



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.pass4itsure.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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

Which of the following provides a security professional with most information about the system's security posture?

- A. Phishing, spamming, sending trojans
- B. Social engineering, company site browsing tailgating
- C. Wardriving, warchalking, social engineering
- D. Port scanning, banner grabbing service identification

Correct Answer: D

QUESTION 2

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

- A. Spear phishing
- B. Whaling
- C. Vishing
- D. Phishing

Correct Answer: B

QUESTION 3

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-4: Orchestrators
- C. Tier-3: Registries
- D. Tier-2: Testing and accreditation systems

Correct Answer: D

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at



an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter. For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

QUESTION 4

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

- A. Red hat
- B. white hat
- C. Black hat
- D. Gray hat

Correct Answer: B

A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission. White hat hackers can also add teams called "sneakers and/or hacker clubs", red teams, or tiger teams. While penetration testing concentrates on attacking software and computer systems from the beginning ? scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example ? ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long-term con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it. Some other methods of completing these include: ? DoS attacks ? Social engineering tactics ? Reverse engineering ? Network security ? Disk and memory forensics ? Vulnerability research ? Security scanners such as: ? W3af ? Nessus ? Burp suite ? Frameworks such as: ? Metasploit ? Training Platforms These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system `back-doors` which will be used as a link to information or access that a non-ethical hacker, also referred to as `black-hat` or `grey-hat`, might want to succeed in .

**QUESTION 5**

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this: From: jim_miller@companyxyz.com To: michelle_saunders@companyxyz.com Subject: Test message Date: 4/3/2017 14:37 The employee of CompanyXYZ receives your email message. This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

Correct Answer: D

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is common for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can

cause significant problems and sometimes pose a real security threat.

[312-50V12 PDF Dumps](#)

[312-50V12 Exam Questions](#)

[312-50V12 Braindumps](#)