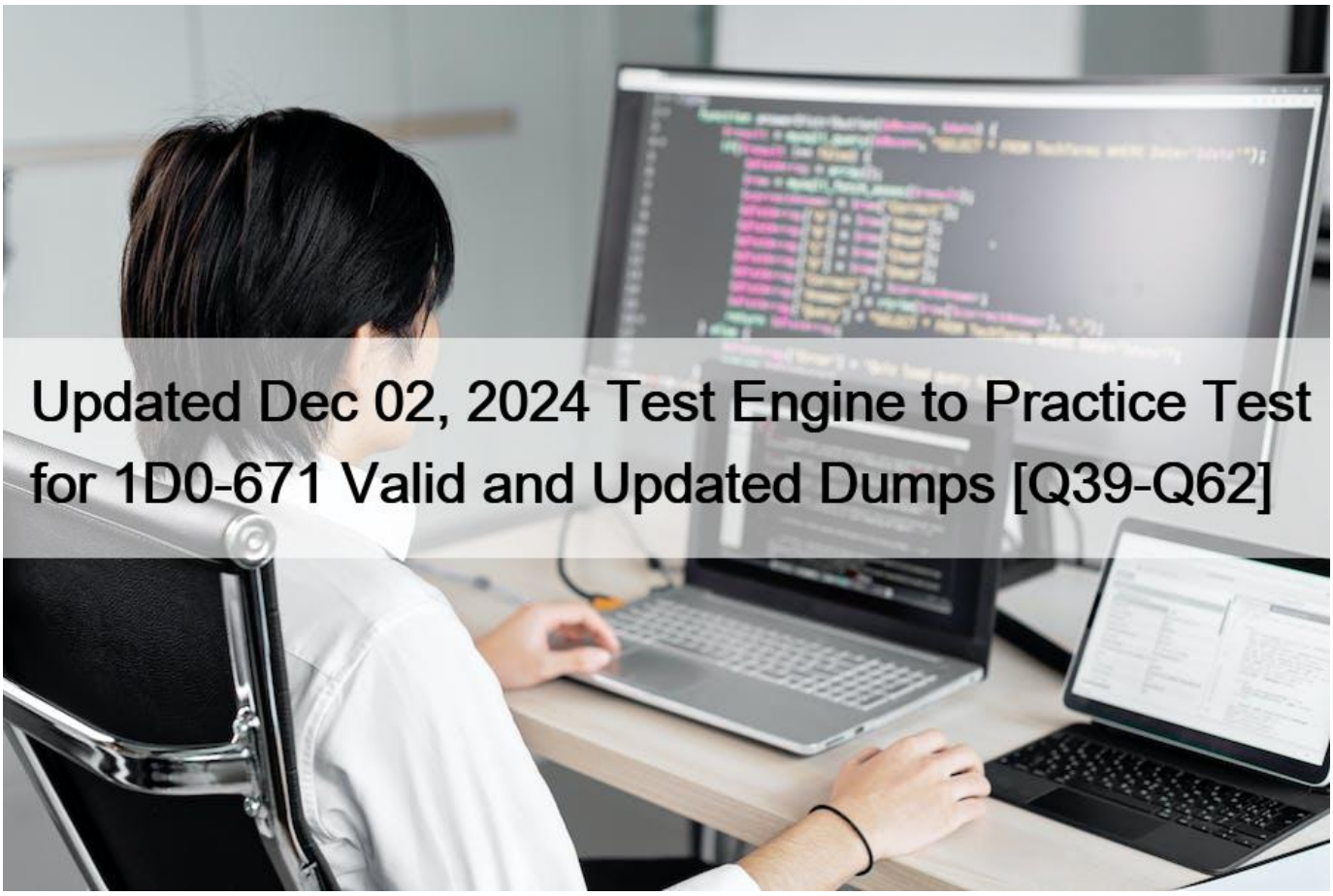
Updated Dec 02, 2024 Test Engine to Practice Test for 1D0-671 Valid and Updated Dumps [Q39-Q62



Updated Dec 02, 2024 Test Engine to Practice Test for 1D0-671 Valid and Updated Dumps
Exam Questions for 1D0-671 Updated Versions With Test Engine

NO.39 What is the main purpose of reviewing a security incident after it has been resolved?
* To bring charges against the ISP that carries the hacker’s account
* To discover and report that a piece of hardware or software has purportedly failed
* To learn what can be changed or improved in your security policy
* To discover who within your company should be reprimanded

NO.40 Which of the following is a primary weakness of asymmetric-key encryption?
* It is slow because it requires extensive calculations by the computer.
* It can lead to the corruption of encrypted data during network transfer.
* It is reliant on the Secure Sockets Layer (SSL) standard, which has been compromised.
* It is difficult to transfer any portion of an asymmetric key securely.

NO.41 At the beginning of an IPsec session, which activity occurs during the Internet Key Exchange (IKE)?
* Determining the number of security associations

* Negotiating the authentication method
* Determining the network identification number
* Negotiating the version of IP to be used

NO.42 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.43 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?
* Filtering traffic at the firewall
* Changing your ISP
* Installing Apache Server rather than Microsoft IIS
* Placing the database and the Web server on separate systems

NO.44 Which step in security policy implementation ensures that security policy will change as technology advances?
* Log, test and evaluate.
* Secure each resource and service.
* Publish the security policy.
* Repeat the process and keep current.

NO.45 Which of the following is a common problem with proxy servers?
* Proxy servers do not log incoming and outgoing access, so you will not be able to see details of successful and failed connections.
* Proxy servers cannot filter out specific application-layer traffic.
* Proxy servers may return old cached information.
* Because proxy servers do not mask network resources, hackers may be able to access all exposed systems.

NO.46 When Tripwire discovers that a file or database has been altered, how will it alert you?
* Via an e-mail message only
* Via a log file entry only
* Via a pager configured to receive a special signal
* Via e-mail or a log file entry

NO.47 Consider the following diagram:

Which of the following best describes the protocol activity shown in the diagram, along with the most likely potential threat that accompanies this protocol?
* The ICMP Time Exceeded message, with the threat of a denial-of-service attack
* The SIP three-way handshake, with the threat of a buffer overflow
* The TCP three-way handshake, with the threat of a man-in-the-middle attack
* The DNS name query, with the threat of cache poisoning

NO.48 Which of the following standards is used for digital certificates?
* DES
* Diffie-Hellman
* X.509

* RC5

NO.49 Which algorithm can use a 128-bit key, and has been adopted as a standard by various governments and corporations?
* MARS
* RC2
* Advanced Encryption Standard (AES)
* International Data Encryption Algorithm (IDEA)

NO.50 Your firewall is configured to forbid all internal traffic from going out to the Internet. You want to allow internal clients to access all Web traffic.

At a minimum, what ports must you open in regards to the internal systems?
* TCP Port 80 and all ports above 1023
* TCP Ports 80 and 443, and all ports above 1023
* All TCP ports above 80 and below 1023
* TCP Ports 80 and 443

NO.51 Which of the following is most likely to address a problem with an operating system’s ability to withstand an attack that attempts to exploit a buffer overflow?
* Firewall
* Software update
* Intrusion detection system
* Network scanner

NO.52 Which of the following describes the practice of stateful multi-layer inspection?
* Inspecting packets in all layers of the OSI/RM with a packet filter
* Using Quality of Service (QoS) on a proxy-oriented firewall
* Prioritizing voice and video data to reduce congestion
* Using a VLAN on a firewall to enable masquerading of private IP addresses

NO.53 Why can instant messaging (IM) and peer-to-peer (P2P) applications be considered a threat to network security?
* Because they use ports above 1023 and many firewalls are not configured to block this traffic
* Because they are susceptible to VLAN hopping
* Because they usually lie outside the broadcast domain
* Because they use ports below 1023 and many firewalls are not configured to block this traffic

NO.54 Which of the following causes problems with firewalls
* Control FTP
* Data FTP
* Active FTP
* Passive FTP

NO.55 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.56 Which of the following is a primary auditing activity?
* Encrypting data files
* Changing login accounts
* Checking log files
* Configuring the firewall

NO.57 How do activity logs help to implement and maintain a security plan?
* Activity logs provide advice on firewall installation, because they enable network baseline creation.
* Activity logs remind users to log on with strong passwords, because the logs can be analyzed to see if users are complying with policy.
* Activity logs allow you to determine if and how an unauthorized activity occurred.
* Activity logs dissuade would-be hackers from breaching your security.

NO.58 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.59 What is the term for a self-replicating program or algorithm that consumes system resources?
* Illicit server
* Root kit
* Trojan
* Worm

NO.60 Which of the following is considered to be the most secure default firewall policy, yet usually causes the most work from an administrative perspective?
* Configuring the firewall to respond automatically to threats
* Blocking all access by default, then allowing only necessary connections
* Configuring the firewall to coordinate with the intrusion-detection system
* Allowing all access by default, then blocking only suspect network connections

NO.61 What distinguishes hash encryption from other forms of encryption?
* Hash encryption creates a mathematically matched key pair in which one half of the pair encrypts, and the other half decrypts.
* Hash encryption creates a single key that is used to encrypt and decrypt information.
* Hash encryption is the encryption method of choice when conducting e-commerce transactions.
* Hash encryption is used for information that you want never to be decrypted or read.

NO.62 Which of the following is a security principle that allows you to protect your network resources?
* Realize that some high-end systems should stand alone.
* Avoid being suspicious of legitimate activity.
* Deploy security enforcement only in the largest departments.
* Provide training for end users and IT workers.

1D0-671 Exam Dumps - Free Demo & 365 Day Updates: https://www.dumpleader.com/1D0-671_exam.html]