DUMPS ARENA

Computer Hacking Forensic Investigator

ECCouncil 312-49

Version Demo

Total Demo Questions: 12

Total Premium Questions: 531

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

dumpsarena.com

QUESTION NO: 1

Which of the following is NOT a part of pre-investigation phase?

A. Building forensics workstation

B. Gathering information about the incident

C. Gathering evidence data

D. Creating an investigation team

ANSWER: C

QUESTION NO: 2

Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

A. Tokenmon

B. PSLoggedon

C. TCPView

D. Process Monitor

ANSWER: B

QUESTION NO: 3

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

A. Equipment Identity Register (EIR)

B. Electronic Serial Number (ESN)

C. International mobile subscriber identity (IMSI)

D. Integrated circuit card identifier (ICCID)

ANSWER: B

QUESTION NO: 4

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

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

ANSWER: A C D E

QUESTION NO: 5

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort

B. Snort

C. Ettercap

D. RaidSniff

ANSWER: C

QUESTION NO: 6

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto

C. Snort

D. Kismet

ANSWER: C

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? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

A. Email spamming

B. Phishing

C. Email spoofing

D. Mail bombing

ANSWER: D

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

A. Security event was monitored but not stopped

B. Malicious URL detected

C. An email marked as potential spam

D. Connection rejected

ANSWER: C

QUESTION NO: 10

Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

A. Witness Authentication

B. Direct Examination

C. Expert Witness

D. Cross Questioning

ANSWER: B

QUESTION NO: 11

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. Windows 98

B. Linux

C. Windows 8.1

D. Windows XP

ANSWER: D

QUESTION NO: 12

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

A. Web bugs

B. Cross site scripting

C. Hidden fields

D. SQL injection is possible

ANSWER: D