DUMPSQUEEN

EC-Council Certified Security Analyst (ECSA) V10

ECCouncil 412-79v10

Version Demo

Total Demo Questions: 9

Total Premium Questions: 201

Buy Premium PDF

QUESTION NO: 1

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame.

What ports should you open for SNMP to work through Firewalls. (Select 2)

A. 162

B. 160

C. 161

D. 163

ANSWER: A C

QUESTION NO: 2

DMZ is a network designed to give the public access to the specific internal resources and you might want to

do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories.

Identify the attacks that fall under Passive attacks category.

A. Wardriving

B. Spoofing

C. Sniffing

D. Network Hijacking

ANSWER: A

QUESTION NO: 3

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment

B. Host-based Assessment

C. External Assessment

D. Application Assessment

ANSWER: D

QUESTION NO: 4

You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources

B. Evaluating the existing perimeter and internal security

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

---

ANSWER: C

QUESTION NO: 5

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

ANSWER: D

QUESTION NO: 6

Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137

C. 137, 138, 139, 140

D. 133, 134, 139, 142

ANSWER: A

QUESTION NO: 7

Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization

B. Type of testers involved

C. The budget required

D. Expected time required to finish the project

ANSWER: A

QUESTION NO: 8

Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

ANSWER: A

QUESTION NO: 9

Which of the following acts related to information security in the US establish that the management of an organization is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

A. USA Patriot Act 2001

B. Sarbanes-Oxley 2002

C. Gramm-Leach-Bliley Act (GLBA)

D. California SB 1386

ANSWER: A