CS4404 Discussion Assignment 7

give me a guide on how to write assignment using prompt engineering effectvively

Security measures are a major consideration while planning any network.

Compare security needs in “wired” Local Area Networks (LAN) and wireless LAN networks. Which network type do you think requires more stringent security measures?

In your responses to your peers, compare and contrast your answer to those of your peers.

Your Discussion should be a minimum of 200 words in length.

I would like to write a post that comparing and contrasting the security threats between wired LAN network and wireless LAN network.

It shall be paragraphed clearly. And after the comparison, based on the analysis, tell me which network type that discussed requires more stringent security measures and what are the measures.

When it comes to security threats, both wired LAN and wireless LAN networks face their own set of challenges. Wired LAN networks are generally considered to be more secure than wireless LAN networks due to the physical connection required for access. However, wired LAN networks are still susceptible to security threats such as unauthorized access through physical ports, and the potential for network breaches through compromised devices.(*LAN Security and How It Is Hacked*, n.d.)

On the other hand, wireless LAN networks are vulnerable to a wider range of security threats, including eavesdropping, unauthorized access, and rogue access points. Additionally, wireless LAN networks are more susceptible to attacks such as denial of service (DoS) and man-in-the-middle attacks(*What Is Wi-Fi Security? - Cisco*, n.d.).

Based on the analysis, it is clear that wireless LAN networks require more stringent security measures compared to wired LAN networks. Some measures that can be taken to enhance the security of wireless LAN networks include implementing strong encryption protocols such as WPA2 or WPA3(*What Is Wi-Fi Security? - Cisco*, n.d.), using strong and unique passwords for network access, enabling MAC address filtering to restrict access to authorized devices, and regularly updating firmware and security patches on wireless access points and devices(*LAN Security and How It Is Hacked*, n.d.).

Additionally, implementing network segmentation and using virtual private networks (VPNs) can help to further secure wireless LAN networks from potential security threats(*The Future of Security – O’Reilly*, n.d.).

Reference

*LAN security and how it is hacked*. (n.d.). Retrieved January 1, 2024, from https://www.grandmetric.com/lan-security-attacks/

*The Future of Security – O’Reilly*. (n.d.). Retrieved January 1, 2024, from https://www.oreilly.com/radar/the-future-of-security/

*What Is Wi-Fi Security? - Cisco*. (n.d.). Retrieved January 1, 2024, from https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html