Professor Messer’s
CompTIA SY0-501
Security+
Practice Exams

by James “Professor” Messer

Click here to unlock the complete book!

http://www.ProfessorMesser.com
Contents

Introduction

The CompTIA SY0-501 Security+ Certification .......................... i
How to Use This Book .................................................. ii

Practice Exam A

Performance-Based Questions ........................................ 1
Multiple Choice Questions .............................................. 5
Multiple Choice Quick Answers ................................. 37
Detailed Answers ...................................................... 39

Practice Exam B

Performance-Based Questions ........................................ 137
Multiple Choice Questions ............................................. 141
Multiple Choice Quick Answers ................................. 171
Detailed Answers ...................................................... 173

Practice Exam C

Performance-Based Questions ........................................ 267
Multiple Choice Questions ............................................. 271
Multiple Choice Quick Answers ................................. 299
Detailed Answers ...................................................... 301
About the Author

James Messer is an information technology veteran whose career has included supercomputer operations, system administration, network management, and IT security.

James is also the founder and CEO of Messer Studios, a leading publisher of training materials for IT certification exams. With over 84 million videos viewed and 350,000 subscribers, Professor Messer's training has helped thousands of students realize their goals of a profession in information technology.
Introduction

The process of answering a test question is our ultimate test of knowledge. After hours of video watching, book reading, and note taking, do you really know the material? If you're trying to prove yourself, nothing beats getting the right answer.

This book contains three sample exams containing performance-based and multiple-choice questions for the Security+ exam. I've personally curated every question to make sure this Q&A matches the expectations of the SY0-501 Security+ exam.

I hope this book will help you be the smartest one in the room. Best of luck with your studies!

- Professor Messer

The CompTIA SY0-501 Security+ Certification

CompTIA's Security+ certification is the entry point for IT security professionals. If you're planning on securing the data and networks on the world's largest networks, then you're in the right place.

Earning the Security+ certification requires the completion of one exam covering a broad range of security topics. After completing the certification, a CompTIA Security+ certified professional will have an understanding of attack types, network security technologies, secure network architecture concepts, cryptography, and much more.

Here's the breakdown of each domain and the percentage of each topic on the SY0-501 exam:

Domain 1.0 - Threats, Attacks, and Vulnerabilities - 21%
Domain 2.0 - Technologies and Tools - 22%
Domain 3.0 - Architecture and Design - 15%
Domain 4.0 - Identity and Access Management - 16%
Domain 5.0 - Risk Management - 14%
Domain 6.0 - Cryptography and PKI - 12%
How to Use This Book

This book contains three separate 90-question practice exams; Exam A, Exam B, and Exam C. The exams are designed to emulate the format and complexity of the actual Security+ exam.

• Take one exam at a time. The difficulty levels are similar between exam, so it doesn’t matter which exam you take first.

• The actual Security+ exam is 90 minutes in length, so try setting a timer when you start your practice exam. Time management is an important part of the exam.

• The first section of each practice exam is the list of questions. There’s a link after every question that will jump immediately to the quick answer page or the detailed answer page. If you’re using the digital version, your PDF reader keys can quickly jump back to the question page. Adobe Reader in Windows uses Alt-Left arrow and macOS Preview uses Command-[ to move back to the previous view. Be sure to check your PDF reader for specific navigation options.

• The quick answer page is a consolidated list of the answers without any detail or explanation. If you want to quickly check your answer sheet, this is the page for you.

• A detailed answer is available for each exam question. This section repeats the question, the possible answers, and shows the answer with a detailed explanation. This section is formatted to show only one answer per page to avoid giving away the answer to any other questions. Digital readers can use your PDF reader’s back button to quickly jump back to the questions.

• As you go through the exam, write down the answers on a separate sheet of paper. You can check the answers after the 90 minutes have elapsed.

• You can grade your results against the quick answer page. For incorrect responses, be sure to check the detailed answer pages for information on why certain answers were considered correct or incorrect.

• After each detailed answer, a video link is available for more information on the topic. You can click the link in your PDF or use your camera to view the QR (Quick Response) code on the page. Your camera app will provide a notification message that will launch the video page in your browser. The URL is also provided for manual entry.
You have the option of using each practice test as a 90 minute timed exam, or as a casual Q&A. Try stepping through each question, picking an answer, and then jumping to the detailed explanation to learn more about each possible answer.

Here's a scoring chart:

**Less than 63 questions correct / 70% and lower** - Use the exam objectives at the end of each detailed answer to determine where you might need some additional help.

**63 to 72 questions correct / 70% to 80%** - You're so close! Keep working on the areas you're missing and fill in those gaps.

**73 to 81 questions correct / 80% to 90%** - This is a strong showing, but some additional studying will help you earn points on the real exam.

Although the actual Security+ exam does not calculate the final score as a percentage, getting an 85% on the practice exam can be considered a passing grade.

**More than 81 questions correct / over 90%** - You're ready for the real thing! Book your exam and earn your Security+ certification!

The detailed answer pages break down every correct answer and every incorrect answer. Although it's useful to know when you got a question right, it's more important if you understand exactly why a question was marked wrong. If you understand all of the technologies on these sample exams, then you'll be ready for the real thing.
**Practice Exam A**  
**Performance-Based Questions**

**A1.** Match the description with the most accurate attack type. Not all attack types will be used.

**Attack Types:**

<table>
<thead>
<tr>
<th>Hoax</th>
<th>Social Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Spoofing</td>
</tr>
<tr>
<td>Vishing</td>
<td>Whaling</td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>DDoS</td>
</tr>
</tbody>
</table>

- **Attacker obtains bank account number and birth date by calling the victim**  
  Select an Attack Type: *Social Engineering*

- **Attacker modifies a legitimate DNS server to resolve the IP address of a malicious site**  
  Select an Attack Type: *Man-in-the-Middle*

- **Attacker intercepts all communication between a client and a web server**  
  Select an Attack Type: *Hoax*

- **Multiple attackers overwhelm a web server**  
  Select an Attack Type: *Social Engineering*

- **A virus alert appears in your browser from Microsoft with a phone number to call for support**  
  Select an Attack Type: *Spam*
A6. You’ve hired a third-party to gather information about your company’s servers and data. The third-party will not have direct access to your internal network but can gather information from any other source. Which of the following would best describe this approach?

- A. Backdoor testing
- B. Passive reconnaissance
- C. OS fingerprinting
- D. Grey box penetration testing

Quick Answer: 5
The Details: 9

A7. Which of these protocols use TLS to provide secure communication? (Select TWO)

- A. HTTPS
- B. SSH
- C. FTPS
- D. SNMPv2
- E. DNSSEC
- F. SRTP

Quick Answer: 5
The Details: 10

A8. Which of these threat actors would be MOST likely to attack systems for direct financial gain?

- A. Organized crime
- B. Hacktivist
- C. Nation state
- D. Competitor

Quick Answer: 5
The Details: 11

A9. A security incident has occurred on a file server. Which of the following data sources should be gathered to address file storage volatility? (Select TWO)

- A. Partition data
- B. Kernel statistics
- C. ROM data
- D. Temporary file systems
- E. Process table

Quick Answer: 5
The Details: 12
Practice Exam A
Multiple Choice Quick Answers

A6. B
A7. A and C
A8. A
A9. A and D
A1. Match the description with the most accurate attack type. Not all attack types will be used.

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vishing</strong></td>
<td>Attacker obtains bank account number and birth date by calling the victim</td>
<td>SY0-501, Objective 1.2 - Phishing</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://professormesser.link/sy0501010201">http://professormesser.link/sy0501010201</a></td>
</tr>
<tr>
<td><strong>Spoofing</strong></td>
<td>Attacker modifies a legitimate DNS server to resolve the IP address of a malicious site</td>
<td>SY0-501, Objective 1.2 - Spoofing</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://professormesser.link/sy0501010220">http://professormesser.link/sy0501010220</a></td>
</tr>
<tr>
<td><strong>Man-in-the-Middle</strong></td>
<td>Attacker intercepts all communication between a client and a web server</td>
<td>SY0-501, Objective 1.2 - Spoofing</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://professormesser.link/sy0501010220">http://professormesser.link/sy0501010220</a></td>
</tr>
</tbody>
</table>

Social engineering over the telephone continues to be an effective attack vector, and obtaining personal information such as a bank account or birth date would be considered phishing over voice, or vishing.
Multiple attackers overwhelm a web server

**DDoS**

A DoS (Denial of Service) occurs when a service is unavailable due to the effects of a third-party. A DDoS (Distributed Denial of Service) occurs when multiple third-parties work together to create a service outage.

More information:
SY0-501, Objective 1.2 - Denial of Service
http://professormesser.link/sy0501010208

A virus alert appears in your browser from Microsoft with a phone number to call for support

**Hoax**

A threat that seems real but doesn't actually exist is a hoax. In this example, a fake web site message is trying to convince you that this fake threat is actually a real security issue.

More information:
SY0-501, Objective 1.2 - Hoaxes
http://professormesser.link/sy0501010205
A6. You’ve hired a third-party to gather information about your company’s servers and data. The third-party will not have direct access to your internal network but can gather information from any other source. Which of the following would best describe this approach?

- A. Backdoor testing
- B. Passive reconnaissance
- C. OS fingerprinting
- D. Grey box penetration testing

The Answer: B. Passive reconnaissance
Passive reconnaissance focuses on learning as much information from open sources such as social media, corporate websites, and business organizations.

The incorrect answers:
A. Backdoor testing
Some active reconnaissance tests will directly query systems to see if a backdoor has been installed.

C. OS fingerprinting
To fingerprint an operating system, you must actively query and receive responses across the network.

D. Grey box penetration testing
A grey box penetration test is a focused approach that usually provides detailed information about specific systems or applications.

More information:
SY0-501, Objective 1.4 - Penetration Testing
http://professormesser.link/sy0501010401
A7. Which of these protocols use TLS to provide secure communication? (Select TWO)

- A. HTTPS
- B. SSH
- C. FTPS
- D. SNMPv2
- E. DNSSEC
- F. SRTP

The Answer: A. HTTPS and C. FTPS

TLS (Transport Layer Security) is a cryptographic protocol used to encrypt network communication. HTTPS is the Hypertext Transfer Protocol over TLS, and FTPS is the File Transfer Protocol over TLS.

An earlier version of TLS is SSL (Secure Sockets Layer). Although we don't commonly see SSL in use any longer, you may see TLS communication colloquially referenced as SSL.

The incorrect answers:

B. SSH
SSH (Secure Shell) can use symmetric or asymmetric encryption, but those ciphers are not associated with TLS.

D. SNMPv2
SNMPv2 (Simple Network Management Protocol version 2) does not implement TLS, or any encryption, within the network communication.

E. DNSSEC
DNSSEC (DNS security extensions) do not provide any confidentiality of data.

F. SRTP
SRTP (Secure Real-time Transport Protocol) is a VoIP (Voice over IP) protocol used for encrypting conversations. SRTP protocol commonly uses AES (Advanced Encryption Standard) for confidentiality.

More information:
SY0-501, Objective 2.6 - Secure Protocols
http://professormesser.link/sy0501020601
**A8.** Which of these threat actors would be MOST likely to attack systems for direct financial gain?

- A. Organized crime
- B. Hacktivist
- C. Nation state
- D. Competitor

**The Answer:** A. Organized crime

An organized crime actor is motivated by money, and their hacking objectives are usually based around objectives that can be easily exchanged for financial capital.

**The incorrect answers:**

B. Hacktivist

A hacktivist is focused on a political agenda and not commonly on a financial gain.

C. Nation state

Nation states are already well funded, and their primary objective is not usually based on revenue or income.

D. Competitor

A competitor doesn't have any direct financial gain by disrupting a website or stealing customer lists, and often their objective is to disable a competitor’s business or to harm their reputation. If there is a financial gain, it would often be an indirect result of an attack.

**More information:**

SY0-501, Objective 1.3 - Threat Actors
http://professormesser.link/sy0501010301
A9. A security incident has occurred on a file server. Which of the following data sources should be gathered to address file storage volatility? (Select TWO)

- A. Partition data
- B. Kernel statistics
- C. ROM data
- D. Temporary file systems
- E. Process table

**The Answer:** A. Partition data and D. Temporary file systems

Both temporary file system data and partition data are part of the file storage subsystem.

**The incorrect answers:**

B. Kernel statistics
Kernel statistics are stored in memory.

C. ROM data
ROM data is a type of memory storage.

E. Process table
The process table keeps track of system processes, and it stores this information in RAM.

**More information:**

SY0-501, Objective 5.5 - Gathering Forensics Data
http://professormesser.link/sy0501050501
Keep it going!
Get the complete edition of the SY0-501 Security+ Practice Exams on ProfessorMesser.com:

Three 90-question exams
Performance-based Questions
Detailed explanations for every question and answer
Links to additional video training

Click here to unlock the complete book!