

## (Oct-2024) Get professional help from our 1D0-671 Dumps PDF [Q17-Q38]



## (Oct-2024) Get professional help from our 1D0-671 Dumps PDF [Q17-Q38]

(Oct-2024) Get professional help from our 1D0-671 Dumps PDF  
Give You Free Regular Updates on 1D0-671 Exam Questions

**NO.17** Which of the following is the primary weakness of symmetric-key encryption?

- \* Data encrypted using symmetric-key encryption is subject to corruption during transport.
- \* Symmetric-key encryption operates slower than asymmetric-key encryption.
- \* Symmetric-key encryption does not provide the service of data confidentiality.
- \* Keys created using symmetric-key encryption are difficult to distribute securely.

**NO.18** Which ICMP message type is used to synchronize time between two hosts?

- \* Parameter Problem and Time Exceeded
- \* Time Exceeded
- \* Timestamp Request and Reply
- \* Echo Request

**NO.19** You are using a PKI solution that is based on Secure Sockets Layer (SSL).

Which of the following describes the function of the asymmetric-key-encryption algorithm used?

- \* It encrypts the symmetric key.
- \* It encrypts all of the data.
- \* It encrypts the hash code used for data integrity.
- \* It encrypts the X.509 key.

**NO.20** Which tool is best suited for identifying applications and code on a Web server that can lead to a SQL injection attack?

- \* A vulnerability scanner
- \* A packet sniffer
- \* An intrusion-detection system
- \* A network switch

**NO.21** Jason is attempting to gain unauthorized access to a corporate server by running a program that enters passwords from a long list of possible passwords.

Which type of attack is this?

- \* Brute force
- \* Denial of service
- \* Botnet
- \* Buffer overflow

**NO.22** Which of the following tools allows you to implement packet filtering for a network?

- \* Hub
- \* Router
- \* Bridge
- \* Browser

**NO.23** David has enabled auditing on the C, D and E drives of his Web server. This server runs Windows Server 2003 and uses all SCSI components. After David has finished his change, the help desk receives calls from customers complaining that transactions are being completed at an unusually slow rate.

What has David failed to consider?

- \* The performance effects that auditing can have on a system
- \* The restriction that auditing cannot be established on a RAID array in Windows Server 2003
- \* Network latency and system uptime requirements that appear to be system performance problems
- \* The limitation that auditing can be performed on only two disks of a RAID array

**NO.24** Which of the following details should be included in documentation of an attack?

- \* An overview of the security policy and suggestions for the next response plan
- \* Estimates of how much the attack cost the company, and a list of the applications used by the attacker
- \* The time and date of the attack, and the names of employees who were contacted during the response
- \* The network resources involved in the attack, and recommendations for thwarting future attacks

**NO.25** You have implemented a version of the Kerberos protocol for your network.

What service does Kerberos primarily offer?

- \* Authentication
- \* Encryption
- \* Non-repudiation
- \* Data integrity

**NO.26** Which of the following accurately describes an aspect of an access control list (ACL)?

- \* The ACL defines users that have access to a resource on a database server.
- \* The ACL defines the database roles that users have on a database server.
- \* The ACL cannot determine whether a user has access to an object, but can define exactly what the user can do with that object.
- \* The ACL lists entities that can access a database server, but does not provide access levels.

**NO.27** Which technique can help to protect an FTP server?

- \* Place downloads on the same partition as the FTP server binaries.
- \* When setting IP-based blocking rules for the FTP server, move the FTP files to C:ftpfiles for maximum security.
- \* Use separate FTP user accounts from those used to access the Web.
- \* Install the operating system on the same partition as the FTP server.

**NO.28** Why should you notify the hacker's ISP if you have successfully identified a hacker?

- \* You can have the ISP reconfigure the hacker's routing tables.
- \* You can have the ISP terminate the connection so the attack can be stopped.
- \* You can have the ISP retaliate by altering the hacker's login script.
- \* You can have the ISP retaliate by placing a trojan or virus on the hacker's system.

**NO.29** Which attribute of a security matrix considers the number of employees necessary to successfully implement and maintain your system?

- \* Appropriate cost of ownership
- \* Access control
- \* Ease of use
- \* Flexibility and scalability

**NO.30** Which choice lists typical firewall functions?

- \* Creating a VLAN and configuring the intrusion-detection system
- \* Issuing alerts and limiting host access
- \* Logging traffic and creating a choke point
- \* Implementing the security policy and scanning the internal network

**NO.31** Which type of attack exploits routed IP datagrams and is often found at the network layer?

- \* Source routing
- \* SYN flooding
- \* Route mangling
- \* IP spoofing

**NO.32** What is the term for a self-replicating program or algorithm that consumes system resources?

- \* Illicit server
- \* Root kit
- \* Trojan
- \* Worm

**NO.33** An effective way to prevent a user from becoming the victim of a malicious bot is to use a technique in which the user must view a distorted text image, and then type it before he or she is allowed to proceed with a transaction.

This technique is known as a:

- \* CAPTCHA.
- \* zombie.
- \* botnet.

\* SQL injection.

**NO.34** Which type of certificate is used to verify a company's Web server?

- \* Certificate authority certificate
- \* Server certificate
- \* Personal certificate
- \* Software or publisher certificate

**NO.35** At what layer of the OSI/RM does a packet filter operate?

- \* Layer 1
- \* Layer 3
- \* Layer 5
- \* Layer 7

**NO.36** Consider the following diagram involving two firewall-protected networks:

Which of the following is necessary for each of the firewalls to allow private IP addresses to be passed on to the Internet?

- \* Chargeback
- \* Stateful multi-layer inspection
- \* Masquerading
- \* DMZ creation

**NO.37** 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 trojan has attacked the system.
- \* A SQL injection attack has occurred.
- \* A spyware application has been installed.
- \* A root kit has been installed on the system.

**NO.38** Which of the following commands would you use to create a simple personal firewall that blocks all incoming ICMP traffic?

- \* iptables -A INPUT -p icmp -s 10.100.100.0/24 -d 0/0 -j DROP
- \* iptables -A INPUT -p icmp -s 10.100.100.0/255.255.255 -d 0/0 -j KILL
- \* iptables -A INPUT -p icmp -s 0/0 -d 0/0 -j DROP
- \* iptables -A INPUT -p icmp -s 0/0 -d 0/0 -j KILL

**Achieve the 1D0-671 Exam Best Results with Help from CIW Certified Experts:**

<https://www.examcollectionpass.com/CIW/1D0-671-practice-exam-dumps.html>