



CompTIA Security+ Certification Exam SY0-701 Practice Test 7

► Exploiting known vulnerability is a common threat vector for:

 ☐ ☒ Legacy systems/apps (✗ Your answer)

☐ ☒  Unsupported systems/apps (⊗ Missed)

☐ ☐ ☐ Newly released systems/apps


☐ ☐ ☐ Systems/apps with zero-day vulnerability

 Your answer to this question is incorrect or incomplete.

► A solution that simplifies configuration of new wireless networks by allowing non-technical users to easily configure network security settings and add new devices to an existing network is called:

☐ ☐ ☐ WPA


☐ ☒  WPS (⊗ Missed)

 ☐ ☒ WEP (✗ Your answer)

☐ ☐ ☐ WAP

 Your answer to this question is incorrect or incomplete.

► Which of the wireless technologies listed below are considered potential threat vectors and should be avoided due to their known vulnerabilities? (Select all that apply)

 ☒ ☒ WPS (☒ Your answer)

☐ ☐ ☐ WAP

 ☒ ☒ WPA (☒ Your answer)

 ☐ ☐ WAF

👍 ✓ ☒ WPA2 (☒ Your answer)

👍 ✓ ☒ WEP (☒ Your answer)

☒ You correctly answered this question.

► The term "Evil twin" refers to a rogue WAP set up for eavesdropping or stealing sensitive user data. Evil twin replaces the legitimate AP and by advertising its own presence with the same Service Set Identifier (SSID, a.k.a. network name) appears as a legitimate AP to connecting hosts.

👍 ✓ ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► Which of the following answers refers to a threat vector characteristic only to wired networks?

☐ ☐ ☐ ARP Spoofing

☐ ☐ ☐ VLAN hopping

👍 ✓ ☒ Cable tapping (☒ Your answer)

☐ ☐ ☐ Port sniffing

☐ ☐ ☐ All of the above

☒ You correctly answered this question.

► Examples of threat vectors related to Bluetooth communication include: bluesmacking (a type of DoS attack that targets Bluetooth devices by overwhelming them with excessive traffic), bluejacking (the practice of sending unsolicited messages or data to a Bluetooth-enabled device), bluesnarfing (gaining unauthorized access to a Bluetooth device and data theft), and bluebugging (gaining remote control over a Bluetooth device).

👍 ✓ ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► Which of the answers listed below refers to the most probable cause of an unauthorized access caused by the exploitation of a specific network entry point?

☐ ☐ ☐ Outdated AV software

☐ ☐ ☐ Browser cookies

☐ ☒ ☒ Open service ports (☒ Your answer)

☐ ☐ ☐ Insufficient logging and monitoring

☒ You correctly answered this question.

► The importance of changing default usernames and passwords can be illustrated by the example of certain network devices (such as routers), which are often shipped with default and well-known admin credentials that can be looked up on the web.

☐ ☒ ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► Which of the following would be the best solution for a company that needs IT services but lacks any IT personnel?

☐ ☐ ☐ MSA

☐ ☐ ☐ MaaS

☐ ☒ ☐ MSP (☒ Missed)

☐ ☐ ☒ MSSP (☒ Your answer)

☒ Your answer to this question is incorrect or incomplete.

► Which of the terms listed below refers to a third-party vendor offering IT security management services? (Select best answer)

☐ ☐ ☒ MSP (☒ Your answer)

☐ ☐ ☐ MaaS

☐ ☐ ☐ MSA

☐ ☒ ☐ MSSP (⊗ Missed)

☐ Your answer to this question is incorrect or incomplete.

► Which of the following answers refer to common threat vectors that apply to MSPs, vendors, and suppliers in the supply chain? (Select 2 answers)

☐ ☐ ☐ Compliance violations (✗ Your answer)

☐ ☐ ☐ Brand reputation damage (✗ Your answer)

☐ ☒ ☐ Propagation of malware (⊗ Missed)

☐ ☐ ☐ Operational disruptions

☐ ☒ ☐ Social engineering techniques (⊗ Missed)

☐ Your answer to this question is incorrect or incomplete.

► A social engineering technique whereby attackers under disguise of a legitimate request attempt to gain access to confidential information is commonly referred to as:

☐ ☒ ☐ Phishing (⊗ Missed)

☐ ☐ ☐ Smishing

☐ ☐ ☐ Pharming

☐ ☐ ☐ Spoofing (✗ Your answer)

☐ Your answer to this question is incorrect or incomplete.

► Which social engineering attack relies on identity theft?

☐ ☐ ☐ Pretexting

☐ ☐ ☐ Spear phishing

☐ ☐ ☐ Tailgating

☐ ☒ ☒ Impersonation (☑ Your answer)

☒ You correctly answered this question.

► A BEC attack is an example of:

☐ ☐ ☐ Smishing

☐ ☒ ☐ Phishing (🚫 Missed)

☐ ☐ ☐ Vishing

☐ ☐ ☒ Pharming (✖ Your answer)

☒ Your answer to this question is incorrect or incomplete.

► Which of the answers listed below refers to a social engineering technique where an attacker creates a false scenario or situation to deceive the victim into revealing sensitive information?

☐ ☐ ☐ Impersonation

☐ ☐ ☐ Credential harvesting

☐ ☒ ☒ Pretexting (✅ Your answer)

☐ ☐ ☐ Watering hole attack

☒ You correctly answered this question.

► Which of the following terms refers to a platform used for watering hole attacks?

☐ ☐ ☐ Mail gateways

☐ ☒ ☒ Websites (✅ Your answer)



☐ ☐ ☐ PBX systems

☐ ☐ ☐ Web browsers

☒ You correctly answered this question.

► The term "URL hijacking" (a.k.a. "Typosquatting") refers to a deceptive practice involving the deliberate registration of domain names with misspellings or slight variations that closely resemble well-established and popular domain names. The primary goal of this strategy is to exploit the

common typographical errors made by users while entering URLs into their web browser's address bar. Beyond capturing inadvertent traffic, typosquatting may also be used for hosting phishing sites to trick users into divulging sensitive information, distributing malware through deceptive websites, generating ad revenue by redirecting mistyped traffic, or engaging in brand impersonation to harm the reputation of authentic brands or deceive users.




  ☒ True (☒ Your answer)

☐ ☐ ☐ False

☒ You correctly answered this question.

► Which type of application attack relies on introducing external code into the address space of a running program?

 ☐ ☐ Buffer overflow ( Your answer)



☐   Memory injection ( Missed)

☐ ☐ ☐ Replay attack

☐ ☐ ☐ Pointer dereference

☐ Your answer to this question is incorrect or incomplete.

► A collection of precompiled functions designed to be used by more than one Microsoft Windows application simultaneously to save system resources is known as:

  ☒ DLL (☒ Your answer)

☐ ☐ ☐ API





☐ ☐ ☐ EXE

☐ ☐ ☐ INI

☒ You correctly answered this question.


► Which of the answers listed below refers to an application attack that relies on executing a library of code?

☐ ☐ ☐ Memory leak

   DLL injection ( Your answer)

☐ ☐ ☐ Pointer dereference




☐ ☐ ☐ Buffer overflow

 You correctly answered this question.


► A type of exploit in which an application overwrites the contents of a memory area it should not have access to is called:

☐ ☐ ☐ DLL injection





☐   Buffer overflow ( Missed)

 ☐  Memory leak ( Your answer)

☐ ☐ ☐ Privilege escalation

 Your answer to this question is incorrect or incomplete.

► A malfunction in a preprogrammed sequential access to a shared resource is described as:

   Race condition ( Your answer)

☐ ☐ ☐ Concurrency error

☐ ☐ ☐ Multithreading

☐ ☐ ☐ Synchronization error

 You correctly answered this question.

► A type of vulnerability where the state of a resource is verified at one point in time but may change before the resource is actually used is referred to as:

☐ ☐ ☐ TOC

   TOC/TOU ( Your answer)

☐ ☐ ☐ TOU

☐ ☐ ☐ TSIG

☒ You correctly answered this question.

► A malicious application update is a type of malware that can be installed through a seemingly legitimate software update. The introduction of a malicious update into the application code can be enabled through various means, including:

☐ ☐ ☐ Unsigned application code

☐ ☐ ☐ Unencrypted update channel (HTTP vs HTTPS)

☐ ☐ ☐ Fake update website

☐ ☐ ☐ Unauthorized access to update server

☐ ☐ ☐ Compromised software development process

☐ ☒ ☒ All of the above (☒ Your answer)

☒ You correctly answered this question.

► Which of the following answers does not refer to a common type of OS-based vulnerability?

☐ ☐ ☐ Access control and permissions vulnerabilities (weak passwords, privilege escalation)

☐ ☐ ☐ Vulnerabilities in installed applications, system utilities, and device drivers

☐ ☐ ☐ Memory-related vulnerabilities (memory leaks, buffer overflows, race conditions)

☐ ☐ ☐ Patch and update management vulnerabilities (security patch and update delays, malicious updates)

☐ ☐ ☐ Vulnerabilities related to system/security misconfigurations

☐ ☐ ☐ Network-related vulnerabilities (DoS attacks, remote code execution attacks)

☐ ☒ ☒ All of the above answer choices are examples of OS-based vulnerabilities (☒ Your answer)

☒ You correctly answered this question.

Your Final Report

Total marks	29
--------------------	----

Total Questions	25
------------------------	----

Questions correctly answered	16
-------------------------------------	----

Success ratio	64%
Marks secured	19
Percentage secured	65.52%

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 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 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 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 \(/site-map\)](#)

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

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

[Back to top \(https://www.examcompass.com/comptia-security-plus-practice-test-7-exam-sy0-701#top\)](https://www.examcompass.com/comptia-security-plus-practice-test-7-exam-sy0-701#top)

-->