**Vendor:** CIW

**Exam Code:** 1D0-571

**Exam Name:** CIW v5 Security Essentials

**Version:** Demo

**QUESTION 1**
An application is creating hashes of each file on an attached storage device. Which of the following will typically occur during this process?

A. An increase in the amount of time it takes for the system to respond to requests
B. Reduced risk of an attack
C. Increased risk of an attack
D. A reduction in the amount of time it takes for the system to respond to requests

**Correct Answer:** A

**QUESTION 2**
You have been assigned to configure a DMZ that uses multiple firewall components. Specifically, you must configure a router that will authoritatively monitor and, if necessary, block traffic. This device will be the last one that inspects traffic before it passes to the internal network. Which term best describes this device?

A. Screening router
B. Bastion host
C. Proxy server
D. Choke router

**Correct Answer:** D

**QUESTION 3**
A distributed denial-of-service (DDOS) attack has occurred where both ICMP and TCP packets have crashed the company's Web server. Which of the following techniques will best help reduce the severity of this attack?

A. Filtering traffic at the firewall
B. Changing your ISP
C. Installing Apache Server rather than Microsoft IIS
D. Placing the database and the Web server on separate systems

**Correct Answer:** A

**QUESTION 4**
Which of the following is considered to be the most secure default firewall policy, yet usually causes the most work from an administrative perspective?

A. Configuring the firewall to respond automatically to threats
B. Blocking all access by default, then allowing only necessary connections
C. Configuring the firewall to coordinate with the intrusion-detection system
D. Allowing all access by default, then blocking only suspect network connections

**Correct Answer:** B

**QUESTION 5**
Which of the following is most likely to pose a security threat to a Web server?

A. CGI scripts
B. Database connections
C. Flash or Silverlight animation files
D. LDAP servers

**Correct Answer:** A

**QUESTION 6**
What is the first tool needed to create a secure networking environment?

A. User authentication
B. Confidentiality
C. Security policy
D. Auditing

**Correct Answer:** C

**QUESTION 7**
Irina has contracted with a company to provide Web design consulting services. The company has asked her to use several large files available via an HTTP server. The IT department has provided Irina with user name and password, as well as the DNS name of the HTTP server. She then used this information to obtain the files she needs to complete her task using Mozilla Firefox. Which of the following is a primary risk factor when authenticating with a standard HTTP server?

A. HTTP usescleartext transmission during authentication, which can lead to a man-in-the- middle attack.
B. Irina has used the wrong application for this protocol, thus increasing the likelihood of a man-in- the-middle attack.
C. A standard HTTP connection uses public-key encryption that is not sufficiently strong, inviting the possibility of a man-in-the-middle attack.
D. Irina has accessed the Web server using a non-standard Web browser.

**Correct Answer:** A

**QUESTION 8**
Requests for Web-based resources have become unacceptably slow. You have been assigned to implement a solution that helps solve this problem. Which of the following would you recommend?

A. Enablestateful multi-layer inspection on the packet filter
B. Implement caching on the network proxy server
C. Enable authentication on the network proxy server
D. Implement a screening router on the network DMZ

**Correct Answer:** B

**QUESTION 9**
You have discovered that the ls, su and ps commands no longer function as expected. They do not return information in a manner similar to any other Linux system. Also, the implementation of Tripwire you have installed on this server is returning new hash values. Which of the following has most likely occurred?

A. Atrojan has attacked the system.
B. A SQL injection attack has occurred.
C. A spyware application has been installed. D.
A root kit has been installed on the system.

**Correct Answer:**

**QUESTION 10**
Which of the following organizations provides regular updates concerning security breaches and issues?

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

**Correct Answer:** D

**QUESTION 11**
You have been asked to encrypt a large file using a secure encryption algorithm so you can send it via e-mail to your supervisor. Encryption speed is important. The key will not be transmitted across a network. Which form of encryption should you use?

A. Asymmetric
B. PGP
C. Hash
D. Symmetric

**Correct Answer:** D

**QUESTION 12**
Which of the following is the most likely first step to enable a server to recover from a denial-of- service attack in which all hard disk data is lost?

A. Enable virtualization
B. Contact the backup service
C. Contact a disk recovery service
D. Rebuild your RAID 0 array

**Correct Answer:** B

**QUESTION 13**
You purchased a network scanner six months ago. In spite of regularly conducting scans using this software, you have noticed that attackers have been able to compromise your servers over the last month. Which of the following is the most likely explanation for this problem?

A. The network scanner needs to be replaced.
B. The network scanner is no substitute for scans conducted by an individual.
C. The network scanner has atrojan.
D. The network scanner needs an update.

**Correct Answer:** D

**QUESTION 14**
What is the primary use of hash (one-way) encryption in networking?

A. Signing files, for data integrity
B. Encrypting files, for data confidentiality
C. Key exchange, for user authentication
D. User authentication, for non-repudiation

**Correct Answer:** A

**QUESTION 15**
Which of the following will best help you ensure a database server can withstand a recently discovered vulnerability?

A. Updating the company vulnerability scanner and conducting a new scan
B. Adding a buffer overflow rule to the intrusion detection system
C. Reconfiguring the firewall
D. Installing a system update

**Correct Answer:** D

**QUESTION 16**

You have determined that the company Web server has several vulnerabilities, including a buffer overflow that has resulted in an attack. The Web server uses PHP and has direct connections to an Oracle database server. It also uses many CGI scripts. Which of the following is the most effective way to respond to this attack?

A. Installing software updates for the Web server daemon
B. Using the POST method instead of the GET method for a Web form
C. Installing an intrusion detection service to monitor logins
D. Using the GET method instead of the POST method for a Web form

**Correct Answer:** A

**QUESTION 17**
Which of the following standards is used for digital certificates?

A. DES
B. Diffie-Hellman
C. X.509
D. RC5

**Correct Answer:** C

**QUESTION 18**
At the beginning of an IPsec session, which activity occurs during the Internet Key Exchange (IKE)?

A. Determining the number of security associations
B. Negotiating the authentication method
C. Determining the network identification number
D. Negotiating the version of IP to be used

**Correct Answer:** B

**QUESTION 19**
A security breach has occurred in which a third party was able to obtain and misuse legitimate authentication information. After investigation, you determined that the specific cause for the breach was that end users have been placing their passwords underneath their keyboards. Which step will best help you resolve this problem?

A. Discipline specific end users as object lessons to the rest of the staff and reset passwords on all systems immediately.
B. Change all passwords on the company servers immediately and inform end users that their passwords will be changing on a regular basis.
C. Set passwords to expire at specific intervals and establish mandatory continual training sessions.
D. Inform end users that their passwords will be changing on a regular basis and require more complex passwords.

**Correct Answer:** C

**QUESTION 20**
You have implemented a version of the Kerberos protocol for your network. What service does Kerberos primarily offer?

A. Authentication
B. Encryption
C. Non-repudiation
D. Data integrity

**Correct Answer:** A

**QUESTION 21**
Consider the following series of commands from a Linux system: iptables -A input -p icmp -s 0/0 璥 0/0 -j REJECT Which explanation best describes the impact of the resulting firewall ruleset?

A. Individuals on remote networks will no longer be able to use SSH to control internal network resources.
B. Internal hosts will not be able to ping each other using ICMP.
C. Stateful multi-layer inspection has been enabled.
D. Individuals on remote networks will not be able to use ping to troubleshoot connections.

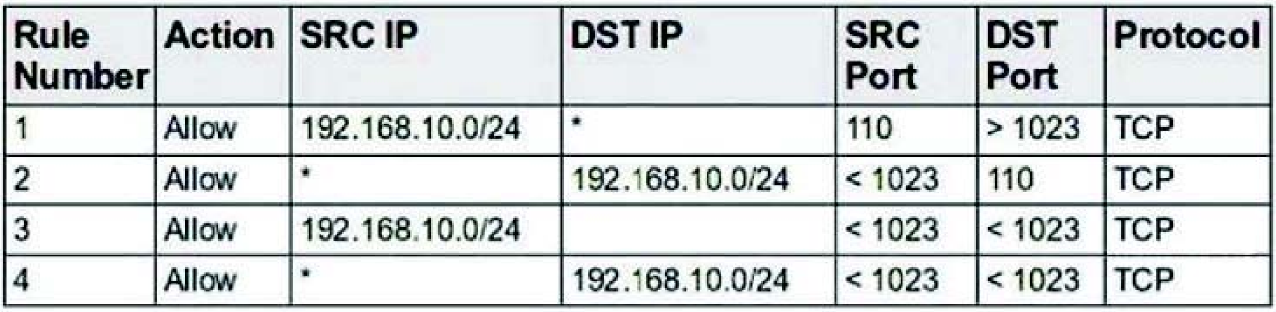
**Correct Answer:** D

**QUESTION 22**
A CGI application on the company's Web server has a bug written into it. This particular bug allows the application to write data into an area of memory that has not been properly allocated to the application. An attacker has created an application that takes advantage of this bug to obtain credit card information. Which of the following security threats is the attacker exploiting, and what can be done to solve the problem?

A. - Buffer overflow - Work with the Web developer to solve the problem
B. - SQL injection - Work with a database administrator to solve the problem
C. - Denial of service - Contact the organization that wrote the code for the Web server
D. - Man-in-the-middle attack - Contact the company auditor

**Correct Answer:** A

**QUESTION 23**
A new server has been placed on the network. You have been assigned to protect this server using a packet-filtering firewall. To comply with this request, you have enabled the following ruleset:



| Rule Number | Action | SRC IP | DST IP | SRC Port | DST Port | Protocol |
|---|---|---|---|---|---|---|
| 1 | Allow | 192.168.10.0/24 | * | 110 | > 1023 | TCP |
| 2 | Allow | * | 192.168.10.0/24 | < 1023 | 110 | TCP |
| 3 | Allow | 192.168.10.0/24 | | < 1023 | < 1023 | TCP |
| 4 | Allow | * | 192.168.10.0/24 | < 1023 | < 1023 | TCP |

Which choice describes the next step to take now that this ruleset has been enabled?

A. From the internal network, use your Web browser to determine whether all internal users can access the Web server.
B. From the internal network, use your e-mail client to determine whether all internal users can access the e-mail server.
C. From the external network, use your Web browser to determine whether all external users can access the Web server.
D. From the external network, use your e-mail client to determine whether all external users can access the e-mail server.

**Correct Answer:** D

**QUESTION 24**
The most popular types of proxy-oriented firewalls operate at which layer of the OSI/RM?

A. Application layer

Submit A Ticket