ECSAV10Q&As

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.passapply.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Joe, an ECSA certified professional, is working on a pen testing engagement for one of his SME clients. He discovered the host file in one of the Windows machines has the following entry:

213.65.172.55 microsoft.com

After performing a Whois lookup, Joe discovered the IP does not refer to Microsoft.com. The network

admin denied modifying the host files.

Which type of attack does this scenario present?

A. DNS starvation

B. DNS poisoning

C. Phishing

D. MAC spoofing

Correct Answer: B

QUESTION 2

StarMotel is a prominent chain of hotels in the world that uses high-tech solutions to ease the stay of their guests. In those high-tech solutions, they deployed RFID cards using which a guest can get access to the allocated hotel room. Keeping an eye on the RFID technology and with an objective of exploiting it, John, a professional hacker, decided to hack it in order to obtain access to any room in the target hotel. In this process, he first pulled an RFID keycard from the trash of the target hotel and identified the master keycard

code in several tries using an RFID card reading and writing tool. Then, he created its clone using a new

RFID card that gave him free reign to roam in any hotel room in the building.

Identify the RFID attack John has performed on the target hotel?

A. RFID spoofing attack

B. Reverse engineering attack

C. RFID replay attack

D. Power analysis attack

Correct Answer: B

QUESTION 3

From where can clues about the underlying application environment can be collected?

A. From source code

B. From file types and directories

C. From executable file

D. From the extension of the file

Correct Answer: D

QUESTION 4

A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

A. Microsoft Internet Security Framework

B. Information System Security Assessment Framework (ISSAF)

C. Bell Labs Network Security Framework

D. The IBM Security Framework

Correct Answer: A

QUESTION 5

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting

B. HTTP fingerprinting

C. FTP fingerprinting

D. SNMP fingerprinting

Correct Answer: C