220-1102 Q&As

CompTIA A+ Certification Exam: Core 2

QUESTION 1

A malicious user was able to export an entire website\\'s user database by entering specific commands into a field on the company\\'s website. Which of the following did the malicious user most likely exploit to extract the data?

A. Cross-site scripting

B. SQL injection

C. Brute-force attack

D. DDoS attack

Correct Answer: B

SQL injection is a type of attack that takes advantage of vulnerabilities in a web application\\'s database query software, allowing an attacker to send malicious SQL commands through the application to the database. These commands can manipulate the database and can lead to unauthorized data access or manipulation. SQL injection: In the scenario described, the malicious user was able to export an entire website\\'s user database by entering specific commands into a field on the company\\'s website, which is a classic example of an SQL injection attack. This type of attack exploits vulnerabilities in the database layer of an application to execute unauthorized SQL commands. Cross-site scripting (A) involves injecting malicious scripts into content from otherwise trusted websites. A brute-force attack (C) is an attempt to gain access to a system by systematically checking all possible keys or passwords until the correct one is found. A DDoS attack

(D) is an attempt to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of internet traffic.

QUESTION 2

A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic. Which of the following types of infections are the workstations most likely experiencing? (Choose two.)

A. Zombies

B. Keylogger

C. Adware

D. Botnet

E. Ransomware

F. Spyware

Correct Answer: AD

In a scenario where several internal workstations are the source of traffic in a DDoS attack, the workstations are most likely infected with one or both of the following:

A. Zombies: Workstations infected with malware and controlled by an external entity to participate in a DDoS attack are often referred to as "zombies." These compromised machines become part of a botnet used for carrying out coordinated attacks.

D. Botnet: A botnet is a network of compromised computers, including workstations, that have been infected with malicious software, turning them into "bots." These bots can be controlled remotely to carry out various malicious activities, including DDoS attacks.

The other options (B. Keylogger, C. Adware, E. Ransomware, and F. Spyware) are types of malware or malicious software but are not directly associated with participating in DDoS attacks like zombies and botnets are.

QUESTION 3

Which of the following ls command options is used to display hidden files and directories?

A. -a

B. -s

C. -lh

D. -t

Correct Answer: A

QUESTION 4

While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

A. SSL key

B. Preshared key

C. WPA2 key

D. Recovery key

Correct Answer: D

QUESTION 5

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the

available RAM?

A. The system is missing updates.

B. The systems utilizing a 32-bit OS.

C. The system\\'s memory is failing.

D. The system requires BIOS updates.

Correct Answer: B

The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use. Therefore, even if the

technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory. The system missing updates, the

system\\'s memory failing, or the system requiring BIOS updates are not likely to cause this issue.

References:

https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715

https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/