# CompTIA

## SY0-601 Exam

### CompTIA Security+ Exam 2023

### Questions & Answers

### Demo

# Version: 74.0

Topic 1, Exam Set 1

## Question: 1

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable To improve security? (Select TWO.)

A. RADIUS
B. PEAP
C. WPS
D. WEP-EKIP
E. SSL
F. WPA2-PSK

**Answer: A, F**

Explanation:

To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

## Question: 2

During an incident a company CIRT determine it is necessary to observe the continued network-based transaction 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 micro segmentation rules.
C. Emulate the malware in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain

**Answer: C**

Explanation:

To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary. Reference: https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/

## Question: 3

Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

A. Production
B. Test
C. Staging
D. Development

**Answer: D**

Explanation:

The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality. Reference: https://www.techopedia.com/definition/27561/development-environment

## Question: 4

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates.
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software

**Answer: C**

Explanation:

The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application

whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run.
Reference: https://www.techopedia.com/definition/31541/application-whitelisting

## Question: 5

A company recently experienced an attack during which its main website was Directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers, Which of the following should the
company implement to prevent this type of attack from occurring In the future?

A. IPsec
B. SSL/TLS
C. ONSSEC
D. SMIME

## Answer: B

Explanation:

To prevent attacks where the main website is directed to the attacker's web server and allowing the attacker to harvest credentials from unsuspecting customers, the company should implement SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt the communication between the web server and the clients. This will prevent attackers from intercepting and tampering with the communication, and will also help to verify the identity of the web server to the clients.