IISFA II0-001 CIFI Practice Questions

Shared by Clarke on 29-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which one of the following is NOT true?

Options:

A- IDS' can generate numerous alerts when not configured correctly
B- False positives alerts make it very difficult to find the real attack
C- Automated responses to alerts must be considered
D- IDS can never be used in a switched environment

Answer:

D

Question 2

Question Type: MultipleChoice

The MBR is easily identified on a Windows XP system by:

Options:

A- It's records in the MFT
B- It begins at offset 0000
C- It is labeled in binary 0A0A0A08
D- Is it not located in the system, but in the CMOS of the host machine

Answer:

B

Question 3

Question Type: MultipleChoice

Why is securing the crime scene critical in the earliest portions of the investigation in order to:

Options:

A- Assess damage in the triage phase
B- To preserve evidence
C- Secure the crime scene
D- This law only dealt with the legality of collecting evidence on foreign soil for domestic investigation of foreign power espionage by federal agencies.

Answer:

B

P2P exams

Question 4

Question Type: MultipleChoice

Stone stepping or server hopping is the technique of hackers to mask their source identity.

Options:

A- True
B- False

Answer:

A

P2P exams

Question 5

Question Type: MultipleChoice

Trojan Horse programs are capable of the following except

Options:

A- Remotely viewing of target system's screen output
B- Modifying files
C- Opening a CDROM drive
D- Viewing webcam installed

E- Keylogging
F- All of the above are possible

Answer:

F

Question 6

Question Type: MultipleChoice

Which email protocol provides remote filing capabilities?

Options:

A- POP3
B- IMAP
C- SNMP
D- SMTP

Answer:

B

Question 7

Question Type: MultipleChoice

Which option best is not an internet email protocol?

Options:

A- SMTP
B- POP3
C- IMAP
D- SNMP

Answer:

D

Question 8

Question Type: MultipleChoice

All are common email headers except?

Options:

A- Bcc
B- X-Receiver
C- Errors-To
D- Mime-Version

Answer:

B

Question 9

Question Type: MultipleChoice

The result of an attack Traceback can be characterized by these three parameters, the degree of which determines success:

Options:

A- confidentiality, integrity, and availability
B- precision, integrity, and timeliness
C- confidentiality, integrity, and accuracy
D- precision, accuracy, and timeliness

Answer:

D

Question 10

Question Type: MultipleChoice

In order to access a desktop computer for a forensics investigation that has a BIOS boot password enabled, which of the following is not a technique to over-ride the password:

Options:

A- Remove the CMOS Battery to reset the password
B- Short the jumper block labeled 'PWD'
C- 'Flash' the BIOS with an update from the manufacturer.
D- Give the Federal Bureau of Investigation jurisdiction to investigate computer crime.

Answer:

D

P2P exams

Question 11

Question Type: MultipleChoice

The following graphic is an example of what tool?

Options:

A- Traceroute tool
B- GPS to IP correlation tool
C- Geosynchronous imaging location
D- Footprinting tool

Answer:

A

P2P exams

Question 12

Question Type: MultipleChoice

How many port/services are available using the TCP/IP suite?

Options:

A- 6,553
B- unlimited
C- 65,535
D- 65,353

Answer:

C

Question 13

Question Type: MultipleChoice

All of the following are critical in the first stages of an investigation except:

Options:

A- Document the scene thoroughly
B- Protect perishable data
C- Secure the crime scene
D- Detain suspects

Answer:

D

To Get Premium Files for II0-001 Visit

https://www.p2pexams.com/products/ii0-001

For More Free Questions Visit

https://www.p2pexams.com/iisfa/pdf/ii0-001

