

Exam	CS0-003 Exam
Title	CompTIA Cybersecurity Analyst (CySA+) Exam
Version	6.0
Product Type	136 Q&A with explanations

QUESTION 1

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H: K/A: L
- B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
- D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official Reference: <https://nvd.nist.gov/vuln-metrics/cvss>

QUESTION 2

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

- A. PAM
- B. IDS
- C. PKI
- D. DLP

Answer: D

Explanation:

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

QUESTION 3

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

- Alerts (17)
 - > Absence of Anti-CSRF Tokens
 - > Content Security Policy (CSP) Header Not Set (6)
 - > **Cross-Domain Misconfiguration (34)**
 - > Directory Browsing (11)
 - > Missing Anti-clickjacking Header (2)
 - > Cookie No HttpOnly Flag (4)
 - > Cookie Without Secure Flag
 - > Cookie with SameSite Attribute None (2)
 - > Cookie without SameSite Attribute (5)
 - > Cross-Domain JavaScript Source File Inclusion
 - > Timestamp Disclosure - Unix (569)
 - > X-Content-Type-Options Header Missing (42)
 - > CORS Header
 - > Information Disclosure - Sensitive Information in URL (2)
 - > Information Disclosure - Suspicious Comments (43)
 - > Loosely Scoped Cookie (5)
 - > Re-examine Cache-control Directives (33)

Which of the following tuning recommendations should the security analyst share?

- A. Set an HttpOnly flag to force communication by HTTPS
- B. Block requests without an X-Frame-Options header
- C. Configure an Access-Control-Allow-Origin header to authorized domains
- D. Disable the cross-origin resource sharing header

Answer: B

Explanation:
The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

QUESTION 4

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook

- D. Affected hosts
- E. Risk score
- F. Education plan

Answer: D, E

Explanation:

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official Reference: <https://www.first.org/cvss/>

QUESTION 5

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

- A. A mean time to remediate of 30 days
- B. A mean time to detect of 45 days
- C. A mean time to respond of 15 days
- D. Third-party application testing

Answer: A

Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

QUESTION 6

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
(
  Get-ADUser $user -Properties primaryGroupID |select-object pr:
  Add-ADGroupMember "Domain Users" -Members $user
  Set-ADUser $user -Replace @{primaryGroupID=513}
)
```

certexam.org

Which of the following scripting languages was used in the script?

- A. PowerShell
- B. Ruby
- C. Python
- D. Shell script

Answer: A

Explanation:

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

QUESTION 7

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

- A. There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access
- B. An on-path attack is being performed by someone with internal access that forces users into port 80
- C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
- D. An error was caused by BGP due to new rules applied over the company's internal routers

Answer: B

Explanation:

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

QUESTION 8

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.certexam.org
3. The Company shall prioritize patching of publicly available systems and services over patching of

internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A)

Name: THOR.HAMMER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Internal System

B)

Name: CAP.SHIELD

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External System

C)

Name: LOKI.DAGGER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External System

D)

Name: THANOS.GAUNTLET

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Internal System

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official Reference: <https://www.first.org/cvss/>

QUESTION 9

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- A. Business continuity plan
- B. Vulnerability management plan
- C. Disaster recovery plan
- D. Asset management plan

Answer: C

Explanation:

QUESTION 10

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

- A. Deploy a CASB and enable policy enforcement
- B. Configure MFA with strict access
- C. Deploy an API gateway
- D. Enable SSO to the cloud applications

Answer: A

Explanation:

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

QUESTION 11

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

- A. CDN
- B. Vulnerability scanner
- C. DNS
- D. Web server

Answer: C

Explanation:

A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a