EC-Council

412-79V9 Exam

EC-Council Certified Security Analyst (ECSA) v9

Thank you for Downloading 412-79V9 exam PDF Demo

You can Buy Latest 412-79V9 Full Version Download

https://www.certkillers.net/Exam/412-79V9

https://www.certkillers.net

Version: 12.0

Question: 1

Which of the following password cracking techniques is used when the attacker has some information about the password?

A. Hybrid Attack
B. Dictionary Attack
C. Syllable Attack
D. Rule-based Attack

Answer: D

Explanation:
Reference:
http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20
Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf
(page 4, rule-based attack)

Question: 2

Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password
B. Account username was not found
C. Incorrect password
D. Username or password incorrect

Answer: C

Question: 3

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:
http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—

What is the table name?

A. CTS
B. QRT
C. EMP
D. ABC

Answer: C

Question: 4

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Answer: B

Question: 5

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

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=8C4dVYe 1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

Question: 6

Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Answer: D

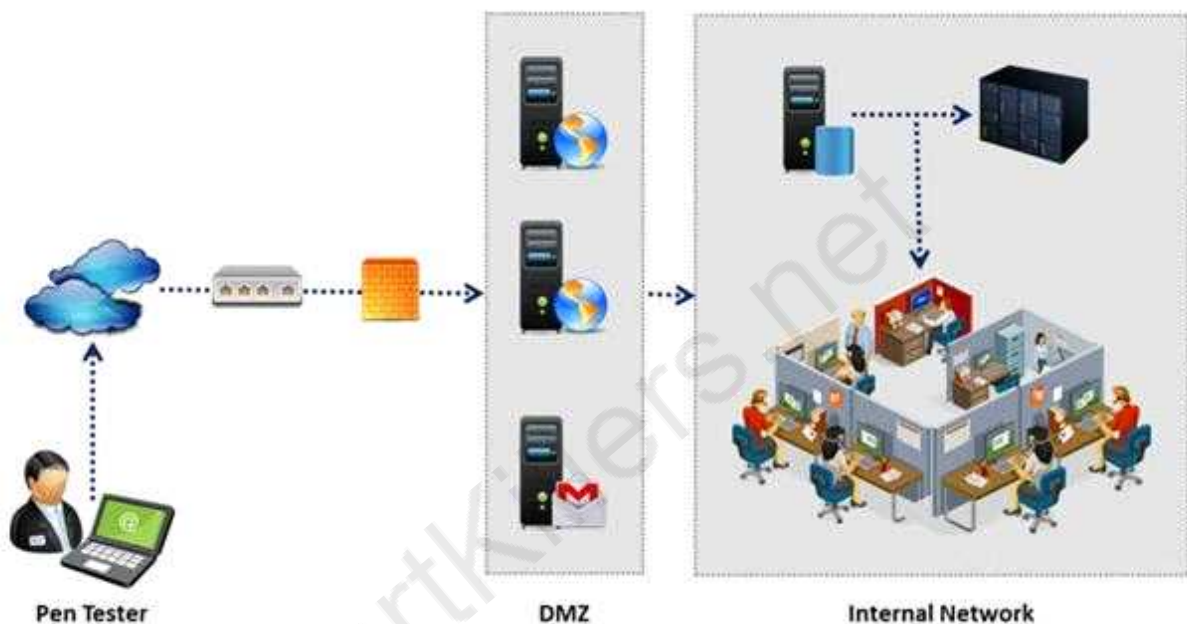Refere' http://en.wikipedia.org/wiki/Glossary

Question: 7

An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.

During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

A. XMAS Scan
B. SYN scan
C. FIN Scan
D. NULL Scan

Answer: B

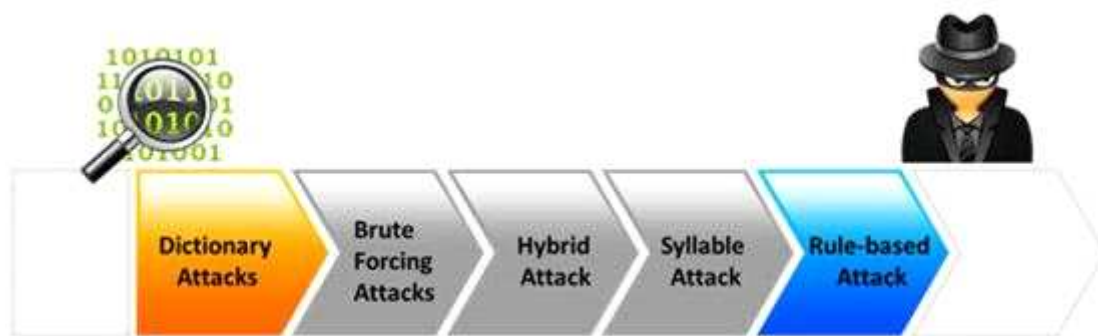## Question: 8

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+crack
ing+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%20combi
nation%20of%20characters%20until%20the%20password%20is%20broken&f=false

Question: 9

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

Rules of Engagement Template

DATE: [Date]

TO: [Name and Address of NASA Official]

FROM: [Name and Address of Third Party performing the Penetration Testing]

CC: [Name and Address of Interested NASA Officials]

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of
               [required activity]

[Name of third party] has been contracted by the National Aeronautics and Space Administration
(NASA). [Name of requesting organization] to perform an audit of NASA's [Name of risk
assessment target]. The corresponding task-order requires the performance of penetration test
procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of
Engagement" is to clearly establish the scope of work and the procedures that will and will not
be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams
B. Decide the desired depth for penetration testing
C. Conduct a brainstorming session with top management and technical teams
D. Have pre-contract discussions with different pen-testers

Answer: C

Question: 10

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

Question: 11

Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

A. Visit Google's search engine and view the cached copy
B. Crawl and download the entire website using the Surfoffline tool and save them to his computer
C. Visit the company's partners' and customers' website for this information
D. Use WayBackMachine in Archive.org web site to retrieve the Internet archive

Answer: D

Question: 12

Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Answer: D

Question: 13

Which of the following is not a characteristic of a firewall?

A. Manages public access to private networked resources
B. Routes packets between the networks
C. Examines all traffic routed between the two networks to see if it meets certain criteria
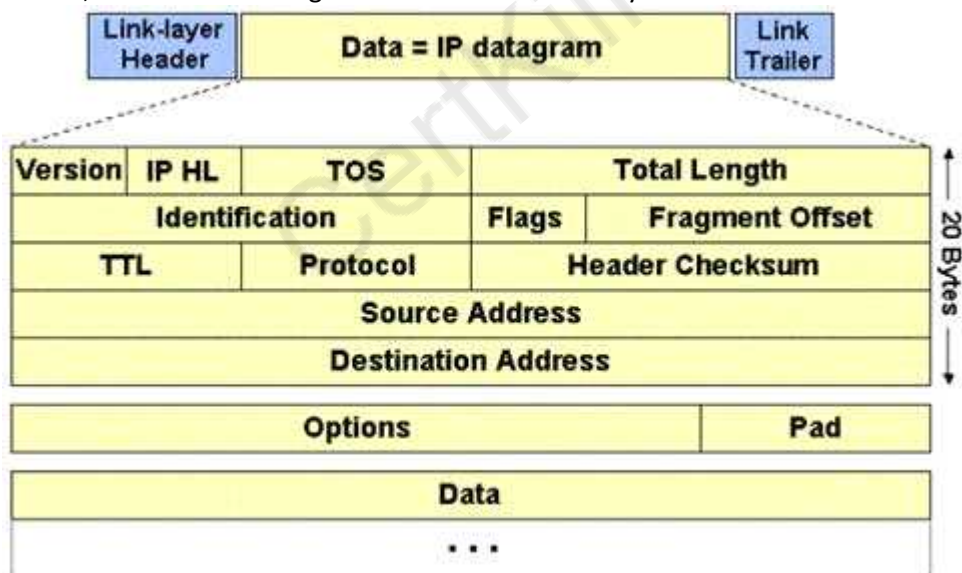D. Filters only inbound traffic but not outbound traffic

Answer: D

Question: 14

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.

The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes
B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

	Answer: C

Explanation:
Reference:
http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

Question: 15

From where can clues about the underlying application environment can be collected?

A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

	Answer: A

Question: 16

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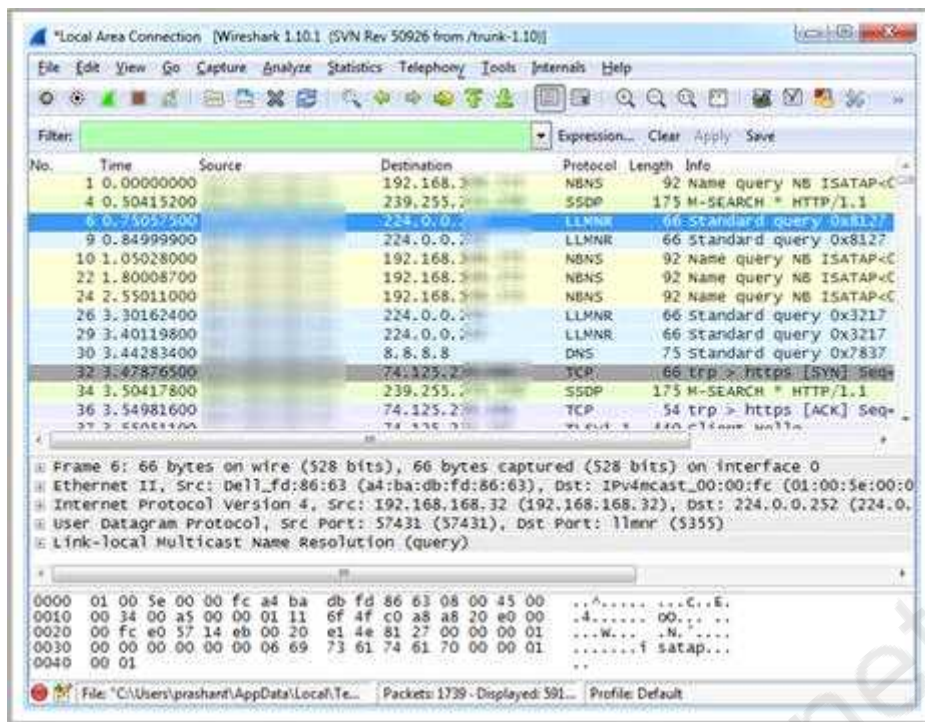http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies

Question: 17

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?

A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

Answer: C

Question: 18

Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs
B. Separated into two 8-character strings
C. Letters are converted to the lowercase
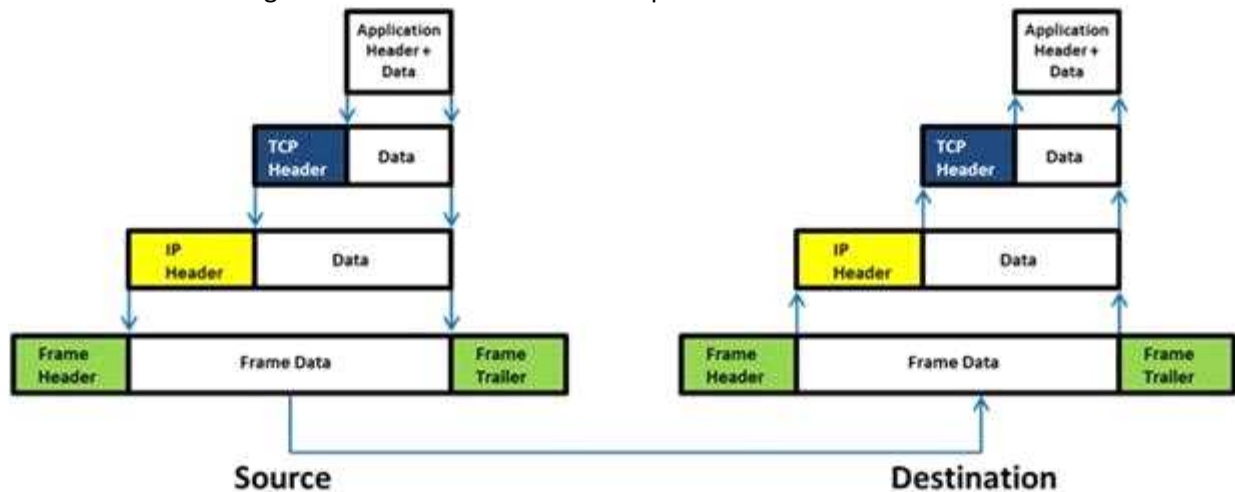D. Padded with NULL to 16 characters

Answer: A

Explanation:
Reference:
http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

Question: 19

Which of the following statement holds true for TCP Operation?

Source   Destination

A. Port numbers are used to know which application the receiving host should pass the data to
B. Sequence numbers are used to track the number of packets lost in transmission
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
D. Data transfer begins even before the connection is established

Answer: D

Question: 20

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

Thank You for trying 412-79V9 PDF Demo

To Buy Latest 412-79V9 Full Version Download visit link below

https://www.certkillers.net/Exam/412-79V9

Start Your 412-79V9 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your 412-79V9 preparation with actual exam questions.

https://www.certkillers.net