Exam

Question 1 of 190

You are in the process of configuring an iSCSI storage area network (SAN) for your network.

You want to configure a Windows Server 2016 system to connect to an iSCSI target defined on a different server system. You also need to define iSCSI security settings, including CHAP and IPsec.

Which tool should you use?

- iSCSI Initiator
- Internet Storage Name Service
- iSCSI under File and Storage Services in Server Manager
- Multipath I/O

Question 2 of 190

Which of the following does not accurately describe an iSCSI SAN?

- Needs dedicated Ethernet cabling.
- Can be implemented on a standard production network with other network traffic.
- Can authenticate connections and encrypt data transmissions.
- Uses port 3260 by default.

Question 3 of 190

Which of the following are typical components of a NAS device? (Select two.)

- [x] One or more NICs
- [x] A minimal network OS
- [ ] An FC switch
- [ ] A dedicated network
- [ ] Initiator server

Question 4 of 190

Which VoIP device helps establish the connection between two VoIP phones?

- VoIP server
- VoIP gateway
- VoIP endpoint
- VoIP codec

Question 5 of 190

How can QoS be configured so that large data transfers will not block VoIP calls by using too much network bandwidth?

- QoS can be configured on network devices to give priority to VoIP traffic.
- QoS can be configured on network devices to limit the size of a file that can be transferred on the network.
- QoS can be configured on network devices to only allow network protocols that throttle network bandwidth usage.
-

QoS can be configured on network devices to set a bandwidth threshold on selected ports.

Question 6 of 190

Which of the following protocols is an open source protocol used by most manufacturers of VoIP systems?

- Session initiation protocol (SIP)
- Stream control transmission protocol (SCTP)
- User datagram protocol (UDP)
- Transmission control protocol (TCP)

Question 7 of 190

Which of the following protocols is used by VoIP to set up, maintain, and terminate a phone call?

- SIP
- RTP
- NTP
- TLS
- SSH

Question 8 of 190

Your company uses VoIP for phone calls. Recently, employees have been complaining about phone calls with unusual sound effects.

Which type of problem is occurring on the VoIP system?

- Latency
- Jitter
- Packet loss
- Echo

Question 9 of 190

You are on a phone call using VoIP. You notice that it takes several seconds for the person on the other end to respond to questions you ask.

Which type of problem is occurring?

- Jitter
- Echo
- Latency
- Packet loss

Question 10 of 190

Which switch features are typically used with VoIP? (Select two.)

- [x] PoE
- [x] VLAN
- [ ] Spanning tree
- [ ] Mirroring

Question 11 of 190

Which of the following features is used with digital IP phones to supply power through a switch port?

- PoE
- VPN
- Trunking
- 802.1x
- Spanning tree

Question 12 of 190

In virtualization, what is the role of the hypervisor?

- A hypervisor allows virtual machines to interact with the hardware without going through the host operating system.
- A hypervisor has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, and motherboard.
- A hypervisor is a software implementation that executes programs like a physical machine.
- A hypervisor is created within the host operating system and simulates a hard disk for the virtual machine.

Question 13 of 190

Which of the following are advantages of virtualization? (Select two.)

- [ ] Centralized administration
- [ ] Easy system migration to different hardware
- [ ] Redundancy of hardware components for fault tolerance
- [ ] Reduced utilization of hardware resources
- [ ] Improved detection of host-based attacks

Question 14 of 190

You want to be able to monitor and filter VM-to-VM traffic within a virtual network.

What should you do?

- Implement a virtual firewall within the hypervisor.
- Create a virtual router with VRF technology.
- Route VM-to-VM traffic through a physical firewall and back to the virtual network.
- Define VLAN memberships on each VM.

Question 15 of 190

Which of the following statements about virtual NICs are true? (Select two.)

- [ ] The type of NIC installed in the physical machine determines the type of virtual NIC that is emulated.
- [ ] Virtual NICs can only communicate with other virtual NICs.
- [ ] Multiple virtual NICs can be added to a virtual machine.
- [ ] Virtual NICs need the appropriate driver installed to function.
- [ ] Virtual NICs don't have a MAC address.

Question 16 of 190

An access point that conforms to the IEEE 802.11b standard behaves similarly to what other networking device?

- ◯ Router
- ◯ Hub
- ◯ Gateway
- ◯ Patch bay
- ◯ Terminal

Question 17 of 190

Which of the following is true of a wireless network SSID?

- ◯ Groups wireless devices together into the same logical network.
- ◯ Is a 48-bit value that identifies an AP.
- ◯ Allows devices to find a specific AP within an ESS.
- ◯ Is used by STAs as they roam between APs.

Question 18 of 190

All of the 802.11 standards for wireless networking support which type of communication path sharing technology?

- ◯ Polling
- ◯ Token passing
- ◯ CSMA/CD
- ◯ CSMA/CA

Question 19 of 190

What is the frequency of 802.11a networking?

- ◯ 900 MHz
- ◯ 1.2 GHz
- ◯ 2.4 GHz
- ◯ 5.75 GHz

Question 20 of 190

How many total channels are available for 802.11g wireless networks?

- ◯ 3
- ◯ 11
- ◯ 12
- ◯ 23
- ◯ 54

Question 21 of 190

Which of the following are frequencies defined by 802.11 committees for wireless networking? (Select two.)

- ☐ 700 MHz
- ☐ 1.9 GHz
- ☐ 2.4 GHz

- [ ] 5.75 GHz
- [ ] 10 GHz

Question 22 of 190

Which data transmission rate is defined by the IEEE 802.11b wireless standard?

- ( ) 2 Mbps
- ( ) 10 Mbps
- ( ) 11 Mbps
- ( ) 56 Mbps

Question 23 of 190

You are designing an update to your client's wireless network. The existing wireless network uses 802.11b equipment; which your client complains runs too slowly. She wants to upgrade the network to run up to 600 Mbps.

Due to budget constraints, your client wants to upgrade only the wireless access points in the network this year. Next year, she will upgrade the wireless network boards in her users' workstations. She has also indicated that the system must continue to function during the transition period.

Which 802.11 standard will work best in this situation?

- ( ) 802.11a
- ( ) 802.11b
- ( ) 802.11c
- ( ) 802.11d
- ( ) 802.11n

Question 24 of 190

Which IEEE wireless standards specify transmission speeds up to 54 Mbps? (Select two.)

- [ ] 802.11a
- [ ] Bluetooth
- [ ] 802.1x
- [ ] 802.11b
- [ ] 802.11g

Question 25 of 190

You are configuring a wireless network with two wireless access points. Both access points connect to the same wired network. You want wireless users to be able to connect to either access point and have the ability to roam between the two access points.

How should you configure the access points?

- ( ) Same SSID, different channel
- ( ) Same SSID, same channel
- ( ) Different SSID, different channel
- ( ) Different SSID, same channel

Question 26 of 190

You have configured a wireless access point to create a small network. You have configured all necessary parameters.

Wireless clients seem to take a long time to find the wireless access point. You want to reduce the time it takes for the clients to connect. What should you do?

- (○) Decrease the beacon interval.
- (○) Enable SSID broadcast.
- (○) Create a wireless profile on the client.
- (○) Change the channel on the access point to a lower number.

Question 27 of 190

You have configured a wireless access point to create a small network. For security, you have disabled SSID broadcast.

From a client computer, you try to browse to find the access point. You see some other wireless networks in the area, but cannot see your network.

What should you do?

- (○) Decrease the beacon interval on the access point.
- (○) Configure a profile on the wireless client.
- (○) Set the channel on the client to match the channel used by the access point.
- (○) Enable the wireless card on the client.

Question 28 of 190

You have a small wireless network that uses multiple access points. The network uses WPA and broadcasts the SSID. WPA2 is not supported by the wireless access points.

You want to connect a laptop computer to the wireless network. Which of the following parameters will you need to configure on the laptop? (Select two.)

- [ ] Preshared key
- [ ] BSSID
- [ ] TKIP encryption
- [ ] AES encryption
- [ ] Channel

Question 29 of 190

You are designing a wireless network for a client. Your client needs the network to support a data rate of at least 150 Mbps. In addition, the client already has a wireless telephone system installed that operates 2.4 GHz.

Which 802.11 standard will work best in this situation?

- (○) 802.11n
- (○) 802.11b
- (○) 802.11a
- (○) 802.11g

Question 30 of 190

Which of the following wireless network protection methods prevents the broadcasting of the wireless network name?

- (○) SSID broadcast
- (○) MAC filtering
- (○) Shared secret key
- (○) 802.1x

Question 31 of 190

Which of the following provides security for wireless networks?

- ◯ WAP
- ◯ WPA
- ◯ 802.3u
- ◯ CSMA/CD
- ◯ 802.11a

Question 32 of 190

Which of the following features are supplied by WPA2 on a wireless network?

- ◯ Encryption
- ◯ Client connection refusals based on MAC address
- ◯ Traffic filtering based on packet characteristics
- ◯ Network identification
- ◯ A centralized access point for clients

Question 33 of 190

You need to configure a wireless network. You want to use WPA2 Enterprise. Which of the following components will be part of your design? (Select two.)

- ☐ TKIP encryption
- ☐ AES encryption
- ☐ WEP encryption
- ☐ 802.1x
- ☐ Open authentication
- ☐ Preshared keys

Question 34 of 190

You want to implement 802.1x authentication on your wireless network. Which of the following will be required?

- ◯ WPA
- ◯ WPA2
- ◯ RADIUS
- ◯ TKIP

Question 35 of 190

You want to implement 802.1x authentication on your wireless network. Where would you configure passwords that are used for authentication?

- ◯ On a RADIUS server
- ◯ On the wireless access point
- ◯ On the wireless access point and each wireless device
- ◯ On a certificate authority (CA)

Question 36 of 190

Your company security policy states that wireless networks are not to be used because of the potential security risk they present to your network.

One day you find that an employee has connected a wireless access point to the network in his office.

What type of security risk is this?

- ◯ Rogue access point
- ◯ Man-in-the-middle
- ◯ Phishing
- ◯ Physical security
- ◯ Social engineering

Question 37 of 190

You want to connect your client computer to a wireless access point that is connected to your wired network at work. The network administrator tells you that the access point is configured to use WPA2 Personal with the strongest encryption method possible. SSID broadcast is turned off.

Which of the following must you configure manually on the client? (Select three.)

- ☐ Preshared key
- ☐ SSID
- ☐ Channel
- ☐ AES
- ☐ TKIP
- ☐ Username and password

Question 38 of 190

You need to add security for your wireless network. You would like to use the most secure method.

Which method should you implement?

- ◯ WEP
- ◯ WPA
- ◯ WPA2
- ◯ Kerberos

Question 39 of 190

What is the speed of an OC-3 connection?

- ◯ 10 Mbps
- ◯ 100 Mbps
- ◯ 155 Mbps
- ◯ 622 Mbps

Question 40 of 190

You have installed an ISDN connection into your home so you can connect to the internet and talk on the phone at the same time. While you are talking on the telephone, what is the maximum data rate of your internet connection?

- ◯ 128 Kbps
- ◯ 64 Kbps
- ◯ 56.8 Kbps

- ◯ 1.544 Mbps

Question 41 of 190

To access the internet through the PSTN, what kind of connectivity device must you use?

- ◯ Modem
- ◯ CSU/DSU
- ◯ DTE
- ◯ TDM
- ◯ Switch

Question 42 of 190

Which of the following technologies uses variable-length packets, adds labels to packets as they enter the WAN cloud, and uses the labels to switch packets and prioritize traffic?

- ◯ SONET
- ◯ ATM
- ◯ Frame relay
- ◯ MPLS
- ◯ ISDN

Question 43 of 190

Which of the following are characteristics of ATM? (Select two.)

- ☐ Adds labels to data units.
- ☐ Uses fixed-length cells of 53 bytes.
- ☐ Supports variable-length packets.
- ☐ Uses POTS in the local loop.
- ☐ Connects to the WAN cloud with a CSU/DSU.

Question 44 of 190

Which WAN connection types use digital communications over public telephone lines? (Select two.)

- ☐ DSL
- ☐ ISDN
- ☐ X.25
- ☐ 56 Kbps dialup
- ☐ SONET
- ☐ ATM

Question 45 of 190

What is the maximum data rate of an ISDN BRI line?

- ◯ 128 Kbps
- ◯ 64 Kbps

- ◯ 1.544 Mbps
- ◯ 256 Kbps

Question 46 of 190

Which of the following describe the channels and data transfer rates used for ISDN BRI? (Select two.)

- ☐ One D channel operating at 16 Kbps
- ☐ Two B channels operating at 64 Kbps each
- ☐ 23 B channels operating at 64 Kbps each
- ☐ One D channel operating at 64 Kbps

Question 47 of 190

What must you install between your network and a T1 line for your network to use the T1 line?

- ◯ CSU/DSU
- ◯ Bridge
- ◯ Gateway
- ◯ Transceiver

Question 48 of 190

A healthcare organization provides mobile clinics throughout the world. Which network technology should you select to transfer patient statistical data to a central database via the internet to ensure network connectivity for any clinic located anywhere in the world, even remote areas?

- ◯ Dial-up
- ◯ Satellite
- ◯ ISDN
- ◯ Cable modem
- ◯ DSL

Question 49 of 190

Which of the following are characteristics of VDSL? (Select two.)

- ☐ Equal download and upload speeds
- ☐ Unequal download and upload speeds
- ☐ Supports both data and voice at the same time
- ☐ Supports only data (not voice)
- ☐ Does not require splitters

Question 50 of 190

Which type of internet service uses the DOCSIS specification?

- ◯ Unshielded twisted pair
- ◯ Shielded twisted pair
- ◯ Fiber optic
- ◯ Coaxial cable

Question 51 of 190

Which of the following forms of networking are highly susceptible to eavesdropping and must be secured accordingly?

- Satellite
- Dial-up
- ISDN
- DSL
- Wireless

Question 52 of 190

Which of the following technologies does GSM use to allow multiple connections on the same frequency?

- Time division multiple access
- Code division multiple access
- Multiple-input and multiple-output
- Frequency division multiple access

Question 53 of 190

You have decided to implement a remote access solution that uses multiple remote access servers. You want to implement RADIUS to centralize remote access authentication and authorization.

Which of the following is a required part of your configuration?

- Configure remote access clients as RADIUS clients.
- Configure the remote access servers as RADIUS servers.
- Configure the remote access servers as RADIUS clients.
- Obtain certificates from a public or private PKI.

Question 54 of 190

RADIUS is primarily used for what purpose?

- Managing access to a network over a VPN.
- Authenticating remote clients before access to the network is granted.
- Managing RAID fault-tolerant drive configurations.
- Controlling entry gate access using proximity sensors.

Question 55 of 190

Which of the following ports are used with TACACS?

- 22
- 49
- 50 and 51
- 1812 and 1813
- 3389

Question 56 of 190

Which of the following protocols or services is commonly used on cable internet connections for user authentication?

- RRAS
- PPP
- PPPoE
- RDP

Question 57 of 190

You are concerned about the amount of traffic that passed through a router on your network. You want to see how the amount of traffic has changed over time.

Which document would help you identify past average network traffic?

- Baseline
- History log
- Event log
- Network diagram

Question 58 of 190

Which type of documentation would you consult to find the location of RJ45 wall jacks and their endpoints in the intermediate distribution closet?

- Wiring schematic
- Baseline
- Policy
- Procedure

Question 59 of 190

You need to find out what kind of laws might apply to the design and operation of your network. Which type of document would you consult?

- Regulation
- Policy
- Procedure
- Baseline

Question 60 of 190

When troubleshooting a router, you want to identify which other devices are connected to the router, as well as the subnet addresses of each connected subnet.

Which type of document would most likely have this information?

- Procedure
- Policy
- Network diagram
- Wiring schematic
- Baseline

Question 61 of 190

Which of the following information are you likely to find in a procedure document?

- Details on how to test and deploy patches.
- A record of the repairs made to a specific device.
- An inventory of the hardware components in a specific device.
- The relationship of routers to other routers on the network.

Question 62 of 190

Which of the following pieces of information are you likely to find in a policy document?

- The IP address assigned to a router interface.
- Average performance statistics for a router.
- A requirement for using encrypted communications for web transactions.
- Steps for completing and validating nightly backups.

Question 63 of 190

You are troubleshooting a workstation connection to the network. During your troubleshooting, you replace the drop cable connecting the computer to the network.

Which type of document should you update?

- Change documentation
- Configuration documentation
- Wiring schematic
- Network diagram

Question 64 of 190

You plan to implement a new security device on your network. Which of the following policies outlines the process you should follow before implementing that device?

- Change management
- Acceptable use
- Resource allocation
- SLA

Question 65 of 190

Which of the following is an example of an internal threat?

- A water pipe in the server room breaks.
- A user accidentally deletes the new product designs.
- A server backdoor allows an attacker on the internet to gain access to the intranet site.
- A delivery man is able to walk into a controlled area and steal a laptop.

Question 66 of 190

Which of the following network strategies connects multiple servers together so that if one server fails, the others immediately take over its tasks, preventing a disruption in service?

- Adapter bonding
- Mirroring
- Storage area networks (SANs)

- ◯ Clustering

Question 67 of 190

If an organization shows sufficient due care, which burden is eliminated in the event of a security breach?

- ◯ Asset loss
- ◯ Liability
- ◯ Investigation
- ◯ Negligence

Question 68 of 190

Purchasing insurance is what type of response to risk?

- ◯ Acceptance
- ◯ Rejection
- ◯ Deployment of a countermeasure
- ◯ Transference

Question 69 of 190

When is choosing to do nothing about an identified risk acceptable?

- ◯ When the cost of protecting the asset is greater than the potential loss.
- ◯ When the threat is likely to occur less than once a year.
- ◯ When the threat is most likely to come from an internal source instead of an external source.
- ◯ When the asset is an intangible asset instead of a tangible asset.

Question 70 of 190

What is the primary goal of business continuity planning?

- ◯ Minimizing the risk of delays and interruptions in services
- ◯ Maintaining business operations with reduced or restricted infrastructure capabilities or resources
- ◯ Minimizing decision-making during the development process
- ◯ Protecting an organization from major computer services failure

Question 71 of 190

You manage the website for your company. The Web1 server hosts the website. This server has the following configuration:

- Dual core processor
- Dual power supplies
- RAID 5 volume
- One RAID controller
- Two 1000 Mbps network adapters

Which component is a single point of failure for the website?

- ◯ Disk storage
- ◯ Network adapter
- ◯ Power supply
- ◯ Disk controller

Question 72 of 190

You manage a website for your company. The website uses three servers configured in a cluster. Incoming requests are distributed automatically between the three servers. All servers use a shared storage device that holds the website contents. Each server has a single network connection and a single power supply.

Considering the availability of your website, which component represents a single point of failure?

- Website storage
- Network adapter
- Power supply
- Web server

Question 73 of 190

Which of the following is not a valid response to a risk discovered during a risk analysis?

- Acceptance
- Assignment
- Mitigation
- Denial

Question 74 of 190

Over the last month, you have noticed a significant increase in the occurrence of inappropriate activities performed by employees. What is the best first response step to take in order to improve or maintain the security level of the environment?

- Terminate all offenders.
- Improve and hold new awareness training.
- Reduce all employee permissions and privileges.
- Initiate stronger auditing.

Question 75 of 190

You plan to implement a new security device on your network. Which of the following policies outlines the process you should follow before implementing that device?

- Change management
- Acceptable use
- Resource allocation
- SLA

Question 76 of 190

Which of the following is defined as a contract that prescribes the technical support or business parameters that a provider will bestow to its client?

- Mutual aid agreement
- Service level agreement
- Final audit report
- Certificate practice statement

Question 77 of 190

What is a service level agreement (SLA)?

- An agreement to support another company in the event of a disaster.
- A contract with a legal entity to limit your asset loss liability.
- A guarantee of a specific level of service.
- A contract with an ISP for a specific level of bandwidth.

Question 78 of 190

Which of the following is a policy that defines appropriate and inappropriate activities and usage for company resources, assets, and communications?

- Acceptable use policy (AUP)
- Business impact analysis (BIA)
- Disaster recovery plan (DRP)
- Business continuity plan (BCP)

Question 79 of 190

Which component of a change and configuration management policy specifies options for reverting a system back to the state it was in before a change was made?

- Feasibility analysis
- Change request
- Authorized downtime
- Rollback

Question 80 of 190

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a cubicle near your office. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using an SSH client with a username of **admin01** and a password of **P@ssW0rd**. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device?

- Use a Telnet client to access the router configuration.
- Change the default administrative username and password.
- Use encrypted type 7 passwords.
- Move the router to a secure server room.
- Use TFTP to back up the router configuration to a remote location.

Question 81 of 190

You are an IT consultant and are visiting a new client's site to become familiar with their network. As you walk around their facility, you note the following:

- When you enter the facility, a receptionist greets you and directs you down the hallway to the office manager's cubicle. The receptionist uses a notebook system that is secured to her desk with a cable lock.
- The office manager informs you that the organization's servers are kept in a locked closet. Only she has the key to the closet. When you arrive on site, you will be required to get the key from her to access the closet.
- She informs you that server backups are configured to run each night. A rotation of external USB hard disks are used as the backup media.
- You notice the organization's network switch is kept in an empty cubicle adjacent to the office manager's workspace.
- You notice that a router/firewall/content filter all-in-one device has been implemented in the server closet to protect the internal network from external attacks.

Which security-related recommendations should you make to this client? (Select two.)

- [ ] Relocate the switch to the locked server closet.
- [ ] Control access to the work area with locking doors and card readers.

- [ ] Replace the key lock on the server closet with a card reader.
- [ ] Replace the USB hard disks used for server backups with a tape drive.
- [ ] Use separate dedicated network perimeter security devices instead of an all-in-one device.

Question 82 of 190

Which of the following is a secure doorway that can be used with a mantrap to allow easy exit, but actively prevent re-entrance through the exit portal?

- ◯ Egress mantraps
- ◯ Turnstiles
- ◯ Locked doors with interior unlock push-bars
- ◯ Electronic access control doors

Question 83 of 190

Which of the following can be used to stop piggybacking from occurring at a front entrance where employees swipe smart cards to gain entry?

- ◯ Deploy a mantrap
- ◯ Install security cameras
- ◯ Use weight scales
- ◯ Use key locks rather than electronic locks

Question 84 of 190

Which of the following is not an example of a physical barrier access control mechanism?

- ◯ One-time passwords
- ◯ Biometric locks
- ◯ Mantraps
- ◯ Fences

Question 85 of 190

What is the primary benefit of CCTV?

- ◯ Reduces the need for locks and sensors on doors.
- ◯ Expands the area visible to security guards.
- ◯ Provides a corrective control.
- ◯ Increases security protection throughout an environment.

Question 86 of 190

Which of the following controls is an example of a physical access control method?

- ◯ Locks on doors
- ◯ Access control lists with permissions
- ◯ Passwords
- ◯ Smart cards
- ◯ Hiring background checks

Question 87 of 190

What is the primary countermeasure to social engineering?

- ◯ A written security policy
- ◯ Traffic filters
- ◯ Heavy management oversight
- ◯ Awareness

Question 88 of 190

Which of the following are examples of social engineering? (Select two.)

- ☐ Shoulder surfing
- ☐ Port scanning
- ☐ Dumpster diving
- ☐ War dialing

Question 89 of 190

How can an organization help prevent social engineering attacks? (Select two.)

- ☐ Publish and enforce clearly written security policies
- ☐ Implement IPsec on all critical systems
- ☐ Educate employees on the risks and countermeasures
- ☐ Utilize 3DES encryption for all user sessions

Question 90 of 190

Which of the following is not a form of social engineering?

- ◯ Impersonating a manager over the phone
- ◯ A virus hoax email message
- ◯ Impersonating a utility repair technician
- ◯ Impersonating a user by logging on with stolen credentials

Question 91 of 190

Which of the following is a common social engineering attack?

- ◯ Hoax virus information emails
- ◯ Using a sniffer to capture network traffic
- ◯ Logging on with stolen credentials
- ◯ Distributing false information about your organization's financial status

Question 92 of 190

Dumpster diving is a low-tech means of gathering information that may be useful for gaining unauthorized access or as a starting point for more advanced attacks. How can a company reduce the risk associated with dumpster diving?

- ◯ Create a strong password policy.
- ◯ Mandate the use of Integrated Windows Authentication.

- Establish and enforce a document destruction policy.
- Secure all terminals with screensaver passwords.

Question 93 of 190

On your way into the back entrance of the building at work one morning, a man dressed as a plumber asks you to let him in so he can fix the restroom. What should you do?

- Let him in.
- Let him in and help him find the restroom. Then let him work.
- Direct him to the front entrance and instruct him to check in with the receptionist.
- Tell him no and quickly close the door.

Question 94 of 190

You have worked as the network administrator for a company for seven months. One day, all picture files on the server become corrupted.

You discover that a user downloaded a virus from the internet onto his workstation, and it propagated to the server. You successfully restore all files from backup, but your boss is adamant that no more events like this one take place.

What should you do?

- Install a network virus detection software solution.
- Disconnect the user from the internet.
- Allow users to access the internet only from terminals that are not attached to the main network.
- Install a firewall.

Question 95 of 190

Which of the following measures are you most likely to implement in order to protect your system from a worm or Trojan horse?

- Firewall
- IPsec
- Antivirus software
- Password policy

Question 96 of 190

Which of the following statements about the use of anti-virus software is correct?

- Once installed, anti-virus software needs to be updated on a monthly basis.
- If servers on a network have anti-virus software installed, workstations do not need anti-virus software installed on them.
- Anti-virus software should be configured to download updated virus definition files as soon as they become available.
- If you install anti-virus software, you no longer need a firewall on your network.

Question 97 of 190

An attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack?

- Spamming
- Replay
- Backdoor
- DDoS

- DoS

Question 98 of 190

Which is a form of attack that either exploits a software flaw or floods a system with traffic in order to prevent legitimate activities or transactions from occurring?

- Brute force attack
- Man-in-the-middle attack
- Privilege escalation
- Denial of service attack

Question 99 of 190

An attacker captures packets as they travel from one host to another with the intent of altering the contents of the packets. Which type of attack is being executed?

- Man-in-the-middle attack
- Passive logging
- Distributed denial of service
- Spamming

Question 100 of 190

Which of the following is the most effective countermeasure against man-in-the middle attacks?

- MIME email
- IPsec
- UDP
- PPP

Question 101 of 190

Which of the following are characteristics of a rootkit? (Select two.)

- [ ] Requires administrator-level privileges for installation.
- [ ] Hides itself from detection.
- [ ] Monitors user actions and opens pop-ups based on user preferences.
- [ ] Uses cookies saved on the hard drive to track user preferences.

Question 102 of 190

Which of the following best describes spyware?

- It monitors the actions you take on your machine and sends the information back to its originating source.
- It monitors user actions that denote personal preferences, then sends pop-ups and ads to the user that match their tastes.
- It is a program that attempts to damage a computer system and replicate itself to other computer systems.
- It is a malicious program that is disguised as legitimate software.

Question 103 of 190

Which option is a program that appears to be a legitimate application, utility, game, or screensaver and performs malicious activities surreptitiously?

- Outlook Express

- Worm
- ActiveX controls
- Trojan horse

Question 104 of 190

What is the main difference between a worm and a virus?

- A worm tries to gather information while a virus tries to destroy data.
- A worm can replicate itself while a virus requires a host for distribution.
- A worm requires an execution mechanism to start while a virus can start itself.
- A worm is restricted to one system while a virus can spread from system to system.

Question 105 of 190

A relatively new employee in the data entry cubical farm was assigned a user account similar to that of all of the other data entry employees. However, audit logs have shown that this user account has been used to change ACLs on several confidential files and has accessed data in restricted areas.

This situation indicates that which of the following has occurred?

- Man-in-the-middle attack
- Social engineering
- Smurf attack
- Privilege escalation

Question 106 of 190

What is modified in the most common form of spoofing on a typical IP packet?

- Source address
- Destination address
- Protocol type field value
- Hash total

Question 107 of 190

Capturing packets as they travel from one host to another with the intent of altering the contents of the packets is a form of which security concern?

- Man-in-the-middle attack
- Passive logging
- DDoS
- Spamming

Question 108 of 190

Which type of denial of service (DoS) attack occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses?

- DNS poisoning
- ARP poisoning
- Spam
- SYN flood

Question 109 of 190

An attacker has obtained the logon credentials for a regular user on your network. Which type of security threat exists if this user account is used to perform administrative functions?

- Privilege escalation
- Social engineering
- Replay
- Impersonation

Question 110 of 190

An attacker sends an unwanted and unsolicited email message to multiple recipients with an attachment that contains malware.

What kind of attack has occurred in this scenario?

- Spam
- Open SMTP relay
- Phishing
- Repudiation attack

Question 111 of 190

A programmer that fails to check the length of input before processing, leaves his code vulnerable to what form of common attack?

- Backdoor
- Session hijacking
- Buffer overflow
- Privilege escalation

Question 112 of 190

You have installed anti-malware software that checks for viruses in email attachments. You configure the software to quarantine any files with problems.

You receive an email with an important attachment, but the attachment is not there. Instead, you see a message that the file has been quarantined by the anti-malware software.

What has happened to the file?

- It has been moved to a secure folder on your computer.
- It has been deleted from your system.
- The infection has been removed, and the file has been saved to a different location.
- The file extension has been changed to prevent it from running.

Question 113 of 190

As you are helping a user with a computer problem, you notice that she has written her password on a note stuck to her computer monitor. You check the password policy of your company and find that the following settings are currently required:

- Minimum password length = 10
- Minimum password age = 4
- Maximum password age = 30
- Password history = 6
- Account lockout clipping level = 3
- Require complex passwords that include numbers and symbols

Which of the following is the best action to take to make remembering passwords easier so that she no longer has to write the password down?

- Implement end-user training.
- Decrease the minimum password length.
- Increase the maximum password age.
- Remove the complex password requirement.
- Increase the account lockout clipping level.

Question 114 of 190

A user named Bob Smith has been assigned a new desktop workstation to complete his day-to-day work. The computer runs Windows 7.

When provisioning Bob's user account in your organization's domain, you assigned an account name of **BSmith** with an initial password of **bw2Fs3d**.

At his first logon, Bob is prompted to change his password, so he changes it to **Fido**, the name of his dog.

What should you do to increase the security of Bob's account? (Select two.)

- [ ] Train users not to use passwords that are easy to guess.
- [ ] Do not allow users to change their own passwords.
- [ ] Require users to set a stronger password upon initial logon.
- [ ] Configure user account names that are not easy to guess.
- [ ] Upgrade the workstation to Windows 8.

Question 115 of 190

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a server room that requires an ID card for entry. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer by connecting it to the console port on the router. You configured the management interface with the username **admin** and the password **password**.

What should you do to increase the security of this device?

- Use an SSH client to access the router configuration.
- Use a stronger administrative password.
- Use a web browser to access the router configuration using an HTTP connection.
- Move the device to a secure data center.

Question 116 of 190

Which of the following attacks, if successful, causes a switch to function like a hub?

- ARP poisoning
- MAC flooding
- MAC spoofing
- Replay

Question 117 of 190

You manage a network that uses switches. In the lobby of your building, there are three RJ45 ports connected to a switch.

You want to make sure that visitors cannot plug their computers into the free network jacks and connect to the network. But employees who plug into those same jacks should be able to connect to the network.

What feature should you configure?

- Port authentication
- Mirroring
-

- Bonding
- Spanning tree
- VLANs

Question 118 of 190

You have decided to implement a remote access solution that uses multiple remote access servers. You want to implement RADIUS to centralize remote access authentication and authorization.

Which of the following would be a required part of your configuration?

- Configure remote access clients as RADIUS clients.
- Configure the remote access servers as RADIUS servers.
- Configure the remote access servers as RADIUS clients.
- Obtain certificates from a public or private PKI.

Question 119 of 190

Which of the following is a platform independent authentication system that maintains a database of user accounts and passwords that centralizes the maintenance of those accounts?

- RRAS
- RADIUS
- NAS
- EAP

Question 120 of 190

Which of the following is a mechanism for granting and validating certificates?

- PKI
- RADIUS
- Kerberos
- AAA

Question 121 of 190

You want to implement an authentication method that uses public and private key pairs. Which authentication method should you use?

- PKI
- EAP
- MS-CHAP v2
- IPsec

Question 122 of 190

You have a web server that will be used for secure transactions for customers who access the website over the internet. The web server requires a certificate to support SSL.

Which method would you use to get a certificate for the server?

- Obtain a certificate from a public PKI.
- Create your own internal PKI to issue certificates.
- Have the server generate its own certificate.

- Run a third-party tool to generate the certificate.

Question 123 of 190

Which of the following is a feature of MS-CHAP v2 that is not included in CHAP?

- Three-way handshake
- Hashed shared secret
- Mutual authentication
- Certificate-based authentication

Question 124 of 190

Which of the following is an example of two-factor authentication?

- A username and a password
- A pass phrase and a PIN
- A token device and a PIN
- A fingerprint and a retina scan

Question 125 of 190

You want to increase the security of your network by allowing only authenticated users to access network devices through a switch.

Which of the following should you implement?

- 802.1x
- Port security
- Spanning tree
- IPsec

Question 126 of 190

Which of the following actions typically involves the use of 802.1x authentication? (Select two.)

- [ ] Controlling access through a wireless access point
- [ ] Controlling access through a switch
- [ ] Controlling access through a router
- [ ] Authenticating remote access clients
- [ ] Authenticating VPN users through the internet

Question 127 of 190

When using Kerberos authentication, which of the following terms is used to describe the token that verifies the user's identity to the target system?

- Coupon
- Voucher
- Ticket
- Hashkey

Question 128 of 190

Which of the following is the most common form of authentication?

- Photo ID
- Fingerprint
- Digital certificate on a smart card
- Password

Question 129 of 190

Which of the following identification and authentication factors are often well-known or easily discovered by others on the same network or system?

- Username
- Password
- PGP secret key
- Biometric reference profile

Question 130 of 190

Which of the following is the strongest form of multi-factor authentication?

- A password and a biometric scan
- Two passwords
- A password, a biometric scan, and a token device
- Two-factor authentication

Question 131 of 190

Which of the following is an example of three-factor authentication?

- Token device, keystroke analysis, cognitive question
- Photo ID, smart card, fingerprint
- Smart card, digital certificate, PIN
- Pass phrase, palm scan, voice recognition

Question 132 of 190

Which of the following best describes one-factor authentication?

- Only Type 1 authentication credentials are accepted.
- Only a single authentication credential is submitted.
- A username without any additional credentials is accepted.
- Multiple authentication credentials may be required, but they are all of the same type.

Question 133 of 190

Telnet is inherently insecure because its communication is in plaintext and is easily intercepted. Which of the following is an acceptable alternative to Telnet?

- SLIP
- SHTTP
- Remote Desktop
- SSH

Question 134 of 190

You want to allow traveling users to connect to your private network through the internet. Users will connect from various locations including airports, hotels, and public access points such as coffee shops and libraries. As such, you won't be able to configure the firewalls that might be controlling access to the internet in these locations.

Which of the following protocols would be most likely to be allowed through the widest number of firewalls?

- PPTP
- L2TP
- SSL
- IPsec
- PPPoE

Question 135 of 190

Which of the following protocols can be used to securely manage a network device from a remote connection?

- SSH
- Telnet
- SFTP
- TLS

Question 136 of 190

Which security protocols use RSA encryption to secure communications over an untrusted network? (Select two.)

- [ ] Secure sockets layer
- [ ] Transport layer security
- [ ] Point-to-point tunneling protocol
- [ ] Internet security association and key management protocol

Question 137 of 190

Which of the following protocols are often added to other protocols to provide secure transmission of data? (Select two.)

- [ ] TLS
- [ ] SSL
- [ ] HTTPS
- [ ] SMTP
- [ ] SNMP

Question 138 of 190

A VPN is used primarily for which purpose?

- Allow remote systems to save on long-distance charges.
- Support secured communications over an untrusted network.
- Allow the use of network-attached printers.
- Support the distribution of public web documents.

Question 139 of 190

IPsec is implemented through two separate protocols. What are these protocols called? (Select two.)

- [ ] AH
- [ ] ESP
- [ ] SSL
- [ ] EPS
- [ ] L2TP

Question 140 of 190

Which of the following network layer protocols provides authentication and encryption services for IP-based network traffic?

- ( ) TCP
- ( ) IPsec
- ( ) SSL
- ( ) L2TP

Question 141 of 190

Which of the following statements about SSL VPN are true? (Select two.)

- [ ] Uses port 443.
- [ ] Encrypts the entire communication session.
- [ ] Uses pre-shared keys for authentication.
- [ ] Encapsulates packets by adding a GRE header.
- [ ] Uses UDP port 500.
- [ ] Provides message integrity using HMAC.

Question 142 of 190

Which of the following can route Layer 3 protocols across an IP network?

- ( ) GRE
- ( ) IPsec
- ( ) SSL
- ( ) PPTP

Question 143 of 190

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match. What do you know about the file?

- ( ) Your copy is the same as the copy posted on the website.
- ( ) You can prove the source of the file.
- ( ) No one has read the file contents as it was downloaded.
- ( ) You will be the only one able to open the downloaded file.

Question 144 of 190

Which of the following networking devices or services prevents the use of IPsec in most cases?

- ◯ Firewall
- ◯ Router
- ◯ NAT
- ◯ Switch

Question 145 of 190

Which of the following attacks tries to associate an incorrect MAC address with a known IP address?

- ◯ ARP poisoning
- ◯ Hijacking
- ◯ Null session
- ◯ MAC flooding

Question 146 of 190

You have just purchased a new network device and are getting ready to connect it to your network. Which of the following should you do to increase its security? (Select two.)

- ☐ Change default account passwords
- ☐ Remove any backdoors
- ☐ Apply all patches and updates
- ☐ Conduct privilege escalation
- ☐ Implement separation of duties

Question 147 of 190

You want to make sure that a set of servers will only accept traffic for specific network services. You have verified that the servers are only running the necessary services, but you also want to make sure that the servers will not accept packets sent to those services.

Which tool should you use?

- ◯ Packet sniffer
- ◯ Port scanner
- ◯ IDS
- ◯ IPS
- ◯ System logs

Question 148 of 190

What security mechanism can be used to detect attacks originating on the internet or from within an internal trusted subnet?

- ◯ Firewall
- ◯ IDS
- ◯ Security alarm
- ◯ Biometric system

Question 149 of 190

What actions can a typical passive intrusion detection system (IDS) take when it detects an attack? (Select two.)

- ☐ The IDS logs all pertinent data about the intrusion.

- [ ] LAN-side clients are halted and removed from the domain.
- [ ] An alert is generated and delivered via email, the console, or an SNMP trap.
- [ ] The IDS configuration is changed dynamically, and the source IP address is banned.

Question 150 of 190

Which of the following activities are considered passive in regards to the function of an intrusion detection system? (Select two.)

- [ ] Monitoring the audit trails on a server
- [ ] Disconnecting a port being used by a zombie
- [ ] Listening to network traffic
- [ ] Transmitting FIN or RES packets to an external host

Question 151 of 190

Which of the following is the most common detection method used by an IDS?

- ○ Signature
- ○ Anomaly
- ○ Behavior
- ○ Heuristic

Question 152 of 190

Which of the following are security devices that perform stateful inspection of packet data, looking for patterns that indicate malicious code? (Select two.)

- [ ] VPN
- [ ] Firewall
- [ ] IDS
- [ ] IPS
- [ ] ACL

Question 153 of 190

Which IDS method searches for intrusion or attack attempts by recognizing patterns or identities listed in a database?

- ○ Heuristics-based
- ○ Anomaly-analysis-based
- ○ Stateful-inspection-based
- ○ Signature-based

Question 154 of 190

You are concerned about protecting your network from network-based attacks from the internet. Specifically, you are concerned about zero day attacks (attacks that have not yet been identified or that do not have prescribed protections).

Which type of device should you use?

- ○ Signature-based IDS
- ○ Anomaly-based IDS
- ○ Anti-virus scanner

- ◯ Network-based firewall
- ◯ Host-based firewall

Question 155 of 190

Which of the following uses hacking techniques to proactively discover internal vulnerabilities?

- ◯ Reverse engineering
- ◯ Penetration testing
- ◯ Inbound scanning
- ◯ Passive reconnaissance

Question 156 of 190

What is the main difference between vulnerability scanning and penetration testing?

- ◯ Vulnerability scanning is performed within the security perimeter; penetration testing is performed outside of the security perimeter.
- ◯ Vulnerability scanning uses approved methods and tools; penetration testing uses hacking tools.
- ◯ The goal of vulnerability scanning is to identify potential weaknesses; the goal of penetration testing is to attack a system.
- ◯ Vulnerability scanning is performed with a detailed knowledge of the system; penetration testing starts with no knowledge of the system.

Question 157 of 190

What is the primary purpose of penetration testing?

- ◯ Test the effectiveness of your security perimeter.
- ◯ Evaluate newly deployed firewalls.
- ◯ Assess the skill level of new IT security staff.
- ◯ Infiltrate a competitor's network.

Question 158 of 190

Which of the following activities are typically associated with a penetration test? (Select two.)

- ☐ Interviewing employees to verify the security policy is being followed
- ☐ Running a vulnerability scanner on network servers
- ☐ Attempting social engineering
- ☐ Running a port scanner
- ☐ Creating a performance baseline

Question 159 of 190

Which of the following types of penetration test teams will provide you information that is most revealing of a real-world hacker attack?

- ◯ Full knowledge team
- ◯ Zero knowledge team
- ◯ Partial knowledge team
- ◯ Split knowledge team

Question 160 of 190

A security administrator is conducting a penetration test on a network. She connects a notebook system running Linux to the wireless network and then uses NMAP to probe various network hosts to see which operating system they are running.

Which process did the administrator use in the penetration test in this scenario?

- ◯ Passive fingerprinting
- ◯ Active fingerprinting
- ◯ Network enumeration
- ◯ Firewalking

Question 161 of 190

Your company is a small start-up that has leased office space in a building shared by other businesses. All businesses share a common network infrastructure. A single switch connects all devices in the building to the router that provides internet access.

You would like to make sure that your computers are isolated from computers used by other companies. Which feature should you request to have implemented?

- ◯ VLAN
- ◯ Spanning tree
- ◯ Port security
- ◯ VPN

Question 162 of 190

A network switch is configured to perform the following validation checks on its ports:

- All ARP requests and responses are intercepted.
- Each intercepted request is verified to ensure that it has a valid IP-to-MAC address binding.
- If the packet has a valid binding, the switch forwards the packet to the appropriate destination.
- If the packet has an invalid binding, the switch drops the ARP packet.

Which security feature was enabled on the switch to accomplish this task?

- ◯ IGMP snooping
- ◯ Port security
- ◯ DHCP snooping
- ◯ Dynamic ARP Inspection

Question 163 of 190

Which of the following actions should you take to reduce the attack surface of a server?

- ◯ Disable unused services.
- ◯ Install anti-malware software.
- ◯ Install the latest patches and hotfixes.
- ◯ Install a host-based IDS.

Question 164 of 190

Which type of security uses MAC addresses to identity devices that are allowed or denied a connection to a switch?

- ◯ Port security
- ◯ Traffic shaping
- ◯ Secure Sockets Layer
- ◯ MAC spoofing

Question 165 of 190

You manage a network that uses switches. In the lobby of your building are three RJ45 ports connected to a switch.

You want to make sure that visitors cannot plug in their computers into the free network jacks and connect to the network, but you want employees who plug into those same jacks should be able to connect to the network.

What feature should you configure?

- Port authentication
- Mirroring
- Bonding
- Spanning tree
- VLANs

Question 166 of 190

In which of the following situations would you use port security?

- You want to prevent sniffing attacks on the network.
- You want to restrict the devices that could connect through a switch port.
- You want to control the packets sent and received by a router.
- You want to prevent MAC address spoofing.

Question 167 of 190

A network switch detects a DHCP frame on the LAN that appears to have come from a DHCP server that is not located on the local network. In fact, it appears to have originated from outside the organization's firewall.

As a result, the switch drops the DHCP message from that server.

Which security feature was enabled on the switch to accomplish this?

- IGMP snooping
- Port security
- DHCP snooping
- Dynamic ARP inspection

Question 168 of 190

You have recently experienced a security incident with one of your servers. After some research, you determine that the hotfix #568994 that has recently been released would have protected the server.

Which of the following recommendations should you follow when applying the hotfix?

- Apply the hotfix immediately to the server; apply the hotfix to other devices only as the security threat manifests itself.
- Apply the hotfix immediately to all servers.
- Test the hotfix, then apply it to all servers.
- Test the hotfix, then apply it to the server that had the problem.

Question 169 of 190

Which of the following is the best recommendation for applying hotfixes to your servers?

- Apply hotfixes immediately as they are released.
- Apply only the hotfixes that apply to software running on your systems.
- Wait until a hotfix becomes a patch, then apply it.

- ◯ Apply all hotfixes before applying the corresponding service pack.

Question 170 of 190

In addition to performing regular backups, what must you do to protect your system from data loss?

- ◯ Store the backup media in an on-site fireproof vault.
- ◯ Regularly test restoration procedures.
- ◯ Restrict restoration privileges to system administrators.
- ◯ Write-protect all backup media.

Question 171 of 190

Why should you store backup media off site?

- ◯ To reduce the possibility of theft.
- ◯ To comply with government regulations.
- ◯ To prevent the same disaster from affecting both the network and the backup media.
- ◯ To make the restoration process more efficient.

Question 172 of 190

You just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a server room that requires an ID card for access. You backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using a Telnet client with the username **admin** and the password **admin**. You used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device? (Select two.)

- ☐ Use an SSH client to access the router configuration.
- ☐ Change the default administrative user name and password.
- ☐ Use encrypted type 7 passwords.
- ☐ Use a web browser to access the router configuration using an HTTP connection.
- ☐ Use TFTP to back up the router configuration to a remote location.

Question 173 of 190

You are in the middle of a big project at work. All of your work files are on a server at the office. You want to be able to access the server desktop, open and edit files, save the files on the server, and print files to a printer connected to a computer at home.

Which protocol should you use?

- ◯ FTP
- ◯ TFTP
- ◯ RDP
- ◯ Telnet
- ◯ SSH

Question 174 of 190

Your organization recently purchased 18 iPad tablets for use by the organization's management team. These devices have iOS pre-installed on them.

To increase the security of these devices, you want to apply a default set of security-related configuration settings.

What is the best approach to take to accomplish this? (Select two. Each option is a part of a complete solution.)

- [ ] Require uses to install the configuration profile.
- [ ] Join the tablets to a Windows domain.
- [ ] Configure security settings in a Group Policy object.
- [ ] Configure and distribute security settings in a configuration profile.
- [ ] Enroll the devices in a mobile device management system.
- [ ] Configure and apply security policy settings in a mobile device management system.

Question 175 of 190

A smart phone was lost at the airport. There is no way to recover the device. Which if the following will ensure data confidentiality on the device?

- ○ Remote wipe
- ○ Screen lock
- ○ GPS
- ○ TPM

Question 176 of 190

The owner of a hotel has contracted you to implement a wireless network to provide internet access for patrons.

The owner has asked that you implement security controls so that only paying patrons are allowed to use the wireless network. She wants them to be presented with a login page when they initially connect to the wireless network. After entering a code provided by the concierge at check-in, they should then be allowed full access to the internet. If a patron does not provide the correct code, they should not be allowed to access the internet.

Under no circumstances should patrons be able to access the internal hotel network where sensitive data is stored.

What should you do?

- ○ Implement a guest network.
- ○ Implement MAC address filtering.
- ○ Implement 802.1x authentication using a RADIUS server.
- ○ Implement pre-shared key authentication.

Question 177 of 190

Beside protecting a computer from under-voltages, a typical UPS also performs which two actions?

- [ ] Protects from over-voltages
- [ ] Conditions the power signal
- [ ] Prevents electric shock
- [ ] Prevents ESD

Question 178 of 190

You are adding a new rack to your data center, which will house two new blade servers and a new switch. The new servers will be used for virtualization.

The only space you have available in the data center is on the opposite side of the room from your existing rack, which already houses several servers, a switch, and a router. You plan to configure a trunk port on each switch and connect them with a straight-through UTP cable that will run across the floor of the data center.

To protect equipment from power failures, you also plan to install a UPS in the rack along with redundant power supplies for the server.

Will this configuration work?

- ○ Yes. This configuration complies with data center best practices.
- ○ No. You should not run a cable across the floor of the data center.

- No. You should not use blade servers for virtualization.
- No. You must use a cross-over cable to connect the two switches together.
- No. You must implement the UPS and power supplies to the rack externally.

Question 179 of 190

Your 24U rack currently houses two 4U server systems. To prevent overheating, you've installed a rack-mounted environment monitoring device within the rack.

Currently, the device shows that the temperature within the rack is 70 degrees Fahrenheit (21 degrees Celsius).

What should you do?

- Nothing. The temperature within the rack is within acceptable limits.
- Install an additional air conditioning unit for the server room.
- Install a humidifier to increase the humidity within the server room.
- Re-orient the cold aisle within the server room so that it is directed toward the air conditioner's return duct.

Question 180 of 190

You are concerned about attacks directed at the firewall on your network. You would like to examine the content of individual frames sent to the firewall.

Which tool should you use?

- Packet sniffer
- Load tester
- Throughput tester
- Event log
- System log

Question 181 of 190

You have heard about a Trojan horse program where the compromised system sends personal information to a remote attacker on a specific TCP port. You want to be able to easily tell whether any of your systems are sending data to the attacker.

Which log should you monitor?

- Firewall
- Application
- Security
- System

Question 182 of 190

You are the network administrator for a growing business. When you were hired, the organization was small, and only a single switch and router were required to support your users. During this time, you monitored log messages from your router and switch directly from each device's console.

The organization has grown considerably in recent months. Now you manage eight individual switches and three routers. It's becoming more and more difficult to monitor these devices and stay on top of issues in a timely manner.

What should you do?

- Use syslog to implement centralized logging.
- Consolidate network resources down to one or two switches.
- Use a remote access utility such as SSH to access router and switch consoles remotely.
- Hire additional resources to help monitor and manage your network infrastructure.

Question 183 of 190

You have been using SNMP on your network for monitoring and management. You are concerned about the security of this configuration.

What should you do?

- ◯ Implement version 3 of SNMP.
- ◯ Combine SNMP with SSL.
- ◯ Use SSH instead of SNMP.
- ◯ Implement a RADIUS solution.

Question 184 of 190

Which of the following are improvements to SNMP that are included within SNMP version 3? (Select two.)

- ☐ Authentication for agents and managers
- ☐ Hashing of the community name
- ☐ Encryption of SNMP messages
- ☐ Use of SFTP for transferring SNMP data

Question 185 of 190

Which protocol uses traps to send notifications from network devices?

- ◯ SNMP
- ◯ SMTP
- ◯ IMAP4
- ◯ ICMP
- ◯ IGMP

Question 186 of 190

Which of the following devices accepts incoming client requests and distributes those requests to specific servers?

- ◯ IPS
- ◯ Load balancer
- ◯ CSU/DSU
- ◯ Caching engine
- ◯ Media converter

Question 187 of 190

Which of the following devices is used on a LAN and offers guaranteed bandwidth to each port?

- ◯ Bridge
- ◯ Switch
- ◯ Router
- ◯ Hub

Question 188 of 190

You are a network administrator for your company. A frantic user calls you one morning exclaiming that nothing is working. What should you do next in your

troubleshooting strategy?

- Establish the symptoms.
- Establish what has changed.
- Identify the affected area.
- Recognize the potential effects of the problem.

Question 189 of 190

You are a network administrator for your company. A user calls and tells you that after stepping on the network cable in her office, that she can no longer access the network.

You go to the office and see that one of the user's stiletto heels has broken and exposed some of the wires in the Cat 5 network cable. You make another cable and attach it from the wall plate to the user's computer.

What should you do next in your troubleshooting strategy?

- Establish what has changed.
- Document the solution.
- Test the solution.
- Recognize the potential effects of the solution.

Question 190 of 190

Users report that the network is down. As a help desk technician, you investigate and determine that a specific router is configured so that a routing loop exists.

What should you do next?

- Determine if escalation is needed.
- Create an action plan.
- Fix the problem.
- Document the problem.