SY0-501Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sy0-501.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. DNS hijacking

B. Cross-site scripting

C. Domain hijacking

D. Man-in-the-browser

E. Session hijacking

Correct Answer: AE

QUESTION 2

A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of traffic. Which of the following should be implemented to prevent a DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer

B. Increase the capacity of the perimeter router to 10 Gbps

C. Install a firewall at the network to prevent all attacks

D. Use redundancy across all network devices and services

Correct Answer: D

QUESTION 3

After successfully breaking into several networks and infecting multiple machines with malware, hackers contact the network owners, demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers

B. Organized crime

C. Insiders

D. Hacktivists

Correct Answer: B

QUESTION 4

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4

B. MD5

C. HMAC

D. SHA

Correct Answer: B

QUESTION 5

A penetration tester was able to connect to a company\\'s internal network and perform scans and staged attacks for the duration of the testing period without being noticed. The SIEM did not alert the security team to the presence of the penetration tester\\'s devices on the network. Which of the following would provide the security team with notification in a timely manner?

A. Implement rogue system detection and sensors

B. Create a trigger on the IPS and alert the security team when unsuccessful logins occur

C. Decrease the correlation threshold for alerts on the SIEM

D. Run a credentialed vulnerability scan

Correct Answer: A