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.geekcert.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

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

Correct Answer: A

QUESTION 2

Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan

B. TCP Connect Scan

C. XMAS Scan

D. Null Scan

Correct Answer: A

QUESTION 3

Which one of the following log analysis tools is a Cisco Router Log Format log analyzer and it parses logs, imports them into a SQL database (or its own built-in database), aggregates them, and generates the dynamically filtered reports, all through a web interface?

A. Event Log Tracker

B. Sawmill

C. Syslog Manager

D. Event Log Explorer

Correct Answer: B

QUESTION 4

External penetration testing is a traditional approach to penetration testing and is more focused on the servers,

infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing

B. White box testing

C. Grey box testing

D. Black box testing

Correct Answer: D

Reference: http://books.google.com.pk/books?id=5m6ta2fgTswCandpg=SA5-PA4andlpg=SA5PA4anddq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+siteandsourc e=blandots=8GkmyUBH2Uandsig=wdBIboWxrhk5QjlQXs3yWOcuk2Qandhl=enandsa=Xandei=SgfVI2LLc3qaOa5gIgOandved=0CCkQ6AEwAQ#v=onepageandq=penetration%20testing%20i s% 20performed%20with%20no%20prior%20knowledge%20of%20the%20siteandf=false

QUESTION 5

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.

Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.

Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.

What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized

B. Send double quotes as the input data to catch instances where the user input is not sanitized

C. Send long strings of junk data, just as you would send strings to detect buffer overruns

D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D