CompTIA

Exam RC0-C02

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Enterprise Security	2
Topic 2: Risk Management and Incident Response	2
Topic 3: Research and Analysis	1
Topic 5: Technical Integration of Enterprise Components	5

Topic 1, Enterprise Security

Question No : 1 - (Topic 1)

Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS server.

Answer: A

Explanation:
There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.
By eliminating all passwords and instead using digital signatures for authentication and authorization of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal.

Question No : 2 - (Topic 1)

A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

Explanation:

In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.
Therefore, the solution is to encrypt each individual partition separately.

Topic 2, Risk Management and Incident Response

Question No : 3 - (Topic 2)

A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system. The report details what seem to be a manageable volume of infrequently exploited security vulnerabilities. The director decides to implement continuous monitoring and other security controls to mitigate the impact of the vulnerabilities. Which of the following should the director require from the developers before agreeing to deploy the system?

A. An incident response plan which guarantees response by tier two support within 15 minutes of an incident.
B. A definitive plan of action and milestones which lays out resolutions to all vulnerabilities within six months.
C. Business insurance to transfer all risk from the company shareholders to the insurance company.
D. A prudent plan of action which details how to decommission the system within 90 days of becoming operational.

Answer: B

Question No : 4 - (Topic 2)

It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

A. Update the blog page to HTTPS
B. Filter metacharacters
C. Install HIDS on the server
D. Patch the web application
E. Perform client side input validation

Answer: B

Explanation:

A general rule of thumb with regards to XSS is to "Never trust user input and always filter meta-characters."

Topic 3, Research and Analysis

Question No : 5 - (Topic 3)

A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

Explanation:

Return on investment = Net profit / Investment
where:Net profit = gross profit – expenses
investment = stock + market outstanding[when defined as?] + claims

or

Return on investment = (gain from investment – cost of investment) / cost of investment
Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %

References:
Gregg, Michael, and Billy Haines, *CASP CompTIA Advanced Security Practitioner Study Guide*, John Wiley & Sons, Indianapolis, 2012, p. 337
http://www.financeformulas.net/Return_on_Investment.html

Topic 5, Technical Integration of Enterprise Components

Question No : 6 - (Topic 5)

An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

A. LDAP/S
B. SAML
C. NTLM
D. OAUTH
E. Kerberos

Answer: B,E

Explanation:
If we're using Active Directory Federated Services, then we are using Active Directory Domain Services (AD DS). AD DS uses Kerberos for authentication.
Active Directory Federated Services provides SAML services.
AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user's own organization is responsible for authenticating the user and providing identity information in

the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions.

Question No : 7 - (Topic 5)

A new IT company has hired a security consultant to implement a remote access system, which will enable employees to telecommute from home using both company issued as well as personal computing devices, including mobile devices. The company wants a flexible system to provide confidentiality and integrity for data in transit to the company's internally developed application GUI. Company policy prohibits employees from having administrative rights to company issued devices. Which of the following remote access solutions has the lowest technical complexity?

A. RDP server
B. Client-based VPN
C. IPSec
D. Jump box
E. SSL VPN

Answer: A

Explanation:

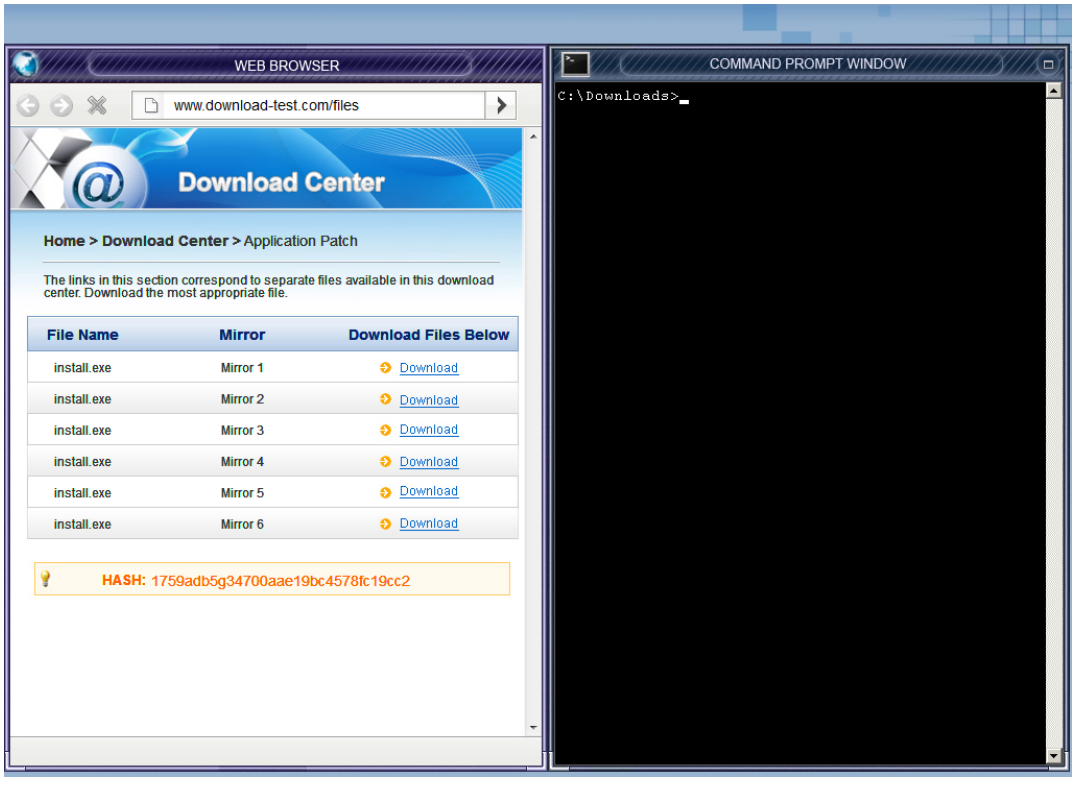
Connecting to a remote desktop server by using a remote desktop connection on a client device is has the lowest technical complexity.

Remote Desktop Services (or Remote Desktop Protocol server) is one of the components of Microsoft Windows that allows a user to take control of a remote computer or virtual machine over a network connection. RDS is Microsoft's implementation of thin client, where Windows software and the entire desktop of the computer running RDS, are made accessible to a remote client machine that supports Remote Desktop Protocol (RDP). With RDS, only software user interfaces are transferred to the client system. All input from the client system is transmitted to the server, where software execution takes place.

Question No : 8 CORRECT TEXT - (Topic 5)

An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner.

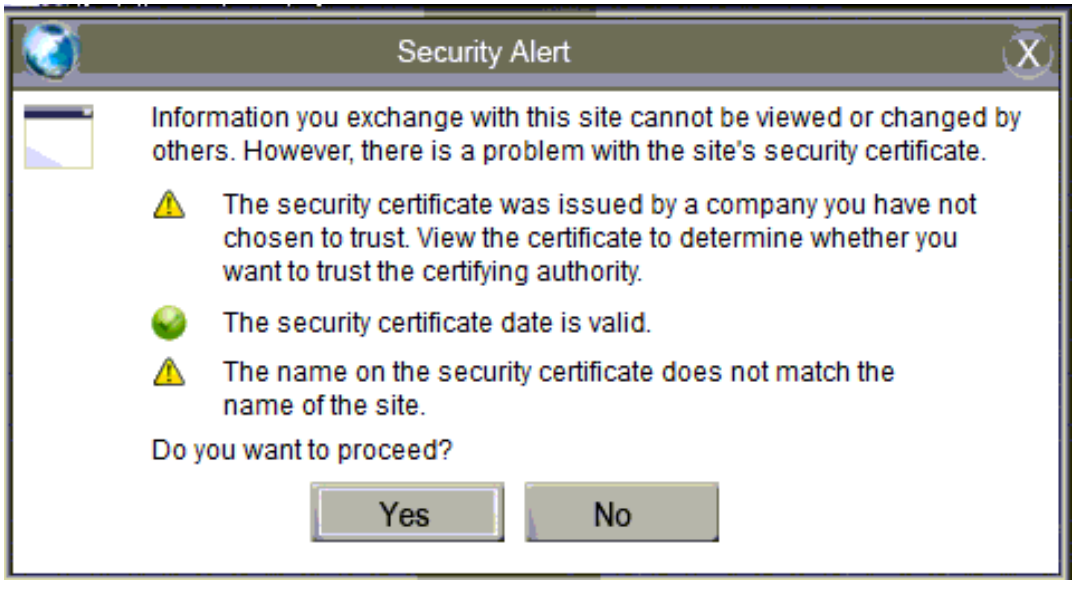
Instructions: The last install that is completed will be the final submission.



Answer: Please check the explanation part for full details on solution.

Explanation:

In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



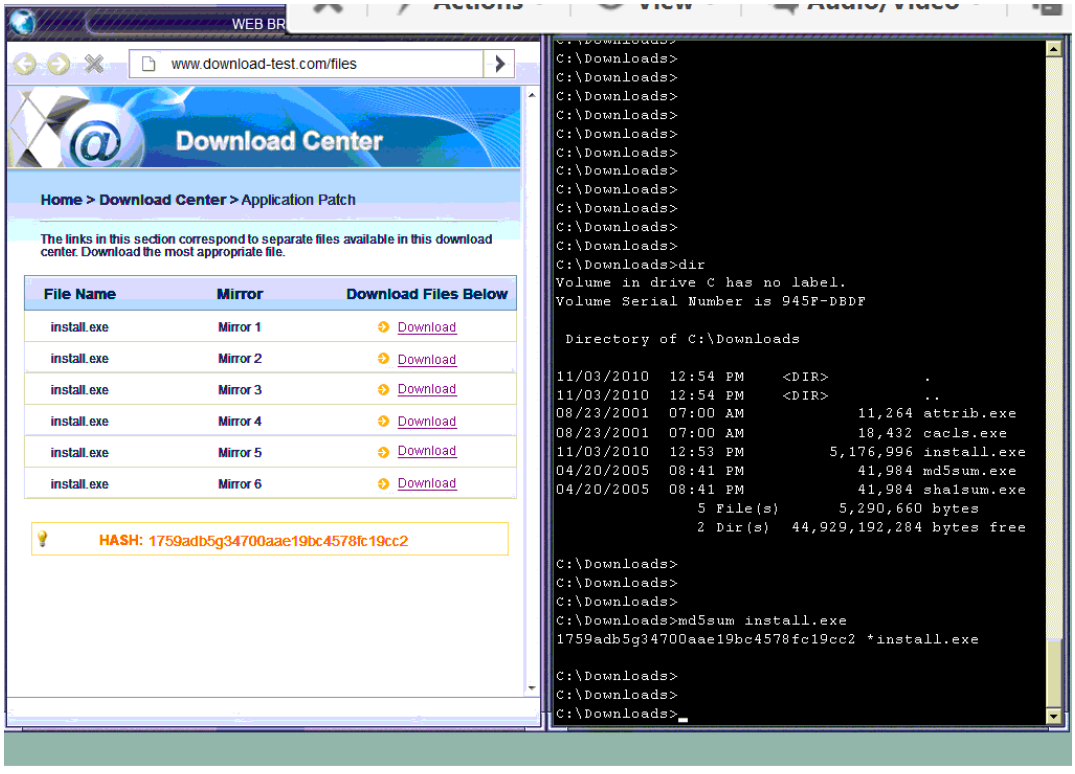
Screen Shot 2015-04-09 at 10

Also, two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:

Screen Shot 2015-04-09 at 10

Since we need to do this in the most secure manner possible, they should not be used.

Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



Screen Shot 2015-04-09 at 10

Finally, type in install.exe to install it and make sure there are no signature verification errors.

We use the MD5Sum utility to view the hash of the downloaded file. If the hash matches the hash shown on the download page, then we know that the file we are downloading has not been modified.

md5sum is a computer program that calculates and verifies 128-bit MD5 hashes, as described in RFC 1321. The MD5 hash (or checksum) functions as a compact digital fingerprint of a file.
Virtually any non-malicious change to a file will cause its MD5 hash to change; therefore md5sum is used to verify the integrity of files. Most commonly, md5sum is used to verify that a file has not changed as a result of a faulty file transfer, a disk error or non-malicious meddling. The md5sum program is installed by default in most Unix, Linux, and Unix-like operating systems or compatibility layers. Other operating systems, including Microsoft Windows and BSD variants — such as Mac OS X - have similar utilities.

References:
https://en.wikipedia.org/wiki/Md5sum

Question No : 9 - (Topic 5)

In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

A. Provide free email software for personal devices.
B. Encrypt data in transit for remote access.
C. Require smart card authentication for all devices.
D. Implement NAC to limit insecure devices access.
E. Enable time of day restrictions for personal devices.

Answer: B,D

Explanation:

In this question, we are allowing access to email and remote connections to the corporate enterprise from personal devices. When providing remote access to corporate systems, you should always ensure that data travelling between the corporate network and the remote device is encrypted.

We need to provide access to devices only if they are on an approved device list. Therefore, we need a way to check the device before granting the device access to the network if it is an approved device. For this we can use NAC (Network Access Control). When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy; including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre-installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the policy is met, the computer is able to access network resources and the Internet, within the policies defined within the NAC system.

NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.

Question No : 10 - (Topic 5)

An IT Manager is concerned about errors made during the deployment process for a new

model of tablet. Which of the following would suggest best practices and configuration parameters that technicians could follow during the deployment process?

A. Automated workflow
B. Procedure
C. Corporate standard
D. Guideline
E. Policy

Answer: D

Explanation:

A guideline is defined as a detailed plan or explanation to guide you in setting standards or determining a course of action.

A guideline is not mandatory but it would suggest the best practices and configuration parameters required in this question.