Pass the Security+ SY0-601 Exam!

BEFORE THE EXAM EXPIRES.

BRIAN FORD COMPTIA SECURITY+, CYSA+, CASP+ INSTRUCTOR

Your Instructor: Brian Ford

Brian@fordsnotes.com

bford@comptia.global

https://linkedin.com/in/brford

@fordsnotes

CompTIA Security+, CySA+, CASP+, and others…

CCIE #2106 (expired)

Certified Novell Instructor (CNI) Novell expired

B.S. Computer Science, SUNY Stony Brook

M.S. Information Assurance, Norwich University

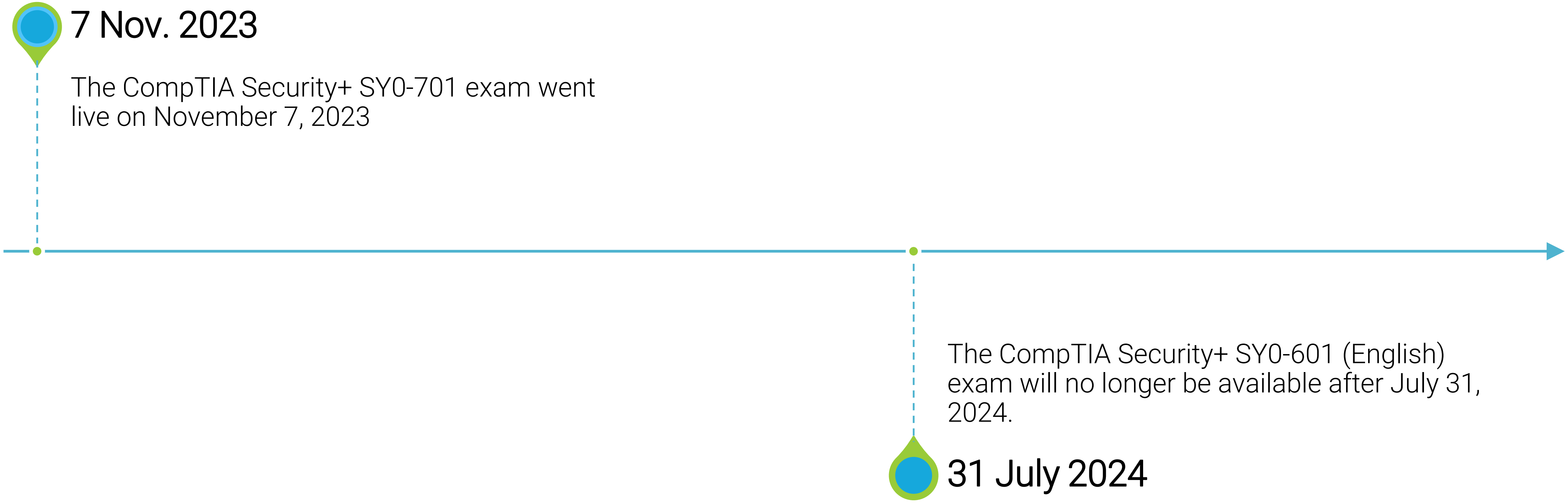
30+ years in IT, Networking, Internet Security

NIST National Initiative on Cybersecurity Education (NICE) Contributor

CISSP
CISM
CompTIA CSAE
CompTIA CSCP
Cisco Certified CyberOps Associate
aws certified Cloud Practitioner Foundational
CompTIA Cloud Essentials+
CompTIA Cloud+
CompTIA CASP+
CompTIA CySA+

COPYRIGHT 2024 BRIAN FORD

Time is running out on SY0-601



7 Nov. 2023

The CompTIA Security+ SY0-701 exam went live on November 7, 2023

The CompTIA Security+ SY0-601 (English) exam will no longer be available after July 31, 2024.

31 July 2024

COPYRIGHT 2024 BRIAN FORD

SY0-601 Domain Weighting (% of Exam)

#	Domain	% of Exam
1	Threats, Attacks, and Vulnerabilities	24%
2	Architecture and Design	21%
3	Implementation	25%
4	Operations and Incident Response	16%
5	Governance, Risk, and Compliance	14%
	Total	100%

COPYRIGHT 2024 BRIAN FORD

Passing the Exam

How is the SY0-601 exam scored?

- From the exam objectives we know that for the SY0-601 exam…
  - Number of questions: Maximum of 90
  - Type of Questions: Multiple-choice and performance-based
  - Length of test: 90 minutes
  - Passing score: 750 (on a scale of 100-900)
- The exam scoring system is not publicly disclosed anywhere.
- Exam score is insignificant.
  - Candidates should care whether they **passed** or **failed**.
  - Pass or fail the printed exam report provides detailed information on topics they got wrong.

Keywords from the Objectives

- Directly from the SY0-601 Exam Outline…
- Compare and contrast …
  - These questions are used to elicit a comparison or contrast response demonstrating an understanding of subtle differences or unexpected similarities between two subjects.
- Explain …
  - These questions are used to test understanding of concepts.
- Given a scenario …
  - Given a scenario, analyze
  - Given an incident, apply
  - Given an incident, utilize
  - These questions are used to describe how to respond or answer to a supposed situation.
- Summarize …
  - These questions test your understanding of main ideas and concepts.

COPYRIGHT 2024 BRIAN FORD

Keywords: Compare and contrast

- Compare and contrast …
  - These questions are used to elicit a comparison or contrast response demonstrating an understanding of subtle differences or unexpected similarities between two subjects.
- Example:

Which of the following statements accurately compares and contrasts symmetric encryption and asymmetric encryption?

A) Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses different keys for encryption and decryption.

B) Symmetric encryption is more secure than asymmetric encryption because it uses longer key lengths.

C) Symmetric encryption is suitable for secure key exchange, while asymmetric encryption is more efficient for bulk data encryption.

COPYRIGHT 2024 BRIAN FORD

Keywords: Explain

- Explain …
  - These questions are used to test understanding of concepts.
- Example

Which of the following best explains the concept of a Security Information and Event Management (SIEM) system?

A) SIEM is a software tool used for vulnerability scanning and penetration testing.

B) SIEM is a network device that provides secure remote access to resources.

C) SIEM is a centralized platform that collects, correlates, and analyzes security events and logs from various sources.

COPYRIGHT 2024 BRIAN FORD

Correct answer: C) SIEM is a centralized platform that collects, correlates, and analyzes security events and logs from various sources.

Explanation: A Security Information and Event Management (SIEM) system is designed to collect and analyze security events and logs from various sources within an organization's IT infrastructure. It provides centralized visibility and correlation of these events to detect and respond to security incidents effectively. SIEM systems enable organizations to monitor and analyze log data, detect patterns, and generate alerts for potential security breaches or abnormal activities. They play a crucial role in threat detection, incident response, and compliance management by providing real-time analysis and reporting capabilities. Therefore, option C is the correct explanation of a SIEM system.

COPYRIGHT 2024 BRIAN FORD

Keywords: Given a scenario

- Given a scenario …
  - Given a scenario, analyze
  - Given an incident, apply
  - Given an incident, utilize
- These questions are used to describe how to respond or answer to a supposed situation.
  - Often there is a scenario presented.

Example Scenario

"Imagine you are a security analyst working for a financial institution. One of the employees received an email from what appears to be a trusted source, requesting sensitive financial information. The email includes a link that directs to a website asking for login credentials. Describe the steps you would take to analyze this situation, identify potential risks, and recommend appropriate actions to mitigate the threat.“

- This is an ‘analyze’ question.
- The subject is “a link that directs to a website asking for login credentials”.
- This question could be rephrased :Describe the steps to investigate this suspect website.

COPYRIGHT 2024 BRIAN FORD

Given a scenario, analyze…

You are a security analyst conducting a risk assessment for a small company. During your assessment, you discover that the company's servers are located in an open and easily accessible area with no physical access controls. Which of the following risks is the company most vulnerable to?

A. Data exfiltration through network attacks
B. Insider threats and unauthorized access
C. Social engineering attacks targeting employees

COPYRIGHT 2024 BRIAN FORD

Answer to ‘Given a scenario, analyze…’

Correct answer: B) Insider threats and unauthorized access

Option B, *insider threats and unauthorized access* is the most appropriate and specific risk associated with the given scenario. **Unauthorized individuals could gain physical access to the servers**, potentially compromising sensitive data, altering configurations, or performing other malicious activities.

Option A, *data exfiltration through network attacks* **could be a risk if the servers were accessible remotely**, but the scenario specifically mentions that the vulnerability lies in the physical access controls.

Option C, *social engineering attacks* targeting employees may be a concern but **is not directly related to the lack of physical access controls to the servers**.

COPYRIGHT 2024 BRIAN FORD

Keywords: Summarize

- Summarize …
  - These questions test your understanding of main ideas and concepts.
- Example

Which of the following best summarizes the concept of social engineering?

A) Social engineering involves the unauthorized access and exploitation of computer networks and systems.

B) Social engineering refers to the use of psychological manipulation to deceive individuals and gain unauthorized access to sensitive information.

C) Social engineering is the practice of implementing security controls and measures to protect against unauthorized access attempts.

COPYRIGHT 2024 BRIAN FORD

Correct answer: B) Social engineering refers to the use of psychological manipulation to deceive individuals and gain unauthorized access to sensitive information.

Explanation: Option B provides the best summary of the concept of social engineering. Social engineering is a tactic used by attackers to exploit human psychology and manipulate individuals into divulging sensitive information or performing actions that may compromise security. It often involves techniques such as phishing, pretexting, baiting, and tailgating, where attackers exploit trust, curiosity, fear, or other emotions to deceive individuals and gain unauthorized access to confidential data or systems.

- Option A is incorrect because it describes unauthorized access and exploitation of computer networks and systems in general, without specifically emphasizing the psychological manipulation aspect of social engineering.
- Option C is incorrect because it describes the practice of implementing security controls and measures in general, without specifically highlighting the deceptive nature of social engineering.
- Option D is incorrect because it focuses on advanced encryption algorithms and protocols, which are not directly related to social engineering. Social engineering primarily targets human vulnerabilities rather than technical encryption mechanisms.

Therefore, option B provides the most accurate and concise summary of the concept of social engineering.

COPYRIGHT 2024 BRIAN FORD

Exams use multiple choice questions

- **Multiple choice questions** are composed of one question with multiple possible answers, including the correct answer and several incorrect answers (**distractors**).
  - Multiple choice questions are often used to test student's knowledge of a broad range of content.
- A type of multiple-choice question might involve matching. Matching questions pair a definition with one of the choices provided.
  - These questions are often used to **assess recognition and recall** and so are most often used where acquisition of detailed knowledge is an important goal.

COPYRIGHT 2024 BRIAN FORD

The “best answer”

- Nobody likes ‘trick’ questions.
  - Questions are developed so that students who know the material can find the correct answer.
  - Questions instruct students to select the “best answer” rather than the “correct answer.”
  - The idea is that there may be more than one ‘correct’ answer to the multiple-choice question, but one correct answer is better than the others.

COPYRIGHT 2024 BRIAN FORD

Distractors

- Distractors are plausible but incorrect answers.
  - Some distractors are statements based on common student misconceptions
  - Distractors draw the test takers attention
- Example

Question: Which of the following is NOT a common type of authentication factor?

A) Something you know

B) Something you have

C) Something you are

Note that these are correct answers
if not for the NOT

D) Something you need

This is the correct answer to the question.

COPYRIGHT 2024 BRIAN FORD

Tips for answering scenario-based questions

- Read each question carefully to make sure you understand what the scenario is presenting and process all important information.
- Do not try to answer the questions prior to reading and understand the scenario.
- **Read all the choices before selecting your answer** and be sure to notice if it is asking you to choose one, two or three.
- Answer all the questions.
  - If you don't know the answer (given 4 choices) you have a 25% chance of guessing correctly, and no points are deducted for incorrect answers.

COPYRIGHT 2024 BRIAN FORD

Tips for answering scenario-based questions

- **Skip any questions you have difficulty answering and come back to them after reviewing** the other questions.
  - Sometimes completing other questions or re-reading the challenging question may give you a different perspective and help you to answer it.
- **Trust your instincts**. Once you have answered a question, don’t change your answer unless you are certain that your first choice is wrong. *Research shows that most changed answers go from the correct choice to an incorrect one.*

COPYRIGHT 2024 BRIAN FORD

Performance Based Questions (PBQs)

- PBQs are designed to test a candidate's ability to solve problems in real-world settings.
- PBQ Types
  - Simulations "are an approximation of an environment or tool, such as a firewall, network diagram, terminal window, or operating system. They typically have restricted system functionality but are designed to allow for multiple possible responses or paths."
  - Virtual environments "are virtual machines/systems running select operating systems and software in a production environment. Because they are full versions of the technology assessed by the exam item, all manner of incorrect steps or paths may be pursued."
  - Virtual PBQs require you use a **reset** to change answers. The **reset** takes the question back to starting state, erasing any selected or entered answers.

COPYRIGHT 2024 BRIAN FORD

Don’t fear the PBQs

- Simulation PBQs use multiple windows.
  - At the start of the question the top window will not cover the entire screen area.
  - There will be a larger, full screen window below.
- Simulation questions have a reset button, virtual PBQs do not.
  - Reset erases all the answers you selected for that question, going back to the starting state.
- You can skip simulation PBQs and return to them later, you cannot do the same with virtual PBQs!
- There can be multiple ways to solve a question or challenge posed in a PBQ.
- Partial credit may be given for answers in any PBQ.

COPYRIGHT 2024 BRIAN FORD

Testing Tips

Scheduling your exam

- ✓Schedule your exam 10 days to 2 weeks before you plan to test.
  - ✓You can re-schedule up to the day before the exam
  - ✓You can change your exam date and time up to 24 hours before the appointment.
  - ✓You are allowed to change the appointment one time at no charge.
- ✓Take a day off after you schedule your exam. Relax.
- ✓The day after your day off spend time reviewing your notes.
  - ✓I suggest doing your own ‘structured review’.
- ✓Don’t take too many practice exams.
  - ✓If you continue taking the practice exam time after time you will memorize those questions and answers.
  - ✓This is a common test taker mistake. Don’t do that.

COPYRIGHT 2024 BRIAN FORD

Where to Test?

Test at Testing Center

Find a Pearson Authorized Testing Center

- These are operated by other companies.
- Pearson and CompTIA define rules.

Plan your travel.

- Late due to traffic is not a valid excuse.
- There is a test window. If you are too late you forfeit.

Arrive 15-30 minutes early.

- There may be many other people testing.
- You may need to wait to sign in
- You may need to wait for a station to be available.

Test at home via On Vue

Before you schedule your exam:

Read the On Vue requirements carefully.

Test your system.

- Make sure your computer and peripherals meets all requirements.

Follow the On Vue instructions to the letter.

- Plan to install the software up to a day early.

Follow all Proctors' instructions.

COPYRIGHT 2024 BRIAN FORD

At the Testing Center

- ✓Print out your Test Appointment confirmation email before you leave for the testing center.
  - ✓Or make sure that you can pull it up on your mobile device.
  - ✓Bring that with you.
- ✓At the testing center you need 2 forms of ID.
  - ✓One should be a government issued ID (Drivers License).
  - ✓One with a picture.
  - ✓The Admin will ask for your signature and take your picture.
- ✓Don’t bring anything else with you to a testing center.
  - ✓If you plan to arrive early leave your books / notes in your car (or don’t bring them).
- ✓Lock up your keys and phone.
  - ✓Lockers should be provided by the Testing Center.
- ✓Before going into the testing room, always ask for a white board and marker for notes.
  - ✓Or paper and pencil for notes
  - ✓You will need to erase / throw away when test completes
  - ✓Don’t try to smuggle anything out!

COPYRIGHT 2024 BRIAN FORD

The Test Begins …

- ✓The test begins after you have sat down at a station and reviewed the CompTIA testing agreement.
  - ✓Sit down and relax.
  - ✓Be quiet.
  - ✓Get comfortable.
  - ✓Don’t look around the room.
  - ✓Before you touch the computer make sure that no one / no thing around you will distract you during the exam.
    - ✓If so, ask for a different seat.
  - ✓Review the testing agreement.
    - ✓The exam begins after you agree to the testing agreement.
  - ✓It’s not over until you complete the survey.

COPYRIGHT 2024 BRIAN FORD

What to do next?

Maintaining your certification

Important: You maintain the highest certification in a stack!

Continuing Education Units (CEUs)

- You enter CEUs at the Certmetrics portal.
- CEUs are earned at a rate of 1 CEU for each hour spent on some activity.
- Activities can be learning, educating others (teaching), or mentoring.
- CEUs are audited
  - My experience has been that the audits are tough.
  - You must demonstrate how the activity relates back to specific topics in the objectives.
- CEUs can only be entered after you have paid your CE fee.

CertMaster CE

- You buy the CertMaster CE version of the course.
- You complete the exercises, labs and exam for the CertMaster CE course.
- Upon completion of the CertMaster CE course you are re-certified.
  - Download and print out your course completion certificate.
  - The CertMaster CE course records your completion.
  - You don’t have to do anything else.
- This is the ‘easy button’.

COPYRIGHT 2024 BRIAN FORD

Security+
CERTIFIED · CE
CompTIA
CERTIFIED
COMPTIA OFFICIAL GLOBAL SKILL CERTIFICATION
Congra
.CompTIA.org
deserve it.
mpTIA's certification program. I wish yo
ome of our most frequently asked questions on our website at
mpTIA.org/Help
someone on our customer service team, you can reach us
Monday through Friday, from 7 a.m. to 7 p.m. CT.

Now pass that SY0-601 exam!

Visit my website https://fordsnotes.com. Follow me on LinkedIn.