Module – 2

N+ - network security, Maintenance and Troubleshooting procedures

* What is SOHO network?

SOHO (Small Office/Home Office) network refers to a small-scale network designed for a limited number of users, typically in a home or small business setting. It usually includes a few devices, such as computers, printers, and routers, connected together to share resources and access the Internet.

* What is NAT?

NAT (Network Address Translation) is a technique that allows multiple devices on a private network to share a single public IP address when accessing the Internet.

* What is PAT?

PAT (Port Address Translation) is a type of NAT that allows multiple devices on a private network to share a single public IP address by using different port numbers to identify each device.

* Different between NAT & PAT.

**NAT:** Maps multiple private IP addresses to multiple public IP addresses.

**PAT:** Maps multiple private IP addresses to a single public IP address using different port numbers.

* What Is ACL?

ACL (Access Control List) is a set of rules that control traffic flow and access to network resources by filtering incoming and outgoing packets based on criteria such as IP address, port number, and protocol.

* What are different Types of ACL?

There are two main types of ACLs (Access Control Lists):

**1. Standard ACLs:** Filter traffic based on source IP address only.

**2. Extended ACLs:** Filter traffic based on source and destination IP addresses, ports, protocols, and other criteria.

* What Is Wildcard Mask?

A wildcard mask is a 32-bit number used in conjunction with an IP address to specify a range of IP addresses. It uses 0s to match bits and 1s to ignore bits, allowing for flexible IP address matching in ACLs and other network configurations.

* Explain Circuit switching

Circuit switching is a method of transmitting data over a network where a dedicated communication channel (or circuit) is established between two devices for the duration of the transmission. The channel is reserved exclusively for the transmission, ensuring a constant bandwidth and low latency.

* What is difference between leased line and broadband?

**Leased line:** Dedicated, guaranteed speed, expensive.

Leased line is like having a private road for your internet, it’s yours alone and always available.

**Broadband:** Shared, variable speed, cost-effective.

Broadband is like sharing a public road with many others, it’s faster when less crowded, but can slow down when many are using it.

* Difference between a POTS line and a leased line

**POTS (Plain Old Telephone Service) line:** A basic phone line for voice calls, typically analog.

**Leased line:** A dedicated, high-speed digital connection for data transmission, often used for business internet or private networks.

* Practice on printer sharing

Done into lab

* Use of IIS

IIS (Internet Information Services) is used for hosting and managing websites, web applications, and services on a Windows server.

* Create FTP server

Done into lab

* What is the difference between cloud and virtualization?

**Virtualization:**

- Creates virtual versions of physical resources (servers, storage, etc.)

- Runs multiple virtual machines (VMs) on a single physical host

- Improves resource utilization and flexibility

**Cloud:**

- A model for delivering computing resources and services over the internet

- Provides on-demand access to a shared pool of resources (servers, storage, etc.)

- Offers scalability, elasticity, and pay-per-use pricing

In short: Virtualization is a technology, while cloud is a service model built on top of virtualization.

* Why are network monitoring tools used?

Network monitoring tools are used to:

1. Detect and troubleshoot network issues

2. Monitor network performance and optimize bandwidth

3. Identify security threats and vulnerabilities

4. Ensure network uptime and availability

5. Analyze network traffic and usage patterns

These tools help administrators maintain network health, prevent downtime, and improve overall network efficiency.

* What is ping ?

Ping (Packet Internet Groper) is a network diagnostic tool that tests whether a device is reachable over a network. It sends a small packet of data to the device and measures the time it takes to receive a response, verifying:

1. Device connectivity

2. Network latency

3. Packet loss

A successful ping indicates the device is online and responding.

* What is traceroute ?

Traceroute is a network diagnostic tool that maps the path data packets take from your device to a destination device on the internet. It shows:

1. The number of hops (routers) between devices

2. The IP address of each hop

3. The time it takes for packets to travel between hops

Traceroute helps identify network congestion, routing issues, and bottlenecks.

* What is Nslookup?

Nslookup (Name Server Lookup) is a network diagnostic tool that resolves domain names to IP addresses and vice versa. It helps:

1. Verify DNS (Domain Name System) records

2. Troubleshoot DNS resolution issues

3. Find IP addresses associated with domain names

Nslookup queries DNS servers to retrieve information about domain names, IP addresses, and mail servers.

* Explain core switches

Core switches are high-performance network switches that serve as the central backbone, connecting multiple sub-networks and providing high-speed data transfer.

* What is network management?

Network management: Monitoring, maintaining, and optimizing a computer network for efficient, secure, and reliable operation.

* Explain Event Viewer

Event Viewer: A Windows tool that displays system events, errors, and warnings. It helps administrators:

1. Troubleshoot system issues

2. Monitor system security

3. Track system changes

4. Identify potential problems

Event Viewer logs events from various sources, including:

- System events

- Security events

- Application events

- Setup events

It provides detailed information to help diagnose and resolve system issues.

* Practice "parental control" or "family safety" option in control pane

Done into lab

* What are network vulnerabilities?

Network vulnerabilities: Weaknesses or flaws in a network's design, configuration, or operation that can be exploited by attackers to gain unauthorized access, disrupt operations, or steal sensitive data.

* What are the types of network security attacks?

Types of network security attacks:

1. Malware attacks

2. Phishing attacks

3. Denial of Service (DoS) attacks

4. Man-in-the-Middle (MitM) attacks

5. SQL Injection attacks

6. Cross-Site Scripting (XSS) attacks

7. Password cracking attacks

8. Trojan horse attacks

9. Ransomware attacks

10. Zero-Day attacks