312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.

B. Monitor all traffic using the firewall rule until a manager can approve it.

C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

Correct Answer: D

QUESTION 2

Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information

B. Social Engineering is the means put in place by human resource to perform time accounting

C. Social Engineering is the act of getting needed information from a person rather than breaking into a system

D. Social Engineering is a training program within sociology studies

Correct Answer: C

QUESTION 3

".....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there."

Fill in the blank with appropriate choice.

A. Evil Twin Attack

B. Sinkhole Attack

C. Collision Attack

D. Signal Jamming Attack

Correct Answer: A

https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks) An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims\\' sensitive details. Most often, the victims of such attacks are ordinary people like you and me. The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions. An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable. ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

QUESTION 4

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance

B. Maintaining access

C. Scanning

D. Gaining access

Correct Answer: D

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they\\'re Password cracking ?Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.?Password attacks ?Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 5

Which service in a PKI will vouch for the identity of an individual or company?

A. KDC

B. CR

C. CBC

D. CA

Correct Answer: D

Latest 312-50V12 Dumps 312-50V12 Exam Questions 312-50V12 Braindumps