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

Company XYZ provides hosting services for hundreds of companies across multiple industries including healthcare, education, and manufacturing. The security architect for company XYZ is reviewing a vendor proposal to reduce company XYZ\\'s hardware costs by combining multiple physical hosts through the use of virtualization technologies. The security architect notes concerns about data separation, confidentiality, regulatory requirements concerning PII, and administrative complexity on the proposal. Which of the following BEST describes the core concerns of the security architect?

A. Most of company XYZ\\'s customers are willing to accept the risks of unauthorized disclosure and access to information by outside users.

B. The availability requirements in SLAs with each hosted customer would have to be re- written to account for the transfer of virtual machines between physical platforms for regular maintenance.

C. Company XYZ could be liable for disclosure of sensitive data from one hosted customer when accessed by a malicious user who has gained access to the virtual machine of another hosted customer.

D. Not all of company XYZ\\'s customers require the same level of security and the administrative complexity of maintaining multiple security postures on a single hypervisor negates hardware cost savings.

Correct Answer: C

The hosting company (Company XYZ) is responsible for the data separation of customer data. If a malicious user gained access to a customer\\'s sensitive data, the customer could sue the hosting company for damages. The result of such a lawsuit could be catastrophic for the hosting company in terms of compensation paid to the customer and loss of revenue due to the damaged reputation of the hosting company.

QUESTION 2

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

Correct Answer: AC

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 3

A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer\\'s AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN\\'s no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation

B. A cost/benefit analysis

C. Quantitative Risk Analysis

D. Qualitative Risk Analysis

Correct Answer: C

Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

QUESTION 4

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled: Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0 Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0 Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0 All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface\\'s MAC is 00-01-42-32-ab-1a A packet capture shows the following: 09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534 09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534 09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534 Which of the following is occurring on the network?

A. A man-in-the-middle attack is underway on the network.

B. An ARP flood attack is targeting at the router.

C. The default gateway is being spoofed on the network.

D. A denial of service attack is targeting at the router.

Correct Answer: D

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

QUESTION 5

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.

Correct Answer: BCF