Free Questions for SY0-601

Shared by Bird on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO most likely use?

Options:

A- An external security assessment
B- A bug bounty program
C- A tabletop exercise
D- A red-team engagement

Answer:

C

Explanation:

A tabletop exercise is a type of simulation exercise that involves discussing hypothetical scenarios and testing the incident response plan in a low-stress environment. A tabletop exercise can help the CSO to validate the business's involvement in the incident response plan by involving key stakeholders, such as senior management, business units, legal department, etc., in the discussion and evaluation of the plan.

Question 2

Question Type: MultipleChoice

A security analyst discovers several jpg photos from a cellular phone during a forensics investigation involving a compromised system The analyst runs a forensics tool to gather file metadata Which of the following would be part of the images if all the metadata is still intact?

Options:

A- The GSS location
B- When the file was deleted

C- The total number of print jobs
D- The number of copies made

Answer:

A

Explanation:

The GPS location would be part of the images if all the metadata is still intact. Metadata is data that describes other data, such as file name, size, date, author, etc. Some metadata can also contain information about the device, software, or location that created or modified the data. For example, some digital cameras and smartphones can embed GPS coordinates into the metadata of photos, which can reveal the location where the photos were taken. This can be useful for forensic analysis, but also pose privacy risks.

Question 3

Question Type: MultipleChoice

Which of the following scenarios describes a possible business email compromise attack?

Options:

A- An employee receives a gift card request m an email that has an executive's name m the display held to the email
B- Employees who open an email attachment receive messages demanding payment m order to access files
C- A service desk employee receives an email from the HR director asking for log-in credentials lo a cloud administrator account
D- An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer:

A

Explanation:

An employee receiving a gift card request in an email that has an executive's name in the display

field to the email describes a possible business email compromise attack. Business email compromise (BEC) is a type of phishing attack that targets employees who have access to financial or sensitive information, such as accounting, human resources, or executive staff. The attacker impersonates a trusted person, such as a manager, vendor, or client, and requests a fraudulent payment, wire transfer, gift card purchase, or personal information. The attacker may spoof the email address or display name, use a look-alike domain, or compromise a legitimate email account to make the request seem authentic.

Question 4

Question Type: MultipleChoice

An analyst observed an unexpected high number of DE authentication on requests being sent from an unidentified device on the network. Which of the following attacks was most likely executed in this scenario?

Options:

A- Jamming
B- Blue jacking
C- Rogue access point
D- Disassociation

Answer:

D

Question 5

Question Type: MultipleChoice

A host was infected with malware. During the incident response. Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would most likely show where the malware originated?

Options:

A- The DNS logs
B- The web server logs

C- The SIP traffic logs
D- The SNMP logs

Answer:

A

Explanation:

The web server logs are records of the requests and responses that occur between a web server and a web client, such as a browser. The web server logs can show where the malware originated by indicating the source IP address, the destination URL, the date and time, the HTTP status code, the user agent, etc., of each request and response. The web server logs can help the incident response team to trace back the malicious website that infected the host with malware.

Question 6

Question Type: MultipleChoice

A user's login credentials were recently compromised During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password However the trusted website does not use a pop-up for entering user colonials Which of the following attacks occurred?

Options:

A- Cross-site scripting
B- SOL injection
C- DNS poisoning
D- Certificate forgery

Answer:

D

Explanation:

The user input credentials into a pop-up window that was not part of the trusted website. This suggests that the attacker was able to forge a certificate and present a fake website that looked like the legitimate one.This is a type of attack known as certificate forgery, which exploits the

trust relationship between users and websites that use SSL/TLS encryption2.

Question 7

Question Type: MultipleChoice

A security team received the following requirements for a new BYOD program that will allow employees to use personal smartphones to access business email:

* Sensitive customer data must be safeguarded

* Documents from managed sources should not be opened in unmanaged destinations.

* Sharing of managed documents must be disabled

* Employees should not be able to download emailed images to their devices

* Personal photos and contact lists must be kept private

* IT must be able to remove data from lost/stolen devices or when an employee no longer works for the company

Which of the following are the best features to enable to meet these requirements? (Select two).

Options:

A- Remote wipe
B- VPN connection
C- Biometric authentication
D- Device location tracking
E- Geofencing
F- Application approve list
G- Containerization

Answer:

A, G

Question 8

Question Type: MultipleChoice

An organization implemented cloud-managed IP cameras to monitor building entry points and

sensitive areas. The service provider enables direct TCP'IP connection to stream live video footage from each camer

a. The organization wants to ensure this stream is encrypted and authenticated Which of the following protocols should be implemented to best meet this objective?

Options:

A- SSH
B- SRTP
C- S/MIME
D- PPTP

Answer:

B

Question 9

Question Type: MultipleChoice

A security analyst reviews web server logs and notices the following line:

```
104.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /profile.php?id=%3cscript%3ealert%28%271%27%29%3cscript%3e HTTP/1.1" 200 11705
"http://www.example.com/downloadreport.php"
104.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /profile.php?id=%3cscript%3ealert%28%27
http%3a%2f%2fwww.evilsite.com%2fupdater.php%27%29%3cscript%3e HTTP/1.1" 200 23713 "http://www.example.com/downloadreport.php"
```

Which of the following vulnerabilities is the attacker trying to exploit?

Options:

A- Token reuse
B- SQL injection
C- Server side request forgery
D- Cross-site scripting

Answer:

D

Question 10

Question Type: MultipleChoice

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems The company follows a strict process to harden systems immediately upon delivery Even with these strict security measures in place an incident occurred from one of the workstations The root cause appears to be that the SoC was tampered with or replaced Which of the following most likely occurred?

Options:

A- Fileless malware
B- A downgrade attack
C- A supply-chain attack
D- A logic bomb
E- Misconfigured BIOS

Answer:

C

Explanation:

A supply-chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or products vital to the supply chain. A supply-chain attack can occur in software or hardware. In this case, the most likely scenario is that the SoC (system on chip) was compromised by a malicious actor before it was delivered to the company, either by tampering with or replacing it with a malicious version.This would allow the attacker to gain access to the company's systems through the specially configured workstations

Question 11

Question Type: MultipleChoice

A threat actor used a sophisticated attack to breach a well-known ride-sharing. company. The threat actor posted on social media that this action was in response to the company's treatment of its drivers Which of the following best describes tm type of throat actor?

Options:

A- Nation-slate
B- Hacktivist

C- Organized crime
D- Shadow IT

Answer:

B

Explanation:

A threat actor who used a sophisticated attack to breach a well-known ride-sharing company and posted on social media that this action was in response to the company's treatment of its drivers is most likely a hacktivist.A hacktivist is a person who uses hacking skills to promote a social or political cause, such as human rights, environmentalism, or anti-corporatism5.