312-50V7^{Q&As}

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

🛠️ **Instant Download** After Purchase

🛠️ **100% Money Back** Guarantee

🛠️ **365 Days** Free Update

🛠️ **800,000+** Satisfied Customers

QUESTION 1

A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Correct Answer: D

QUESTION 2

How do you defend against ARP Spoofing? Select three.

A. Use ARPWALL system and block ARP spoofing attacks

B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets

C. Use private VLANS

D. Place static ARP entries on servers, workstation and routers

Correct Answer: ACD

QUESTION 3

Which of the following statements are true regarding N-tier architecture? (Choose two.)

A. Each layer must be able to exist on a physically independent system.

B. The N-tier architecture must have at least one logical layer.

C. Each layer should exchange information only with the layers above and below it.

D. When a layer is changed or updated, the other layers must also be recompiled or modified.

Correct Answer: AC

QUESTION 4

Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.

B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.

C. Hashing is faster compared to more traditional encryption algorithms.

D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Correct Answer: D

QUESTION 5

A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.

Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.

Fake E-mail

From: FEDEX Packet Service
Subject: FEDEX Packet N0328795951

Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]

Legit E-mail

Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. DO NOT OPEN the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to abuse@fedex.com.

If you have any questions or concerns about services provided by FedEx, please review our services at fedex.com/us/services or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments.

Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail.

How do you ensure if the e-mail is authentic and sent from fedex.com?

A. Verify the digital signature attached with the mail, the fake mail will not have Digital ID at all

B. Check the Sender ID against the National Spam Database (NSD)

C. Fake mail will have spelling/grammatical errors

D. Fake mail uses extensive images, animation and flash content

Correct Answer: A