DUMPSQUEEN

EC-Council Certified Security Analyst (ECSA)

ECCouncil 412-79

Version Demo

Total Demo Questions: 15

Total Premium Questions: 203

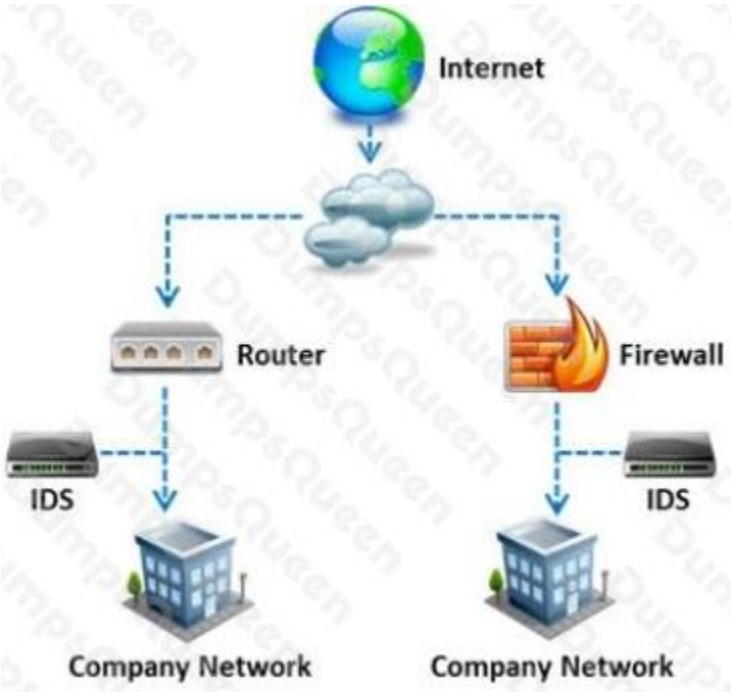
Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.

B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.

C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.

D. HIDS requires less administration and training compared to NIDS.

ANSWER: C

QUESTION NO: 2

TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

A. Simple Network Management Protocol (SNMP)

B. Network File system (NFS)

C. Internet Control Message Protocol (ICMP)

D. Transmission Control Protocol (TCP)

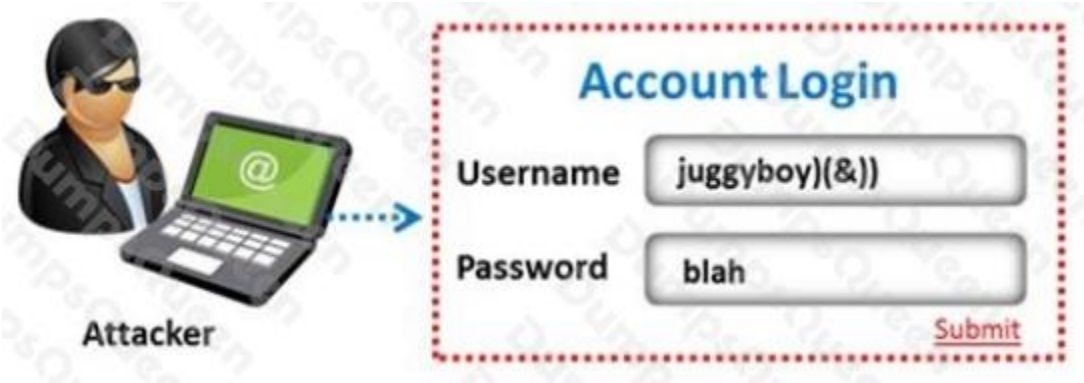
ANSWER: A

QUESTION NO: 3

The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first.

Identify the injection attack represented in the diagram below:



A. Frame Injection Attack

B. LDAP Injection Attack

C. XPath Injection Attack

D. SOAP Injection Attack

ANSWER: B

Explanation:

Reference: e https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf (page 3 to 5)

QUESTION NO: 4

Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

A. Anonymous Information Gathering

B. Private Information Gathering

C. Passive Information Gathering

D. Active Information Gathering

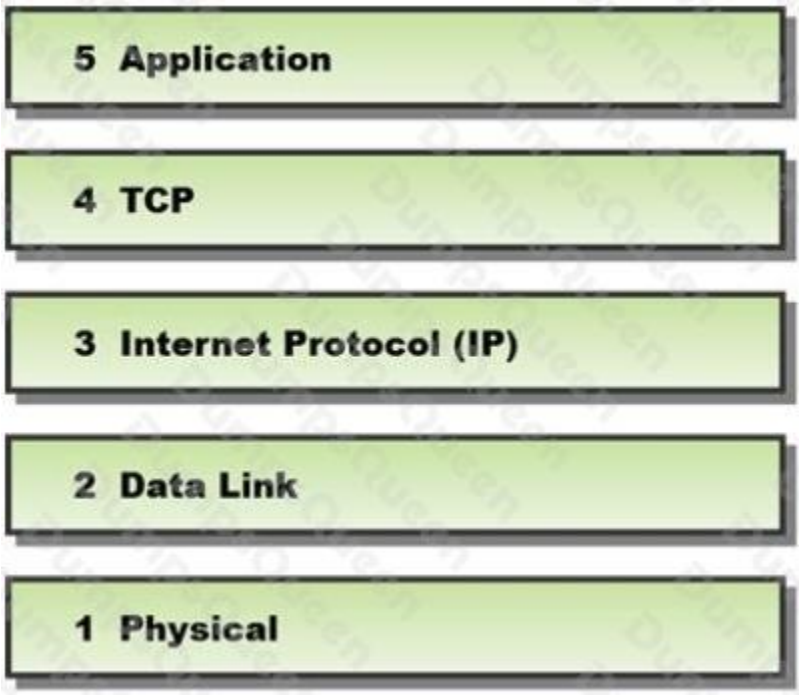
ANSWER: D

Explanation:

Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

QUESTION NO: 5

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: 6

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

A. ASCII value of the character

B. Binary value of the character

C. Decimal value of the character

D. Hex value of the character

ANSWER: D

Explanation:

https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnIg1xZ78ScUvuIlTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

QUESTION NO: 7

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway

B. Stateful multilayer inspection firewall

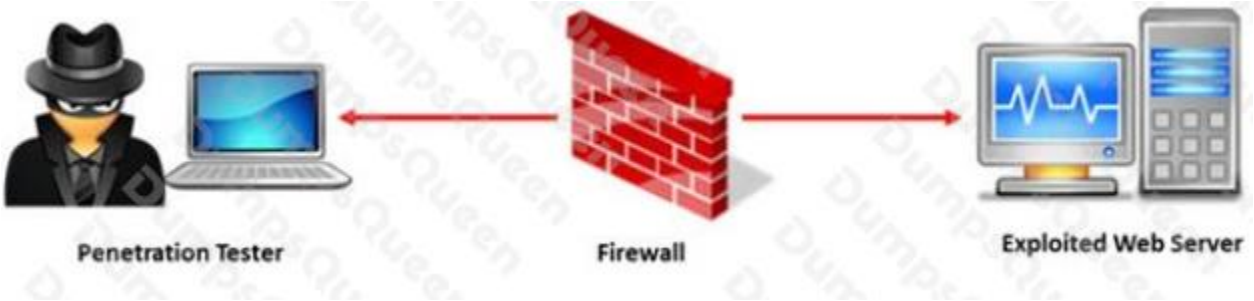
C. Packet filter

D. Application level gateway

ANSWER: C

QUESTION NO: 8

A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing

B. Blind testing and double blind testing

C. Blind testing and unannounced testing

D. Announced testing and unannounced testing

ANSWER: D

QUESTION NO: 9

Which one of the following is a useful formatting token that takes an int * as an argument, and writes the number of bytes already written, to that location?

A. "%n"

B. "%s"

C. "%p"

D. "%w"

ANSWER: A

QUESTION NO: 10

Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

A. 802.11b

B. 802.11g

C. 802.11-Legacy

D. 802.11n

ANSWER: A

QUESTION NO: 11

One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

A. ROCHESTON fileformat:+ppt

B. ROCHESTON ppt:filestring

C. ROCHESTON filetype:ppt

D. ROCHESTON +ppt:filesearch

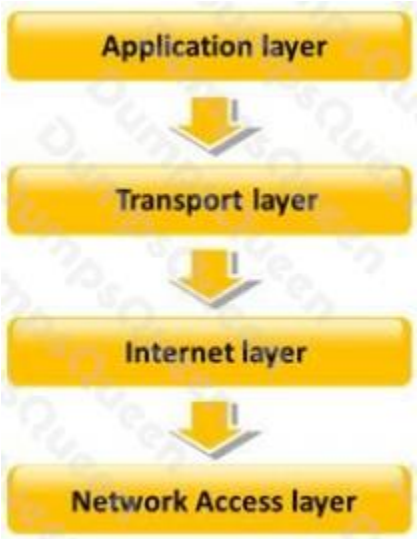
ANSWER: C

Explanation:

Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx (specific document types)

QUESTION NO: 12

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer

B. Network Access layer

C. Internet layer

D. Application layer

ANSWER: C

QUESTION NO: 13

In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique

B. IDS evasion technique

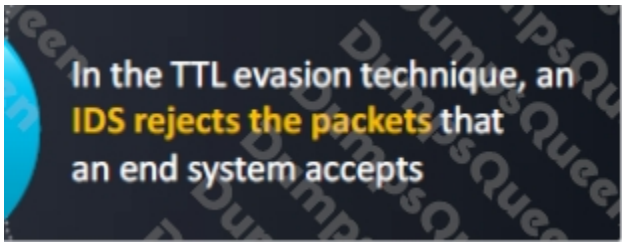
C. UDP evasion technique

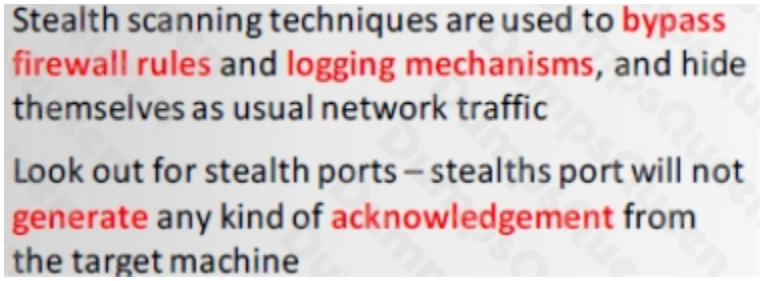
D. TTL evasion technique

ANSWER: D

Explanation:

Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)





QUESTION NO: 14

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

ANSWER: A

QUESTION NO: 15

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