

## CompTIA Security+ Certification Exam SY0-701 Practice Test 2

► Which of the following terms describes the process of identifying differences between an organization's current security posture and its desired security posture?

☐ ☐ ☐ Tabletop exercise

☒ ☒ ☒ Gap analysis (☒ Your answer)

☐ ☐ ☐ Security awareness training

☐ ☐ ☐ Risk assessment

☒ You correctly answered this question.

► The term "Zero Trust security" refers to a cybersecurity model that eliminates implicit trust from networks and requires all users and devices to be continuously verified before being granted access to resources. The implementation of the Zero Trust security involves two distinct components: a Data Plane, responsible for defining and managing security policies, and a Control Plane, responsible for enforcing the security policies established by the Data Plane.

☐ ☐ ☒ True (☒ Your answer)

☐ ☒ ☒ False (☒ Missed)

☒ Your answer to this question is incorrect or incomplete.

► Which of the answers listed below refers to a Zero Trust Control Plane security approach that takes into account user identity, device security, network conditions, and other contextual information to enable dynamic access decisions?

☐ ☐ ☒ Implicit trust (☒ Your answer)

☐ ☐ ☐ Monitoring and logging

☐ ☒ Adaptive identity ( Missed)

☐ ☐ ☐ Microsegmentation

Your answer to this question is incorrect or incomplete.

► What are the key components of the Zero Trust Control Plane's Policy Decision Point (PDP)?  
(Select 2 answers)

☒ ☒ Policy Engine (PE) (☒ Your answer)

☐ ☐ ☐ Monitoring and logging

☐ ☐ ☐ Policy Enforcement Point (PEP)

☐ ☐ ☐ Microsegmentation

☒ ☒ Policy Administrator (PA) (☒ Your answer)

☒ You correctly answered this question.

► In the Zero Trust security architecture, the Policy Enforcement Point (PEP) is a Data Plane component that enforces the security policies defined at the Control Plane by the Policy Decision Point (PDP).

☒ ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► An access control vestibule (a.k.a. mantrap) is a physical security access control system used to prevent unauthorized users from gaining access to restricted areas. An example mantrap could be a two-door entrance point connected to a guard station wherein a person entering from the outside remains locked inside until he/she provides authentication token required to unlock the inner door.

☒ ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► Which of the following statements about honeypots are true? (Select 2 answers)

☐ ☐ ☐ Honeypots are always part of a honeynet

👉 ✓ ☒ Honeypots mimic real systems to attract cyber attackers (☒ Your answer)

☐ ☐ ☐ Honeypots are a type of anti-malware solution

👉 ✓ ☒ Honeypots contain apparent vulnerabilities that are closely monitored by a security team (☒ Your answer)

☐ ☐ ☐ Honeypots are used to launch attacks on cyber attackers

☒ You correctly answered this question.

► What is a honeynet in the context of cybersecurity?

☐ ☐ ☐ A network of IDSs

👉 ✓ ☒ A network of honeypots (☒ Your answer)

☐ ☐ ☐ A network of infected hosts

☐ ☐ ☐ A network of IPSs

☒ You correctly answered this question.

► Which of the answers listed below refers to a honeynet example?

☐ ☐ ☐ A network of fake websites

☐ ☐ ☐ A network of fake servers


☐ ☐ ☐ A network of fake databases


☐ ☐ ☐ A network of fake file shares

👉 ✓ ☒ All of the above (☒ Your answer)

☒ You correctly answered this question.


► A honeyfile can be any type of file (e.g., a document, email message, image, or video file) containing real user data intentionally placed within a network or system to attract potential attackers or unauthorized users.

 ☐ ☒ True (✖ Your answer)

☐ ☒  False (⊗ Missed)


☒ Your answer to this question is incorrect or incomplete.

▶ A honeyfile can be used for:

 ☐ ☒ Attracting cyber attackers (✖ Your answer)


☐ ☐ ☐ Triggering alerts when accessed

☐ ☐ ☐ Monitoring network activity

☐ ☒  All of the above (⊗ Missed)

☒ Your answer to this question is incorrect or incomplete.

▶ What is a honeytoken?

 ☐ ☒ A decoy file that is designed to attract attackers (✖ Your answer)


☐ ☐ ☐ A unique identifier assigned to a honeyfile

☐ ☐ ☐ A decoy system that is designed to lure potential attackers

☐ ☒  A unique identifier that is designed to track attackers (⊗ Missed)

☒ Your answer to this question is incorrect or incomplete.


▶ Which of the following should not be used as honeytokens? (Select all that apply)

☐ ☒  Active user account credentials (⊗ Missed)

 ☐ ☒ Database entries mimicking real data (✖ Your answer)

☐ ☒  Actual URLs to live websites or resources (⊗ Missed)

 ☐ ☒ Dummy server logs with enticing information (✖ Your answer)

 ☐ ☒ Fake identifiers, including usernames, passwords, email addresses, and IP addresses (✖ Your answer)

☒ Your answer to this question is incorrect or incomplete.

► A process used by organizations to assess and evaluate the potential impact of disruptive incidents or disasters on their critical business functions and operations is referred to as:

☐ ☐ ☐ BPA

☐ ☒ ☐ BIA (⊗ Missed)

☐ ☐ ☐ SLE

☐ ☐ ☒ BCP (⊗ Your answer)

☒ Your answer to this question is incorrect or incomplete.

► A hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates is known as:

☐ ☒ ☐ PKI (⊗ Missed)

☐ ☐ ☐ RA

☐ ☐ ☐ PKCS

☐ ☐ ☒ CA (⊗ Your answer)

☒ Your answer to this question is incorrect or incomplete.

► Which of the answers listed below best describes the characteristics of a public-private key pair?

☐ ☐ ☐ Both keys are examples of a symmetrical key

☐ ☐ ☐ Two keys that are identical

☐ ☒ ☒ A pair of keys where one is used for encryption and the other for decryption (☒ Your answer)

☐ ☐ ☐ Both keys are examples of a shared key

☒ You correctly answered this question.

► What is the typical use of a public key?

☐ ☒ ☐ Data encryption (⊗ Missed)


☐ ☐ ☐ Data decryption

 ☐ ☒ User/device authentication (✖ Your answer)

☐ ☐ ☐ All of the above

☒ Your answer to this question is incorrect or incomplete.


► Key escrow is a cryptographic technique that enables storing copies of encryption keys with a trusted third party. A Recovery Agent (RA) is a trusted third party (an individual, entity, or system) who is authorized to assist in the retrieval of encryption keys and data on behalf of the data owner. Key escrow and RA are both used to ensure that encrypted data can be decrypted even if the data owner loses access to their encryption key. Since key escrow and RAs are both components of a single security solution, the only way to implement key escrow systems is with the use of RAs.

 ☐ ☒ True (✖ Your answer)

☐ ☒  False (⊗ Missed)

☒ Your answer to this question is incorrect or incomplete.

► Which of the following answers refers to a data storage device equipped with hardware-level encryption functionality?

 ☐ ☒ HSM (✖ Your answer)


☐ ☐ ☐ TPM

☐ ☐ ☐ EFS

☐ ☒  SED (⊗ Missed)

☒ Your answer to this question is incorrect or incomplete.

► Which of the answers listed below refers to software technology designed to provide confidentiality for an entire data storage device?

 ☐ ☒ TPM (✖ Your answer)

☐ ☒  FDE (⊗ Missed)

☐ ☐ ☐ EFS

☐ ☐ ☐ HSM

 Your answer to this question is incorrect or incomplete.

► An MS Windows component that enables encryption of individual files is called:

☐ ☐ ☐ SED

☐ ☒  EFS ( Missed)

 ☐  BitLocker ( Your answer)

☐ ☐ ☐ FDE




 Your answer to this question is incorrect or incomplete.

► Which of the following software application tools are specifically designed for implementing encryption algorithms to secure data communication and storage? (Select 2 answers)

☐ ☐ ☐ VPN

☐ ☒  GPG ( Missed)

☐ ☐ ☐ SSH


 ☐  IPsec ( Your answer)

 ☒ ☒ PGP (☒ Your answer)

 Your answer to this question is incorrect or incomplete.

► What is the name of a network protocol that secures web traffic via SSL/TLS encryption?

☐ ☐ ☐ SFTP


 ☒ ☒ HTTPS (☒ Your answer)

☐ ☐ ☐ FTPS

☐ ☐ ☐ SNMP

☒ You correctly answered this question.

► Which of the answers listed below refers to a deprecated TLS-based method for secure transmission of email messages?

 ☐ ☐ ☒ S/MIME (✖ Your answer)

☐ ☐ ☐ STARTTLS

☐ ☐ ☐ DKIM

☐ ☒  SMTPS (⊗ Missed)


 Your answer to this question is incorrect or incomplete.

► Which of the following answers refers to an obsolete protocol used for secure data transfer over the web?

☐ ☐ ☐ SMTPS

☐ ☐ ☐ SRTP

☐ ☒  SHTTP (⊗ Missed)

 ☐ ☐ ☒ S/MIME (✖ Your answer)

 Your answer to this question is incorrect or incomplete.

## Your Final Report

Total marks	29
Total Questions	25
Questions correctly answered	9
Success ratio	36%
Marks secured	12
Percentage secured	41.38%

## Security+

### CompTIA Security+ Certification Exam SY0-601 Practice Tests

[Security+ Practice Test 1 \(/comptia-security-plus-practice-test-1-exam-sy0-601\)](#)

[Security+ Practice Test 2 \(/comptia-security-plus-practice-test-2-exam-sy0-601\)](#)

[Security+ Practice Test 14 \(/comptia-security-plus-practice-test-14-exam-sy0-601\)](#)

[Security+ Practice Test 15 \(/comptia-security-plus-practice-test-15-exam-sy0-601\)](#)



[Security+ Practice Test 3 \(/comptia-security-plus-practice-test-3-exam-sy0-601\)](#)

[Security+ Practice Test 4 \(/comptia-security-plus-practice-test-4-exam-sy0-601\)](#)

[Security+ Practice Test 5 \(/comptia-security-plus-practice-test-5-exam-sy0-601\)](#)

[Security+ Practice Test 6 \(/comptia-security-plus-practice-test-6-exam-sy0-601\)](#)

[Security+ Practice Test 7 \(/comptia-security-plus-practice-test-7-exam-sy0-601\)](#)

[Security+ Practice Test 8 \(/comptia-security-plus-practice-test-8-exam-sy0-601\)](#)

[Security+ Practice Test 9 \(/comptia-security-plus-practice-test-9-exam-sy0-601\)](#)

[Security+ Practice Test 10 \(/comptia-security-plus-practice-test-10-exam-sy0-601\)](#)

[Security+ Practice Test 11 \(/comptia-security-plus-practice-test-11-exam-sy0-601\)](#)

[Security+ Practice Test 12 \(/comptia-security-plus-practice-test-12-exam-sy0-601\)](#)

[Security+ Practice Test 13 \(/comptia-security-plus-practice-test-13-exam-sy0-601\)](#)

[Security+ Practice Test 16 \(/comptia-security-plus-practice-test-16-exam-sy0-601\)](#)

[Security+ Practice Test 17 \(/comptia-security-plus-practice-test-17-exam-sy0-601\)](#)

[Security+ Practice Test 18 \(/comptia-security-plus-practice-test-18-exam-sy0-601\)](#)

[Security+ Practice Test 19 \(/comptia-security-plus-practice-test-19-exam-sy0-601\)](#)

[Security+ Practice Test 20 \(/comptia-security-plus-practice-test-20-exam-sy0-601\)](#)

[Security+ Practice Test 21 \(/comptia-security-plus-practice-test-21-exam-sy0-601\)](#)

[Security+ Practice Test 22 \(/comptia-security-plus-practice-test-22-exam-sy0-601\)](#)

[Security+ Practice Test 23 \(/comptia-security-plus-practice-test-23-exam-sy0-601\)](#)

[Security+ Practice Test 24 \(/comptia-security-plus-practice-test-24-exam-sy0-601\)](#)

[Security+ Practice Test 25 \(/comptia-security-plus-practice-test-25-exam-sy0-601\)](#)

[Security+ Practice Test 26 \(/comptia-security-plus-practice-test-26-exam-sy0-601\)](#)

## **CompTIA Security+ Certification SY0-601 Practice Tests by Exam Topic**

[Social Engineering Quiz \(/comptia-security-plus-certification-exam-sy0-601-social-engineering-quiz\)](#)

[Malware Quiz \(/comptia-security-plus-certification-exam-sy0-601-malware-quiz\)](#)

[Password Attacks Quiz \(/comptia-security-plus-certification-exam-sy0-601-password-attacks-quiz\)](#)

[Network Attacks Quiz \(/comptia-security-plus-certification-exam-sy0-601-network-attacks-quiz\)](#)

[Penetration Testing Quiz \(/comptia-security-plus-certification-exam-sy0-601-penetration-testing-quiz\)](#)

[Cloud Computing Quiz \(/comptia-security-plus-certification-exam-sy0-601-cloud-computing-quiz\)](#)

[Virtualization Quiz \(/comptia-security-plus-certification-exam-sy0-601-virtualization-quiz\)](#)

[Cryptographic Concepts Quiz \(/comptia-security-plus-certification-exam-sy0-601-cryptographic-concepts-quiz\)](#)

[Secure Network Protocols Quiz \(/comptia-security-plus-certification-exam-sy0-601-secure-network-protocols-quiz\)](#)

[Wireless Security Quiz \(/comptia-security-plus-certification-exam-sy0-601-wireless-security-quiz\)](#)

**[Public Key Infrastructure Quiz \(/comptia-security-plus-certification-exam-sy0-601-public-key-infrastructure-quiz\)](#)**

**[Command-Line Utilities Quiz \(/comptia-security-plus-certification-exam-sy0-601-command-line-utilities-quiz\)](#)**

**[Digital Forensics Quiz \(/comptia-security-plus-certification-exam-sy0-601-digital-forensics-quiz\)](#)**

**[Security Controls Quiz \(/comptia-security-plus-certification-exam-sy0-601-security-controls-quiz\)](#)**

**[Risk Management Concepts Quiz \(/comptia-security-plus-certification-exam-sy0-601-risk-management-concepts-quiz\)](#)**

## **Exam Glossaries**

**[Malware Glossary \(/malware-glossary\)](#)**

**[CompTIA Security+ SY0-601 Exam Objectives \(https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-601-exam-objectives-\(6-0\).pdf\)](https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-601-exam-objectives-(6-0).pdf)**

## **Security+**

### **CompTIA Security+ Certification Exam SY0-701 Practice Tests**

**[Security+ Practice Test 1 \(/comptia-security-plus-practice-test-1-exam-sy0-701\)](#)**

**[Security+ Practice Test 2 \(/comptia-security-plus-practice-test-2-exam-sy0-701\)](#)**

**[Security+ Practice Test 3 \(/comptia-security-plus-practice-test-3-exam-sy0-701\)](#)**

**[Security+ Practice Test 4 \(/comptia-security-plus-practice-test-4-exam-sy0-701\)](#)**

**[Security+ Practice Test 5 \(/comptia-security-plus-practice-test-5-exam-sy0-701\)](#)**

**[Security+ Practice Test 6 \(/comptia-security-plus-practice-test-6-exam-sy0-701\)](#)**

**[Security+ Practice Test 7 \(/comptia-security-plus-practice-test-7-exam-sy0-701\)](#)**

**[Security+ Practice Test 8 \(/comptia-security-plus-practice-test-8-exam-sy0-701\)](#)**

**[Security+ Practice Test 9 \(/comptia-security-plus-practice-test-9-exam-sy0-701\)](#)**

**[CompTIA Security+ SY0-701 Exam Objectives \(https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-701-exam-objectives-\(5-0\).pdf\)](https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-701-exam-objectives-(5-0).pdf)**

---

**[Site Map \(/site-map\)](/site-map)**

**[Privacy Policy \(/privacy-policy\)](/privacy-policy)**

**[Terms & Conditions \(/terms-and-conditions\)](/terms-and-conditions)**

---

**[Back to top \(https://www.examcompass.com/comptia-security-plus-practice-test-2-exam-sy0-701#top\)](https://www.examcompass.com/comptia-security-plus-practice-test-2-exam-sy0-701#top)**

-->