412-79V10 Q&As

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/412-79v10.html

100% Passing Guarantee
100% Money Back Assurance

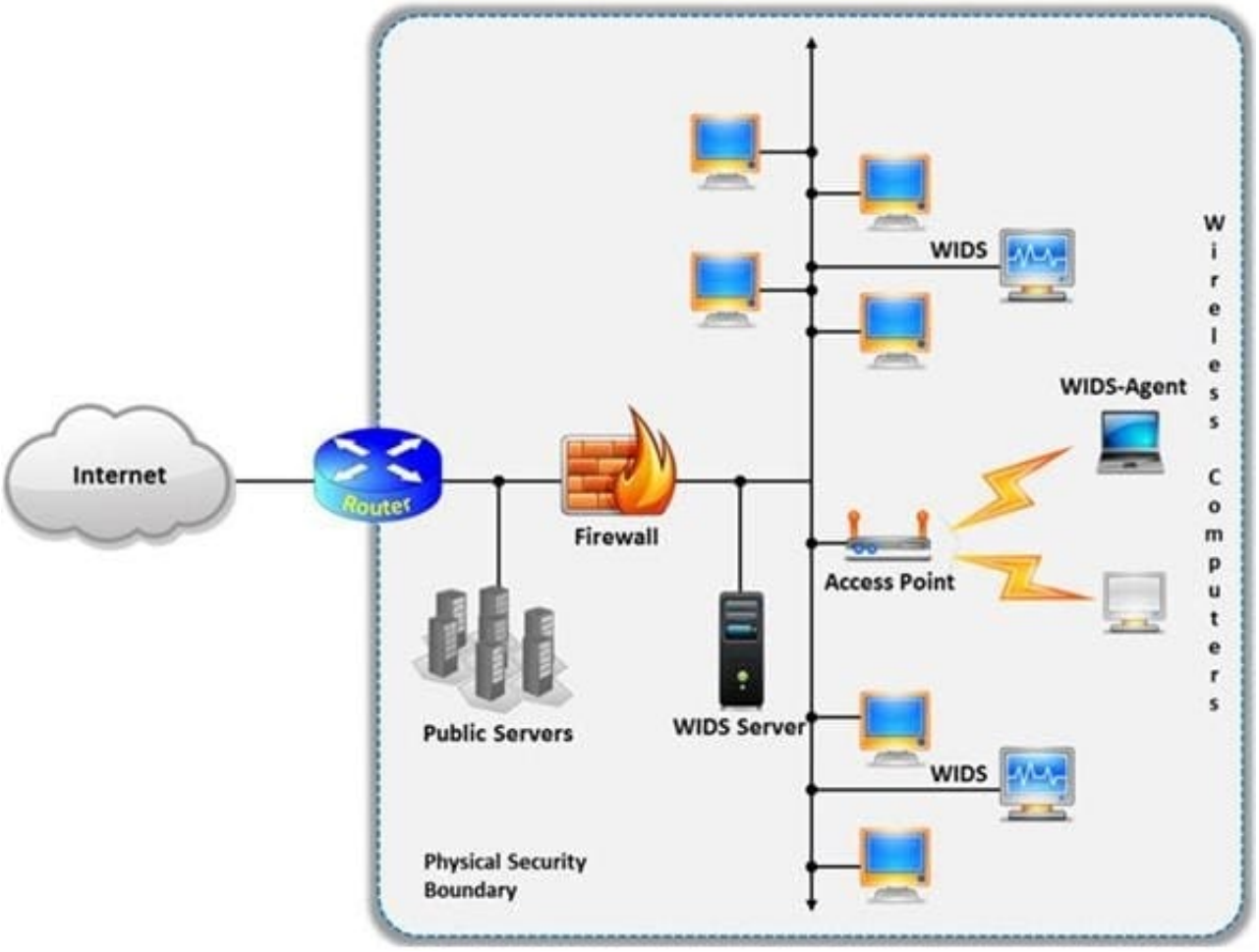
Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



A. Social engineering

B. SQL injection

C. Parameter tampering

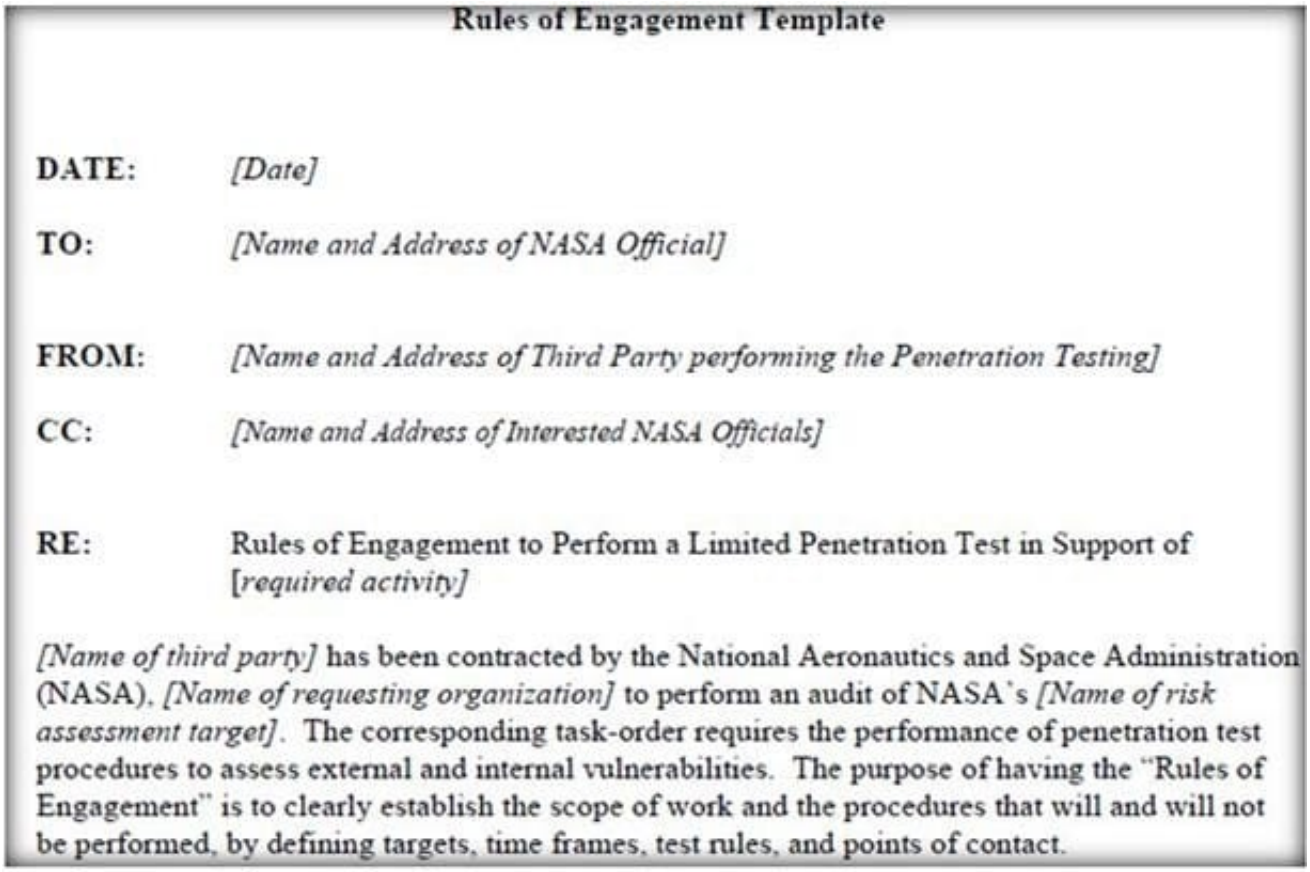
D. Man-in-the-middle attack

Correct Answer: D

Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 2

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

Correct Answer: C

QUESTION 3

What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes

B. Sort Server Includes

C. Server Sort Includes

D. Slide Server Includes

Correct Answer: A

QUESTION 4

In the example of a /etc/passwd file below, what does the bold letter string indicate?

nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid

B. Group number

C. GECOS information

D. User number

Correct Answer: D

QUESTION 5

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)

Correct Answer: A

QUESTION 6

Which of the following is not the SQL injection attack character?

A. $

B. PRINT

C. #

D. @@variable

Correct Answer: A

QUESTION 7

A firewall\\'s decision to forward or reject traffic in network filtering is dependent upon which of the following?

A. Destination address

B. Port numbers

C. Source address

D. Protocol used

Correct Answer: D

Reference: http://www.vicomsoft.com/learning-center/firewalls/ (what does a firewall do)

QUESTION 8

The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

A. Nortells Unified Security Framework

B. The IBM Security Framework

C. Bell Labs Network Security Framework

D. Microsoft Internet Security Framework

Correct Answer: C

QUESTION 9

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0-1023

Correct Answer: D

Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 10

Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash. Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.

Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.

Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.

Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

A. Clever Fuzz Testing

B. Dumb Fuzz Testing

C. Complete Fuzz Testing

D. Smart Fuzz Testing

Correct Answer: D

QUESTION 11

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

Correct Answer: A

QUESTION 12

Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

A. Sunbelt Network Security Inspector (SNSI)

B. CORE Impact

C. Canvas

D. Microsoft Baseline Security Analyzer (MBSA)

Correct Answer: C

QUESTION 13

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

Correct Answer: D

https://books.google.nl/books?id=0RfANAwOUdICandpg=PA720andlpg=PA720anddq=%22xx+no tation%22 +binaryandsource=blandots=pGMqass7tiandsig=rnIg1xZ78ScUvuIlTmDY3r7REucandhl= nlandsa=Xandei=8C4dVYe1NorgasrzgoALandved=0CEQQ6AEwBQ#v=onepageandq=%22xx%20n otation%22% 20binaryandf=false

QUESTION 14

Which one of the following acts related to the information security in the US fix the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

A. California SB 1386

B. Sarbanes-Oxley 2002

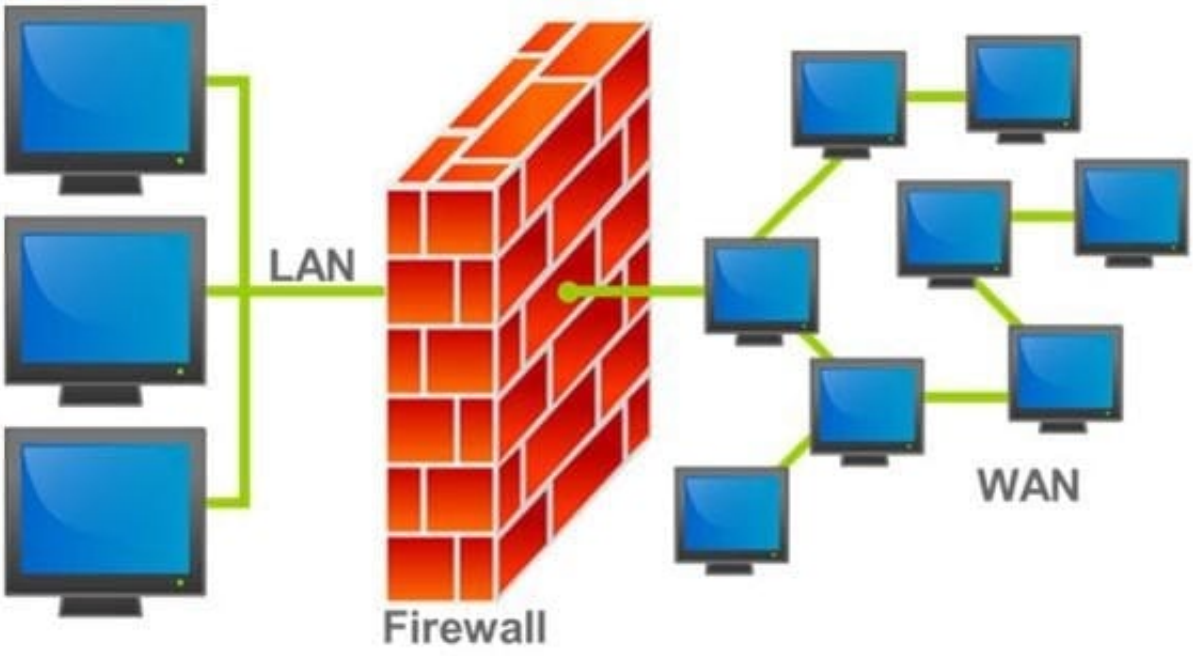
C. Gramm-Leach-Bliley Act (GLBA)

D. USA Patriot Act 2001

Correct Answer: B

QUESTION 15

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Appliance based firewalls cannot be upgraded

B. Firewalls implemented on a hardware firewall are highly scalable

C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D. Operating system firewalls are highly configured

Correct Answer: C