Free Questions for II0-001 by go4braindumps

Shared by Wright on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

It is possible to place IDS in a switched environment effectively with the use of a Spanning Port

Options:

A- True

B- False

Answer:

A

Question 2

Question Type: MultipleChoice

Slack space is the space in a file cluster that is not actively used by the file.

Options:

A- True

B- False

Answer:

A

Question 3

Question Type: **MultipleChoice**

Free space is unallocated file space within a partition.

Options:

A- True

B- False

Answer:

A

Question 4

Question Type: MultipleChoice

Slack space is space not used within a partition of a hard drive.

Options:

A- True

B- False

Answer:

B

Question 5

Question Type: MultipleChoice

For proper investigative methods to be valid, they must:

Options:

A- Be a standard method

B- Be replicatable

C- Adhere to best practice

D- All of the above

Answer:

B

Question 6

Question Type: **MultipleChoice**

All of the following are states a file cluster can exist in an Microsoft XP operating system except:

Options:

A- Allocated

B- Unallocated

C- Inode cluster fragment

D- Allocated deleted

Answer:

C

Question 7

Question Type: MultipleChoice

Training employees on Incident Response Teams authority is critical because:

Options:

A- They will need cooperation during an incident.

B- There is no other executive trained on incidents.

C- According to law, jurisdiction must be granted by local authorities.

D- Federal law prohibits any authority granting.

Answer:

A

Question 8

Question Type: MultipleChoice

An event is considered an incident when it meets or exceed which standard?

Options:

A- ISO7799

B- ISO17799

C- BS7799

D- None of the above

Answer:

D

Question 9

Question Type: MultipleChoice

Which of the following is a challenge for performing a Trace back?

Options:

A- Dynamic IP Addresses

B- Spoofing

C- Server Hopping

D- All of the above

Answer:

D

Question 10

Question Type: MultipleChoice

Host based intrusion devices traditionally analyze log files for:

Options:

A- Anomalies in the application operations that may suggest a compromise or a repetitive attack.

B- Network traffic

C- Distributed Denial of Service Attacks

D- System hardware or software errors

Answer:

A

Question 11

Question Type: MultipleChoice

Foot printing is the process of accumulating data on a _____ host system.

Options:

A- Attack Source

B- Attack target

C- Attack intermediary

D- Dark Network

Answer:

A

Question 12

Question Type: **MultipleChoice**

The following are detective controls for a malicious attack except:

Options:

A- Network Intrusion Detection

B- CCTV

C- Electronic Frontier Firewall

D- Tripwire

Answer:

C