Exam	**SY0-601**
Title	**CompTIA Security+ 2021 Exam**
Version	**62.0**
Product Type	**491 Q&A with explanations**

QUESTION 1
A company has discovered unauthorized devices area 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

Explanation:

Answer: A, F
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-Sharead Key) is a security protocol that uses stronger encryption than WEP and WP
A. It requires a pre-sharead 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 networkbased transaction between a callback domain and the malwarea 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 malwarea in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain

Explanation:

Answer: C
To observe the continued network-based transaction between a callback domain and the malwarea 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 malwarea 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 malwarea 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-dmzso-important/

QUESTION 3
Which of the following environment utilizes dummy dataa 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

Explanation:

Answer: D
The environment that utilizes dummy dataa 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 softwarea and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy dataa can be used in the development environment to simulate real-world scenarios and test the softwarea's functionality. Reference: https://www.techopedia.com/definition61/development-environment

---

QUESTION 4
A desktop support technician recently installed a new document-scanning softwarea 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 softwarea updataes.
C. The softwarea was not added to the application whitelist.
D. The system was isolated from the network due to infected softwarea

Explanation:

Answer: C
The most likely cause of the document-scanning softwarea program not responding when launched by the end user is that the softwarea was not added to the application whitelist. An application whitelist is a list of approved softwarea applications that area allowed to run on a system. If the softwarea is not on the whitelist, it may be blocked from running by the system's security policies.

Adding the softwarea to the whitelist should resolve the issue and allow the program to run.
Reference: https://www.techopedia.com/definition41/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

Explanation:

Answer: B
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.

QUESTION 6
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A split-tunnel VPN
D. Load-balanced servers

Explanation:

Answer: B
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.
To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

QUESTION 7
A security analyst has received several reports of an issue on an internal web application. Users state they area having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

```
Internet address      Physical address      Type
192.168.1.1           ff-ec-ab-00-aa-78     dynamic
192.168.1.5           ff-00-5e-48-00-fb     dynamic
192.168.1.8           00-0c-29-1a-e7-fa     dynamic
192.168.1.10          fc-41-5e-48-00-ff     dynamic
224.215.54.47         fc-00-5e-48-00-fb     static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking

Explanation:

Answer: C
The output of the œnetstat -ano command shows that there area two connections to the same IP address and port number. This indicates that there area two active sessions between the client and server.
The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client's browser.
Based on the output of the œnetstat -ano command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.
ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

QUESTION 8

A company recently experienced an attack during which 5 main website was directed to the atacker'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. DNSSEC
D. S/MIME

Explanation:

Answer: C
The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.
To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC.
DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records area not modified during transit and prevents DNS hijacking attacks.

QUESTION 9

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A spill-tunnel VPN
D. Load-balanced servers

Explanation:

Answer: B
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.
To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

QUESTION 10
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details area harvested?

A. Whaling
B. Spam
C. Invoice scam
D. Pharming

Explanation:

Answer: A
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details area harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

QUESTION 11
If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical dataa?

A. Perfect forward secrecy
B. Elliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption

Explanation:

Answer: A
Perfect forward secrecy would ensure that it cannot be used to decrypt all historical dataa. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

QUESTION 12
Which of the following environments can be stood up in a short period of time, utilizes either dummy dataa or actual dataa, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon
duration of time?

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

Explanation: