412-79 Q&As

EC-Council Certified Security Analyst (ECSA)

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

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

https://www.geekcert.com/412-79.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

At what layer of the OSI model do routers function on?

A. 5

B. 1

C. 4

D. 3

Correct Answer: D

QUESTION 2

Sectors in hard disks typically contain how many bytes?

A. 256

B. 512

C. 1024

D. 2048

Correct Answer: B

QUESTION 3

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expecteD.

A. Hard Drive Failure

B. Scope Creep

C. Unauthorized expenses

D. Overzealous marketing

Correct Answer: B

QUESTION 4

The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. (Note: The objective of this question is to test whether the student can

read basic information from log entries and interpret the nature of attack.) Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]:

IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version- query: 212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:

194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07

[5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:

198.173.35.164:4221 -> 172.16.1.107:80 Apr 26

05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb [12509]: (login) session opened for

user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[12521]:

(su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:

24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect:

172.16.1.107:23

-> 213.28.22.189:4558 From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A.

An IDS evasion technique

B.

A buffer overflow attempt

C.

A DNS zone transfer

D.

Data being retrieved from 63.226.81.13

Correct Answer: A

QUESTION 5

What will the following command produce on a website login page?What will the following command produce on a website? login page?

SELECT email, passwd, login_id, full_name FROM members WHERE email = \\'someone@somehwere.com\\'; DROP TABLE members; --\\'

A. This command will not produce anything since the syntax is incorrect

B. Inserts the Error! Reference source not found. email address into the members table

C. Retrieves the password for the first user in the members table

D. Deletes the entire members table

Correct Answer: D