TestpassportQ&A

Higher Quality Better Service!

We offer free update service for one year

Http://www.testpassport.com

Exam : **CAS-004**

Title : CompTIA Advanced Security Practitioner (CASP+) Exam

Version : DEMO

1.A company suspects a web server may have been infiltrated by a rival corporation.
The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heinz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

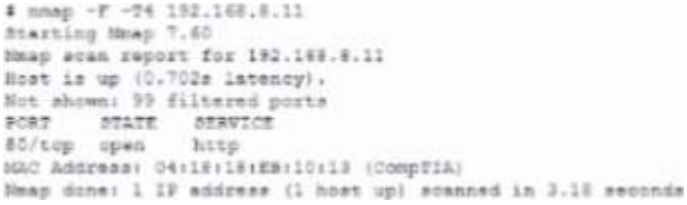
```
system ("ls -l -a #{path}")
```

Which of the following is an appropriate security control the company should implement?
A. Restrict directory permission to read-only access.
B. Use server-side processing to avoid XSS vulnerabilities in path input.
C. Separate the items in the system call to prevent command injection.
D. Parameterize a query in the path variable to prevent SQL injection.
Answer: C

2.An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)
A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL
Answer: B,F
Explanation:
Reference:
https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)

3.Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure.
Which of the must occur to ensure the integrity of the image?
A. The image must be password protected against changes.
B. A hash value of the image must be computed.
C. The disk containing the image must be placed in a seated container.
D. A duplicate copy of the image must be maintained
Answer: B

4.A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:



A. A SCAP assessment.
B. Reverse engineering
C. Fuzzing
D. Network interception.
Answer: A

5.A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?
A. 0.5
B. 8
C. 50
D. 36,500
Answer: A
Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/