312-50V12$^{\text{Q\&As}}$

Certified Ethical Hacker Exam (CEHv12)

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

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

QUESTION 1

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

Correct Answer: B

Identifying operating systems, services, protocols and devices,

Collecting unencrypted information about usernames and passwords,

Capturing network traffic for further analysis are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network.

When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

QUESTION 2

In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy

B. A legitimate communication path within a computer system or network for transfer of data

C. It is a kernel operation that hides boot processes and services to mask detection

D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Correct Answer: A

QUESTION 3

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue

communication with that computer even after being physically disconnected. Now, Clark gains access to Steven\\'s iPhone through the infected computer and is able to monitor and read all of Steven\\'s activity on the iPhone, even after the

device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

A. IOS trustjacking

B. lOS Jailbreaking

C. Exploiting SS7 vulnerability

D. Man-in-the-disk attack

Correct Answer: A

An iPhone client\\'s most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that. This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults. After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs. This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn\\'t need the casualty\\'s endorsement and can be directed simply from the PC side. Getting a live stream of the gadget\\'s screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly. It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn\\'t anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

QUESTION 4

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company\\'s network. You have

configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place. Your peer, Peter Smith who works at the

same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

Correct Answer: A

QUESTION 5

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the

same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered

in a form are linked to Boneys account.

What is the attack performed by Boney in the above scenario?

A. Session donation attack

B. Session fixation attack

C. Forbidden attack

D. CRIME attack

Correct Answer: A

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker\\'s account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker\\'s account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

312-50V12 VCE Dumps 312-50V12 Study Guide 312-50V12 Braindumps