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.leads4pass.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 policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy

B. Paranoid Policy

C. Promiscuous Policy

D. Prudent Policy

Correct Answer: B

QUESTION 2

Which one of the following log analysis tools is used for analyzing the server\\'s log files?

A. Performance Analysis of Logs tool

B. Network Sniffer Interface Test tool

C. Ka Log Analyzer tool

D. Event Log Tracker tool

Correct Answer: C

QUESTION 3

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 4

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)

B. HTTP (Hypertext Transfer Protocol)

C. SMTP (Simple Mail Transfer Protocol)

D. Telnet

Correct Answer: A

QUESTION 5

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime

B. Increases detection and reaction time

C. Increases response time

D. Both a and c

Correct Answer: A

Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection- systems (economic advantages, first para)

QUESTION 6

What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?

A. Connect Scanning Techniques

B. SYN Scanning Techniques

C. Stealth Scanning Techniques

D. Port Scanning Techniques

Correct Answer: C

Reference: http://wwww.pc-freak.net/tutorials/hacking_info/arkin%20network%20scanning% 20techniques.pdf (page 7

QUESTION 7

How many bits is Source Port Number in TCP Header packet?

A. 48

B. 32

C. 64

D. 16

Correct Answer: D

QUESTION 8

In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack

B. Authorization Attack

C. Authentication Attack

D. Frame Injection Attack

Correct Answer: B

Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

QUESTION 9

Which one of the following 802.11 types has WLAN as a network support?

A. 802.11b

B. 802.11-Legacy

C. 802.11n

D. 802.11g

Correct Answer: C

QUESTION 10

What is the maximum value of a "tinyint" field in most database systems?

A. 222

B. 224 or more

C. 240 or less

D. 225 or more

Correct Answer: D

Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJandpg=SA3-PA3andlpg=SA3PA3anddq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+databa se +systemsandsource=blandots=NscGk-R5randsig=1hMOYByxt7ebRJ4UEjbpxMijTQsandhl=enandsa=Xandei=pvgeVJnTCNDkaI_fgugOandved=0CDYQ6AEwAw#v=onepageandq=maximum%20value%20of%20a%20%E2%80%9Ctin yint%E2%80%9D%20field%20in%20most%20database%20systemsandf=false

QUESTION 11

Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks

B. To protect the confidentiality, integrity, and availability of data

C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms

D. To certify the accuracy of the reported financial statement

Correct Answer: A

Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

QUESTION 12

Which of the following information gathering techniques collects information from an organization\\'s web-based calendar and email services?

A. Anonymous Information Gathering

B. Private Information Gathering

C. Passive Information Gathering

D. Active Information Gathering

Correct Answer: D

Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

QUESTION 13

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

Correct Answer: C

QUESTION 14

Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump

B. Capinfos

C. Tshark

D. Idl2wrs

Correct Answer: B

QUESTION 15

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack

B. Insecure cryptographic storage attack

C. Hidden field manipulation attack

D. Man-in-the-Middle attack

Correct Answer: B