Latest Version: 6.0

Question: 1

Which of the following is MOST likely to use an RJ-11 connector to connect a computer to an ISP using a POTS line?

A. Multilayer switch
B. Access point
C. Analog modem
D. DOCSIS modem

Answer: C

Explanation:
OBJ-1.2 An analog modem is a device that converts the computer's digital pulses to tones that can be carried over analog telephone lines and vice versa. DSL is the other type of Internet connection that uses an RJ-11 connection to a phone line. A DOCSIS modem is a cable modem and would require a coaxial cable with an F-type connector. An access point is a wireless device that connects to an existing network using twisted pair copper cables and an RJ-45 connector. A multilayer switch can use either twisted pair copper cables using an RJ-45 connector or a fiber optic cable using an MTRJ, ST, SC, or LC connector.

Question: 2

You are configuring a point-to-point link between two routers and have been assigned an IP of 77.81.12.14/30. What is the network ID associated with this IP assignment?

A. 77.81.12.12
B. 77.81.12.13
C. 77.81.12.14
D. 77.81.12.15

Answer: A

Explanation:
OBJ-1.4 In classless subnets using variable length subnet mask (VLSM), the network ID is the first IP address associated within an assigned range. In this example, the CIDR notation is /30, so each subnet will contain 4 IP addresses. Since the IP address provided is 77.81.12.14/30, the network ID is 77.81.12.12/30, the first router is 77.81.12.13/30, the second router is 77.81.12.14/30, and the broadcast address is 77.81.12.15/30.

Question: 3

You just heard of a new ransomware attack that has been rapidly spreading across the internet that takes advantage of a vulnerability in the Windows SMB protocol. To protect your network until Microsoft releases a security update, you want to block the port for SMB at your firewall to prevent becoming a victim of this attack. Which of the following ports should you add to your blacklist?

A. 123
B. 143
C. 445
D. 514

Answer: C

Explanation:
OBJ-1.5 Server Message Block (SMB) uses ports 139 and 445, and is a network file sharing protocol that runs on top of the NetBIOS architecture in Windows environments. When the WannaCryransomware was spreading rapidly across the internet, you could help protect your organization's network by blocking ports 139 and 445 at your firewall to prevent your machines from getting infected over the internet. Network Time Protocol (NTP) uses port 123 and is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Internet Message Access Protocol (IMAP) uses port 143 and is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. System Logging Protocol (Syslog) uses port 514 and is a way network devices can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices. Devices can use a Syslog agent to send out notification messages under a wide range of specific conditions.

Question: 4

Which of the following ports is used by LDAP by default?

A. 53
B. 389
C. 427
D. 3389

Answer: B

Explanation:
OBJ-1.5 LDAP uses port 389 by default. LDAP (Lightweight Directory Access Protocol) Standard for accessing and updating information in an X.500-style network resource directory. Unless secure communications are used, LDAP is vulnerable to packet sniffing and Man-in-the-Middle attacks. It is also

usually necessary to configure user permissions on the directory. LDAP version 3 supports simple authentication or Simple Authentication and Security Layer, which integrates it with Kerberos or TLS.

Question: 5

You have just finished installing a new web application and need to connect it to your Microsoft SQL database server. Which port must be allowed to enable communications through your firewall between the web application and your database server?

A. 1433
B. 1521
C. 3306
D. 3389

Answer: A

Explanation:
OBJ-1.5 Microsoft SQL uses ports 1433, and is a proprietary relational database management system developed by Microsoft that is fully compatible with the structured query language (SQL). MySQL uses ports 3306 and is an open-source relational database management system that is fully compatible with the structured query language (SQL). SQLnet uses ports 1521 and is a relational database management system developed by Oracle that is fully compatible with the structured query language (SQL). Remote Desktop Protocol (RDP) uses port 3389 and is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

Question: 6

The network install is failing redundancy testing at the MDF. The traffic being transported is a mixture of multicast and unicast signals. Which of the following devices would BEST handle the rerouting caused by the disruption of service?

A. Layer 3 switch
B. Proxy server
C. Layer 2 switch
D. Smart hub

Answer: A

Explanation:
OBJ-2.1 A layer 3 switch is the best option because, in addition to its capability of broadcast traffic reduction, it provides fault isolation and simplified security management. This is achieved through the use of IP address information to make routing decisions when managing traffic between LANs. Multicast and unicast are layer 3 messaging flows, so you need a router or layer 3 switch to route them across the

network. A smart hub is a layer 1 device. A proxy server operates at layer 4, but would still require a router or layer 3 switch to route the traffic.

Question: 7

Which of the following describes a design where traffic is shared between multiple network servers to provide greater throughput and reliability?

A. Load balancing
B. MPLS trunking
C. VLAN tagging
D. Multiplexing

Answer: A

Explanation:
OBJ-3.3 Load balancing is a technique used to spread work across multiple computers, network links, or other devices. Multiprotocol Label Switching is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. VLAN tagging is used to keep traffic from different networks separate when traversing shared links and devices within a network topology. Multiplexing is the technology that is able to combine multiple communication signals together in order for them to traverse an otherwise single signal communication medium simultaneously.

Question: 8

Which of the following type of sites would be used if your organization needs to be able to shift operations to the site and allow business operations to continue immediately?

A. Cold site
B. Warm site
C. Hot site
D. Cloud site

Answer: C

Explanation:
OBJ-3.3 A hot site is a real-time replication of an existing network environment. All data generated and stored at the primary site is immediately replicated and backed up at the disaster recovery site. A warm site is a type of facility an organization uses to recover its technology infrastructure when its primary data center goes down. A warm site features an equipped data center but no customer data. A cold site is a backup facility with little or no hardware equipment installed. A cold site is essentially an office space with basic utilities such as power, cooling system, air conditioning, and communication

equipment, etc. A cloud site is a virtual recovery site that allows you to create a recovery version of your organization's enterprise network in the cloud. Cloud sites are useful when your disaster recovery plan includes migrating to a telework or remote operations environment.

Question: 9

Which of the following levels would a notice condition generate?

A. 1
B. 3
C. 5
D. 7

Answer: C

Explanation:
OBJ-3.1 The severity levels range from zero to seven, with zero being the most severe and seven being the least severe. Level 0 is used for an emergency and is considered the most severe condition because the system has become unstable. Level 1 is used for an alert condition and means that there is a condition that should be corrected immediately. Level 2 is used for a critical condition, and it means that there is a failure in the system's primary application and it requires immediate attention. Level 3 is used for an error condition, and it means that something is happening to the system that is preventing the proper function. Level 4 is used for warning conditions and it may indicate that an error will occur if action is not taken soon. Level 5 is used for notice conditions and it means that the events are unusual, but they are not error conditions. Level 6 is used for information conditions and it is a normal operational message that requires no action. Level 7 is used for debugging conditions and is just information that is useful to developers as they are debugging their networks and applications.

Question: 10

Which of the following levels would an error condition generate?

A. 1
B. 3
C. 5
D. 7

Answer: B

Explanation:
OBJ-3.1 The severity levels range from zero to seven, with zero being the most severe and seven being the least severe. Level 0 is used for an emergency and is considered the most severe condition because the system has become unstable. Level 1 is used for an alert condition and means that there is a condition that should be corrected immediately. Level 2 is used for a critical condition, and it means that

there is a failure in the system's primary application and it requires immediate attention. Level 3 is used for an error condition, and it means that something is happening to the system that is preventing the proper function. Level 4 is used for warning conditions and it may indicate that an error will occur if action is not taken soon. Level 5 is used for notice conditions and it means that the events are unusual, but they are not error conditions. Level 6 is used for information conditions and it is a normal operational message that requires no action. Level 7 is used for debugging conditions and is just information that is useful to developers as they are debugging their networks and applications.

Question: 11

Which of the following types of fire suppression systems utilizes halocarbon or inert gas to suffocate the fire when the system is activated?

A. Clean agent system
B. Wet pipe system
C. Pre-action system
D. HVAC system

Answer: A

Explanation:
OBJ-3.3 Special suppression systems, like a clean agent system, use either a halocarbon agent or inert gas. When releases, the agents will displace the oxygen in the room with the inert gas and suffocates the fire. A fire suppression system is an engineered set of components that are designed to extinguish an accidental fire in a workplace or datacenter. A wet pipe system is the most basic type of fire suppression system, and it involved using a sprinkler system and pipes that always contain water in the pipes. A pre-action system minimizes the risk of accidental release from a wet pipe system. With a pre-action system, both a detector actuation like a smoke detector and a sprinkler must be tripped prior to water being released. Heating Ventilation and Air Conditioning (HVAC) units are responsible for maintaining the proper temperature and humidity within a datacenter.

Question: 12

Dion Training Solutions is launching their brand new website. The website needs to be continually accessible to our students and reachable 24x7. Which networking concept would BEST ensure that the website remains up at all times?

A. Snapshots
B. Warm site
C. Cold site
D. High availability

Answer: D

Explanation:
OBJ-3.3 High availability is a concept that uses redundant technologies and processes to ensure that a system is up and accessible to the end-users at all times. Snapshots, warm sites, and cold sites may be useful for recovering from a disaster-type event, but they will not ensure high availability. High availability (HA) is a component of a technology system that eliminates single points of failure to ensure continuous operations or uptime for an extended period.

Question: 13

You are conducting an intensive vulnerability scan to detect which ports might be open to exploitation. During the scan, one of the network services becomes disabled and impacts the production server. Which of the following sources of information would provide you with the most relevant information for you to use in determining which network service was interrupted and why?

A. Syslog
B. Network mapping
C. Firewall logs
D. NIDS

Answer: A

Explanation:
OBJ-3.1 The Syslog server is a centralized log management solution. By looking through the Syslog server's logs, the technician could determine which service failed on which server since all the logs are retained on the Syslog server from all of the network devices and servers. Network mapping is conducted using active and passive scanning techniques and could help determine which server was offline, but not what caused the interruption. Firewall logs would only help determine why the network connectivity between a host and destination may have been disrupted. A network intrusion detection system (NIDS) is used to detect hacking activities, denial of service attacks, and port scans on a computer network. It is unlikely to provide the details needed to identify why the network service was interrupted.

Question: 14

A third-party vendor has just released patches to resolve a major vulnerability. There are over 100 critical devices that need to be updated. What action should be taken to ensure the patch is installed with minimal downtime?

A. Test the patch in a lab environment and then install it in the production network during the next scheduled maintenance
B. Download and install all patches in the production network during the next scheduled maintenance period
C. Deploy the patch in a lab environment to quickly conduct testing, get approval for an emergency change, and then immediately install it in the production environment

D. Configure endpoints to automatically download and install the patches

Answer: C

Explanation:
OBJ-3.2 Patches should always be tested first. Once successfully tested, deployment to the production environment can then be accomplished.

Question: 15

Which of the following errors would be received if raw data is accidentally changed as it transits the network?

A. Giant
B. CRC error
C. Runt
D. Encapsulation error

Answer: B

Explanation:
OBJ-3.1 Cyclic Redundancy Checksum (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data as it transits the network. The CRC number in the interface statistics is the number of packets that were received that failed the cyclic redundancy checksum, or CRC check upon receipt. If the checksum generated by the sender doesn't match the one calculated by this interface upon receipt, a CRC error is counted and the packet is rejected. Encapsulation is a process by which a lower-layer protocol receives data from a higher-layer protocol and then places the data into the data portion of its frame. Thus, encapsulation is the process of enclosing one type of packet using another type of packet. A giant is any ethernet frame that exceeds the 802.3 frame size of 1518 bytes. A runt is an ethernet frame that is less than 64 bytes in size.

Question: 16

Which of the following policies or plans would dictate the complexity requirements for a wireless network's shared secret key?

A. Password policy
B. Acceptable use policy
C. Data loss prevention policy
D. Remote access policy

Answer: A

Explanation:
OBJ-3.2 A password policy is a set of rules created to improve computer security by motivating users to create dependable, secure passwords and then store and utilize them properly. This document promotes strong passwords by specifying a minimum password length, complexity requirements, requiring periodic password changes, and placing limits on the reuse of passwords. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict the ways in which the network, website, or system may be used and sets guidelines as to how it should be used. A data loss prevention policy is a document that defines how organizations can share and protect data. It guides how data can be used in decision-making without it being exposed to anyone who should not have access to it. The goal of a data loss prevention policy is to minimize accidental or malicious data loss. A remote access policy is a document which outlines and defines acceptable methods of remotely connecting to the internal network.

Question: 17

Which of the following policies or plans would dictate how an organization would respond to an unplanned outage of their primary internet connection?

A. Business continuity plan
B. Incident response plan
C. Disaster recovery plan
D. System life cycle plan

Answer: A

Explanation:
OBJ-3.2 A business continuity plan is a document that outlines how a business will continue operating during an unplanned disruption in service. A business continuity plan is more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, your human capital and business partners, and essentially every other aspect of the business that might be affected. A disaster recovery plan is a documented, structured approach that documents how an organization can quickly resume work after an unplanned incident. These unplanned incidents include things like natural disasters, power outages, cyber attacks, and other disruptive events. An incident response plan contains a set of instructions to help our network and system administrators detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work. System life cycle plans, also known as life cycle planning, describes the approach to maintaining an asset from creation to disposal. In the information technology world, we normally have a 5-phase lifecycle that is used for all of our systems and networks Planning, Design, Transition, Operations, and Retirement.

Question: 18

Which of the following type of sites would contain little to no hardware and could take days or weeks to become ready for use during a disaster?

A. Cold site
B. Warm site
C. Hot site
D. Cloud site

Answer: A

Explanation:
OBJ-3.3 A cold site is a backup facility with little or no hardware equipment installed. A cold site is essentially an office space with basic utilities such as power, cooling system, air conditioning, and communication equipment, etc. A warm site is a type of facility an organization uses to recover its technology infrastructure when its primary data center goes down. A warm site features an equipped data center but no customer data. A hot site is a real-time replication of an existing network environment. All data generated and stored at the primary site is immediately replicated and backed up at the disaster recovery site. A cloud site is a virtual recovery site that allows you to create a recovery version of your organization's enterprise network in the cloud. Cloud sites are useful when your disaster recovery plan includes migrating to a telework or remote operations environment.

Question: 19

A small office has an Internet connection that drops out at least two times per week. It often takes until the next day for the service provider to come out and fix the issue. What should you create with the service provider to reduce this downtime in the future?

A. NDA
B. SLA
C. AUP
D. MOU

Answer: B

Explanation:
OBJ-3.2 A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end-user that defines the level of service expected from the service provider. SLAs are output-based that their purpose is specifically to define what the customer will receive. If the customer requires faster response times, it should be in the SLA. An acceptable use policy (AUP) is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used. A memorandum of understanding (MOU) is important because it defines the responsibilities of each party in an agreement, provides the scope and authority of the agreement, clarifies terms and outlines compliance issues. A non-disclosure agreement (NDA) is a legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.

Question: 20

A company-wide audit revealed employees are using company laptops and desktops for personal use. To prevent this from occurring, in which document should the company incorporate the phrase “Company-owned IT assets are to be used to perform authorized company business only"?

A. NDA
B. MOU
C. SLA
D. AUP

Answer: D

Explanation:
OBJ-3.2 Acceptable Use Policy dictates what types of actions an employee can or cannot do with company-issued IT equipment. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict the ways in which the network, website, or system may be used and sets guidelines as to how it should be used. A memorandum of understanding (MOU) is important because it defines the responsibilities of each party in an agreement, provides the scope and authority of the agreement, clarifies terms, and outlines compliance issues. A non-disclosure agreement (NDA) is a legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to. A service level agreement (SLA) is a commitment between a service provider and a client for particular aspects of the service, such as quality, availability, or responsibilities.