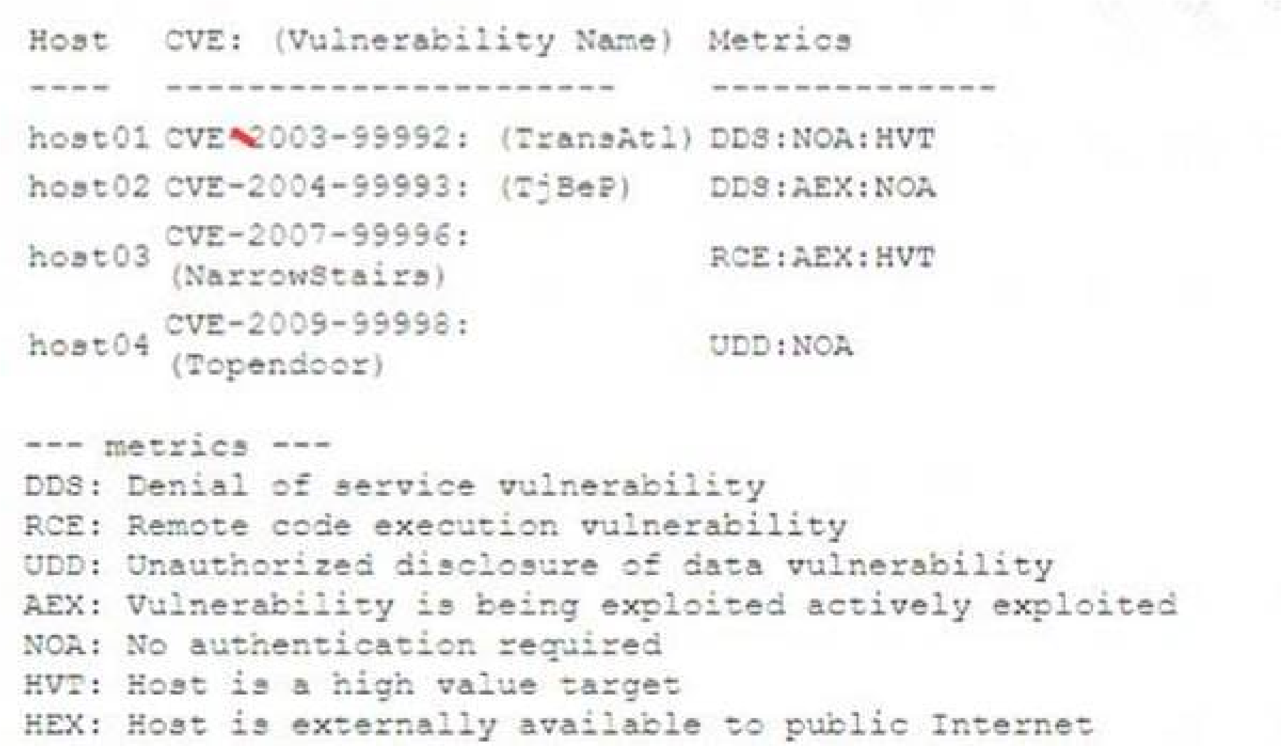
CS0-003$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

QUESTION 1

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:



```
Host   CVE: (Vulnerability Name)   Metrics
----   ---------------------       -------------
host01 CVE-2003-99992: (TransAtl)  DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)     DDS:AEX:NOA
host03 CVE-2007-99996:             RCE:AEX:HVT
        (NarrowStairs)
host04 CVE-2009-99998:             UDD:NOA
        (Topendoor)

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01

B. host02

C. host03

D. host04

Correct Answer: C

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

QUESTION 2

A development team is discussing the implementation of parameterized queries to address several software vulnerabilities. Which of the following is the most likely type of vulnerability the team is trying to remediate?

A. SQL injection

B. CSRF

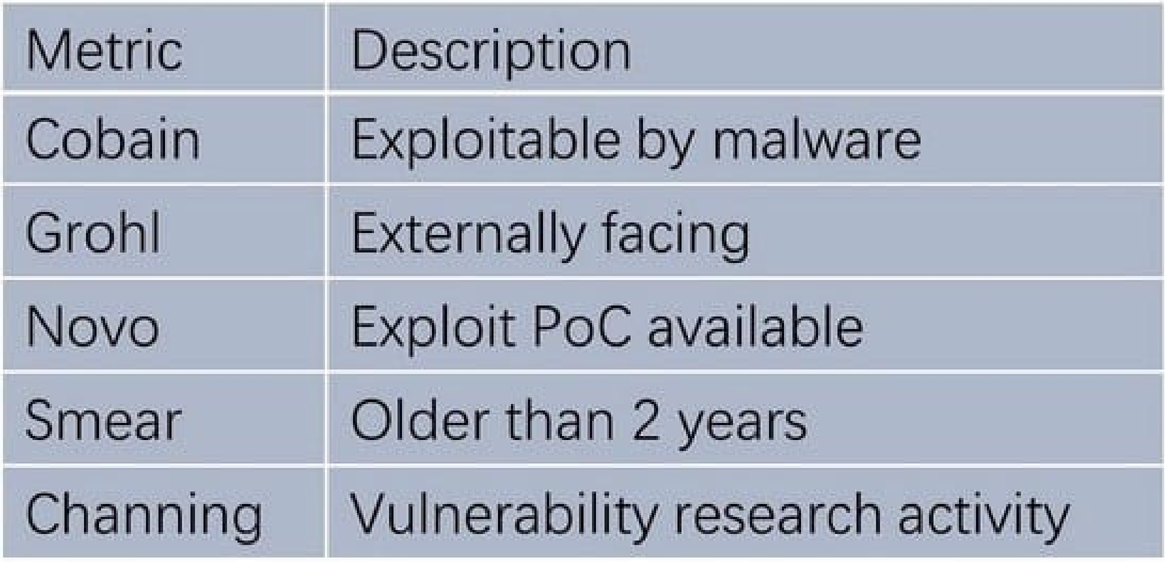
C. On-path attack

D. XSS

Correct Answer: A

QUESTION 3

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:



Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No

B. TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

C. ENameless: Cobain: Yes Grohl: No

Novo: Yes

Smear: No

Channing: No

D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Correct Answer: B

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear

and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION 4

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

A. Non-credentialed scanning

B. Passive scanning

C. Agent-based scanning

D. Credentialed scanning

Correct Answer: B

Passive scanning involves monitoring network traffic to identify vulnerabilities without actively probing or interacting with the devices. This method is relatively non-intrusive and can provide valuable information without directly affecting the

systems.

However, it\\'s important to note that passive scanning might not identify all vulnerabilities, so a combination of passive scanning and periodic credentialed scanning might be a balanced approach to ensure accurate vulnerability assessment

while minimizing disruption.

QUESTION 5

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff

B. Ensuring that malicious websites cannot be visited

C. Blocking all scripts downloaded from the internet

D. Disabling all staff members’ ability to run downloaded applications

Correct Answer: A