◂ 64

CompTIA Security+ Certification Practice Test 9 (Exam SY0-401)

Send results by email

Name   [Enter your name]

Email   [Enter your email]

[Send Results]

▸ The practice of gaining unauthorized access to a Bluetooth device is referred to as:

○ ○ ○ Pharming

○ ✔ 👎 Bluesnarfing (✘ Missed)

○ ○ ○ Vishing

○ ○ ○ Bluejacking

▬ Your answer to this question is incorrect.

▸ What is war chalking?

○ ○ ○ Manipulating a user into disclosing confidential information

○ ○ ○ Finding unsecured wireless networks

○ ○ ○ Gaining unauthorized access to restricted areas by following another person

○ ✔ 👎 Marking unsecured wireless networks (✘ Missed)

▬ Your answer to this question is incorrect.

▸ Which of the answers listed below refers to an attack aimed at exploiting the vulnerability of WEP?

○ ○ ○ MITM attack

○ ○ ○ Smurf attack

○ ✔ 👎 IV attack (✘ Missed)

○ ○ ○ Xmas attack

▬ Your answer to this question is incorrect.

▸ Which of the following solutions simplifies configuration of new wireless networks by providing non-technical users with a capability to easily configure network security settings and add new devices to an existing network?

○ ○ ○ WPA

○ ✔ 👎 WPS (✘ Missed)

In order to provide you with the best online experience this website uses cookies.

○ ○ ○ WEP

By using our website, you agree to our use of cookies. **Learn more**

○ ○ ○ WAP

[I agree]

■ Your answer to this question is incorrect.

▶ Which of the answers listed below refers to a Wi-Fi Protected Setup (WPS) exploit?

○ ○ ○ Smurf attack

○ ○ ○ Watering hole attack

○ ✔ 👎 PIN recovery (✖ Missed)

○ ○ ○ Birthday attack

○ ○ ○ URL hijacking

■ Your answer to this question is incorrect.

▶ Which of the following wireless security features are not recommended and should not be used due to their known vulnerabilities? (Select 2 answers)

☐ ✔ 👎 WPS (✖ Missed)

☐ ☐ ☐ WAP

☐ ☐ ☐ WPA2

☐ ☐ ☐ WAF

☐ ✔ 👎 WEP (✖ Missed)

■ Your answer to this question is incorrect.

▶ What type of action allows an attacker to exploit the XSS vulnerability?

○ ✔ 👎 Code injection (✖ Missed)

○ ○ ○ Banner grabbing

○ ○ ○ PIN recovery

○ ○ ○ Input validation

■ Your answer to this question is incorrect.

▶ Which of the answers listed below refers to a common target of cross-site scripting?

○ ○ ○ Physical security

○ ○ ○ Alternate sites

○ ✔ 👎 Dynamic web pages (✖ Missed)

○ ○ ○ Removable storage

■ Your answer to this question is incorrect.

▶ Which of the following answers refers to a countermeasure against code injection?

○ ○ ○ Fuzzing

○ ✔ 👎 Input validation (✖ Missed)

○ ○ ○ XSRF

○ ○ ○ Directory traversal

▶ An HTTP exploit which allows attackers to access restricted directories and execute commands outside of the web server's root directory is known as:

○ ○ ○ Dictionary attack

○ ○ ○ URL hijacking

○ ○ ○ Watering hole attack

○ ✔ 👎 Directory traversal attack (✖ Missed)

▶ A temporary area of memory allocated with a fixed size for holding data while it's waiting to be transferred to another location is known as:

○ ○ ○ Cache

○ ○ ○ Header

○ ○ ○ Local Shared Object (LSO)

○ ✔ 👎 Buffer (✖ Missed)

▶ A type of attack aimed at exploiting vulnerability that is present in already released software but unknown to the software developer is called:

○ ○ ○ Xmas attack

○ ✔ 👎 Zero-day attack (✖ Missed)

○ ○ ○ IV attack

○ ○ ○ Replay attack

▶ Which of the following acronyms refers to flash cookies?

○ ○ ○ RPO

○ ○ ○ BCP

○ ✔ 👎 LSO (✖ Missed)

○ ○ ○ CRP

▶ A type of exploit that relies on overwriting the contents of memory in order to cause unpredictable results in an application is called:

○ ○ ○ IV attack

○ ○ ○ SQL injection

○ ✔ 👎 Buffer overflow (✖ Missed)

○ ○ ○ Fuzz test

▶ What kind of general term is used to describe the process of securing a computer system?

○ ○ ○ Patching

○ ○ ○ Baseline configuration

○ ✔ 👎 Hardening (✖ Missed)

○ ○ ○ Fuzzing

◼ Your answer to this question is incorrect.

▶ Which of the following security control types fall(s) into the category of detection controls? (Select all that apply)

☐ ☐ ☐ Warning signs

☐ ✔ 👎 CCTV monitoring (✖ Missed)

☐ ☐ ☐ Hardware locks

☐ ✔ 👎 Motion sensors (✖ Missed)

☐ ✔ 👎 IDS (✖ Missed)

◼ Your answer to this question is incorrect.

▶ The process of OS hardening involves: (Select all that apply)

☐ ☐ ☐ Risk assessment

☐ ☐ ☐ Identification of critical systems and components

☐ ✔ 👎 Disabling unnecessary services (✖ Missed)

☐ ✔ 👎 Password protection (✖ Missed)

☐ ✔ 👎 Disabling unnecessary accounts (✖ Missed)

◼ Your answer to this question is incorrect.

▶ Which of the security control types listed below fall(s) into the category of preventative controls? (Select all that apply)

☐ ☐ ☐ IDSs

☐ ✔ 👎 Fencing (✖ Missed)

☐ ✔ 👎 Hardware locks (✖ Missed)

☐ ☐ ☐ Motion sensors

☐ ☐ ☐ Warning signs

☐ ✔ 👎 Mantraps (✖ Missed)

◼ Your answer to this question is incorrect.

▶ A monitored host containing no valuable data specifically designed to detect unauthorized access attempts is known as:

○ ○ ○ Flood guard

○ ○ ○ Trojan horse

○ ○ ○ Captive portal

○ ✔ 👎 Honeypot (✖ Missed)

⊟ Your answer to this question is incorrect.

▸ Penetration testing: (Select all that apply)

☐ ✔ 👎 Bypasses security controls (✖ Missed)

☐ ☐ ☐ Only identifies lack of security controls

☐ ✔ 👎 Actively tests security controls (✖ Missed)

☐ ✔ 👎 Exploits vulnerabilities (✖ Missed)

☐ ☐ ☐ Passively tests security controls

⊟ Your answer to this question is incorrect.

▸ Penetration test with the full prior knowledge on how the system that is to be tested works is called:

○ ○ ○ White hat

○ ○ ○ Fuzz test

○ ✔ 👎 White box (✖ Missed)

○ ○ ○ Black box

⊟ Your answer to this question is incorrect.

▸ The practice of finding vulnerability in an application by feeding it incorrect input is known as:

○ ○ ○ Input validation

○ ○ ○ Exception handling

○ ○ ○ Application hardening

○ ✔ 👎 Fuzzing (✖ Missed)

⊟ Your answer to this question is incorrect.

▸ Which of the following programming aspects are critical in secure application development process? (Select 2 answers)

☐ ☐ ☐ Patch management

☐ ✔ 👎 Input validation (✖ Missed)

☐ ☐ ☐ Password protection

☐ ✔ 👎 Error and exception handling (✖ Missed)

☐ ☐ ☐ Application whitelisting

⊟ Your answer to this question is incorrect.

▸ A computer system used to divert the attacker's attention from corporate network is known as:

○ ○ ○ Logic bomb

○ ○ ○ Trojan horse

○ ○ ○ UTM appliance **In order to provide you with the best online experience this website uses cookies.**

○ ✔ 👎 Honeypot (✖ Missed)

■ Your answer to this question is incorrect.

▸ Which of the following answers refers to a user interface element on mobile devices controlling access to a device after the device is switched on?
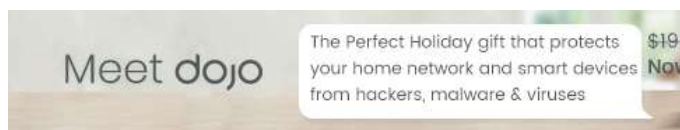
○ ○ ○ Captive portal

○ ✔ 👎 Screen lock (✘ Missed)

○ ○ ○ Recovery agent

○ ○ ○ Hardware lock

■ Your answer to this question is incorrect.

Try Again (/component/communityquiz/quiz/10-comptia-security-plus-certification/61-comptia-security-plus-certification-practice-test-9-exam-sy0-401?Itemid=101)

Security+

CompTIA Security+ Certification Exam SY0-401 Practice Tests

Security+ Practice Test 1 (/comptia-security-plus-practice-test-1-exam-sy0-401)

Security+ Practice Test 2 (/comptia-security-plus-practice-test-2-exam-sy0-401)

Security+ Practice Test 3 (/comptia-security-plus-practice-test-3-exam-sy0-401)

Security+ Practice Test 4 (/comptia-security-plus-practice-test-4-exam-sy0-401)

Security+ Practice Test 5 (/comptia-security-plus-practice-test-5-exam-sy0-401)

Security+ Practice Test 6 (/comptia-security-plus-practice-test-6-exam-sy0-401)

Security+ Practice Test 7 (/comptia-security-plus-practice-test-7-exam-sy0-401)

Security+ Practice Test 8 (/comptia-security-plus-practice-test-8-exam-sy0-401)

Security+ Practice Test 9 (/comptia-security-plus-practice-test-9-exam-sy0-401)

Security+ Practice Test 10 (/comptia-security-plus-practice-test-10-exam-sy0-401)

Security+ Practice Test 11 (/comptia-security-plus-practice-test-11-exam-sy0-401)

Security+ Practice Test 12 (/comptia-security-plus-practice-test-12-exam-sy0-401)

CompTIA Security+ Certification SY0-401 Practice Tests by Exam Topic

Malware Quiz (/malware-quiz)

Port Numbers Quiz (/comptia-security-plus-certification-port-numbers-quiz)

Exam Glossaries

Malware Glossary (/malware-glossary)

CompTIA Security+ Certification Exam Acronym Glossary (/comptia-security-plus-certification-exam-glossary)

CompTIA Security+ SY0-401 Exam Objectives (http://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf)