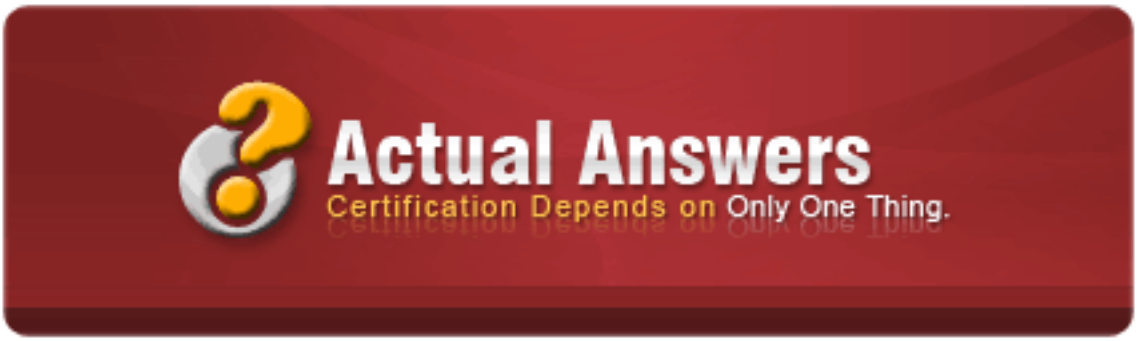
CompTIA SY0-301



CompTIA Security+ 2012

Version: Demo 12.4

Topic 1, Volume B

QUESTION NO: 1

Matt, an attacker, drops a USB flash drive labeled "CEO's music collection" in the reception area of a bank hoping an employee will find it. The drive actually contains malicious code. Which of the following attacks is this?

A. Vishing
B. Social engineering
C. Spim
D. Impersonation

Answer: B
Explanation:

Topic 2, Volume A

QUESTION NO: 2

Pete, an IT security technician, has been tasked with implementing physical security controls for his company's workstations. Which of the following BEST meets this need?

A. Host-based firewalls
B. Safe
C. Cable locks
D. Remote wipe

Answer: C
Explanation:

QUESTION NO: 3

Which of the following security concepts can Matt, a security administrator, implement to support integrity?

A. Digital signatures
B. Trust models
C. Key escrow

D. Recovery agents

Answer: A
Explanation:

Topic 3, Volume D

QUESTION NO: 4

Sara, a security analyst, suspects that a rogue web server is running on the network. Which of the following would MOST likely be used to identify the server's IP address?

A. Port scanner
B. Telnet
C. Traceroute
D. Honeypot

Answer: A
Explanation:

Topic 4, Volume C

QUESTION NO: 5

Which of the following provides authentication, authorization, and accounting services?

A. PKI
B. WPA2
C. NTLMv2
D. RADIUS

Answer: D
Explanation:

Topic 1, Volume B

QUESTION NO: 6

Users have reported that when they go to the company website they are sent to a competitor's site instead. Which of the following is the MOST likely explanation?

A. Someone has employed ARP poisoning against the company.
B. Someone has employed DNS poisoning against the company.
C. Someone has accidentally unplugged the company's web server.
D. The competitor has a more powerful web server.

Answer: B
Explanation:

Topic 2, Volume A

QUESTION NO: 7

Grandfather-Father-Son and Tower of Hanoi are common:

A. Trojans that collect banking information.
B. Backup tape rotation strategies.
C. Penetration testing best practices.
D. Failover practices in clustering.

Answer: B
Explanation:

Topic 4, Volume C

QUESTION NO: 8

Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

A. Phishing
B. Shoulder surfing
C. Impersonation
D. Tailgating

Answer: C

Explanation:

QUESTION NO: 9

A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing
B. Mantrap
C. A guard
D. Video surveillance

Answer: B

Explanation:

Topic 3, Volume D

QUESTION NO: 10

Sara, the security engineer, has discovered that a breach is in progress on a non-production system of moderate importance. Which of the following should Sara collect FIRST?

A. Memory dump, ARP cache
B. Live system image, route table
C. Temp files, hosts file
D. Offline system image, router logs

Answer: A

Explanation: