



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.pass4itsure.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**

While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?

- A. Keep the information of file for later review
- B. Destroy the evidence
- C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
- D. Present the evidence to the defense attorney

Correct Answer: C

QUESTION 2

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

- A. Circuit-level proxy firewall
- B. Packet filtering firewall
- C. Application-level proxy firewall
- D. Statefull firewall

Correct Answer: D

QUESTION 3

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

**QUESTION 4**

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. 163
- D. 161

Correct Answer: AD

QUESTION 5

What does the superblock in Linux define?

- A. filesynames
- B. diskgeometr
- C. location of the firstinode
- D. available space

Correct Answer: C

QUESTION 6

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

- A. Stringsearch
- B. grep
- C. dir
- D. vim

Correct Answer: B

QUESTION 7

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?



- A. IPSEC does not work with packet filtering firewalls
- B. NAT does not work with IPSEC
- C. NAT does not work with statefull firewalls
- D. Statefull firewalls do not work with packet filtering firewalls

Correct Answer: B

QUESTION 8

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded

sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

- A. Intruding into a honeypot is not illegal
- B. Entrapment
- C. Intruding into a DMZ is not illegal
- D. Enticement

Correct Answer: B

QUESTION 9

E-mail logs contain which of the following information to help you in your investigation? (Select up to 4)

- A. user account that was used to send the account
- B. attachments sent with the e-mail message
- C. unique message identifier
- D. contents of the e-mail message
- E. date and time the message was sent

Correct Answer: ACDE

QUESTION 10

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not



give a response. In what state are these ports?

- A. Open
- B. Stealth
- C. Closed
- D. Filtered

Correct Answer: A

QUESTION 11

Study the log given below and answer the following question: 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 Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A.
Disallow UDP53 in from outside to DNS server
- B.
Allow UDP53 in from DNS server to outside
- C.



Disallow TCP53 in from secondaries or ISP server to DNS server

D.

Block all UDP traffic

Correct Answer: A

QUESTION 12

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

- A. Change the default community string names
- B. Block all internal MAC address from using SNMP
- C. Block access to UDP port 171
- D. Block access to TCP port 171

Correct Answer: A

QUESTION 13

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

- A. bench warrant
- B. wire tap
- C. subpoena
- D. search warrant

Correct Answer: D

QUESTION 14

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Ping trace
- B. Tracert



C. Smurf scan

D. ICMP ping sweep

Correct Answer: D

QUESTION 15

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case.

B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.

C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.

D. All forms should be placed in the report file because they are now primary evidence in the case.

Correct Answer: B

[412-79 PDF Dumps](#)

[412-79 Practice Test](#)

[412-79 Braindumps](#)