Latest Version: 36.0

Question: 1

An attacker exploited an unpatched vulnerability in a web framework, and then used an application service account that had an insecure configuration to download a rootkit The attacker was unable to obtain root privileges Instead the attacker then downloaded a crypto-currency mining program and subsequently was discovered The server was taken offline, rebuilt, and patched. Which of the following should the security engineer suggest to help prevent a similar scenario in the future?

A. Remove root privileges from the application service account
B. Implement separation of duties.
C. Properly configure SELinux and set it to enforce.
D. Use cron to schedule regular restarts of the service to terminate sessions.
E. Perform regular uncredentialed vulnerability scans

Answer: E

Question: 2

An engineer wants to assess the OS security configurations on a company's servers. The engineer has downloaded some files to orchestrate configuration checks When the engineer opens a file in a text editor, the following excerpt appears:

```
<?xml version="1.0" encoding="UTF-8"?>
<cdf:Benchmark id="server-check" resolved="0" xml:lang="en">
        ...
        xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1" xccdf-1.1.xsd
        ...
</cdf:Benchmark>
```

Which of the following capabilities would a configuration compliance checker need to support to interpret this file?

A. Nessus
B. Swagger file
C. SCAP
D. Netcat
E. WSDL

Answer: C

Question: 3

A Chief Information Security Officer (CISO) has created a survey that will be distributed to managers of mission-critical functions across the organization The survey requires the managers to determine how long their respective units can operate in the event of an extended IT outage before the organization suffers monetary losses from the outage To which of the following is the survey question related? (Select TWO)

A. Risk avoidance
B. Business impact
C. Risk assessment
D. Recovery point objective
E. Recovery time objective
E. Mean time between failures

Answer: B, D

Question: 4

Following a recent security incident on a web server the security analyst takes HTTP traffic captures for further investigation The analyst suspects certain jpg files have important data hidden within them. Which of the following tools will help get all the pictures from within the HTTP traffic captured to a specified folder?

A. tshark
B. memdump
C. nbtstat
D. dd

Answer: A

Question: 5

A large, multinational company currently has two separate databases One is used for ERP while the second is used for CRM To consolidate services and infrastructure, it is proposed to combine the databases The company's compliance manager is asked to review the proposal and is concerned about this integration Which of the following would pose the MOST concern to the compliance manager?

A. The attack surface of the combined database is lower than the previous separate systems, so there likely are wasted resources on additional security controls that will not be needed
B. There are specific regulatory requirements the company might be violating by combining these two types of services into one shared platform.
C. By consolidating services in this manner, there is an increased risk posed to the organization due to the number of resources required to manage the larger data pool.
D. Auditing the combined database structure will require more short-term resources, as the new system will need to be learned by the auditing team to ensure all security controls are in

Answer: B