



CompTIA

SY0-501 EXAM

CompTIA Security+

Product: Demo

For More Information:

<https://www.dumpsplanet.com/SY0-501-dumps>

Question: 1

A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select TWO)

- A. Replay
- B. Rainbow tables
- C. Brute force
- D. Pass the hash
- E. Dictionary

Answer: DE

Question: 2

Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

- A. Spyware
- B. Crypto-malware
- C. Rootkit
- D. Backdoor

Answer: C

Question: 3

A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

- A. Obtain a list of passwords used by the employee.
- B. Generate a report on outstanding projects the employee handled
- C. Have the employee surrender company identification.

D. Have the employee sign an NDA before departing

Answer: A

Question: 4

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

- A. A perimeter firewall and IDS
- B. An air gapped compiler network
- C. A honeypot residing in a DMZ
- D. An ad hoc network with NAT
- E. A bastion host

Answer: C

Question: 5

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

- A. Roll back changes in the test environment
- B. Verify the hashes of files
- C. Archive and compress the files
- D. Update the secure baseline

Answer: A

Question: 6

A user clicked an email link that led to a website that infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not detected or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

- A. The user's account was over-privileged
- B. Improper error handling triggered a false negative in all three controls
- C. The email originated from a private email server with no malware protection
- D. The virus was a zero-day attack

Answer: C

Question: 7

An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment DNSSEC at the organization?

- A. LDAP
- B. TPM
- C. TLS
- D. SSL
- E. PW

Answer: C

Question: 8

A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

- A. Vulnerability scanning
- B. Penetration testing
- C. Application fuzzing
- D. User permission

Answer: A

Question: 9

An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

- A. WPA+CCMP
- B. WPA2+CCMP
- C. WPA+TWP
- D. WPA2+TWP

Answer: D

Question: 10

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review. Which servers are up without having the administrator on call? The security analyst is hesitant to give the application team full access due to other critical applications

running on the road balancer. Which of the following is the BEST solution for the security analyst to process the request?

- A. Give the application team administrator access during off hours
- B. Disable other critical applications before granting the team access.
- C. Give the application team read-only access
- D. Share the account with the application team

Answer: A

Question: 11

Which of the following cryptographic attacks would salting of passwords render ineffective?

- A. Brute force
- B. Dictionary
- C. Rainbow tables
- D. Birthday

Answer: D

Question: 12

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- A. LDAP services
- B. Kerberos services
- C. NTLM services
- D. CHAP services

Answer: C

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-501 Exam Questions With Answers.

Dumps Planet also provides you extra 20% discount on the purchase of SY0-501 exam. Use Coupon code like “dp20%”

<https://www.dumpsplanet.com/SY0-501-dumps>

Money Back Guarantee



<https://www.dumpsplanet.com/>