DUMPSARENA

GIAC Security Essentials

GIAC GSEC

Version Demo

Total Demo Questions: 15

Total Premium Questions: 279

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment

B. Business Impact Analysis

C. Disaster Recovery Planning

D. Lessons Learned

ANSWER: B

QUESTION NO: 2

Which of the following items are examples of preventive physical controls? Each correct answer represents a complete solution. Choose three.

A. Biometric access controls

B. Closed-circuit television monitors

C. Fire extinguishers

D. Locks and keys

ANSWER: A C D

QUESTION NO: 3

Which of the following are network connectivity devices?

Each correct answer represents a complete solution. Choose all that apply.

A. Network analyzer

B. Bridge

C. Brouter

D. Firewall

E. Repeater

F. Hub

ANSWER: B C E F

QUESTION NO: 4

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?

Each correct answer represents a complete solution. Choose all that apply.

A. rm private.txt #11 Nov 2009 02:59:58 am

B. touch -d "11 Nov 2009 02:59:58 am" private.txt

C. touch private.txt #11 Nov 2009 02:59:58 am

D. touch -t 200911110259.58 private.txt

ANSWER: B D

QUESTION NO: 5

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.

What will be the key functions of the sensors in such a physical layout?

Each correct answer represents a complete solution. Choose all that apply.

A. To collect data from operating system logs

B. To notify the console with an alert if any intrusion is detected

C. To analyze for known signatures

D. To collect data from Web servers

ANSWER: B C

QUESTION NO: 6

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as.

A. False negative

B. False positive

C. True positive

D. True negative

ANSWER: B

QUESTION NO: 7

Which Linux file lists every process that starts at boot time?

A. inetd

B. netsrv

C. initd

D. inittab

ANSWER: D

QUESTION NO: 8

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.

B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.

C. Take photographs of all persons who have had access to the computer.

D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.

ANSWER: D

QUESTION NO: 9

A folder D:\Files\Marketing has the following NTFS permissions:

• Administrators: Full Control

• Marketing: Change and Authenticated

• Users: Read

It has been shared on the server as "MARKETING", with the following share permissions:

• Full Control share permissions for the Marketing group

Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

A. No access

B. Full Control

C. Read

D. Change

ANSWER: C

QUESTION NO: 10

Which of the following are the types of intrusion detection systems?

Each correct answer represents a complete solution. Choose all that apply.

A. Host-based intrusion detection system (HIDS)

B. Client-based intrusion detection system (CIDS)

C. Server-based intrusion detection system (SIDS)

D. Network intrusion detection system (NIDS)

ANSWER: A D

QUESTION NO: 11

What file instructs programs like Web spiders NOT to search certain areas of a site?

A. Robots.txt

B. Restricted.txt

C. Spider.txt

D. Search.txt

ANSWER: A

QUESTION NO: 12

Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

A. Anonymous authentication

B. Mutual authentication

C. Open system authentication

D. Shared key authentication

ANSWER: C D

QUESTION NO: 13

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?

Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption

B. Ease of maintenance

C. Load balancing

D. Failover

ANSWER: C D

QUESTION NO: 14

Your IT security team is responding to a denial of service attack against your server. They have taken measures to block offending IP addresses. Which type of threat control is this?

A. Detective

B. Preventive

C. Responsive

D. Corrective

ANSWER: D

QUESTION NO: 15

Which of the below choices should an organization start with when implementing an effective risk management process?

A. Implement an incident response plan

B. Define security policy requirements

C. Conduct periodic reviews

D. Design controls and develop standards for each technology you plan to deploy

ANSWER: B