```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal
B. SQL injection
C. API
D. Request forgery

Correct Answer: D

QUESTION 402
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images
B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
C. Define a vulnerability scan to assess container images before being introduced on the environment
D. Create a dedicated VPC for the containerized environment

Correct Answer: A

QUESTION 403
A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to Implement a high availability pair to:

A. decrease the mean ne between failures
B. remove the single point of failure
C. cut down the mean tine to repair
D. reduce the recovery time objective

Correct Answer: B

QUESTION 404
A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack type?

A. Request forgery
B. Session replay
C. DLL injection
D. Shimming

Correct Answer: A

QUESTION 405
An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops
B. Containers
C. Thin clients
D. Workstations

Correct Answer: C

QUESTION 406
A routine audit of medical billing claims revealed that several claims were submitted without the subscriber's knowledge. A review of the audit logs for the medical billing company's system indicated a company employee downloaded customer records and adjusted the direct deposit information to a personal bank account. Which of the following does this action describe?

A. Insider threat
B. Social engineering
C. Third-party risk
D. Data breach

Correct Answer: D

QUESTION 407
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps
B. A Telnet session
C. An SSH connection
D. SFTP traffic

Correct Answer: A

QUESTION 408
An amusement park is implementing a biometric system that validates customers' fingerprints to ensure they are not sharing tickets The park's owner values customers above all and would prefer customers' convenience over security. For this reason, which of the following features should the security team prioritize FIRST?

A. LOW FAR
B. Low efficacy
C. Low FRR
D. Low CER

Correct Answer: B

QUESTION 409
A forensics investigator is examining a number of unauthorized payments that were reported on the 00mpany's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

```
<a href="https://www.company.com/payto.do?routing=00001111&acct=22223334&amount=250">Click here to unsubscribe</a>
```

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. Broken authentication
C. XSS
D. XSRF

Correct Answer: D

QUESTION 410
Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

A. Implement proper network access restrictions
B. Initiate a bug bounty program
C. Classify the system as shadow IT.
D. Increase the frequency of vulnerability scans

Correct Answer: A

QUESTION 411
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.
C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.

Correct Answer: D
Explanation:
https://subscription.packtpub.com/book/networking_and_servers/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans

A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non-credentialed scan on the network and finds that there are three missing patches. The scan does not provide many details on these missing patches. The administrator installs the missing patches to keep the systems up to date as they can only operate on the information produced for them.

QUESTION 412
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR
B. PCI DSS
C. ISO 27000
D. NIST 800-53

Correct Answer: D
Explanation:
NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.

QUESTION 413
A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical servers must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA. Which of the following will the engineer MOST likely use to achieve this objective?

A. A forward proxy
B. A stateful firewall
C. A jump server
D. A port tap

Correct Answer: B

QUESTION 414
Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

Correct Answer: B

QUESTION 415
Which of the following control types would be BEST to use to identify violations and incidents?

A. Detective
B. Compensating
C. Deterrent
D. Corrective
E. Recovery
F. Preventive

Correct Answer: A

QUESTION 416

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices. Which of the following is a cost-effective approach to address these concerns?

A. Enhance resiliency by adding a hardware RAID.
B. Move data to a tape library and store the tapes off-site
C. Install a local network-attached storage.
D. Migrate to a cloud backup solution

Correct Answer: D

QUESTION 417
An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?

A. Antivirus
B. IPS
C. FTP
D. FIM

Correct Answer: D
Explanation:
Data tampering prevention can include simple security measures such as the encryption of data, and can include lengths such as using file integrity monitoring (FIM) systems for better security.

https://www.cypressdatadefense.com/blog/data-tampering-prevention/
https://www.cypressdatadefense.com/blog/data-tampering-prevention/

QUESTION 418
A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?

A. Update the base container image and redeploy the environment.
B. Include the containers in the regular patching schedule for servers
C. Patch each running container individually and test the application
D. Update the host in which the containers are running

Correct Answer: C
Explanation:
A container image vulnerability is a security risk that is embedded inside a container image . While vulnerable images themselves don't pose an active threat, if containers are created based on a vulnerable image, the containers will introduce the vulnerability to a live environment.

QUESTION 419
A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?

A. SIEM correlation dashboards
B. Firewall syslog event logs
C. Network management solution login audit logs
D. Bandwidth monitors and interface sensors