RC0-C02^Q&As

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

Pass CompTIA RC0-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 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

Correct Answer: A

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 2

A Security Administrator has some concerns about the confidentiality of data when using SOAP. Which of the following BEST describes the Security Administrator\\'s concerns?

A. The SOAP header is not encrypted and allows intermediaries to view the header data. The body can be partially or completely encrypted.

B. The SOAP protocol supports weak hashing of header information. As a result the header and body can easily be deciphered by brute force tools.

C. The SOAP protocol can be easily tampered with, even though the header is encrypted.

D. The SOAP protocol does not support body or header encryption which allows assertions to be viewed in clear text by intermediaries.

Correct Answer: A

QUESTION 3

Several business units have requested the ability to use collaborative web-based meeting places with third party vendors. Generally these require user registration, installation of client-based ActiveX or Java applets, and also the ability for the user to share their desktop in read-only or read-write mode. In order to ensure that information security is not compromised, which of the following controls is BEST suited to this situation?

A. Disallow the use of web-based meetings as this could lead to vulnerable client-side components being installed, or a malicious third party gaining read-write control over an internal workstation.

B. Hire an outside consultant firm to perform both a quantitative and a qualitative risk- based assessment. Based on the outcomes, if any risks are identified then do not allow web-based meetings. If no risks are identified then go forward and allow for these meetings to occur.

C. Allow the use of web-based meetings, but put controls in place to ensure that the use of these meetings is logged and tracked.

D. Evaluate several meeting providers. Ensure that client-side components do not introduce undue security risks. Ensure that the read-write desktop mode can either be prevented or strongly audited.

Correct Answer: D

QUESTION 4

A medium-sized company has recently launched an online product catalog. It has decided to keep the credit card purchasing in-house as a secondary potential income stream has been identified in relation to sales leads. The company has decided to undertake a PCI assessment in order to determine the amount of effort required to meet the business objectives. Which compliance category would this task be part of?

A. Government regulation

B. Industry standard

C. Company guideline

D. Company policy

Correct Answer: B

QUESTION 5

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.

Correct Answer: C

QUESTION 6

Company XYZ provides cable television services to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.

B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.

C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.

D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Correct Answer: C

The question states that "all three companies must share customer data for the purposes of accounting, billing, and customer authentication". The simplest solution is a federated solution. In a federated solution, you have a single

authentication provider.

In this question, the parent company should be the authentication provider. The authentication provider is known as the IdP (Identity Provider). The IdP is the partner in a federation that creates security tokens for users. The other two

subsidiaries, the telephone and Internet services providers will be the SP (Service Provider). The SP is the partner in a federation that consumes security tokens for providing access to applications.

QUESTION 7

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.

Correct Answer: CE

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 8

A team is established to create a secure connection between software packages in order to list employee\\'s remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

A. Network Administrator, Database Administrator, Programmers

B. Network Administrator, Emergency Response Team, Human Resources

C. Finance Officer, Human Resources, Security Administrator

D. Database Administrator, Facilities Manager, Physical Security Manager

Correct Answer: C

QUESTION 9

The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management\\'s directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.

B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.

C. Publish a policy that addresses the security requirements for working remotely with company equipment.

D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Correct Answer: C

The question states that "the organization has not addressed telecommuting in the past". It is therefore unlikely that a company policy exists for telecommuting workers. There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies. In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.

QUESTION 10

The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the company\\'s internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following recommendations should be implemented to keep the device from posing a security risk to the company?

A. A corporate policy to prevent sensitive information from residing on a mobile device and anti-virus software.

B. Encryption of the non-volatile memory and a corporate policy to prevent sensitive information from residing on a mobile device.

C. Encryption of the non-volatile memory and a password or PIN to access the device.

D. A password or PIN to access the device and a corporate policy to prevent sensitive information from residing on a mobile device.

Correct Answer: C

QUESTION 11

A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems

B. Implement an application layer firewall to protect the payroll system interface

C. Monitor the system\\'s security log for unauthorized access to the payroll application

D. Perform reconciliation of all payroll transactions on a daily basis

Correct Answer: A

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need

another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the

payroll system and limit any damage to other systems if the payroll system is attacked.

QUESTION 12

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

A. LDAP/S

B. SAML

C. NTLM

D. OAUTH

E. Kerberos

Correct Answer: BE

If we\\'re using Active Directory Federated Services, then we are using Active Directory Domain Services (AD DS). AD DS uses Kerberos for authentication. Active Directory Federated Services provides SAML services. AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user\\'s own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions.

QUESTION 13

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Correct Answer: C

Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a network-based denial of service attack in the production environment is as such `OUT OF SCOPE\\'.

QUESTION 14

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

Correct Answer: A

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 15

An information security assessor for an organization finished an assessment that identified critical issues with the human resource new employee management software application. The assessor submitted the report to senior management but nothing has happened. Which of the following would be a logical next step?

A. Meet the two key VPs and request a signature on the original assessment.

B. Include specific case studies from other organizations in an updated report.

C. Schedule a meeting with key human resource application stakeholders.

D. Craft an RFP to begin finding a new human resource application.

Correct Answer: C

You have submitted the report to senior management. It could be that the senior management are not that bothered about the HR application or they are just too busy to respond.

This question is asking for the logical next step. The next step should be to inform people that are interested in the HR application about your findings. To ensure that the key human resource application stakeholders fully understand the

implications of your findings, you should arrange a face-to-face meeting to discuss your report.