SY0-601Q&As

CompTIA Security+

QUESTION 1

An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation.

Which of the following method did attacker to insert the contacts without having \\'Physical access to device?

A. Jamming

B. BluJacking

C. Disassoaatm

D. Evil twin

Correct Answer: B

bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

QUESTION 2

A security analyst reviews a company\\'s authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

A. Dictionary

B. Rainbow table

C. Spraying

D. Brute-force

Correct Answer: D

QUESTION 3

Two companies are in the process of merging. The companies need to decide how to standardize their information security programs. Which of the following would best align the security programs?

A. Shared deployment of CIS baselines

B. Joint cybersecurity best practices

C. Both companies following the same CSF

D. Assessment of controls in a vulnerability report

Correct Answer: C

QUESTION 4

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site Upon investigation, a security analyst the identifies the following:

1.

The legitimate websites IP address is 10.1.1.20 and eRecruit local resolves to the IP

2.

The forged website\\'s IP address appears to be 10.2.12.99. based on NetFtow records

3.

AH three at the organization\\'s DNS servers show the website correctly resolves to the legitimate IP

4.

DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

A. A reverse proxy was used to redirect network traffic

B. An SSL strip MITM attack was performed

C. An attacker temporarily pawned a name server

D. An ARP poisoning attack was successfully executed

Correct Answer: C

DNS (server cache) poisoning is also referred to as a "Redirection Attack" per the official CompTIA Certmaster study guide. The user was redirected to a website that looked like the legitimate one.

QUESTION 5

During an incident, a company\\'s CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physical move the PC to a separate internet pint of presence

B. Create and apply microsegmentation rules.

C. Emulate the malware in a heavily monitored DMZ segment.

D. Apply network blacklisting rules for the adversary domain

Correct Answer: B

AH secure in entire packet