



# 312-50V12<sup>Q&As</sup>

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**

Sam, a professional hacker, targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS IAM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

- A. Social engineering
- B. insider threat
- C. Password reuse
- D. Reverse engineering

Correct Answer: A

Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS user's credentials within the hands of an attacker. If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user. With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials. An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials. These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use. For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here. During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

**QUESTION 2**

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows

that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP



Correct Answer: A

[https://en.wikipedia.org/wiki/MAC\\_filtering](https://en.wikipedia.org/wiki/MAC_filtering) MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices. It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network. The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws. On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources. MAC address filtering adds an extra layer of security that checks the device's MAC address against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn't join the network.

---

### QUESTION 3

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

- A. Bluesmacking
- B. BlueSniffing
- C. Bluejacking
- D. Bluesnarfing

Correct Answer: C

<https://en.wikipedia.org/wiki/Bluejacking> Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message

in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's

possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

---

### QUESTION 4



One of your team members has asked you to analyze the following SOA record. What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028

B. 3600

C. 604800

D. 2400

E. 60

F. 4800

Correct Answer: A

---

#### QUESTION 5

Given below are different steps involved in the vulnerability-management life cycle.

1) Remediation 2) Identify assets and create a baseline 3) Verification 4) Monitor 5) Vulnerability scan 6) Risk assessment

Identify the correct sequence of steps involved in vulnerability management.

A. 2-->5-->6-->1-->3-->4

B. 2-->1-->5-->6-->4-->3

C. 2-->4-->5-->3-->6--> 1

D. 1-->2-->3-->4-->5-->6

Correct Answer: A

[Latest 312-50V12 Dumps](#)

[312-50V12 Study Guide](#)

[312-50V12 Braindumps](#)