**20MCA104 - Advanced Computer Networks**

**ASSIGNMENT 2**

**Subject - Summarise the following: 1. Bluetooth 2. Firewall and VPN**

**Submitted by**

**Nimya Satheesh**

**S2 MCA**

**Roll No : 26**

**BLUETOOTH**

* Bluetooth is a short range wireless communication technology, computers and other devices can easily communicate with each other using Bluetooth.
* It can used to exchange of data between different devices.
* It is an Personal Area Network(PAN)
* The maximum connectivity range of Bluetooth is about 30 feet.
* Bluetooth connections are secure wireless connections.
* Devices connected through Bluetooth are generally secure and safe against hacking.

History : Bluetooth was Developed in 1994,The name "Bluetooth" is taken from a 10th- century Danish king named Harald Bluetooth, Bluetooth was intended as a wireless replacement for cables. It uses the same 2.4GHz frequency as some other wireless technologies in the home or office, such as cordless phones and WiFi routers. It creates a 10- meter (33-foot) radius wireless network, called a Personal area network(PAN)or piconet, which can network between two and eight devices. The first consumer Bluetooth device was launched in 1999.

* Bluetooth range and transmission speeds are typically lower than Wi-Fi
* The maximum range of Bluetooth is 10 meters.
* Data can be exchanged at a rate of 1 megabit per second to 2Mbps in the second generation of the technology.
* Eg: Bluetooth is used to pair mobile devices with other mobile or fixed devices, Earbuds,Car, fridge, mouse to a computer, printer.

**Advantages of Bluetooth:-**

* Connections are encrypted, preventing third party involvement.
* It allow the user limit, device that restricts connection through that specific device.

**Downsides to Bluetooth:-**

* drain battery power.
* Connected range is limited.
* Pairing process may also be difficult.

**Application of Bluetooth:-**

* wireless communication between a mobile phone and wireless headset.
* Wireless communication between smartphone and smart door lock.
* Transfer of files between two devices.

**FIREWALL**

* firewall is a network security system that monitors and controls incoming and outgoing networking traffic based on previously defined a set of network rules.
* The purpose of firewall is to prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks
* Firewalls has established since the late 1980’s

1. Generation 1 Virus :

Late 1980’s, virus attacks on stand-alone PC’s affected all businesses and drove anti-virus products.

1. Generation 2 Networks :

Mid 1990’s, attacks from the internet affected all business and drove creation of the firewall.

1. Generation 3 Applications :

Early 2000’s, exploiting vulnerabilities in applications which affected most businesses and drove Intrusion Prevention Systems Products (IPS).

1. Generation 4 Payload :

Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks which affected most businesses and drove anti-bot and sandboxing products.

1. Generation 5 Mega :

Approx. 2017, large scale, multi-vector, mega attacks using advance attack tools and is driving advance threat prevention solutions.

**Functions of Firewall:-**

* Network Threat Prevention
* Application and Identity-Based Control
* Hybrid Cloud Support
* Scalable Performance
* Network Traffic Management and Control
* Access Validation

**Types of Firewall:-**

1- Packet-filtering firewalls : To checks the packet’s source and destination IP addresses. Divided into two types stateful and stateless.

2- Proxy Firewall:- To filter network traffic at the application level.

3- Stateful Multi-layer Inspection (SMLI) Firewall:- Filter packets at the network layer, transport layer, and application layer, to comparing them against known trusted packets.

4- Next-generation firewall (NGFW):- To combine traditional firewall technology with additional functionality.

5- Network address translation (NAT) firewalls:- To connected with multiple devices with other networks using IP address.

**VPN**

* VPN - Virtual private network
* VPN secure connection on public network, It is an encrypted connection.
* Encrypted the IP addresses from public to make the browsing more secure and private.
* The VPN provide increases in functionality , management of the private network and security.
* VPN establishing a virtual point to point connection through the dedicated circuits
* VPN cannot make online connections with anonymous, but VPN can increase privacy and security.

**Types of VPN:-**

1- Remote access: To provide access to an enterprise network.

2- Site-to-site: To connects two networks.

3- Extranet-based site-to-site: site-to-site configuration.

**VPN works :-**

1. connect to a virtual private network service, it authenticates client with a VPN server.
2. The server encrypted all the data send and receive.
3. VPN creates an encrypted tunnel over the internet, To secure the data traveling between source and destination.
4. To ensure each data packet is secure, the VPN wraps it in an outer packet, the data is encrypted through encapsulation.
5. When the data arrives at the server, the outer packet is removed through a decryption process.