**Miguel Sanchez – CIDM 6303 Networking Notes**

**Understanding the OSI Model – N10-008 CompTIA Network+: 1.1**

* The professor is reviewing the OSI (Open Systems Interconnection) model which is a conceptual framework used in information technology to describe the flow of data across a network.
* The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
* Each layer serves a specific purpose, from managing physical connections and signaling to handling data encryption and application-level communication.
* The OSI model can be used in networking, troubleshooting, and understanding real-world scenarios.
* Layers are associated with tangible elements like cables, MAC addresses, IP addresses, and protocols such as TCP and UDP.
* Applications like Wireshark are packet capture applications used to analyze network traffic and illustrate how different layers of the OSI model are represented in the captured data.

**VLANs and Trunking – N10-008 CompTIA Network+ : 2.3**

* VLANs (Virtual Local Area Networks) and trunking have various methods to implement and benefits.
* Network administrators often segment networks into different broadcast domains for security and organizational purposes.
* VLANs offer a solution to logically separate broadcast domains within a switch, avoiding the inefficiencies of physically separated switches which can be a logistical nightmare for organizations (especially banks as in my case).
* Trunking, specifically IEEE 802.1Q standard or dot1Q, enables the extension of multiple VLANs over a single connection between switches, promoting more efficient network management.
  + The process involves adding a VLAN header to ethernet frames for identification, and the VLAN trunking configuration allows communication between devices on different VLANs.
* VLANs and trunking can be used in voice over IP phone and computer connections.
* The reason why VLANs and trunking is such a popular solution for networking is because they help optimize network resources and improving quality of service for voice communication.

**Security Policies – N10-008 CompTIA Network+: 3.2**

* Cybersecurity focuses on the importance of robust credentials, specifically usernames and passwords. This is the first defense mechanism against potential attackers.
* The importance of having strong, unpredictable passwords with increased randomness, helps protect against brute force attacks.
* Avoiding common and easily guessable passwords is extremely critical.
* Best practices for passwords include a combination of uppercase, lowercase, and special characters is necessary for added security.
* A strong password to be eight characters or longer, with multiple words or phrases.
* Avoid reusing passwords, companies use systems that recognize and discourage the use of the same passwords.
* Organizations implement acceptable use policies (AUPs) to guide technology use, ensuring clarity on acceptable and unacceptable practices.
* Bring Your Own Device (BYOD) policies poses security challenges, prompting the need for separation of personal and company data and the implementation of Mobile Device Managers (MDMs) to enforce security measures.
* Remote access policies address security concerns when users access networks outside physical office premises, outlining encryption requirements, credentials, and hardware specs.
* For new hires there should be IT agreements and configuring accounts. For offboarding there must be procedures to ensure secure data handling when employees leave.
* Data Loss Prevention (DLP) solutions play a big role in identifying and blocking the transfer of sensitive information (i.e. as Social Security or credit card numbers). These DLP solutions help mitigate risks associated with data leaks.
* Maintaining a dynamic and constantly updated security policy is needed to meet the evolving nature of Technology.

**Networking Hardening N10-008 CompTIA Network+ : 4.3**

* Network administrators commonly use SNMP (Simple Network Management Protocol) to query and receive information about devices on a network, but SNMP versions 1 and 2 lack proper security due to the absence of encryption.
* SNMP version 3 is recommended for encrypted communication, but not all devices support it.
* Router Advertisement (RA) guard is a technique to protect against on-path attacks or denial of service by validating router advertisements in IPv6 networks.
* Port security on switches prevents unauthorized access by monitoring and limiting the number of MAC addresses on a specific interface.
* Dynamic ARP Inspection (DAI) on switches helps prevent ARP spoofing attacks by validating ARP requests and responses based on a predefined list.
* Securing the control plane of network devices is crucial, involving measures like firewalling, quality of service configuration, and rate limiting for management traffic.
* Port isolation restricts communication between devices on the same network, enhancing security, and administratively disabling unused interfaces prevents unauthorized access.
* Closing unnecessary ports on devices using firewalls and limiting access to essential services improves security.
* Changing default credentials, creating strong passwords, and implementing DHCP snooping enhance device security.
* VLAN segregation is advised to separate user and management traffic.
* Regular firmware updates are essential for addressing security vulnerabilities, and maintaining a library of firmware versions is useful for troubleshooting.
* Network access control using 802.1X authentication adds an extra layer of security by requiring valid authentication before granting access to the network.
* Role-based access control and Access Control Lists (ACLs) help manage user permissions and restrict access based on specific criteria.
* Firewalls with rule-based configurations can control traffic by allowing or denying based on rule criteria, with an implicit deny at the end to log unmatched traffic.

**Common Wireless Issues – N10-008 CompTIA Network+ : 5.4**

* Wireless Channel Overlapping - Overlapping channels on wireless networks create interference, especially in areas with multiple access points.
  + In the 2.4 GHz frequency range, channels 1 through 11 are available in the United States.
  + Best practice is to use access points on channels 1, 6, and 11(non-overlapping) to avoid interference.
  + Frequency and Access Point Placement - Adding access points on channels that overlap (e.g., channel 8) can cause network performance issues You need to place access points in the right spots where they to avoid overlap this is essential for the best wireless network results.
* Signal Attenuation and Range - Signal strength decreases with distance from the access point, resulting in slower network connections. As well as having obstructions in the range of the connection (such as doors, walls and etc).
* Control access point power output or replace antennas to enhance signal strength.
* Coaxial cable between access point and antenna introduces signal loss, higher at 5 GHz than 2.4 GHz.
* SSID and Authentication - In crowded areas, selecting the correct SSID is crucial for security and proper connection.
  + Different authentication methods exist (PSK, 802.1X) depending on the network environment (home vs. enterprise).
* Encryption Compatibility - Ensure wireless device encryption matches the supported types on the access point to enable a successful connection.
  + Legacy devices may need alternative access points or upgrades to connect to modern networks.
* Captive Portal and Authentication Timeframes - Captive portals prompt user authentication; authentication has set timeframes.
  + Different authentication databases (LDAP, RADIUS) store user credentials.
* Client Disassociation Attacks - Disassociation attacks disconnect devices from the wireless network, observed in Wireshark packet captures.
  + Resolving disassociation attacks involves removing the attacker or upgrading to the latest 802.11 standards.