CompTIA CySA+ (CS0-003)

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(s): A

---

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

A. PAM

B. IDS

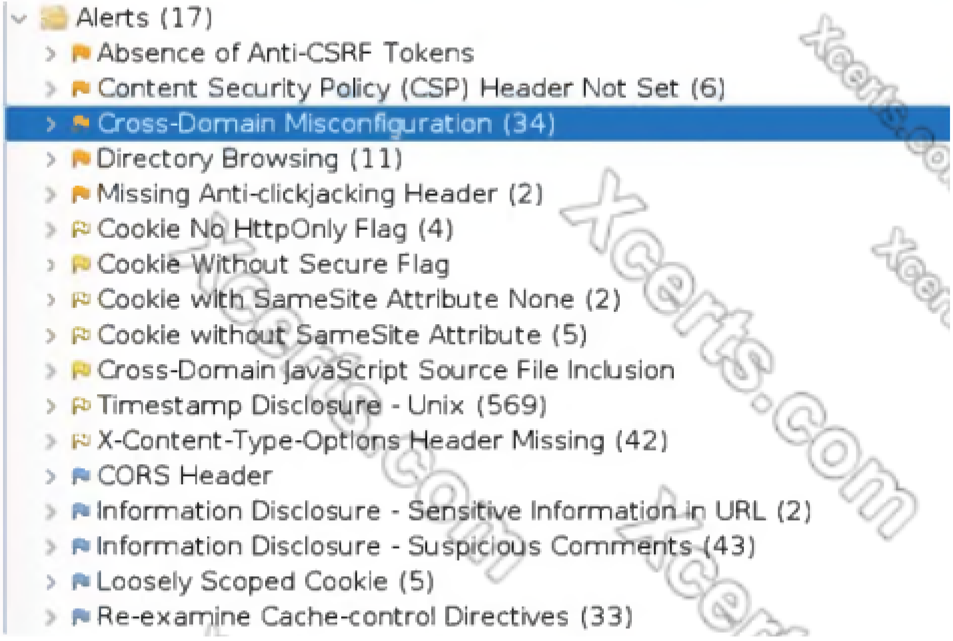
C. PKI

D. DLP

Answer(s): D

---

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(s): C

---

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(s): D E

---

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

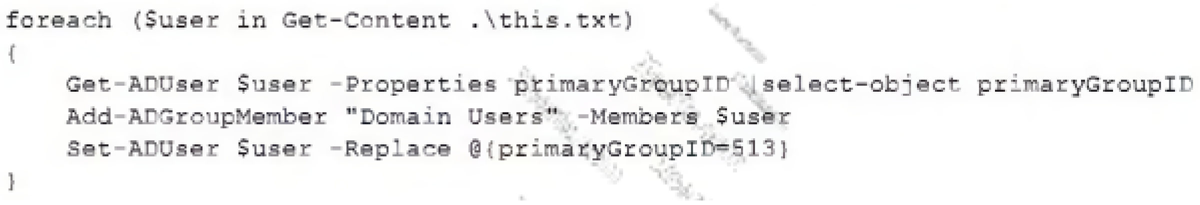
C. A mean time to respond of 15 days

D. Third-party application testing

Answer(s): C

---

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 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(s): A

---

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(s): B

---

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.
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.HAMMERCVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:HInternal System

B. Name: CAP.SHIELDCVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:NExternal System

C. Name: LOKI.DAGGERCVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:HExternal System

D. Name: THANOS.GAUNTLETCVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:NInternal System

Answer(s): B

---

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(s): A

---

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(s): A

---

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(s): C

---

12. 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(s): D

---

13. 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(s): B

---

14. 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(s): C E

---

15. During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production

B. Ensure that all implemented coding libraries are regularly checked

C. Use application security scanning as part of the pipeline for the CI/CD flow

D. Implement proper input validation for any data entry form

Answer(s): C

---

16. 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

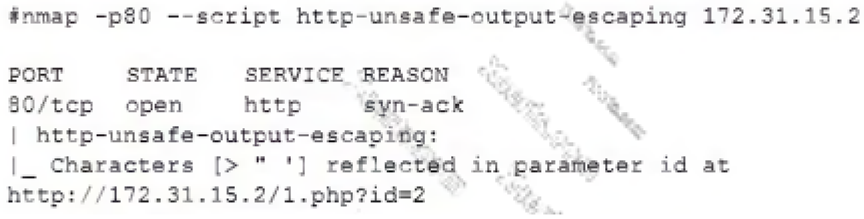
C. Unsupported operating systems

D. Lack of maintenance windows

Answer(s): A

---

17. The security team reviews a web server for XSS and runs the following Nmap scan:



```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE REASON
80/tcp   open     http     syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and " as the parameters used m the attempt

B. The vulnerable parameter ID http://172.31.15.2/1.php?id-2 and unfiltered characters returned

C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe

D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer(s): D

---

18. Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users

B. Schedule a review with all teams to discuss what occurred

C. Create an executive summary to update company leadership

D. Review regulatory compliance with public relations for official notification

Answer(s): B

---

19. A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A. Code analysis

B. Static analysis

C. Reverse engineering

D. Fuzzing

Answer(s): C

---

20. An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk

B. Primary boot partition

C. Malicious files

D. Routing table

E. Static IP address

Answer(s): D