ExamCompass
CompTIA Practice Exams

(/./)

CompTIA Security+ Certification Exam SY0-501 Practice Test 1

▸ Harmful programs used to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems are commonly referred to as:

○ ○ ○ Adware

👍 ✔ ☑ Malware (☑ Your answer)

○ ○ ○ Ransomware

○ ○ ○ Spyware

☑ You correctly answered this question.

▸ Which of the following statements apply to the definition of a computer virus? (Select 3 answers)

☐ ✔ 👎 A self-replicating computer program containing malicious segment (✖ Missed)

👍 ✔ ☑ Requires its host application to be run to make the virus active (☑ Your answer)

☐ ☐ ☐ A standalone malicious computer program that replicates itself over a computer network

☐ ☐ ☐ Can run by itself without any interaction

👍 ✔ ☑ Attaches itself to an application program or other executable component (☑ Your answer)

👍 ☐ ➖ A self-contained malicious program or code that does need a host to propagate itself (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▸ Which of the terms listed below refers to an example of a crypto-malware?

○ ○ ○ Backdoor

👍 ✔ ☑ Ransomware (☑ Your answer)

○ ○ ○ Keylogger

○ ○ ○ Rootkit

☑ You correctly answered this question.

▸ Malware that restricts access to a computer system by encrypting files or locking the entire system down until the user performs requested action is known as:

○ ○ ○ Grayware

○ ○ ○ Adware

👆 ✔ ☑ Ransomware (☑ Your answer)

○ ○ ○ Spyware

☑ You correctly answered this question.

▸ A standalone malicious computer program that typically propagates itself over a computer network to adversely affect system resources and network bandwidth is called:

○ ○ ○ Spyware

👆 ✔ ☑ Worm (☑ Your answer)

○ ○ ○ Trojan

○ ○ ○ Spam

☑ You correctly answered this question.

▸ A type of software that performs unwanted and harmful actions in disguise of a legitimate and useful program is known as a Trojan horse. This type of malware may act like a legitimate program and have all the expected functionalities, but apart from that it will also contain a portion of malicious code that the user is unaware of.

👆 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ A collection of software tools used by a hacker to mask intrusion and obtain administrator-level access to a computer or computer network is known as:

👆 ✔ ☑ Rootkit (☑ Your answer)

○ ○ ○ Spyware

○ ○ ○ Backdoor

○ ○ ○ Trojan

☑ You correctly answered this question.

▸ Which of the following answers lists an example of spyware?

👆 ✔ ☑ Keylogger (☑ Your answer)

○ ○ ○ Vulnerability scanner

○ ○ ○ Computer worm

○ ○ ○ Packet sniffer

☑ You correctly answered this question.

▸ What is adware?

○ ○ ○ Unsolicited or undesired electronic messages

○ ○ ○ Malicious program that sends copies of itself to other computers on the network

👆 ✔ ☑ Software that displays advertisements (☑ Your answer)

○ ○ ○ Malicious software that collects information about users without their knowledge

☑ You correctly answered this question.

▸ Malicious software collecting information about users without their knowledge/consent is known as:

○ ○ ○ Crypto-malware

○ ○ ○ Adware

○ ○ ○ Ransomware

👍 ✔ ☑ Spyware (☑ Your answer)

☑ You correctly answered this question.

▸ A malware-infected networked host under remote control of a hacker is commonly referred to as:

○ ○ ○ Trojan

○ ○ ○ Worm

👍 ✔ ☑ Bot (☑ Your answer)

○ ○ ○ Honeypot

☑ You correctly answered this question.

▸ Which of the terms listed below applies to a collection of intermediary compromised systems that are used as a platform for a DDoS attack?

○ ○ ○ Honeynet

👍 ✔ ☑ Botnet (☑ Your answer)

○ ○ ○ Quarantine network

○ ○ ○ Malware

☑ You correctly answered this question.

▸ Which type of Trojan enables unauthorized remote access to a compromised system?

○ ○ ○ pcap

👍 ✔ ☑ RAT (☑ Your answer)

○ ○ ○ MaaS

○ ○ ○ pfSense

☑ You correctly answered this question.

▸ Malicious code activated by a specific event is called:

○ ○ ○ Backdoor

👍 ✔ ☑ Logic bomb (☑ Your answer)

○ ○ ○ Dropper

○ ○ ○ Retrovirus

☑ You correctly answered this question.

▶ Which of the following answers refers to an undocumented (and often legitimate) way of gaining access to a program, online service, or an entire computer system?

○ ○ ○ Logic bomb

○ ○ ○ Trojan horse

○ ○ ○ Rootkit

👍 ✔ ☑ Backdoor (☑ Your answer)

☑ You correctly answered this question.

▶ An unauthorized practice of obtaining confidential information by manipulating people into disclosing sensitive data is referred to as:

○ ○ ○ Shoulder surfing

○ ○ ○ Privilege escalation

👍 ✔ ☑ Social engineering (☑ Your answer)

○ ○ ○ Penetration testing

☑ You correctly answered this question.

▶ A fraudulent email requesting its recipient to reveal sensitive information (e.g. user name and password) used later by an attacker for the purpose of identity theft is an example of: (Select all that apply)

👍 ✔ ☑ Phishing (☑ Your answer)

☐ ☐ ☐ Watering hole attack

☐ ✔ 👎 Social engineering (✖ Missed)

☐ ☐ ☐ Bluejacking

☐ ☐ ☐ Vishing

➖ Your answer to this question is incorrect or incomplete.

▸ A social engineering technique whereby attackers under disguise of legitimate request attempt to gain access to confidential information they shouldn't have access to is commonly referred to as:

◯ ✔ 👎 Phishing (✖ Missed)

👆 ◯ ➖ Privilege escalation (✖ Your answer)

◯ ◯ ◯ Backdoor access

◯ ◯ ◯ Shoulder surfing

➖ Your answer to this question is incorrect or incomplete.

▸ Phishing scams targeting a specific group of people are referred to as:

◯ ◯ ◯ Vishing

👆 ✔ ☑ Spear phishing (☑ Your answer)

◯ ◯ ◯ Spoofing

◯ ◯ ◯ Whaling

☑ You correctly answered this question.

▸ Phishing scams targeting people holding high positions in an organization or business are known as:

◯ ◯ ◯ Vishing

◯ ◯ ◯ Bluesnarfing

👆 ✔ ☑ Whaling (☑ Your answer)

◯ ◯ ◯ Bluejacking

◯ ◯ ◯ Pharming

☑ You correctly answered this question.

▸ The practice of using a telephone system to manipulate user into disclosing confidential information is called:

○ ○ ○ Whaling

○ ○ ○ Spear phishing

👆 ✔ ☑ Vishing (☑ Your answer)

○ ○ ○ Pharming

☑ You correctly answered this question.

▸ What is tailgating?

○ ○ ○ Acquiring unauthorized access to confidential data

○ ○ ○ Looking over someone's shoulder to get information

👆 ✔ ☑ Gaining unauthorized access to restricted areas by following another person (☑ Your answer)

○ ○ ○ Manipulating a user into disclosing confidential information

☑ You correctly answered this question.

▸ Which social engineering attack relies on identity theft?

👆 ✔ ☑ Impersonation (☑ Your answer)

○ ○ ○ Dumpster diving

○ ○ ○ Watering hole attack

○ ○ ○ Shoulder surfing

☑ You correctly answered this question.

▸ In computer security, the term "Dumpster diving" is used to describe a practice of sifting through trash for discarded documents containing sensitive data. Found documents containing names and surnames of the employees along with the information about positions held in the company and

other data can be used to facilitate social engineering attacks. Having the documents shredded or incinerated before disposal makes dumpster diving less effective and mitigates the risk of social engineering attacks.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸A situation in which an unauthorized person can view another user's display or keyboard to learn their password or other confidential information is referred to as:

○ ○ ○ Spear phishing

○ ○ ○ Tailgating

👍 ✔ ☑ Shoulder surfing (☑ Your answer)

○ ○ ○ Spoofing

☑ You correctly answered this question.

Your Final Report	
Total marks	28
Total Questions	25
Questions correctly answered	22
Success ratio	88%
Marks secured	25
Percentage secured	89.29%

Security+

CompTIA Security+ Certification Exam SY0-501 Practice Tests

CompTIA Security+ Certification SY0-501 Practice Tests by Exam Topic

Public Key Infrastructure (PKI) Quiz (/comptia-security-plus-certification-exam-sy0-501-public-key-infrastructure-quiz)

Exam Glossaries

Malware Glossary (/malware-glossary)

CompTIA Security+ SY0-501 Exam Objectives (https://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-501-exam-objectives.pdf)

LIFE + MBA   DO BOTH.

Accelerate your development
with our Executive MBA ❯