you might be ready for the real thing!

Allow the results from your practice exam to direct your review ahead of your certification exam. Ask yourself: Are you retaining all the material? And are you understanding it well?

CompTIA Security+ SY0-501

WEEK 1

1. Welcome to Security+ 2. Infrastructure Security Devices *32 min.*	3. Application and Traffic Analysis 4. Network Segmentation and Separation with VLANs *26 min.*	5. Proper Placement of Technology to Improve Security 6. ACL Case Study *23 min.*	7. Design Considerations 8. Leveraging Best Practices, Frameworks, and Guidelines *24 min.*	9. NAT and PAT Case Study 10. Firewall and Switch Protection Mechanisms *29 min.*

EXTRA MILE

Explore the CompTIA website to learn more about the Security+ exam, its requirements, and available resources.

Download CBT Nuggets apps to your various mobile devices so you can have your training with you when you're on the go!

"With self-discipline most anything is possible."

– Theodore Roosevelt

WEEK 2

11. Virtualization Overview

12. IPsec, Protocols, and Well-known Ports

34 min.

13. ICMP and a Few More Protocols

14. Checking for and Using Secure Protocols

24 min.

15. Security for WiFi

16. VPNs and Updates for Mobile Security

23 min.

17. Case Study: Technology and Tools

18. Risk Overview

37 min.

19. Risk Calculation

19 min.

EXTRA MILE

Consider purchasing an exam preparation book to further supplement your training. (There are lots of good ones, so choose the one you feel will best meet your unique needs!)

Visit the CBT Nuggets blog to learn more about how to get the most out of your practice exam experience!

Take the Practice Exams! Use the results to drive your ongoing study.*
Transcender CompTIA Cert - SY0-501

*Keep in mind that you've just started the training - so you probably won't ace the exam. This is just to establish a benchmark for future practice exam performance.

WEEK 3

20. Attack Vectors, Risk Management, and Recovery

21. Third-Party Risk from Integration

23 min.

22. Change Management and Account Auditing

23. Data Loss Prevention (DLP)

28 min.

24. Forensics

25. Incident Response Concepts

32 min.

26. Security Awareness, RBAC, and Data Labeling

27. Passwords, Best Practices, and Standards

30 min.

28. Environmental Controls

29. Physical Security

24 min.

EXTRA MILE

Create flashcards! It's a little old school, but it works! Or, take advantage of free, online resources that can help like cram.com.

Schedule your certification exam with an approved testing site.

Obtain and review the CompTIA Security+ exam objectives.

"Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible."

– St. Francis of Assisi

WEEK 4

30. Business Continuity 31. Planning Ahead for Security *27 min.*	32. Fault Tolerance 33. Controls for Confidentiality *33 min.*	34. Tools and Controls for Data Integrity 35. Availability and Safety *25 min.*	36. Malware: Adware - Spyware 37. Trojans, Backdoors, and More Malware *31 min.*	38. Attack Types MITM - Spear Fishing 39. Attack Types: Xmas - Client Side *35 min.*

EXTRA MILE

Retake the Practice Exams! Use the results to drive your ongoing study.*
Transcender CompTIA Cert - SY0-501

*Generally speaking, you should be able to score about 90% on the practice exams if you expect to succeed on your certification exam.

"The results you achieve will be in direct proportion to the effort you apply."

– Denis Waitley

WEEK 5

40. Password Attacks and Watering Holes 41. Social Engineering Threats *28 min.*	42. Vishing and Why Social Engineering Works 43. Wireless Attacks *28 min.*	44. Cross-site and Injection Attacks 45. Application Attacks *30 min.*	46. Monitoring and Device Hardening 47. Network Access and Data Protection *35 min.*	48. Baselines, Detection, and Reporting 49. Analyzers and Scanners *32 min.*

EXTRA MILE

Join the CBT Nuggets Learners Community on Slack! Join other CBT Nuggets learners in a community where you can post questions, share study resources, and connect with IT experts all over the world.

*Please allow 48 hours for your request to join the community to be processed.

"Success is dependent on effort."

– Sophocles

50. Tools for a Security Posture Assessment

51. Discovering and Assessing Threats

27 min.

52. Penetration Testing

53. Techniques for Securing Apps

25 min.

54. Application Security Controls

55. App Development and Deployment Concepts

28 min.

56. Mobile Device Security Overview

57. Mobile Device Policies

27 min.

58. Benefits of Following a Mobile Device Policy
59. Mobile Devices and Auto-Wipe
60. Security Considerations for Mobile Devices

15 min.

61. Host Security

62. Hardware and Virtualization Security

25 min.

EXTRA MILE

Consider activating a free trial for CompTIA's CertMaster, allowing you to assess your preparedness for the exam.

"When you link desire with effort you can accomplish extraordinary things and lead an extraordinary life."

- Michael Josephson

63. Strategies and Controls to Reduce Risk

64. Data Security

19 min.

65. Securing Data with H/W, Controls, and Policy

66. Elements of Secure Systems

18 min.

67. Security in Static Environments

68. AAA Concepts

25 min.

69. Authentication Protocols and Services

70. Multifactor Authentication

33 min.

71. Authentication Controls

72. Management and Controls for Access and Identity

29 min.

73. Controlling Access via Authorization

19 min.

EXTRA MILE

LEARN WHAT TO EXPECT ON YOUR EXAM:
• You need to earn 750 to pass the exam
• You will have a maximum of 90 minutes to complete your exam

"Success is the sum of small efforts, repeated day in and day out."

- R. Collier

WEEK 8

74. Account Management

75. Symmetric and Asymmetric Encryption

40 min.

76. Cryptography Considerations

77. Crypto Key Management

34 min.

78. Hashing and Encryption Protocols

79. Comparing Cryptography Algorithms

38 min.

80. PKI Overview

81. PKI and Digital Certificate Uses

23 min.

82. Layered Security Case Study

11 min.

EXTRA MILE

Gather support for your training by sharing your training goals with friends, family, and colleagues.

"To be prepared is half the victory."

- Miguel de Cervantes

WEEK 9

83. Attack Types and Vectors
84. Vulnerabilities as Part of IoT
85. Certificate Warnings and Trust Models
23 min.

86. Threat Actor Types and Ethics
87. Reconnaissance Information Gathering Concepts
88. Hacking Vocabulary and Terms
23 min.

89. Malware Concepts
90. Case Study: A System Compromised by Malware
91. Network Scanning Overview
20 min.

92. Factors Driving Vulnerability Management
93. Trojans
94. Port Security
27 min.

95. Scanning Methodologies
96. Focused Vulnerability Scanning
97. Sniffing Overview
28 min.

98. Vulnerability Scanning
99. Case Study: Slow Performance
19 min.

EXTRA MILE

Retake the Practice Exams! Use the results to drive your ongoing study.*
Transcender CompTIA Cert - SY0-501

*Use your results to drive your final review ahead of your exam!

"No one succeeds without effort. Those who succeed owe their success to perserverance."

- Ramana Maharshi

| 100. Social Engineering Overview

101. System Hacking Stages and Goals

24 min. | 102. Buffer Overflow
103. OWASP BWAP

24 min. | 104. Honeypots and Honeynets

105. Centralized Identity Management

26 min. | 106. SSO, Kerberos, and Security Threats

107. Incident Response

30 min. | 108. Penetration Testing Legally

109. SCAP Overview Considerations for Mobile Devices

16 min. | 110. Case Study #1

21 min. |

EXTRA MILE

Consider activating a free trial for CompTIA's CertMaster, allowing you to assess your preparedness for the exam.

"When you link desire with effort you can accomplish extraordinary things and lead an extraordinary life."

- Michael Josephson

THE BIG DAY!

Take the exam.

Get a good night's sleep ahead of your exam!

Brag about it! Tweet us or let us know how your exam went and what you're doing to celebrate your success!