EC-COUNCIL

412-79v10

Certified Security Analyst (ECSA) V10

Question: 52

Which of the following defines the details of services to be provided for the client's organization and the list of services required for performing the test in the organization?
A . Draft
B . Report
C . Requirement list
D . Quotation

Answer: D

Question: 53

Which of the following methods is used to perform server discovery?
A . Banner Grabbing
B . Who is Lookup
C . SQL Injection
D . Session Hijacking

Answer: B

Question: 54

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer.

Where should Harold navigate on the computer to find the file?
A . %systemroot%LSA
B . %systemroot%repair
C . %systemroot%system32driversetc

D . %systemroot%system32LSA

Answer: B

Question: 55

What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?
A . Server Side Includes
B . Sort Server Includes
C . Server Sort Includes
D . Slide Server Includes

Answer: A

Question: 56

Which of the following will not handle routing protocols properly?
A . "Internet-router-firewall-net architecture"
B . "Internet-firewall-router-net architecture"
C . "Internet-firewall -net architecture"
D . "Internet-firewall/router(edge device)-net architecture"

Answer: B

Question: 57

Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?
A . AES
B . DES (ECB mode)
C . MD5
D . RC5

Answer: C

Question: 58

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs.

He looks up the behavior on the Internet, but cannot find anything related.

What organization should Frank submit the log to find out if it is a new vulnerability or not?
A . CVE

B . IANA
C . RIPE
D . APIPA

Answer: A

Question: 59

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

Answer: C

Question: 60

War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks.

Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?
A . Airsnort
B . Aircrack
C . WEPCrack
D . Airpwn

Answer: A

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!