1D0-570
CIW v5 Security Professional Exam

Version 14.5

1D0-570

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

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

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

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

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

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

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

1D0-570

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
C. The permissions of the deleted file
D. The linked library of the deleted file

Answer: A

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

QUESTION NO: 10

Which of the following is a common element of a penetration test?

A. A DOS attack
B. A DDOS attack
C. Scanning the firewall
D. Scanning internal network hosts

Answer: C

QUESTION NO: 11

An attacker has just installed a root kit on a system. Which of the following stages of the hacker process has this hacker completed?

A. Attack
B. Control
C. Discovery
D. Penetration

Answer: B

QUESTION NO: 12

A systems administrator discovered that her system's log files have been tampered with. Which stage of the hacker process does this discovery indicate?

A. Control
B. Discovery
C. Penetration
D. Spreading to other systems

Answer: A

QUESTION NO: 13

Your supervisor asks you to recommend a firewall. The firewall must provide the following services: The ability to filter specific traffic types (e.g., HTTP, SIP, POP3) User authentication Web page caching for later use which type of firewall would you recommend?

A. Proxy
B. Stateful
C. Packet filter
D. Circuit-based

Answer: A

QUESTION NO: 14

Which of the following is a common way for an attacker to spread from one compromised system to another?

A. DOS attack
B. Dictionary attack
C. Trust relationship
D. Brute-force attack

Answer: C

QUESTION NO: 15

Which of the following describes the goal of a gap analysis?

A. To eliminate threats that exists on the network
B. To show the status of existing security practices at the firewall
C. To create a baseline of activity on the network and for the local host
D. To show the difference between planned security and actual practice

Answer: D

QUESTION NO: 16

Which information would a chief executive officer (CEO) want to know in relation to a gap analysis?

A. Details concerning the security infrastructure
B. Information about issues that affect shareholders
C. A broad overview of the security issues faced by the security team
D. The cost of software and devices required to provide security for the network

Answer: B

QUESTION NO: 17

Your supervisor has asked you to conduct an audit of the Human Resources department's desktop systems. Which consideration is most important when preparing for the audit?

A. The names of any employees who are on vacation
B. The importance of the data held in the desktop systems
C. Whether the Human Resources department employees are currently distracted by any new or unusual projects
D. The number of employees who have worked in the Human Resources department within the last six months

Answer: C

QUESTION NO: 18

Which tool can best help you determine if a denial-of-service attack is underway?

A. A system that has SNMP enabled
B. Intrusion-detection software
C. The /var/log/messages file
D. Event Viewer

Answer: B