CompTIA Security+ Certification Exam SY0-701 Practice Test 9

▸ As opposed to simple DoS attacks that usually are performed from a single system, a DDoS attack uses multiple compromised computer systems to perform the attack against its target. The intermediary systems that are used as a platform for the attack (often referred to as zombies, and collectively as a botnet) are the secondary victims of the DDoS attack.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ A type of DDoS attack where an attacker exploits vulnerabilities in certain services or protocols to generate responses that are much larger than the original request is referred to as:

👍 ✔ ☑ Amplified DDoS attack (☑ Your answer)

○ ○ ○ Volumetric DDoS attack

○ ○ ○ Reflected DDoS attack

○ ○ ○ Application DDoS attack

☑ You correctly answered this question.

▸ What defines a reflected DDoS attack?

○ ○ ○ Overwhelming the target with a high volume of traffic to saturate its bandwidth

○ ○ ○ Exploiting vulnerabilities in network protocols to consume resources and disrupt services

👍 ✔ ☑ Utilizing third-party servers to reflect and amplify attack traffic towards the target (☑ Your answer)

○ ○ ○ Targeting vulnerabilities in applications or web servers to exhaust resources

☑ You correctly answered this question.

▸ A DNS amplification attack is a type of DDoS attack wherein an attacker sends a small, specially crafted DNS query containing a spoofed IP address (the victim's IP) to a compromised DNS server. Upon receiving the query, the DNS server generates a much larger response packet, which is then sent to the victim's IP address, causing potential disruption due to overwhelming traffic.

👍 ✔ ☑ True (☑ Your answer)

O O O False

☑ You correctly answered this question.

▸ Which of the answers listed below refers to a cyberattack technique that relies on providing false DNS information to a DNS resolver for the purpose of redirecting or manipulating the resolution of domain names to malicious IP addresses?

👍 ✔ ☑ DNS spoofing (☑ Your answer)

O O O Credential stuffing

O O O URL hijacking

O O O Domain hijacking

☑ You correctly answered this question.

▸ Remapping a domain name to a rogue IP address is an example of what kind of exploit?

O O O URL hijacking

👍 ✔ ☑ DNS cache poisoning (☑ Your answer)

O O O Domain hijacking

O O O ARP poisoning

☑ You correctly answered this question.

▸ When domain registrants due to unlawful actions of third parties lose control over their domain names, they fall victim to:

○ ○ ○ Sybil attack

👍 ✔ ☑ Domain hijacking (☑ Your answer)

○ ○ ○ Typosquatting

○ ○ ○ URL hijacking

☑ You correctly answered this question.

▶ Which of the following can be classified as malicious activity indicator on a wireless network?

👍 ✔ ☑ Rogue AP (☑ Your answer)

○ ○ ○ Jump server

○ ○ ○ Unmanaged switch

○ ○ ○ Network tap

☑ You correctly answered this question.

▶ The practice of gaining unauthorized access to a Bluetooth device is known as:

○ ○ ○ Phishing

👍 ○ ➖ Bluejacking (✖ Your answer)

○ ○ ○ Smishing

○ ✔ 👎 Bluesnarfing (✖ Missed)

➖ Your answer to this question is incorrect or incomplete.

▶ A wireless disassociation attack is a type of: (Select 2 answers)

👍 ☐ ➖ Downgrade attack (✖ Your answer)

☐ ✔ 👎 Deauthentication attack (✖ Missed)

☐ ☐ ☐ Brute-force attack

☐ ✔ 👎 DoS attack (✖ Missed)

👍 ☐ ➖ Cryptographic attack (✖ Your answer)

⊟ Your answer to this question is incorrect or incomplete.

▶ A wireless jamming attack is a type of:

◯ ◯ ◯ Cryptographic attack

👆 ✔ ☑ DoS attack (☑ Your answer)

◯ ◯ ◯ Brute-force attack

◯ ◯ ◯ Downgrade attack

☑ You correctly answered this question.

▶ Which of the answers listed below refers to RFID vulnerability?

◯ ◯ ◯ Spoofing

◯ ◯ ◯ Eavesdropping

👆 ◯ ⊟ RFID cloning (✖ Your answer)

◯ ◯ ◯ Data interception

◯ ◯ ◯ Replay attack

◯ ◯ ◯ DoS attack

◯ ✔ 👎 All of the above (✖ Missed)

⊟ Your answer to this question is incorrect or incomplete.

▶ Which of the following is a vulnerability characteristic to NFC communication?

◯ ◯ ◯ Eavesdropping

👆 ◯ ⊟ Data interception (✖ Your answer)

◯ ◯ ◯ Replay attacks

◯ ◯ ◯ DoS attacks

◯ ✔ 👎 All of the above (✖ Missed)

⊟ Your answer to this question is incorrect or incomplete.

▶ Which wireless attack focuses on exploiting vulnerabilities found in WEP?

○ ✔ 👎 IV attack (✖ Missed)

👍 ○ ⬛ War driving (✖ Your answer)

○ ○ ○ SSID spoofing

○ ○ ○ Bluejacking

⬛ Your answer to this question is incorrect or incomplete.

▶ Which of the statements listed below can be used to describe the characteristics of an on-path attack? (Select all that apply)

☐ ✔ 👎 An on-path attack is also known as MITM attack (✖ Missed)

👍 ✔ ☑ Attackers place themselves on the communication route between two devices (☑ Your answer)

👍 ✔ ☑ Attackers intercept or modify packets sent between two communicating devices (☑ Your answer)

☐ ☐ ☐ Attackers do not have access to packets exchanged during the communication between two devices

⬛ Your answer to this question is incorrect or incomplete.

▶ A network replay attack occurs when an attacker captures sensitive user data and resends it to the receiver with the intent of gaining unauthorized access or tricking the receiver into unauthorized operations.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▶ What are the characteristic features of a session ID? (Select 3 answers)

👍 ☐ ⬛ Typically stored on the server side (✖ Your answer)

👍 ✔ ☑ A unique identifier assigned by the website to a specific user (☑ Your answer)

☐ ☐ ☐ Contains user's authentication credentials, e.g., username and password

👍 ✔ ☑ A piece of data that can be stored in a cookie, or embedded as an URL parameter (☑ Your answer)

☐ ✔ 👎 Typically stored on the client side (in the user's browser) rather than on the server (✖ Missed)

☐ ☐ ☐ A unique identifier assigned to a server

⊟ Your answer to this question is incorrect or incomplete.

▶ In a session replay attack, an attacker intercepts and steals a valid session ID of a user and resends it to the server with the intent of gaining unauthorized access to the user's session or tricking the server into unauthorized operations on behalf of the legitimate user.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▶ A technique that allows an attacker to authenticate to a remote server without extracting cleartext password from a digest is called:

○ ✔ 👎 Pass the hash (✖ Missed)

👍 ○ ⊟ Replay attack (✖ Your answer)

○ ○ ○ Brute-force attack

○ ○ ○ Spraying attack

⊟ Your answer to this question is incorrect or incomplete.

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

👍 ✔ ☑ Code injection (☑ Your answer)

○ ○ ○ Privilege escalation

○ ○ ○ Session hijacking

○ ○ ○ Packet sniffing

☑ You correctly answered this question.

▸ Which of the following exploits targets a protocol used for managing and accessing networked resources?

○ ○ ○ CSRF/XSRF attack

○ ○ ○ XML injection attack

👍 ✔ ☑ LDAP injection attack (☑ Your answer)

○ ○ ○ SQL injection attack

☑ You correctly answered this question.

▸ Which type of exploit targets web applications that generate content used to store and transport data?

○ ○ ○ SQL injection attack

👍 ○ ⬛ CSRF/XSRF attack (✖ Your answer)

○ ✔ 👎 XML injection attack (✖ Missed)

○ ○ ○ LDAP injection attack

⬛ Your answer to this question is incorrect or incomplete.

▸ Which of the following facilitate(s) privilege escalation attacks? (Select all that apply)

👍 ✔ ☑ System/application vulnerabilities (☑ Your answer)

☐ ☐ ☐ Password hashing

👍 ✔ ☑ System/application misconfigurations (☑ Your answer)

☐ ☐ ☐ Network segmentation

👍 ✔ ☑ Social engineering techniques (☑ Your answer)

☑ You correctly answered this question.

▸ Which of the statements listed below apply to the CSRF/XSRF attack? (Select 3 answers)

☐ ✔ 👎 Exploits the trust a website has in the user's web browser (✖ Missed)

👍 ✔ ☑ A user is tricked by an attacker into submitting unauthorized web requests (☑ Your answer)

☐ ✔ 👎 Website executes attacker's requests (✖ Missed)

👍 ☐ ⬛ Exploits the trust a user's web browser has in a website (✖ Your answer)

👍 ☐ ⬛ A malicious script is injected into a trusted website (✖ Your answer)

👍 ☐ ⬛ User's browser executes attacker's script (✖ Your answer)

⬛ Your answer to this question is incorrect or incomplete.

▶ A dot-dot-slash attack is also referred to as:

○ ○ ○ Disassociation attack

○ ○ ○ On-path attack

👍 ✔ ☑ Directory traversal attack (☑ Your answer)

○ ○ ○ Downgrade attack

☑ You correctly answered this question.

Your Final Report

Total marks	34
Total Questions	25
Questions correctly answered	15
Success ratio	60%
Marks secured	22
Percentage secured	64.71%

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 14 (/comptia-security-plus-practice-test-14-exam-sy0-601)

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

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)

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)

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)

-->