Title: The Importance of Computer Networking in Cybersecurity:

*Name: Sanada Thomas*

*Class: Cybersecurity*

*Teacher: Shannon Moffatt*

*Due Date: 25/4/2023*

Abstract:

Cybersecurity has become a major concern in today's technology-driven world. The increasing use of the internet, cloud computing, and mobile devices has made it easier for cybercriminals to carry out attacks on individuals and organizations. Computer networking plays a crucial role in cybersecurity by providing the infrastructure necessary for secure communication and information exchange. This research paper provides a comprehensive review of the importance of computer networking in cybersecurity. The paper discusses the basics of computer networking, different types of networks, and the importance of network security protocols. The research paper also explores the latest cybersecurity threats and how computer networking can help mitigate them. The paper concludes by highlighting the critical role of computer networking in ensuring the security of information in today's digital world.

Introduction:

The use of technology in our daily lives has increased exponentially in recent years. From smartphones to laptops and tablets, technology has revolutionized the way we communicate, work, and access information. However, as our reliance on technology has grown, so has the threat of cybercrime. Cybercriminals can steal sensitive data, cause system failures, and disrupt critical services. Cybersecurity has become a crucial concern for individuals, organizations, and governments alike. Computer networking plays a crucial role in cybersecurity by providing the infrastructure necessary for secure communication and information exchange.

Basics of Computer Networking:

Computer networking is the practice of connecting computer devices or systems for the purpose of sharing resources and data. It has become an integral part of modern technology, as it facilitates communication, collaboration, and data sharing. However, computer networking also introduces various security risks and threats, making it essential to implement effective cyber security measures. This research paper will explore the importance of computer networking in cyber security and will discuss the different types of networks, network topologies, and networking devices.

Importance of Computer Networking in Cyber Security:

Computer networks are vulnerable to various security risks and threats, such as unauthorized access, data theft, malware attacks, and network intrusions. Cyber security is the practice of protecting computer networks and systems from these threats. Effective cyber security measures help to prevent unauthorized access, protect sensitive data, and maintain network availability.

Computer networking plays a vital role in cyber security, as it enables the implementation of various security measures, such as firewalls, intrusion detection systems, and encryption. Networking devices, such as routers and switches, provide network administrators with the ability to manage and control network traffic, monitor network activity, and implement security policies. Therefore, computer networking is a crucial aspect of cyber security that enables organizations to protect their data, systems, and networks from cyber threats.

Importance of Network Security Protocols:

Network security protocols are essential for protecting networks from unauthorized access, data theft, and cyber-attacks. Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are used to encrypt data transmitted over the internet. The Internet Protocol Security (IPsec) protocol is used to secure data transmitted over a network. Firewalls are used to block unauthorized access to a network, and Intrusion Detection and Prevention Systems (IDPS) are used to detect and prevent attacks.

Cybersecurity Threats:

Cybersecurity threats are evolving rapidly, and new threats are emerging every day. Some of the most common cybersecurity threats include malware, ransomware, phishing attacks, and Distributed Denial of Service (DDoS) attacks. These threats can cause significant financial losses, reputational damage, and disruption of services.

Role of Computer Networking in Cybersecurity:

Computer networking is a critical component of cybersecurity. It provides the infrastructure necessary for secure communication and information exchange. Networks can be secured using a combination of security protocols, firewalls, and IDPS. By implementing robust network security measures, organizations can protect their sensitive data and prevent cyber-attacks.

Types of Networks:

There are several types of computer networks, including LAN, WAN, MAN, WLAN, and PAN.

1. LAN (Local Area Network):

A LAN is a network that connects devices within a limited geographical area, such as a home, office, or building. LANs are usually owned and managed by a single organization and are used for internal communication and data sharing.

1. WAN (Wide Area Network):

A WAN is a network that connects devices over a wide geographical area, such as a city, country, or even worldwide. WANs are typically owned and managed by multiple organizations and are used for long-distance communication and data sharing.

1. MAN (Metropolitan Area Network):

A MAN is a network that connects devices within a metropolitan area, such as a city or town. MANs are usually owned and managed by a single organization or a consortium of organizations and are used for high-speed data transmission and communication.

1. WLAN (Wireless Local Area Network):

A WLAN is a wireless network that connects devices within a limited geographical area, such as a home, office, or building. WLANs use wireless communication technologies, such as Wi-Fi, to enable data transmission and communication.

1. PAN (Personal Area Network):

A PAN is a network that connects devices within a personal space, such as a room or a person's body. PANs are typically used for personal communication and data sharing, such as connecting a smartphone to a smartwatch or a wireless headset.

Network Topologies:

The network topology refers to the way in which devices are connected in a network. There are several network topologies, including star, bus, ring, mesh, and hybrid.

1. Star Topology:

In a star topology, devices are connected to a central hub or switch. The central hub or switch acts as a mediator between the connected devices, enabling data transmission and communication.

1. Bus Topology:

In a bus topology, devices are connected to a central cable or bus. Data transmission occurs along the central cable, with each connected device receiving and transmitting data as required.

1. Ring Topology:

In a ring topology, devices are connected in a circular manner, with each device connected to its adjacent devices. Data transmission occurs in a circular fashion, with each device receiving and transmitting data as required.

1. Mesh Topology:

In a mesh topology, devices are connected in a complex web of interconnections, with each device connected to multiple other devices. Data transmission occurs along multiple paths, with each device receiving and transmitting data through multiple routes.

1. Hybrid Topology:

a computer network topology that combines two or more different topologies into a single network. This allows for the benefits of each topology to be utilized, while minimizing their individual drawbacks. example of a hybrid topology is a network that combines a bus topology with a ring topology. This type of network can provide a high degree of fault tolerance and scalability, as well as efficient data transmission.

Hybrid topologies can be more complex than single topologies, but they offer advantages in terms of performance, reliability, and scalability. They are commonly used in large enterprise networks where high availability and fault tolerance are critical requirements.

Network Devices:

Networking devices are hardware devices that are used to connect and manage networks. These devices play a critical role in establishing communication and transferring data between devices within a network. Here are the purpose and function of the most commonly used networking devices:

1. Routers: A router is a networking device that is used to connect different networks together. Its primary purpose is to direct data traffic between different networks. Routers use routing tables to determine the best path for data to travel from one network to another. This process is called routing. Routers are also used to provide security by implementing access control lists and filtering rules.
2. Switches: A switch is a networking device that connects devices within a network. The primary function of switches is to direct data traffic between devices within the network. When data is received by a switch, it checks the destination address of the data packet and forwards it to the appropriate device. Switches are more efficient than hubs because they only send data to the device that needs it.
3. Hubs: A hub is a networking device that connects devices within a network. Its primary function is to receive data from one device and then broadcast that data to all other devices connected to the hub. Hubs are not used as much today because they are less efficient than switches. Hubs are also less secure than switches because they do not filter or block data packets.
4. Firewalls: A firewall is a networking device that is used to monitor and control traffic entering and leaving a network. Its primary function is to protect the network from unauthorized access and cyber attacks. Firewalls work by inspecting data packets and applying filtering rules to block or allow traffic based on the rules defined by the network administrator. Firewalls can be configured to allow or block traffic based on source and destination IP addresses, port numbers, and protocols.

In conclusion, networking devices play a critical role in establishing communication and transferring data between devices within a network. Understanding the purpose and function of networking devices is essential for building a secure and efficient network infrastructure. Routers, switches, hubs, and firewalls are the most commonly used networking devices, each with their own unique functions and capabilities.

Conclusion:

In conclusion, computer networking plays a critical role in cybersecurity. The use of networks to share resources and information has become an essential part of modern-day communication. Networks must be secured using a combination of security protocols, firewalls, and IDPS to prevent unauthorized access, data theft, and cyber-attacks. The importance of computer networking in cybersecurity cannot be overstated, and organizations must prioritize network security to protect their sensitive data and services.

References:

1. Barney, N., & Lutkevich, B. (2022). network security. *Networking*. https://www.techtarget.com/searchnetworking/definition/network-security#:~:text=Why%20is%20network%20security%20important,stolen%20assets%20and%20reputational%20harm.
2. Frontpor. (2022, January 31). *Explore the Importance of Computer Networking | Warwick*. Warwick Communications. https://www.warwickinc.com/blog/the-importance-of-computer-networking/
3. NI Business Info. (n.d.). *Benefits of computer networks | nibusinessinfo.co.uk*. https://www.nibusinessinfo.co.uk/content/benefits-computer-networks

Part 2: Application

I've been brought on by Secure Assets Financial, a financial institution, to perform a security audit of their network. I begin by conducting a basic network scan and identify the following potential security vulnerabilities:

* Outdated software and operating systems on several servers and workstations.
* Weak passwords and a lack of multi-factor authentication for some user accounts.
* Unsecured ports and protocols that could allow for unauthorized access.
* Lack of encryption for sensitive data in transit and at rest.
* Unpatched security vulnerabilities in some applications and systems.

b) Based on these vulnerabilities, I suggest the following measures to secure the network and prevent future attacks:

* Establish and enforce strong password policies, as well as implementing multi-factor authentication to prevent unauthorized access to the network.
* Shut down or limit unnecessary ports and protocols to decrease the network's attack surface.
* Encourage the use of encryption for all sensitive data in transit and at rest to prevent data theft or interception.
* Develop and implement a patch management strategy to ensure that all security vulnerabilities are promptly addressed.
* Ensure that all software and operating systems are kept up to date with the latest patches and updates.

c) To maintain the security of the network, you create a plan that includes the following steps:

* Implement a regular schedule of network scans and vulnerability assessments to identify any new security vulnerabilities and prioritize remediation efforts.
* Develop and implement a regular schedule for software and operating system updates to ensure that the network is protected against the latest security threats.
* Implement network segmentation and access controls to limit access to sensitive data and systems.
* Regular employee training and education on security best practices to raise awareness and reduce the risk of human error.
* Regular backup and disaster recovery testing to ensure that critical data can be restored in the event of a breach or outage.
* Regular security audits and penetration testing to identify any new vulnerabilities and ensure that the security measures in place are effective.