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

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

QUESTION 1

Arrange the WEP cracking process in the correct order:

I. aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1

II. aircrack-ng -s capture.ivs

III. airmon-ng start eth1

IV.

airodump-ng --ivs --write capture eth1

V.

aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1

A.

IV-->I-->V-->III-->II

B.

III-->IV-->V-->II-->I

C.

III-->IV-->I-->V-->II

D.

IV-->I-->V-->III-->II

Correct Answer: C

QUESTION 2

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 3

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company\\'s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)

B. Simple Network Management Protocol (SNMP)

C. Telnet

D. Secure Shell (SSH)

Correct Answer: D

QUESTION 4

Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

A. Microsoft Baseline Security Analyzer (MBSA)

B. CORE Impact

C. Canvas

D. Network Security Analysis Tool (NSAT)

Correct Answer: C

QUESTION 5

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. More RESET packets to the affected router to get it to power back up

B. RESTART packets to the affected router to get it to power back up

C. The change in the routing fabric to bypass the affected router

D. STOP packets to all other routers warning of where the attack originated

Correct Answer: C

Latest ECSAV10 Dumps ECSAV10 Study Guide ECSAV10 Braindumps