Vendor: EC-Council

Exam Code: 412-79v8

Exam Name: EC-Council Certified Security Analyst (ECSA) v8

Version: DEMO

QUESTION 1
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: C

QUESTION 2
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
Explanation:
http://en.wikipedia.org/wiki/Glossary

QUESTION 3
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:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/20/ip_security/provisioning/guide/IPsecPG1.html

QUESTION 4
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:
http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%

20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf (page 4, rule-based attack)

QUESTION 5
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 6
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

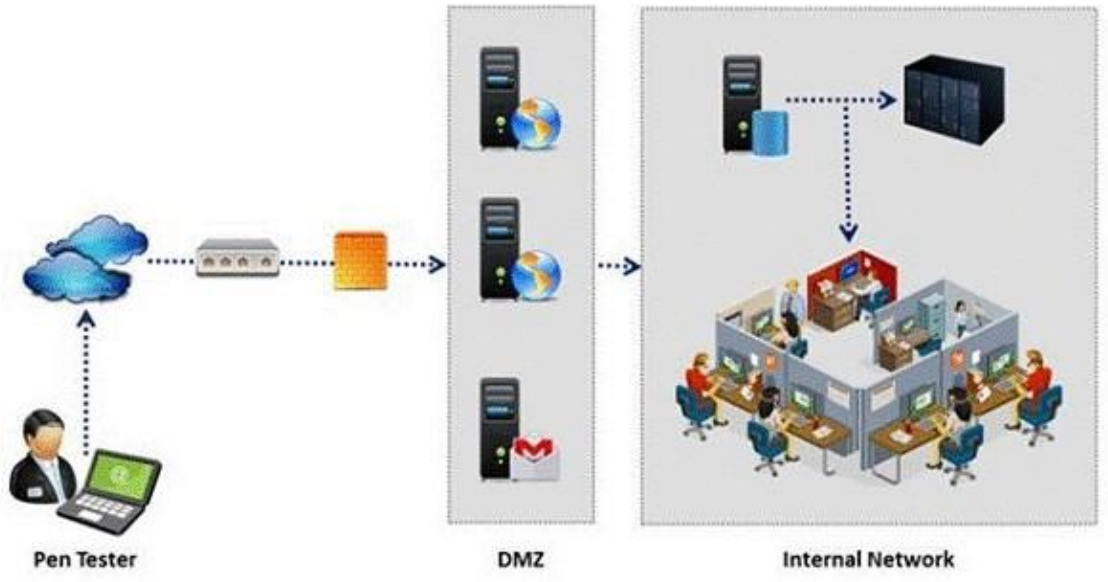
QUESTION 7
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is beingused?

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

Answer: B

QUESTION 8

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.

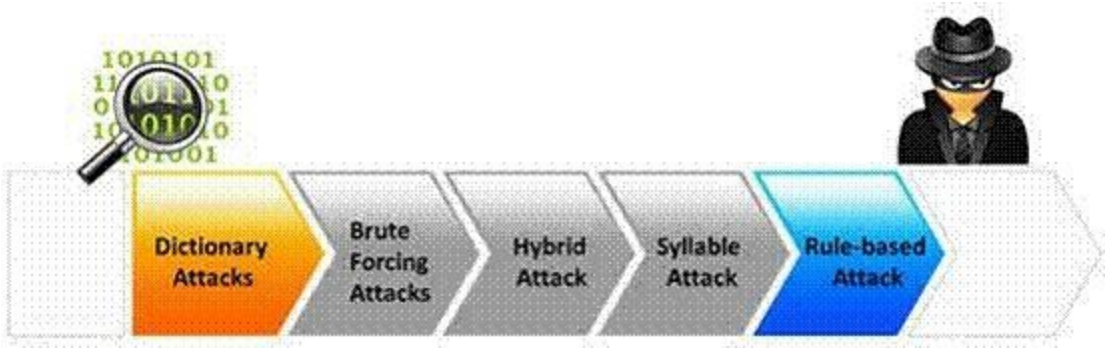


During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

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

Answer: B

QUESTION 9
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.

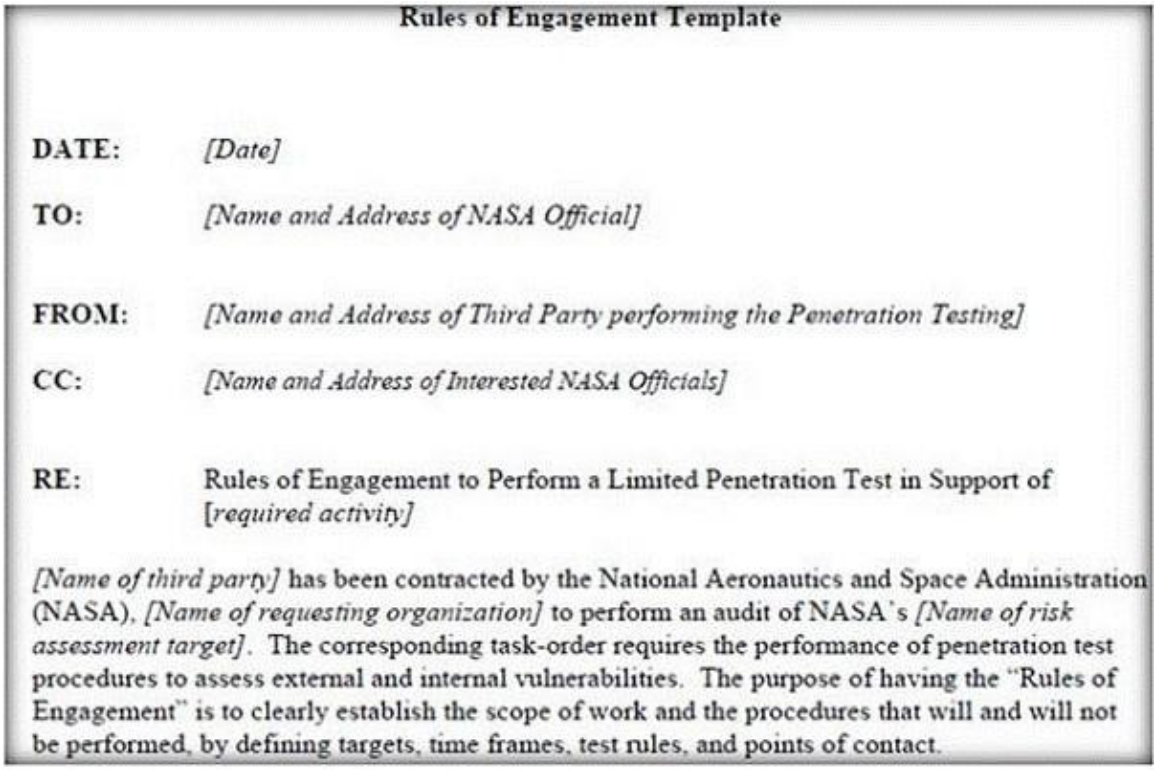


Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack
B. Rule-based attack
C. Hybrid attack
D. Dictionary attack

Answer: A

QUESTION 10
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: B

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014