QUESTION 661
A security engineer discovers a PC may have been breached and accessed by an outside agent.
The engineer wants to find out how this breach occurred before remediating the damage.
Which of the following should the security engineer do FIRST to begin this investigation?

A. Create an image of the hard drive
B. Capture the incoming and outgoing network traffic
C. Dump the contents of the RAM
D. Parse the PC logs for information on the attacker.

Answer: A

QUESTION 662
A hospital is using a functional magnetic resonance imaging (fMRI) scanner, which is controlled legacy desktop connected to the network.
The manufacturer of the fMRI will not support patching of the legacy system.
The legacy desktop needs to be network accessible on TCP port 445.
A security administrator is concerned the legacy system will be vulnerable to exploits.
Which of the following would be the BEST strategy to reduce the risk of an outage while still providing for security?

A. Install HIDS and disable unused services.
B. Enable application whitelisting and disable SMB.
C. Segment the network and configure a controlled interface
D. Apply only critical security patches for known vulnerabilities.

Answer: C

QUESTION 663
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
F. Mean time between failures

Answer: BD

QUESTION 664
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 665
A company has completed the implementation of technical and management controls as required by its adopted security, ponies and standards.
The implementation took two years and consumed s the budget approved to security projects.
The board has denied any further requests for additional budget.
Which of the following should the company do to address the residual risk?

A. Transfer the risk
B. Baseline the risk.
C. Accept the risk
D. Remove the risk

Answer: C

QUESTION 666
An e-commerce company that provides payment gateways is concerned about the growing expense and time associated with PCI audits of its payment gateways and external audits by customers for their own compliance reasons.
The Chief Information Officer (CIO) asks the security team to provide a list of options that will:
1. Reduce the overall cost of these audits
2. Leverage existing infrastructure where possible
3. Keep infrastructure costs to a minimum
4. Provide some level of attestation of compliance
Which of the following will BEST address the CIO"s concerns? (Select TWO)

A. Invest in new UBA to detect report, and remediate attacks faster
B. Segment the network to reduce and limit the audit scope
C. Undertake ISO certification for all core infrastructure including datacenters.
D. Implement a GRC system to track and monitor controls
E. Implement DLP controls on HTTP'HTTPS and email
F. Install EDR agents on all corporate endpoints

Answer: CE

QUESTION 667
An employee decides to log into an authorized system.
The system does not prompt the employee for authentication prior to granting access to the console, and it cannot authenticate the network resources.
Which of the following attack types can this lead to if it is not mitigated?

A. Memory leak
B. Race condition
C. Smurf
D. Resource exhaustion

Answer: C

QUESTION 668
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 669
A company is implementing a new secure identity application, given the following requirements
- The cryptographic secrets used in the application must never be exposed to users or the OS
- The application must work on mobile devices.
- The application must work with the company's badge reader system
Which of the following mobile device specifications are required for this design? (Select TWO).

A. Secure element
B. Biometrics
C. UEFI
D. SEAndroid
E. NFC
F. HSM

Answer: BE

QUESTION 670
A small firm's newly created website has several design flaws.
The developer created the website to be fully compatible with ActiveX scripts in order to use various digital certificates and trusting certificate authorities.
However, vulnerability testing indicates sandboxes were enabled, which restricts the code's access to resources within the user's computer.
Which of the following is the MOST likely cause of the error"?

A. The developer inadvertently used Java applets.
B. The developer established a corporate account with a non-reputable certification authority.
C. The developer used fuzzy logic to determine how the web browser would respond once ports 80 and 443 were both open
D. The developer did not consider that mobile code would be transmitted across the network.

Answer: A

QUESTION 671
An organization is integrating an ICS and wants to ensure the system is cyber resilient.
Unfortunately, many of the specialized components are legacy systems that cannot be patched.
The existing enterprise consists of mission-critical systems that require 99.9% uptime.
To assist in the appropriate design of the system given the constraints, which of the following MUST be assumed?

A. Vulnerable components
B. Operational impact due to attack
C. Time criticality of systems
D. Presence of open-source software

Answer: A

QUESTION 672
A company wants to implement a cloud-based security solution that will sinkhole malicious DNS requests.
The security administrator has implemented technical controls to direct DNS requests to the cloud servers but wants to extend the solution to all managed and unmanaged endpoints that may have user-defined DNS manual settings.
Which of the following should the security administrator implement to ensure the solution will protect all connected devices?

A. Implement firewall ACLs as follows

```
PERMIT UDP ANY CLOUD_SERVER EQ 53
DENY UDP ANY ANY EQ 53
```

B. Implement NAT as follows:

ORIGINAL				TRANSLATED			
SRC IP	SRC PORT	DST IP	DST PORT	SRC IP	SRC PORT	DST IP	DST PORT
SAME	SAME	SAME	53	PAT POOL	SAME	CLOUD SERVER	53

C. Implement DHCP options as follows:

```
DHCP DNS1: CLOUD_SERVER1
DHCP DNS2: CLOUD_SERVER2
```

D. Implement policy routing as follows:

```
100 PERMIT UDP ANY ANY ANY 53
200 PERMIT UDP PAT_POOL ANY CLOUD_SERVER 53
IP ROUTE_MAP 200 200
```

Answer: D

QUESTION 673
The Chief Information Security Officer (CISO) of an organization is concerned with the transmission of cleartext authentication information across the enterprise.
A security assessment has been performed and has identified the use of ports 80. 389. and 3268.
Which of the following solutions would BEST address the CISO's concerns?

A. Disable the ports that are determined to contain authentication information
B. Force HTTPS. enable LDAPS. and disable cleartext global catalog communication.
C. Deploy a VPN between networks that transmits authentication information via cleartext
D. Proxy HTTP traffic and migrate to a more secure directory service

Answer:

QUESTION 674
A security analyst has been assigned incident response duties and must instigate the response on a Windows device that appears to be compromised.
Which of the following commands should be executed on the client FIRST?

A. `C:\>psexec.exe \\localhost -u Acct\IRSRVAcct -p IRResponse1! -c mdd_1.3.exe -oo F:\memory.dmp`
B. `C:\>dc3dd.exe if=\\.\c: of=d:\response\img1.dd hash=md5 log=F:\response\logs.log`
C. `C:\>fciv.exe -v -md5sum -xml hashlogs.xml`
D. `C:\>wmic.exe /ActPC01:\\root\default Path SystemRestore Call createRestorePoint "10Jan2018" AllowSr /t`

Answer: A

QUESTION 675
Which of the following risks does expanding business into a foreign country carry?

A. Data sovereignty laws could result in unexpected liability
B. Export controls might decrease software costs
C. Data ownership might revert to the regulatory entities in the new country
D. Some security tools might be monitored by legal authorities

Answer: A

QUESTION 676
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