DUMPSBOSS.

EC-Council Certified Security Analyst

ECCouncil 412-79v8

Version Demo

Total Demo Questions: 10

Total Premium Questions: 200

Buy Premium PDF

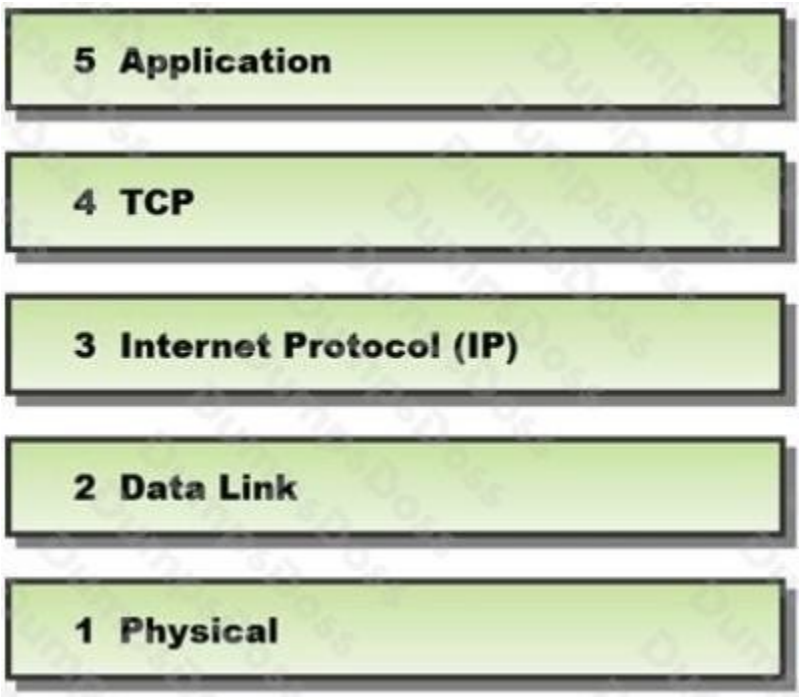
https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application

B. Level 2 – Data Link

C. Level 4 – TCP

D. Level 3 – Internet Protocol (IP)

ANSWER: D

Explanation:

Reference:
http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION NO: 2

Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement

B. Rules of Behavior Agreement

C. Liability Insurance

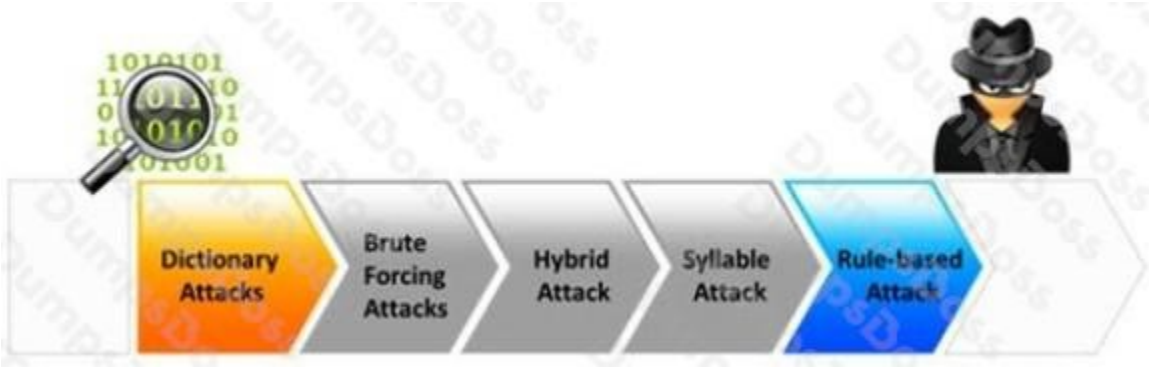
D. Non-Disclosure Agreement

ANSWER: D

QUESTION NO: 3

Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to a system.



Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack

B. Rule-based attack

C. Hybrid attack

D. Dictionary attack

ANSWER: A

Explanation:

Reference:
http://books.google.com.pk/books?id=m2qZNW4dcyIC&pg=PA237&lpg=PA237&dq=password+cracking+attacks+tries+every+combination+of+characters+until+the+password+is+broken&source=bl&ots=RKEUUo6LYj&sig=MPEfFBEpoO0yvOwMxYCoPQuqM5g&hl=en&sa=X&ei=ZdwdVJm3CoXSaPXsgPgM&ved=0CCEQ6AEwAQ#v=onepage&q=password%20cracking%20attacks%20tries%20every%20combination%20of%20characters%20until%20the%20password%20is%20broken&f=false

QUESTION NO: 4

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 NO: 5

What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

A. 1, 2, 3, 4, 5

B. Low, medium, high, serious, critical

C. Urgent, dispute, action, zero, low

D. A, b, c, d, e

ANSWER: B

QUESTION NO: 6

Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.

What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks

B. Service Level Configuration Attacks

C. Inside Attacks

D. URL Tampering Attacks

ANSWER: A

QUESTION NO: 7

Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL

B. ACT_FLOOD

C. ACT_KILL_HOST

D. ACT_ATTACK

ANSWER: A

QUESTION NO: 8

Which of the following is not a condition specified by Hamel and Prahalad (1990)?

A. Core competency should be aimed at protecting company interests

B. Core competency is hard for competitors to imitate

C. Core competency provides customer benefits

D. Core competency can be leveraged widely to many products and markets

ANSWER: A

Explanation:

Reference: http://www.studymode.com/essays/Hamel-Prahalad-Core-Competency-1228370.html

QUESTION NO: 9

Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

A. DNSSEC

B. Netsec

C. IKE

D. IPsec

ANSWER: D

Explanation:

Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

QUESTION NO: 10

John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan

B. Penetration testing software project management plan

C. Penetration testing project scope report

D. Penetration testing schedule plan

ANSWER: A

Explanation:

Rfere

http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false