Networking Essentials and Security

[Name of the Writer]

[Name of the Institution]

Networking Essentials and Security

**Q1**

VTY (virtual terminal) is a program that emulates the functionality of a classical terminal. It is connected through the LAN or WAN interface on the device. However, a Cisco device should be configured with an IP address to make a VTY connection. A program like PuTTy is required for creating a VTY connection on a Cisco device (Brenton et al., 2000).

**Q2**

There are several reasons why we configure an IP address on a switch. A switch doesn't require to have an IP address configured, but at layer 2 switches IP addresses are required for the management of switches. It is also important to configure the IP address on layer 3 switches so that it allows the host to communicate with other parts of the network (Lewis, 2003).

**Q3**

By default, speed or duplex is automatically configured on Cisco switches. However, you can manually configure the speed or duplex setting on Cisco switches using duplex and speed command in configuration mode (Lewis, 2003). The thing which needs to be considered while manually configuring the speed or duplex setting is that it disables auto-MDIX(Medium-dependent interface).

**Q4**

 If two devices on the same switch are assigned to different VLANs, they will not be able to communicate with each other because routers are required for the communication between two LANs.

**Q5**

A trunk port is a port which is used to carry traffic for all the VLANs. However, a Cisco switch requires a VLAN trunking protocol (VTP) to automatically detect trunk ports in a switch (Lewis, 2003).

**Q6**

 A switch at the root of the spanning tree is also known as the root bridge. The root bridge is a special bridge at the top of the spanning tree (. However, root bridges are designated in multiple VLAN environments by allocating a switch with a root bridge and making a connection with VLAN (What is a Root Bridge, 2019).

**Q7**

When a network is configured statically to send traffic for specific destinations is known as static routing. In static routing, a user configures IP address and subnet mask statically according to the destination. On the other side, Dynamic routing allows us to automatically assign IP addresses to the devices in a network using different routing protocols according to the requirements of a network. There are different dynamic routing protocols which include RIP, EIGRP, ISIS, OSPF and BGP (Rick, 2008).

**Q8**

 Static routing is used when you have very few devices to connect in a network while dynamic routing is used when there are a lot of devices in a network, and you can't configure each device statically (Rick, 2008). However, static and dynamic routing can be used on the same router usually on a home network when some devices such as printers don't work properly in a DHCP network and require a static IP address to work properly.

**Q9**

There are many advantages to using network address translation (NAT). NAT can be used in different scenarios depends on the situation. Sometimes it can be used to save the IP address space and sometimes it can be used to increase the flexibility and reliability of a network. NAT provides an extra layer of security for a network which is the main advantage of using it (Tsirtsis & Srisuresh, 2000).

**Q10**

Administrative distance is used in the routers to select the best path when there are two or more routes to the same destination. It describes the reliability of a routing protocol. However administrative distance value should be small because the smaller value will make the protocol more reliable (Dye et al., 2007).

**Q11**

Packet filtering firewall is a firewall technique used to monitor incoming & outcoming packets and allowing them to enter or stop in a network based on the source IP address, ports & protocols, and destination IP addresses, ports & protocols. However, a circuit-level gateway is used to monitor incoming and outcoming traffic and make decisions on which traffic to enter a network based on sessions or virtual circuits (Dye et al., 2007).

**Q12**

The security functions which are included in an all-in-one security appliance URL filter, Spam filter, Web content filter, Intrusion detection system, Malware inspection, antispyware, traffic shaping, etc. (Frahim et al., 2014).

**Q13**

A standard ACL allows for prioritizing the network traffic according to the source IP address while extended ACL provides better control for prioritizing traffic in a network. Extended ACLs can use source & destination IP address, TCP or UDP source & destination port and protocol ID for prioritizing traffic in a network (Dye et al., 2007).

**Q14**

 Wireless clients will use the SSID and channel to identify a specific wireless access point.

**Q15**

MIMO (multiple-input, multiple-output) approach is used to transfer and receive two or more unique data streams through one radio channel while channel bonding allows for the bonding of two wireless channels.

**Q16**

There are different encryption methods which can be used to encrypt sensitive information such as passwords. The strongest encryption method is the AES (advanced encryption standard) method. Many software and hardware products this encryption method to secure their data. In this method, data is encrypted in blocks, unlike other encryption methods in which data is encrypted bit by bit (Heron, 2009).

**Q17**

VLAN pooling implementation automatically partitions a single broadcast domain into multiple VLANs. It is a feature which enables to group multiple VLANs to form a VLAN pool.

**Q18**

Independent Computer Architecture (ICA) is the protocol which is used to route frames back and forth between wireless network and the wired LAN>

**Q19**

Shared key authentication with WEP uses a shared secret that allows to connect and authenticate with access points. However, it is not a secure method as a shared key can send a plain text query to clients which can create vulnerabilities. Shared authentication has a serious flaw and is open to offline dictionary attacks.

**Q20**

There are different steps involve in an IT asset lifecycle which includes planning, procurement & acquiring, deploy & discover, maintain & manage, and retire (Asset Life Cycle Management, 2019). In the maintenance phase of an IT asset lifecycle, updates and patches are applied.

**Q21**

Fixed fire suppression systems are used to protect areas containing important equipment which include switches, data processing rooms, and process control rooms. They aim to stop a developing fire and alert people about it quickly. While portable fire suppression systems are used to stop small fires before they increase and become big fires. They are flexible and can be taken anywhere as compared to the fixed fire suppression systems.

**Q22**

Mission critical system is very important for the survival of a business or company. It has a huge impact on business operations. Any interruption in a mission-critical system can affect the overall business operations of an organization. Mission critical system is a system that the organization relies on to do their tasks without losing data.

**Q23**

It is important to destroy old versions of the security plan to protect the organization. A security plan contains all the sensitive information of the organization. If the old security plan is not destroyed, it allows an individual or organization to exploit information of your organization so that they can find out information regarding the ins and outs of the security.

**Q24**

 A defense system is a physical security system that establishes controls to make sure that the attacker will not be able to move further forward after destroying one level of security and get access to further data.

**Q25**

We can verify that a website is using HTTPS by capturing the packet of a website using Wireshark. With the help of Wireshark, we can verify that a website is using HTTPS. We can also verify our website is using HTTPS with the help of SSL certificate which provides security to the website.

**Q26**

 In a CSRF/XSRF, the attacker forces a user to open a link which will provide the information of the user to the attacker. In case of XSS, the attacker makes the victim browser to run a script that will create vulnerabilities when a user visits a website while in case of CSRF/XSRF a malicious site forces the victim's browser to send an injected request to a site.

**Q27**

The role of a CA in a PKI is to issue trusted digital certificate which makes sure that the individual granted a unique certificate.

**Q28**

FTPS is a protocol which is used to transfer files from one location to another and add security to the FTP. However, SFTP is a protocol which is an extension of SSH that includes more security as compared to FTPS. FTPS uses two channels, and SFTP uses a single channel to facilitate data transfer.

**Q29**

Cisco Meraki AutoVPN technology which is used to create a site to site VPN. Cisco Meraki MX devices are configured as the VPN tunnel endpoints.

**Q30**

Sniffer-detect script with the NMAP utility allows a user to scan and detect any active IP on the network. After detecting the IP, it checks with IP is legal or an outside attack.

**Q31**

IPS differ from an IDS in the way that they detect attacks. IDS analyze network traffic for signatures that match known cyber attacks while IPS not only analyzes network traffic but also stop the packet from being delivered.

**Q32**

In black box testing, QA engineers do not have access to the source code. They just check that everything is working fine according to the point of view of the user. While in grey box testing QA engineers have some access to the source code to as compared to QA engineers in black box testing but still they do the same process which is done in black box testing (Khan, 2012).

**Q33**

DHCP snooping is used to provide network security. It is a layer 2 security technology built into the OS of a network switch to prevent malicious traffic in a network.

**Q34**

Enticement and Entrapment basically have the same concept. However, enticement is legal, but entrapment is not legal. Enticement is the process of tempting someone into your trap while entrapment is the process in which a government agency forces a person to commit a crime.

**References**

Khan, M. E., & Khan, F. (2012). A comparative study of white box, black box, and grey box testing techniques. Int. J. Adv. Comput. Sci. Appl, 3(6).

Lewis, W. (2003). CCNP Cisco Networking Academy Program: Multilayer Switching Companion Guide. Cisco Press.

Brenton, C., Abuhoff, B., Hamilton, A., & Kessler, G. C. (2000). Mastering Cisco Routers. Sybex.

Rick, G. (2008). Routing Protocols and Concepts, CCNA exploration companion guide. Pearson Education India.

What is a Root Bridge (Switch), Bridge (Switch) Priority Value and Bridge (Switch)ID. (2019). Omnisecu.com. Retrieved from <http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-a-root-bridge-switch.php>

Tsirtsis, G., & Srisuresh, P. (2000). Network address translation-protocol translation (NAT-PT) (No. RFC 2766).

Dye, M., McDonald, R., & Rufi, A. (2007). Network Fundamentals, CCNA Exploration Companion Guide: CCNA Exploration Companion Guide. Cisco Press.

Frahim, J., Santos, O., & Ossipov, A. (2014). Cisco ASA: all-in-one firewall, IPS, and VPN adaptive security appliance. Pearson Education.

Heron, S. (2009). Advanced encryption standard (AES). Network Security, 2009(12), 8-12.

Asset Life Cycle Management -. (2019). Ncs-grp.com. Retrieved from <http://www.ncs-grp.com/asset-life-cycle-management/>