QUESTION 646
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 647
A video-game developer has received reports of players who are cheating.
All game players each have five capabilities that are ranked on a scale of 1 to 10 points, with 10 total points available for balance.
Players can move these points between capabilities at any time.
The programming logic is as follows:
- A player asks to move points from one capability to another
- The source capability must have enough points to allow the move
- The destination capability must not exceed 10 after the move
- The move from source capability to destination capability is then completed
The time stamps of the game logs show each step of the transfer process takes about 900ms.
However, the time stamps of the cheating players show capability transfers at the exact same time.
The cheating players have 10 points in multiple capabilities.
Which of the following is MOST likely being exploited to allow these capability transfers?

A. TOC/TOU
B. CSRF
C. Memory leak
D. XSS
E. SQL injection
F. Integer overflow

Answer: F

QUESTION 648

The Chief Executive Officer (CEO) of a fast-growing company no longer knows all the employees and is concerned about the company's intellectual property being stolen by an employee.
Employees are allowed to work remotely with flexible hours, creating unpredictable schedules. Roles are poorly defined due to frequent shifting needs across the company.
Which of the following new initiatives by the information security team would BEST secure the company and mitigate the CEO's concerns?

A. Begin simulated phishing campaigns for employees and follow up with additional security awareness training.
B. Seed company fileshares and servers with text documents containing fake passwords and then monitor for their use.
C. Implement DLP to monitor data transfer between employee accounts and external parties and services
D. Report data from a user-behavior monitoring tool and assign security analysts to review it daily

Answer: C

QUESTION 649
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:
- Involve business owners and stakeholders
- Create an applicable scenario
- Conduct a biannual verbal review of the incident response plan
- Report on the lessons learned and gaps identified
Which of the following exercises has the CEO requested?

A. Parallel operations
B. Full transition
C. Internal review
D. Tabletop
E. Partial simulation

Answer: C

QUESTION 650
Several days after deploying an MDM for smartphone control, an organization began noticing anomalous behavior across the enterprise Security analysts observed the following:
- Unauthorized certificate issuance
- Access to mutually authenticated resources utilizing valid but unauthorized certificates
- Granted access to internal resources via the SSL VPN
To address the immediate problem security analysts revoked the erroneous certificates.
Which of the following describes the MOST likely root cause of the problem and offers a solution?

A. The VPN and web resources are configured with too weak a cipher suite and should be rekeyed to support AES 256 in GCM and ECC for digital signatures and key exchange
B. A managed mobile device is rooted exposing its keystore and the MDM should be reconfigured to wipe these devices and disallow access to corporate resources
C. SCEP is configured insecurely which should be enabled for device onboarding against a PKI for mobile-exclusive use
D. The CA is configured to sign any received CSR from mobile users and should be reconfigured to permit CSR signings only from domain administrators.

Answer: B

QUESTION 651
A security administrator is opening connectivity on a firewall between Organization A and Organization B Organization

B just acquired Organization A.
Which of the following risk mitigation strategies should the administrator implement to reduce the risk involved with this change?

A. DLP on internal network nodes
B. A network traffic analyzer for incoming traffic
C. A proxy server to examine outgoing web traffic
D. IPS/IDS monitoring on the new connection

Answer: D

QUESTION 652
An organization is facing budget constraints The Chief Technology Officer (CTO) wants to add a new marketing platform but the organization does not have the resources to obtain separate servers to run the new platform.
The CTO recommends running the new marketing platform on a virtualized video-conferencing server because video conferencing is rarely used.
The Chief Information Security Officer (CISO) denies this request.
Which of the following BEST explains the reason why the CISO has not approved the request?

A. Privilege escalation attacks
B. Performance and availability
C. Weak DAR encryption
D. Disparate security requirements

Answer: D

QUESTION 653
A cloud architect needs to isolate the most sensitive portion of the network while maintaining hosting in a public cloud.
Which of the following configurations can be employed to support this effort?

A. Create a single-tenancy security group in the public cloud that hosts only similar types of servers
B. Privatize the cloud by implementing an on-premises instance.
C. Create a hybrid cloud with an on-premises instance for the most sensitive server types.
D. Sandbox the servers with the public cloud by server type

Answer: C

QUESTION 654
A financial services company has proprietary trading algorithms, which were created and are maintained by a team of developers on their private source code repository.
If the details of this operation became known to competitors, the company's ability to profit from its trading would disappear immediately.
Which of the following would the company MOST likely use to protect its trading algorithms?

A. Single-tenancy cloud
B. Managed security service providers
C. Virtual desktop infrastructure
D. Cloud security broker

Answer: A

QUESTION 655
A security administrator is performing an audit of a local network used by company guests and executes a series of commands that generates the following output:

```
On Host A
Internet address  Physical address  Type
10.100.0.1        00:0a:91:45:0a:1b Dynamic

On Host B
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00

On Host A
Internet address  Physical address  Type
10.100.0.1        08:0a:di:fa:b1:00 Dynamic
```

Which of the following actions should the security administrator take to BEST mitigate the issue that transpires from the above information?

A. Implement switchport security
B. Implement 802 1X
C. Enforce static ARP mappings using GPO
D. Enable unicast RPF

Answer: A

QUESTION 656
An attacker wants to gain information about a company's database structure by probing the database listener. The attacker tries to manipulate the company's database to see if it has any vulnerabilities that can be exploited to help carry out an attack.
To prevent this type of attack, which of the following should the company do to secure its database?

A. Mask the database banner
B. Tighten database authentication and limit table access
C. Harden web and Internet resources
D. Implement challenge-based authentication

Answer: B

QUESTION 657
An organization based in the United States is planning to expand its operations into the European market later in the year Legal counsel is exploring the additional requirements that must be established as a result of the expansion. The BEST course of action would be to

A. revise the employee provisioning and deprovisioning procedures
B. complete a quantitative risk assessment
C. draft a memorandum of understanding
D. complete a security questionnaire focused on data privacy.

Answer: D

QUESTION 658
A company is deploying a DIP solution and scanning workstations and network drives for documents that contain potential Pll and payment card data. The results of the first scan are as follows:

Fileshare	PII findings	Payment card findings	Access permissions
Human resources	125,098	0	Administrator; DLP-Scan; HR_admins; HR-Staff; Help Desk
Marketing	13,987	56	Administrator; DLP-Scan; Mrkt-Staff; Mrkt-Admin; Everyone
Payroll	456,765	1,236	Administrator; DLP-Scan; Payroll-Staff; Comptroller; Payroll-Admin; Internal-Audit
Accounts payable	13,873	978	Administrator; DLP-Scan; Comptroller; AP-Staff; AP-admin; Internal-Audit
Desktop support	0	0	Administrator; DLP-Scan; Help-Desk; Everyone

The security learn is unable to identify the data owners for the specific files in a timely manner and does not suspect malicious activity with any of the detected files.
Which of the following would address the inherent risk until the data owners can be formally identified?

A. Move the files from the marketing share to a secured drive.
B. Search the metadata for each file to locate the file's creator and transfer the files to the personal drive of the listed creator.
C. Configure the DLP tool to delete the files on the shared drives
D. Remove the access for the internal audit group from the accounts payable and payroll shares

Answer: A

QUESTION 659
A security engineer wants to introduce key stretching techniques to the account database to make password guessing attacks more difficult.
Which of the following should be considered to achieve this? (Select TWO)

A. Digital signature
B. bcrypt
C. Perfect forward secrecy
D. SHA-256
E. P-384
F. PBKDF2
G. Record-level encryption

Answer: BF

QUESTION 660
As part of an organization's ongoing vulnerability assessment program, the Chief Information Security Officer (CISO) wants to evaluate the organization's systems, personnel, and facilities for various threats.
As part of the assessment the CISO plans to engage an independent cybersecurity assessment firm to perform social engineering and physical penetration testing against the organization's corporate offices and remote locations.
Which of the following techniques would MOST likely be employed as part of this assessment? (Select THREE).

A. Privilege escalation
B. SQL injection
C. TOC/TOU exploitation
D. Rogue AP substitution
E. Tailgating
F. Vulnerability scanning
G. Vishing
H. Badge skimming

Answer: EGH