ECSAV10^{Q&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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

You have compromised a lower-level administrator account on an Active Directory network of a small

company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of

the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

A. Poison the DNS records with false records

B. Enumerate MX and A records from DNS

C. Establish a remote connection to the Domain Controller

D. Enumerate domain user accounts and built-in groups

Correct Answer: D

QUESTION 2

What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment

B. Service-based Assessment Solutions

C. Product-based Assessment Solutions

D. Tree-based Assessment

Correct Answer: A

QUESTION 3

GenSec Inc, a UK-based company, uses Oracle database to store all its data. The company also uses Oracle DataBase Vault to restrict users access to specific areas of their database. GenSec hired a senior penetration tester and security auditor named Victor to check the vulnerabilities of the company\'s Oracle DataBase Vault. He was asked to find all the possible vulnerabilities that can bypass the company\'s Oracle DB Vault. Victor tried different kinds of attacks to penetrate into the company\'s Oracle DB Vault and succeeded. Which of the following attacks can help Victor to bypass GenSec\'s Oracle DB Vault?

A. Man-in-the-Middle Attack

B. Denial-of-Service Attack

C. Replay Attack

D. SQL Injection

Correct Answer: D

QUESTION 4

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open

B. The firewall failed-bypass

C. The firewall failed-closed

D. The firewall ACL has been purged

Correct Answer: A

QUESTION 5

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes

B. Type 12 ICMP codes

C. Type 3 ICMP codes

D. Type 7 ICMP codes

Correct Answer: C