Vendor: CompTIA

Exam Code: CS0-003

Exam Name: CompTIA Cybersecurity Analyst (CySA+) Exam

Version: DEMO

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/I: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:
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).

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:
PAM (privileged access management) is a security framework that helps organizations manage and control access to privileged accounts and systems.
IDS (intrusion detection system) is a security technology that monitors network traffic for malicious activity.
PKI (public key infrastructure) is a set of technologies that enable secure communication over public networks.
DLP (data loss prevention) is a security technology that helps organizations prevent the unauthorized disclosure of sensitive data.
Of the above options, only DLP is specifically designed to prevent the exposure of PII outside of an organization. PAM, IDS, and PKI can all be used to help protect PII, but they are not specifically designed for this purpose.

QUESTION 3
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: DE
Explanation:
Affected hosts: The vulnerability scan report should clearly list the hosts or systems that are

affected by the identified vulnerabilities. This information is crucial for understanding the scope of the vulnerabilities and taking appropriate remediation actions.
Risk score: Vulnerability scans often assign risk scores or severity ratings to each identified vulnerability. These scores help prioritize remediation efforts by indicating the potential impact and exploitability of the vulnerabilities. Including risk scores in the report provides an understanding of the relative severity of the identified vulnerabilities.

QUESTION 4
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: C
Explanation:
By having a mean time to respond of 15 days, the organization can act swiftly when a potential attack is detected or a patch is released.

QUESTION 5
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 primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

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

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

Answer: A
Explanation:
The syntax in the given script, such as cmdlet names starting with "Get-", "Add-", "Set-", and the use of the pipeline "|", is characteristic of PowerShell scripting. Moreover, the use of Active Directory cmdlets like "Get-ADUser," "Add-ADGroupMember," and "Set-ADUser" indicates that this script is designed to interact with Active Directory, which aligns with PowerShell's primary use case in managing Windows environments and Active Directory services.

QUESTION 6
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:
The fact that the company's internal portal is sometimes accessible through HTTP (port 80) and other times through HTTPS (port 443) suggests that someone with internal access is actively manipulating the network traffic. An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies communication between two parties. By forcing users into using HTTP instead of HTTPS, the attacker can potentially capture sensitive information transmitted over the network, such as login credentials or session data.
An issue with the SSL certificate (Option A) would generally result in HTTPS not working at all, rather than it being intermittently accessible.
A web server unable to handle an increasing amount of HTTPS requests (Option C) would likely result in performance issues or server errors, but it wouldn't selectively redirect users to HTTP.
BGP (Border Gateway Protocol) is used for routing between autonomous systems on the internet, and it generally would not cause the internal portal to switch between HTTP and HTTPS. It is more relevant to external internet routing.

QUESTION 7
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.
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

Answer: B
Explanation:
Based on the security policy and the CVSSv3.1 Base Scores, vulnerability B (CAP.SHIELD) with a high impact on confidentiality should be the highest priority to patch. It is an externally accessible system, and since confidentiality takes precedence over availability, it should be addressed before other vulnerabilities.

QUESTION 8
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:
A disaster recovery plan (DRP) is a document that outlines the steps that an organization will take to recover from a disaster. This includes identifying the organization's critical systems and data, developing a plan to restore those systems and data, and testing the plan regularly.

QUESTION 9
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 security solution that helps organizations manage and secure their cloud applications. CASBs can be used to enforce security policies, monitor cloud usage, and detect and block malicious activity.
In this case, the Chief Information Security Officer (CISO) wants to reduce the risk of shadow IT by enforcing security policies on the high-risk cloud applications. A CASB can be used to do this by providing visibility into cloud usage, identifying unauthorized applications, and enforcing security policies.

QUESTION 10
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 DDoS attack is a type of attack that floods a target with more traffic than it can handle. This can cause the target to become unavailable to legitimate users.
The DNS logs will show the IP addresses of the devices that were sending the traffic to the target. This information can be used to identify the attackers.
The other logs may also be helpful in investigating a DDoS attack, but they are less likely to provide the same level of detail as the DNS logs.

QUESTION 11
A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Answer: D
Explanation:
The Cyber Kill Chain is a framework for understanding and responding to cyberattacks. It describes seven stages that an attacker must complete in order to successfully compromise a system.
In this case, the malicious actor has already gained access to the internal network through social engineering. This means that the actor has completed the Reconnaissance and Delivery stages of the Cyber Kill Chain. The actor is now in the Exploitation stage, where they are attempting to gain control of the system.

QUESTION 12
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

A. Exploitation
B. Reconnaissance
C. Command and control
D. Actions on objectives

Answer: B
Explanation:
Reconnaissance is the first step in most attack frameworks. It is the process of gathering information about a target in order to plan an attack. This information can include things like the target's network topology, IP addresses, and open ports.
In this case, the analyst has found that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This is a clear sign that the IP address is being used for reconnaissance.

QUESTION 13

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconing
B. Domain Name System hijacking
C. Social engineering attack
D. On-path attack
E. Obfuscated links
F. Address Resolution Protocol poisoning

Answer: CE
Explanation:
Social engineering attack: This is a type of attack that relies on tricking the victim into clicking on a malicious link or opening an attachment. In this case, the concealed URL in the email is likely a malicious link that will lead the victim to a website that is controlled by the attacker. Once the victim clicks on the link, the attacker can then install malware on the victim's computer or steal their personal information.
Obfuscated links: This is a technique used to hide the true destination of a link. This can be done by using a variety of methods, such as using shortened URLs or encoding the URL in a way that makes it difficult to read. In this case, the concealed URL in the email is likely obfuscated, which makes it more difficult for the victim to identify as malicious.

QUESTION 14
An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems
B. Legacy systems
C. Unsupported operating systems
D. Lack of maintenance windows

Answer: A
Explanation:
Proprietary systems are systems that are owned by their developer or vendor, and the company does not have access to the source code or other necessary information to upgrade or patch the system. This can make it difficult to remediate vulnerabilities in proprietary systems, as the company may need to rely on the vendor to provide a patch or update.
In this case, the two critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This suggests that the systems are proprietary, and the company is unable to remediate the vulnerabilities without the vendor's assistance.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**