EC-Council Certified Security Analyst

ECCouncil 412-79v8 Dumps Available Here at:

https://www.certification-questions.com/eccouncil-exam/412-79v8-dumps.html

Enrolling now you will get access to 200 questions in a unique set of 412-79v8 dumps

Question 1

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

Options:

A. Invalid username or password

B. Account username was not found

C. Incorrect password

D. Username or password incorrect

Answer: C

Question 2

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?

Options:

A. CTS

B. QRT

C. EMP

D. ABC

Answer: C

Question 3

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

Options:

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

Answer: B

Question 4

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

Options:

A. Required Work Efforts

B. References

C. Research

D. Glossary

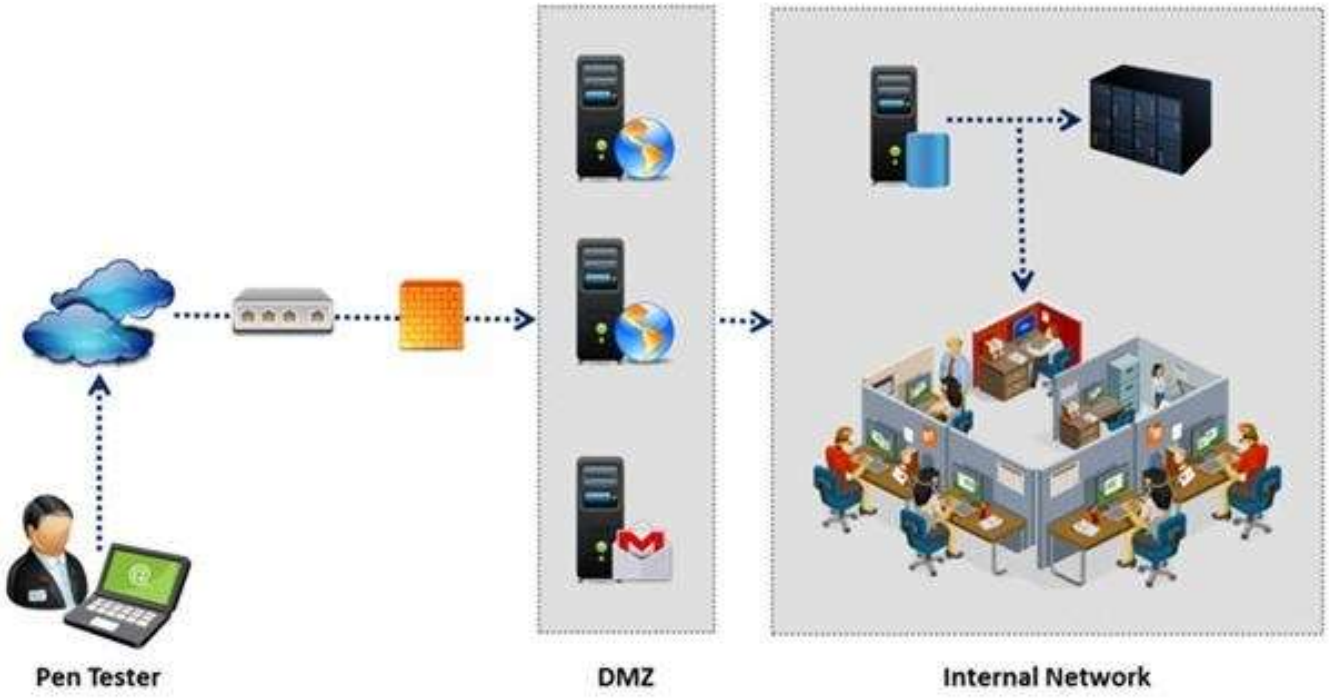
Answer: D

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

Question 5

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?

Options:

A. XMAS Scan

B. SYN scan

C. FIN Scan

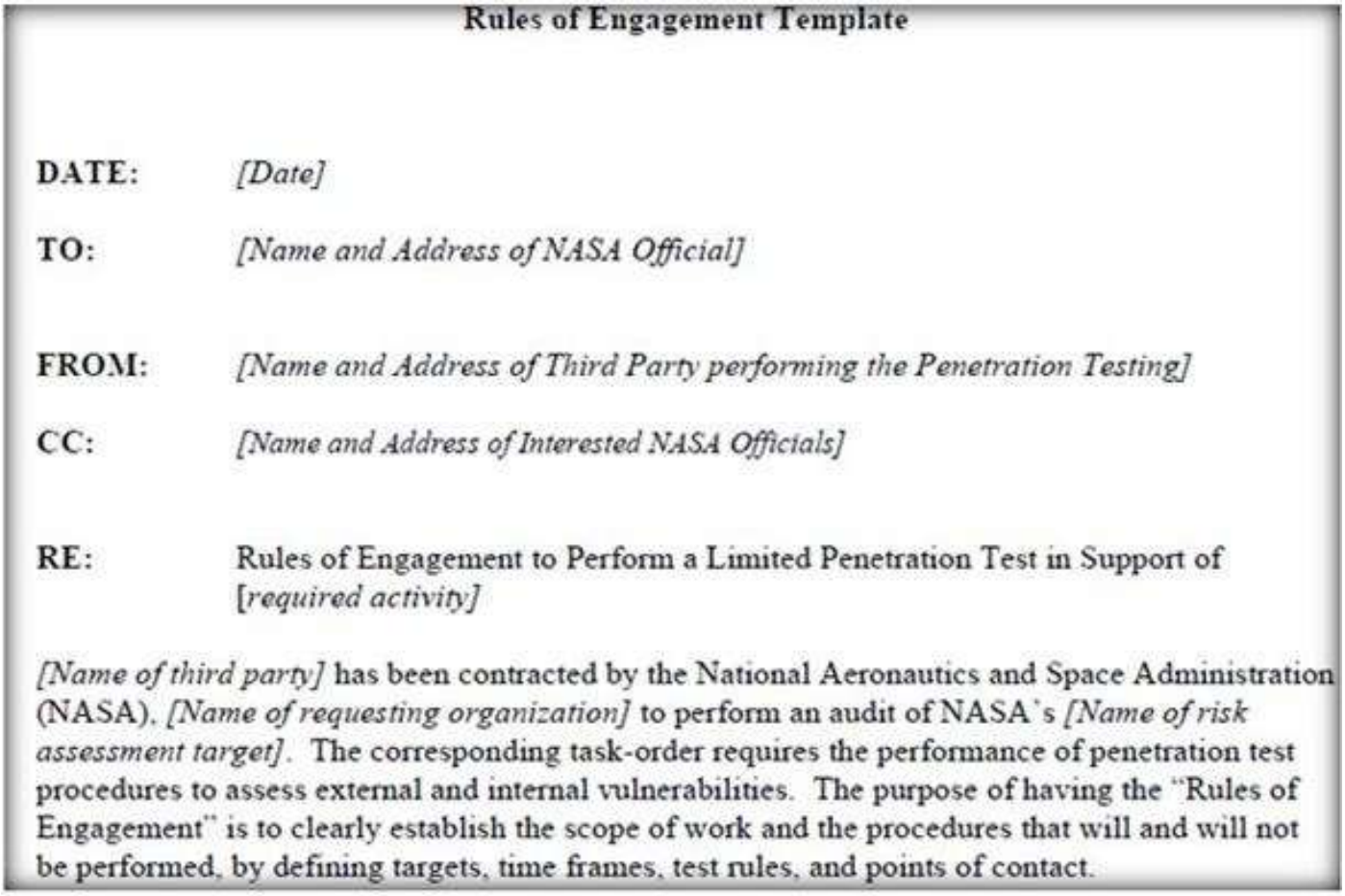
D. NULL Scan

Answer: B

Question 6

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?

Options:

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 7

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?

Options:

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 8

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?

Options:

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 9

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.

Options:

A. Web Penetration Testing

B. Functionality Testing

C. Authorization Testing

D. Source Code Review

Answer: D

Question 10

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

Options:

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

Would you like to see more? Don't miss our 412-79v8 PDF file at:

https://www.certification-questions.com/eccouncil-pdf/412-79v8-pdf.html