SSCP$^{\text{Q\&As}}$

System Security Certified Practitioner (SSCP)

QUESTION 1

What do the ILOVEYOU and Melissa virus attacks have in common?

A. They are both denial-of-service (DOS) attacks.

B. They have nothing in common.

C. They are both masquerading attacks.

D. They are both social engineering attacks.

Correct Answer: C

While a masquerading attack can be considered a type of social engineering, the Melissa and ILOVEYOU viruses are examples of masquerading attacks, even if it may cause some kind of denial of service due to the web server being flooded with messages. In this case, the receiver confidently opens a message coming from a trusted individual, only to find that the message was sent using the trusted party\\'s identity. Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter

10: Law, Investigation, and Ethics (page 650).

QUESTION 2

Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident\\'s effects is part of:

A. Incident Evaluation

B. Incident Recognition

C. Incident Protection

D. Incident Response

Correct Answer: D

These are core functions of the incident response process.

"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process. "Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the

initiation of the incident response process.

"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.

References

CBK, pp. 698 - 703

QUESTION 3

Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication

B. Administration

C. Accounting

D. Authorization

Correct Answer: B

Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

also see:

The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A\\'s" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.

Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

QUESTION 4

Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:

A. Authentication

B. Integrity

C. Replay resistance and non-repudiations

D. Confidentiality

Correct Answer: D

AH provides integrity, authentication, and non-repudiation. AH does not provide encryption which means

that NO confidentiality is in place if only AH is being used. You must make use of the Encasulating Security

Payload if you wish to get confidentiality. IPSec uses two basic security protocols: Authentication Header

(AH) and Encapsulation Security Payload.

AH is the authenticating protocol and the ESP is the authenticating and encrypting protocol that uses

cryptographic mechanisms to provide source authentication, confidentiality and message integrity.

The modes of IPSEC, the protocols that have to be used are all negotiated using Security Association.

Security Associations (SAs) can be combined into bundles to provide authentication, confidentialility and layered communication.

Source:

TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.

also see:

Shon Harris, CISSP All In One uide, 5th Edition, Page 758

QUESTION 5

Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site

B. Warm Site

C. Internal Hot Site

D. Dual Data Center

Correct Answer: C

Internal Hot Site--This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery.

Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following:

Dual Data Center--This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.

External Hot Site--This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time.

Warm Site--A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster.

Cold Site--A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21265-21291). Auerbach Publications. Kindle Edition.