QUESTION 727
The Chief Information Security Officer (CISO) of a new company is looking for a comprehensive assessment of the company's application services.
Which of the following would provide the MOST accurate number of weaknesses?

A. White-box penetration test
B. Internal vulnerability scanning
C. Internal controls audit
D. Third-party red-team engagement

Answer: A

QUESTION 728
An organization is creating requirements for new laptops that will be issued to staff One of the company's key security objectives is to ensure the laptops nave hardware-enforced data-at-rest protection tied to permanent hardware identities.
The laptops must also provide attestation for secure boot processes.
To meet these demands, which of the following BEST represent the features that should be included in the requirements set? (Select TWO.)

A. TPM2.0e
B. Opal support
C. MicroSD token authenticator
D. TLS1.3
E. Shim and GRUB
F. ARMv7 with TrustZone

Answer: AE

QUESTION 729
Within change management, which of the following ensures functions are earned out by multiple employees?

A. Least privilege
B. Mandatory vacation
C. Separator of duties
D. Job rotation

Answer: A

QUESTION 730

An administrator wants to ensure hard drives cannot be removed from hosts and men installed into and read by unauthorized hosts.
Which of the following techniques would BEST support this?

A. Access control lists
B. TACACS+ server for AAA
C. File-level encryption
D. TPM with sealed storage

Answer: A

QUESTION 731
A security administrator is confirming specific ports and IP addresses that are monitored by the IPS- IDS system as well as the firewall placement on the perimeter network between the company and a new business partner.
Which of the following business documents defines the parameters the security administrator must confirm?

A. BIA
B. ISA
C. NDA
D. MOU

Answer: A

QUESTION 732
A security analyst is attempting to identify code that is vulnerable to butler and integer overflow attacks.
Which of the following code snippets is safe from these types of attacks?

A.
```
int buff[100];
memcpy(buff, argv[1]);
```

B.
```
int buff[10];
char *ptr = (char *) malloc(10);
```

C.
```
char buff[200];
strcpy(buffer, argv[1]);
```

D.
```
char buff[500];
printf("Buffer = %s\n, buffer)
```

Answer: A

QUESTION 733
A security analyst is comparing two virtual servers that were bum from the same image and patched at the same regular intervals.
Server A is used to host a public-facing website, and Server B runs accounting software inside the firewalled accounting network.
The analyst runs the same command and obtains the following output from Server A and Server B. respectively:

Server A
```
certutil -hashfile c:\windows\system32\notepad.exe MD5
MD5 hash of c:\windows\system32\notepad.exe:
631f2ecc66a1d36feb0ab09087b290ca
CertUtil: -hashfile command completed successfully.
```

Server B
```
certutil -hashfile c:\windows\system32\notepad.exe MD5
MD5 hash of c:\windows\system32\notepad.exe:
ee7d823ccd657e3b19e35de8a66e2ef3
CertUtil: -hashfile command completed successfully.
```

Which of the following will the analyst most likely use NEXT?

A. Exploitation tools
B. Hash cracking tools
C. Malware analysis tools
D. Log analysis tools

Answer: A

QUESTION 734
A developer needs to provide feedback on a peer's work during the SDLC.
While reviewing the code changes, the developers session ID tokens for a web application will be transmitted over an unsecure connection.
Which of the following code snippets should the developer recommend implement to correct the vulnerability?

A.
```
Cookie cookie = new Cookie("primary");
cookie.secure(true);
```

B.
```
String input = request.getParameter ("input");
String character Pattern = "[./a-zA-Z0-9?"=%]";
If (! input. matches (character Pattern))
{
out.println ("Invalid Input");
}
```

C.
```
<webapp>
<session-config>
<session-timeout>15</session-timeout>
</session-config>
</webapp>
```

D.
```
<input type="text" maxlength="30" name="ecpSessionPW" size="40" readonly="true"
value='<%=ESAPI.encoder().encodeForHTML(request.getParameter("SessionPW"))%>'/>
```

Answer: A

QUESTION 735
A system administrator recently conducted a vulnerability scan of the internet. Subsequently, the organization was successfully attacked by an adversary.
Which of the following in the MOST likely explanation for why the organization network was compromised?

A. There was a false positive since the network was fully patched.
B. The system administrator did not perform a full system sun.
C. The systems administrator performed a credentialed scan.
D. The vulnerability database was not updated.

Answer: B

QUESTION 736
A company recently deployed an agent-based DLP solution to all laptop in the environment.
The DLP solution is configured to restrict the following:
- USB ports
- FTP connections
- Access to cloud-based storage sites
- Outgoing email attachments
- Saving data on the local C: drive

Despite these restrictions, highly confidential data was from a secure fileshare in the research department. Which of the following should the security team implement FIRST?

A. Application whitelisting for all company-owned devices

B. A secure VDI environment for research department employees
C. NIDS/NIPS on the network segment used by the research department
D. Bluetooth restriction on all laptops

Answer: A

QUESTION 737
A security is testing a server finds the following in the output of a vulnerability scan:

```
PORT STATE SERVICE
139/tcp open netbios-ssn
Host script results:
| samba-vuln-cve-2012-1264:
| SAMBA remote heap overflow
| State: VULNERABLE
| Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
| Description:
| Samba versions 4.1.3 and all versions previous to this are affected by
| a vulnerability that allows remote code execution as the "root" user
| from an anonymous connection.
|
|_ Disclosure date: 2012-03-15
```

Which of the following will the security analyst most likely use NEXT to explore this further?

A. Exploitation framework
B. Reverse engineering tools
C. Vulnerability scanner
D. Visualization tool

Answer: A

QUESTION 738
Which of the following is the MOST likely reason an organization would decide to use a BYOD policy?

A. It enables employees to use the devices they are already own, thus reducing costs.
B. It should reduce the number of help desk and tickets significantly.
C. It is most secure, as the company owns and completely controls the devices.
D. It is the least complex method for systems administrator to maintain over time

Answer: A

QUESTION 739
A network service on a production system keeps crashing at random times. The systems administrator suspects a bug in the listener is causing the service to crash, resuming in the a DoS. Which the service crashes, a core dump is left in the /tmp directory.
Which of the following tools can the systems administrator use to reproduction hese symptoms?

A. Fuzzer
B. Vulnerability scanner
C. Core dump analyzer
D. Debugger

Answer: A

QUESTION 740
A company runs a well -attended, on-premises fitness club for its employees, about 200 of them each day.
Employees want to sync center's login and attendance program with their smartphones.
Human resources, which manages the contract for the fitness center, has asked the security architecture to help draft security and privacy requirements.

Which of the following would BEST address these privacy concerns?

A. Use biometric authentication.
B. Utilize geolocation/geofencing.
C. Block unauthorized domain bridging.
D. Implement containerization

Answer: A

QUESTION 741
Which of the following is MOST likely to be included in a security services SLA with a third-party vendor?

A. The standard of quality for anti-malware engines
B. Parameters for applying critical patches
C. The validity of program productions
D. Minimum bit strength for encryption-in-transit.

Answer: A

QUESTION 742
While traveling to another state, the Chief Financial (CFO) forgot to submit payroll for the company.
The CFO quickly gained to the corporate through the high-speed wireless network provided by the hotel and completed the desk.
Upon returning from the business trip, the CFO was told no one received their weekly pay due to a malware on attack on the system.
Which of the following is the MOST likely of the security breach?

A. The security manager did not enforce automate VPN connection.
B. The company's server did not have endpoint security enabled.
C. The hotel and did require a wireless password to authenticate.
D. The laptop did not have the host-based firewall properly configured.

Answer: A

QUESTION 743
A security manager wants to implement a policy that will management with the ability to monitor employees' activities with minimum impact to productivity.
Which of the following policies Is BEST suited for this scenario?

A. Separation of duties
B. Mandatory vacations
C. Least privilege
D. Incident response

Answer: A