ISLEVER

1D0-570

CIW v5 Security Professional Exam

DEMO

https://www.islever.com/1d0-570.html

https://www.islever.com/ciw.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

The chief operations officer (COO) has questioned the need for end-user training. Which of the following is the most effective response?

A. Indicate that you will not be responsible for the next virus outbreak.
B. Remind the CEO about the last virus attack and the expense incurred.
C. Explain that the cost of end-user training is a fraction of the cost of the last security breach caused by end users.
D. Provide statistics that definitively show how end-user training reduces the likelihood of security breaches on the corporate network.

Answer: C
Explanation:

QUESTION NO: 2

You want to learn more about a security breach that was recently discovered in a Windows server. Which organization should you consult?

A. ISO
B. SANS
C. CERT
D. IETF

Answer: C
Explanation:

QUESTION NO: 3

In a Linux system, which command can be used to view the activities of a user who has logged in to an account?

A. Vnc
B. Who
C. Monitor
D. Console chars

Answer: A
Explanation:

QUESTION NO: 4

Which resource contains settings that you can modify to activate and deactivate network services in a Windows XP system?

A. Ntldr
B. The registry
C. Pagefile.sys
D. The Windows/tmp/ directory

Answer: B
Explanation:

QUESTION NO: 5

An unauthorized user has overwritten a router's configuration. After being caught, the user indicated that he was able to obtain the password by sniffing the router's network communications. Which service was exploited?

A. Tftp
B. IOS
C. Old firmware
D. The enable command

Answer: A
Explanation:

QUESTION NO: 6

A compromised system was given to your IT administrator for storage until police can investigate the system further. Which of the following will police and other legal personnel expect from the IT administrator in order for this system to be considered valid evidence?

A. A chain of custody
B. A parked hard drive
C. A mirrored hard drive
D. A summary of events

Answer: A
Explanation:

QUESTION NO: 7

After a system has been compromised, which activity is expected if you plan to analyze the system for a legal investigation?

A. Keeping the system in the production environment until analysis is required
B. Removing the system immediately from the production environment
C. Keeping the system RAM in a separate environment
D. Removing the hard drive

Answer: B
Explanation:

QUESTION NO: 8

A malicious user has deleted essential files from a Web server during a system compromise. The affected Linux system does not have an undelete utility. A systems expert has been able to recover this file. What was the systems expert able to find in order to initiate the recovery process?

A. The in ode of the deleted file
B .The name of the deleted file
B. The permissions of the deleted file
C. The linked library of the deleted file

Answer: A
Explanation:

QUESTION NO: 9

Which of the following best describes the executive summary in a forensic report?

A. A list of forensic tasks assigned to managers
B. A simple, short overview of the report's findings
C. A simple, short overview of the tools used to investigate the system
D. One or two small charts or graphs, accompanied by a report of the tools used to investigate the system

Answer: B
Explanation:

QUESTION NO: 10