**Module 6. Network security, Maintenance and**

**Troubleshooting procedures**

**Topic: A SOHO Networks**

* **Beginner Question**

1. What is SOHO network?

* SOHO stands for Small Office and Home Office Networks. It allows computers in a home office or remote office to connect to a corporate network, or access centralized, shared resources. It is a LAN (local area network) mainly referred to as a business category involving a small number of workers usually from 01 to 10.

1. What does SOHO mean networking?

* Small Office and Home Office Networks
* **Intermediate Question**

1. How does a SOHO network work?

* It allows computers in a home office or remote office to connect to a corporate network, or access centralized, shared resources.

1. Issues with Soho Networking?

* Unlike larger businesses, small businesses generally cannot afford to hire a professional staff to manage their networks. Small businesses also are more likely targets of security attacks than households due to their financial and community position.
* **Advance Question**

1. How Small is the “S” in SOHO?

* The "S" in SOHO stands for "Small." SOHO is an acronym that commonly refers to "Small Office/Home Office." It is used to describe businesses, workplaces, or offices that are typically smaller in scale and located in a home or small office setting, as opposed to larger corporate offices or commercial spaces. So, the "S" in SOHO emphasizes the small scale of the office or workspace it describes.

1. SOHO Routers vs. Home Routers?

* The SOHO router falls between these two types. In terms of price, it is a little more expensive than residential but less expensive than enterprise. While covering nearly the same functionality as a large company's network, it is tailored for the needs of small businesses.

**Topic: NAT & PAT**

* **Beginner Question**

1. What is NAT?

* NAT stands for Network Address Translation. It is a networking technique used to modify network address information in packet headers while in transit through a router or firewall, primarily for the purpose of conserving IP addresses and enhancing security.

1. What is PAT?

* PAT stands for Port Address Translation. It is a specific form of Network Address Translation (NAT) that is used in computer networking to allow multiple devices within a private network to share a single public IP address while differentiating them based on port numbers.

1. Different between NAT & PAT?

* NAT stands for Network Address Translation. PAT stands for Port Address Translation. In NAT, Private IP addresses are translated into the public IP address. In PAT, Private IP addresses are translated into the public IP address via Port numbers.
* **Intermediate Question**

1. However, Will Nat work?

* Yes, Network Address Translation (NAT) works and is a fundamental technology used in computer networking to enable multiple devices within a private network to share a single public IP address for accessing the internet. NAT works by translating the private IP addresses of devices in the local network to a single public IP address when they communicate with external servers or devices on the internet.

1. Explain NAT?

* Network Address Translation (NAT) is a fundamental networking technology used to allow multiple devices within a private network to share a single public IP address for accessing resources on the internet. NAT operates at the network layer (Layer 3) of the OSI model and serves several important purposes
* **Advance Question**

1. What is different between Static & Dynamic NAT?

* The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not.

1. NAT stand for?

* Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet.

1. PAT stand for?

* PAT stands for Port Address Translation. It is a specific variant of Network Address Translation (NAT) used in computer networking to enable multiple devices within a private network to share a single public IP address for internet access. PAT accomplishes this by translating both the source IP address and port number of outgoing packets from devices on the private network, allowing them to be uniquely identified on the internet.

**Topic: Authentication and Access Control**

* **Beginner Question**

1. What Is Acl?

* ACL stands for Access Control List. It is a security feature used in computer networking and information technology to control and manage access to resources, systems, or network devices. An ACL is a set of rules or entries that specify which users, groups, or network entities are allowed or denied access to specific resources or services.

1. What Are Different Types of Acl?

* There are two main different types of Access-list namely:

Standard Access-list – These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite.

Extended Access-list – These are the ACL that uses source IP, Destination IP, source port, and Destination port.

* **Intermediate Question**

1. Explain Standard Access List?

* Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. These are the Access-list which are made using the source IP address only.

1. Explain Extended Access List?

* An extended access control list (ACL) can determine what traffic is allowed or denied access, acting as a gatekeeper for your network. It can give the system administrator setting up the network a higher degree of flexibility and control.
* **Advance Question**

1. What Is Wildcard Mask?

* A wildcard mask, in the context of networking and subnetting, is a bit mask used to specify which portions of an IP address or subnet should be considered significant (matched) and which portions are "wildcarded" or treated as don't-care values. It's often used in conjunction with access control lists (ACLs) or route filtering to define patterns for matching IP addresses or subnets.

1. In Which Directions We Can Apply an Access List?

* The standard Access-list is generally applied close to the destination (but not always). The extended Access-list is generally applied close to the source (but not always). We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.

**Topic: WAN Technologies**

* **Beginner Question**

1. Fiber-optic communication

* Fiber-optic communication is a method of transmitting information using optical fibers, which are thin strands of glass or plastic that carry data in the form of light pulses. This technology is widely used for long-distance and high-speed data transmission in telecommunications, internet connectivity, cable television, and various other applications.

1. What is Leased Line

* A leased line, also known as a dedicated line or private line, is a communication service provided by telecommunications companies that offers a dedicated and continuous line of communication between two or more locations. Leased lines are used primarily for data, voice, and internet connectivity and are popular among businesses and organizations that require reliable, high-quality, and symmetrical (equal upload and download speeds) connections.

1. Explain Circuit switching

* Circuit switching is a traditional method of establishing a dedicated communication path or circuit between two devices for the duration of a conversation or data transfer. This method was widely used in older telephone networks and is still used in some specialized applications today.
* **Intermediate Question**

1. Explain Packet Switching

* Packet switching is a fundamental networking technology used in modern data communication systems, including the internet. It involves breaking data into small packets or chunks, which are then individually routed through a network to their destination. Unlike circuit switching, where a dedicated path is established for the entire duration of a communication, packet switching allows multiple packets from different sources to share network resources simultaneously.

1. What is difference between leased line and broadband?

* Unlike broadband, where the connection is shared among many users (contenders), resulting in slowdowns, a leased line is dedicated to a single user and is not shared with any other users, ensuring that speed remains constant.

1. How much is a 100mb Leased Line?

* The cost of a 100 Mbps leased line can vary significantly based on several factors, including your geographic location, the service provider, the level of service, and contract terms. Leased line pricing can also depend on whether the line is for dedicated internet access, point-to-point connectivity between two locations, or a multipoint connection to link multiple sites.
* **Advance Question**

1. Difference between a POTS line and a leased line?

* What is the difference between a POTS line and a leased line? A leased-line is a permanent connection by a common carrier between two end-points. A POTS line which connects to other POTS line by way of the common carriers switching equipment.

1. What is the process of packet switching?

* Packet switching is the transfer of small pieces of data across various networks. These data chunks or “packets” allow for faster, more efficient data transfer. Often, when a user sends a file across a network, it gets transferred in smaller data packets, not in one piece.

1. Difference between circuit switching and packet switching?

* Circuit switching and packet switching are two fundamentally different methods of routing and managing data in telecommunications and networking. They have distinct characteristics and use cases.

1. Practice on printer sharing

* Done.

1. Use of IIS [ Via "add and remove" feature from control panel. "appwiz.cpl" command]

* Done.

**Topic: Communication technologies Cloud and Virtualization**

* **Beginner Question**

1. What is virtualization?

* Virtualization enables the hardware resources of a single computer to be divided into multiple virtual computers, called virtual machines (VMs).

1. What are two types of virtualization in cloud?

* Types Of Virtualization In Cloud Computing

Server Virtualization.

Application Virtualization.

Network Virtualization.

Desktop Virtualization.

Storage Virtualization.

* **Intermediate Question**

1. What are the two types of virtualization?

* Server virtualization. Server virtualization is a process that partitions a physical server into multiple virtual servers.

1. Storage virtualization.
2. Network virtualization.
3. Data virtualization.
4. Application virtualization.
5. Desktop virtualization.
6. What is VMware virtualization technology?

* Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency.
* **Advance Question**

1. What is the difference between cloud and virtualization?

* In short, virtualization creates simulated versions of a machine's software or hardware components, while cloud computing is a model that enables users to access a shared pool of resources conveniently. We will explore virtualization vs. cloud computing and see what they mean for applications.

1. What are the benefits of implementing virtualization in cloud computing?

* Benefits of Virtualization in Cloud Computing

1. Protection From System Failures.
2. Hassle-Free Data Transfers.
3. Firewall and Security Support.
4. Smoother IT Operations.
5. Cost-Effective Strategies.
6. Disaster Recovery Is Efficient and Easy.
7. Quick and Easy Set Up.
8. Cloud Migration Becomes Easy.

**Topic: Monitoring Tools**

* **Beginner Question**

1. Why are network monitoring tools used?

* Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime. These systems can detect devices and other elements that comprise or touch the network, as well as provide status updates.

1. Explain firewalls

* A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
* **Intermediate Question**

1. Explain core switches

* A core switch is the network switch installed at the backbone of the layered or hierarchy network. These data switches are responsible for routing and data switching at the core layer of the network.

1. Explain client systems

* Client Systems means the Client's information technology infrastructure, including computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Client or through the use of third-party services.
* **Advance Question**

1. What is network management?

* Network management refers to the process of administering, monitoring, and maintaining computer networks to ensure they operate efficiently, securely, and reliably. It involves a combination of hardware, software, policies, and practices aimed at optimizing network performance and minimizing downtime. Network management is crucial in organizations of all sizes, from small businesses to large enterprises, as it helps ensure that their networks meet their operational and business requirements.

1. Explain Event Viewer

* The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer. Examples of these are programs that don't start as expected, or automatically downloaded updates. Event Viewer is especially useful for troubleshooting Windows and application errors.

1. Practice "parental control" or "family safety" option in control panel

* Done.

**Topic: Network Security, Network vulnerabilities**

* **Beginner Question**

1. What are network vulnerabilities?

* What Is A Network Vulnerability? A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach.

1. What are the types of network security attacks?

* Here are some common types of network security attacks:

Malware Attacks:

Viruses: Malicious software that attaches itself to legitimate programs and spreads when the infected program is executed.

Worms: Self-replicating malware that spreads across a network without the need for user interaction.

Trojans: Malware disguised as legitimate software, often used to create backdoors or steal data.

Phishing Attacks:

Phishing: Attackers send fraudulent emails or messages that appear to be from a trusted source to trick recipients into revealing sensitive information, such as passwords or financial details.

Spear Phishing: A targeted form of phishing where attackers tailor their messages to specific individuals or organizations.

Denial of Service (DoS) and Distributed Denial of Service

(DDoS) Attacks:

DoS Attack: Floods a network or system with traffic or requests, overwhelming it and causing it to become inaccessible to legitimate users.

DDoS Attack: Utilizes a network of compromised devices (a botnet) to launch a coordinated DoS attack, making it even more difficult to mitigate.

Man-in-the-Middle (MitM) Attacks:

eavesdropping: Attackers intercept and potentially modify communications between two parties without their knowledge.

Session hijacking: Attackers take control of an established session between two parties, often to steal sensitive information.

Brute Force and Password Attacks: Brute Force Attack: Attackers systematically try all possible combinations of passwords until they find the correct one.

Dictionary Attack: Attackers use a list of commonly used passwords or words from a dictionary to guess passwords.

SQL Injection: Attackers inject malicious SQL (Structured Query Language) code into input fields or queries to gain unauthorized access to a database or manipulate data.

Cross-Site Scripting (XSS): Attackers inject malicious scripts into web applications, which are then executed by unsuspecting users' browsers. This can lead to the theft of session cookies or other sensitive data.

Ransomware Attacks: Malware that encrypts a victim's data, rendering it inaccessible until a ransom is paid to the attacker for the decryption key.

Social Engineering Attacks: Attackers manipulate or deceive individuals into divulging sensitive information or performing actions that compromise security.

Insider Threats: Attacks or security breaches initiated by individuals within an organization who have access to sensitive information and systems.

IoT (Internet of Things) Attacks: Exploitation of vulnerabilities in IoT devices to gain access to networks or disrupt services.

Zero-Day Exploits: Attacks that target vulnerabilities in software or hardware that are not yet known to the vendor or have no available patches.

DNS Spoofing and Cache Poisoning: Manipulating the Domain Name System (DNS) to redirect users to malicious websites or intercept their traffic.

Packet Sniffing: Unauthorized interception of network traffic to capture sensitive data, such as login credentials or financial information.

Eavesdropping and Wiretapping: Illegally monitoring communication channels to intercept sensitive information.

Clickjacking: Deceptive techniques that trick users into clicking on something different from what they perceive, often leading to unintended actions.

* **Intermediate Question**

1. What is virus in network security?

* A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code.

1. What is the difference between virus and antivirus?

* Computer virus is a malicious program, which has the ability to replicate and execute itself. An antivirus software is a computer program used to scan files. It detects, prevents, identifies and eliminates computer viruses and other malicious software.
* **Advance Question**

1. Who is vulnerable in network security?

* One of the most common process vulnerabilities is an authentication weakness, where users, and even IT administrators, use weak passwords. Human vulnerabilities are created by user errors that can expose networks, hardware, and sensitive data to malicious actors.

1. How do you assess vulnerability?

* Assessing vulnerabilities is a critical aspect of maintaining the security of computer networks, systems, and applications. Vulnerabilities are weaknesses or flaws in software, hardware, or configurations that can be exploited by attackers to compromise the integrity, confidentiality, or availability of your systems and data.

1. What are the principles of network security?

* What are the 3 Principles of Information Security? The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

1. What is a firewall to use for?

* What do firewalls do? Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet.

1. configure advanced firewall setting?

* Done.

6. configure "date and time" opti

* Done.