

Exam	350-701
Title	Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) Exam
Version	14.0
Product Type	599 Q&A with explanations

QUESTION 1

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

- A. Smurf
- B. distributed denial of service
- C. cross-site scripting
- D. rootkit exploit

Answer: C

Explanation:

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.

Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.

For example the code below is written in hex: <a

```
href=javascript:alert(&#x28'XSS')>Click Here</a>
```

is equivalent to:

```
<a href=javascript:alert('XSS')>Click Here</a>
```

Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

QUESTION 2

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

- A. user input validation in a web page or web application
- B. Linux and Windows operating systems
- C. database
- D. web page images

Answer: A

Explanation:

SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:

Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

```
txtUserId = getRequestString("UserId" );  
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:

```
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
```

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE.

A hacker might get access to all the user names and passwords in this database.

QUESTION 3

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

- A. Check integer, float, or Boolean string parameters to ensure accurate values.
- B. Use prepared statements and parameterized queries.
- C. Secure the connection between the web and the app tier.
- D. Write SQL code instead of using object-relational mapping libraries.
- E. Block SQL code execution in the web application database login.

Answer: A, B

Explanation:

QUESTION 4

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

- A. Patch for cross-site scripting.
- B. Perform backups to the private cloud.
- C. Protect against input validation and character escapes in the endpoint.
- D. Install a spam and virus email filter.
- E. Protect systems with an up-to-date antimalware program

Answer: D, E

Explanation:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

QUESTION 5

Which two mechanisms are used to control phishing attacks? (Choose two)

- A. Enable browser alerts for fraudulent websites.
- B. Define security group memberships.
- C. Revoke expired CRL of the websites.
- D. Use antispyware software.
- E. Implement email filtering techniques.

Answer: A, E

Explanation:

QUESTION 6

Which two behavioral patterns characterize a ping of death attack? (Choose two)

- A. The attack is fragmented into groups of 16 octets before transmission.
-

- B. The attack is fragmented into groups of 8 octets before transmission.
- C. Short synchronized bursts of traffic are used to disrupt TCP connections.
- D. Malformed packets are used to crash systems.
- E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: B, D

Explanation:

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

QUESTION 7

Which two preventive measures are used to control cross-site scripting? (Choose two)

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. Same Site cookie attribute should not be used.

Answer: A, B

Explanation:

QUESTION 8

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
- B. A spear phishing campaign is aimed at a specific person versus a group of people.
- C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
- D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

Spear phishing is carefully designed to get a single recipient to respond. Criminals select an

individual target within an organization, using social media and other public information "" and craft a fake email tailored for that person.

QUESTION 9

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

QUESTION 10

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

- A. STIX
- B. XMPP
- C. pxGrid
- D. SMTP

Answer: A

Explanation:

TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

QUESTION 11

Which two capabilities does TAXII support? (Choose two)

- A. Exchange
- B. Pull messaging
- C. Binding
- D. Correlation
- E. Mitigating

Answer: AB

Explanation:

The Trusted Automated eXchange of Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.

TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.

Although there is no "binding" capability in the list but it is the best answer here.

QUESTION 12

Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

- A. exploits
- B. ARP spoofing
- C. denial-of-service attacks
- D. malware
- E. eavesdropping

Answer: A, D

Explanation:

Malware means "malicious software" , is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.

Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.

An exploit is a code that takes advantage of a software vulnerability or security flaw.

Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

QUESTION 13

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

- A. url
- B. terminal
- C. profile
- D. selfsigned

Answer: C

Explanation:

A trustpoint enrollment mode, which also defines the trustpoint authentication mode, can be

performed via 3 main methods:

1. Terminal Enrollment "" manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal.
2. SCEP Enrollment "" Trustpoint authentication and enrollment using SCEP over HTTP.
3. Enrollment Profile "" Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile.

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructurepki/211333-IOSPKI-Deployment-Guide-Initial-Design.html>

QUESTION 14

What are two rootkit types? (Choose two)

- A. registry
- B. virtual
- C. bootloader
- D. user mode
- E. buffer mode

Answer: C, D

Explanation:

The term "rootkit"™ originally comes from the Unix world, where the word "root"™ is used to describe a user with the highest possible level of access privileges, similar to an "Administrator"™ in Windows. The word "kit"™ refers to the software that grants root-level access to the machine. Put the two together and you get "rootkit"™, a program that gives someone "" with legitimate or malicious intentions "" privileged access to a computer. There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

QUESTION 15

Which form of attack is launched using botnets?

- A. EIDDOS
- B. virus
- C. DDOS
- D. TCP flood

Answer: C

Explanation:

A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.

QUESTION 16

Which threat involves software being used to gain unauthorized access to a computer system?

- A. virus
- B. NTP amplification
- C. ping of death
- D. HTTP flood

Answer: A

Explanation:

QUESTION 17

Which type of attack is social engineering?

- A. trojan
- B. phishing
- C. malware
- D. MITM

Answer: B

Explanation:

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

QUESTION 18

Which two key and block sizes are valid for AES? (Choose two)

- A. 64-bit block size, 112-bit key length
- B. 64-bit block size, 168-bit key length
- C. 128-bit block size, 192-bit key length
- D. 128-bit block size, 256-bit key length
- E. 192-bit block size, 256-bit key length

Answer: C, D

Explanation:

The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

QUESTION 19

Which two descriptions of AES encryption are true? (Choose two)

- A. AES is less secure than 3DES.
-

- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

Answer: B, D

Explanation:

QUESTION 20

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

Answer: A

Explanation:

The data plane of any network is responsible for handling data packets that are transported across the network.

(The data plane is also sometimes called the forwarding plane.)

Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?).

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates.

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/securitybook/security-overview.html>

QUESTION 21

Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

- A. 3DES
- B. RSA
- C. DES
- D. AES

Answer: B

Explanation:

Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve
