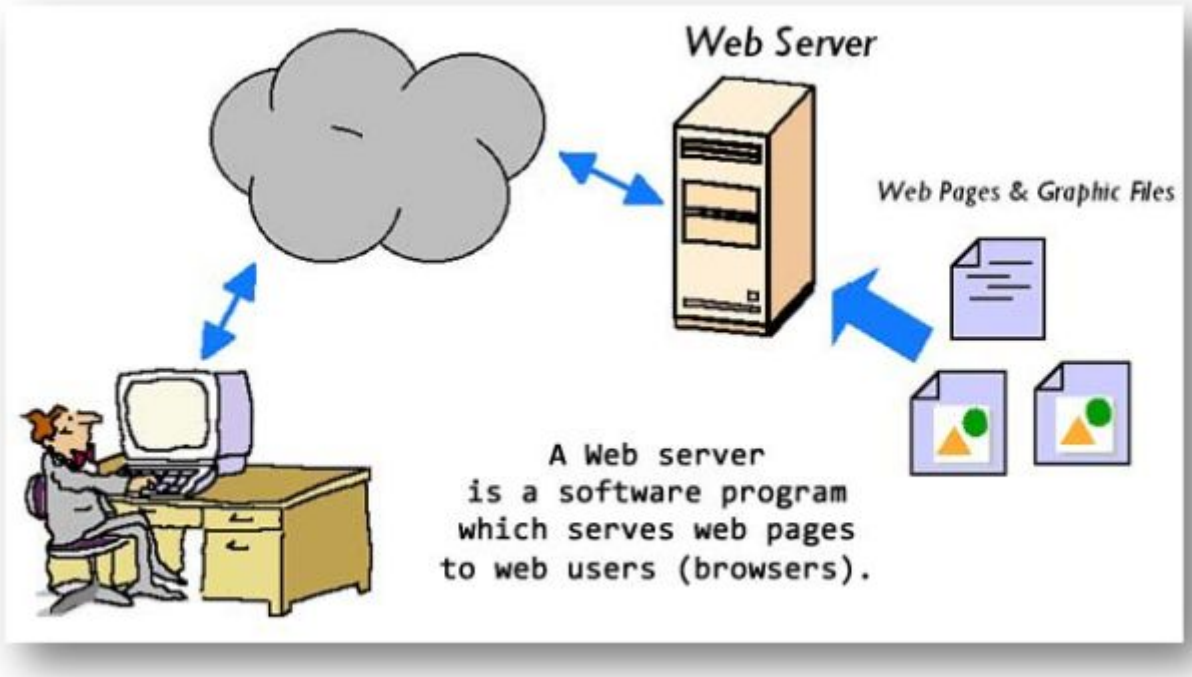
Deliverable 1

Questions

1. What is a web server?



A web server is a computer system or software that stores websites and delivers them to users over the internet. When you type a website address into your browser, the browser sends a request to the web server, which finds the correct webpage, image, or file and sends it back so it can be displayed on your screen. Web servers can refer to both the physical machines in data centers that stay online 24/7 and the software programs that handle requests, such as Apache, Nginx, or Microsoft IIS. In short, a web server is what makes websites accessible by responding to browser requests and sending back the content you want to see.

2. What are some different web server applications?

Application 1

Apache HTTP Server

Apache is the most widely used open-source web server in the world. It’s known for its stability, flexibility, and huge library of modules that let you customize features like security, URL rewriting, authentication, caching, and more. Apache uses a process-based architecture, meaning it creates separate threads to handle requests, which is great for compatibility but can use more memory under heavy load. It runs on almost every operating system, including Linux, Windows, and macOS, and is commonly used for hosting websites, applications, and APIs.

Application 2

Nginx

Nginx (pronounced “engine-x”) is a high-performance web server built to handle large numbers of concurrent connections efficiently. Unlike Apache’s process-based model, Nginx uses an event-driven architecture that makes it extremely fast and lightweight. It’s commonly used for high-traffic sites, reverse proxying, load balancing, caching, and serving static files. Many large companies (Netflix, Spotify, Airbnb) use Nginx because it scales very well and reduces server load.

Application 3

Microsoft IIS (Internet Information Services)

IIS is Microsoft’s web server built into Windows Server, commonly used in enterprise environments where organizations already rely on Microsoft technologies. It integrates tightly with ASP.NET, Active Directory, and Windows authentication, making it ideal for hosting .NET applications and internal corporate sites. IIS includes graphical management tools, request filtering, logging, and built-in security features, and it’s known for being beginner-friendly due to its GUI and Windows integration.

3. What is virtualization?

Virtualization is a technology that lets you run multiple operating systems or computing environments on a single physical computer. Instead of each operating system needing its own separate machine, virtualization uses software called a hypervisor to divide one physical computer’s hardware into several virtual machines (VMs). Each VM acts like its own independent computer with its own CPU, memory, storage, and operating system.

This allows you to run Windows, Linux, and other systems all on the same physical hardware without them interfering with each other. Virtualization improves efficiency, reduces hardware costs, makes testing and labs easier, and allows safe experimentation without damaging the main system. It’s commonly used in IT, cloud computing, servers, homelabs, and cybersecurity labs.

4. What is virtualbox?

VirtualBox is a free, open-source virtualization software that lets you run multiple operating systems on your computer at the same time. It creates virtual machines (VMs)—isolated environments where you can install Windows, Linux, macOS (with limitations), and more, without affecting your main system.

With VirtualBox, you can test software, practice networking labs, run server environments, or try different operating systems safely. It includes features like snapshots (to save the state of a VM), shared folders, USB pass-through, networking modes (NAT, bridged, host-only), and support for 64-bit and multi-core processors. VirtualBox is widely used for homelabs, cybersecurity training, development, and IT education because it works on Windows, macOS, and Linux, and doesn’t require expensive hardware.

5. What is a virtual machine?

A virtual machine (VM) is a software-based computer that runs inside your real, physical computer. It behaves exactly like a separate physical machine, with its own virtual CPU, memory, storage, and operating system. You can install Windows, Linux, or other systems inside a VM without changing anything on your main computer. VMs run on top of virtualization software (like VirtualBox, VMware, or Hyper-V), and they let you test software, run servers, practice networking, experiment safely, or isolate risky tasks. Because each VM is

isolated, anything that happens inside it won't affect your actual computer, making it perfect for IT labs, cybersecurity, and learning new systems.

6. In the context of virtualization, what does host machine and guest machine mean?

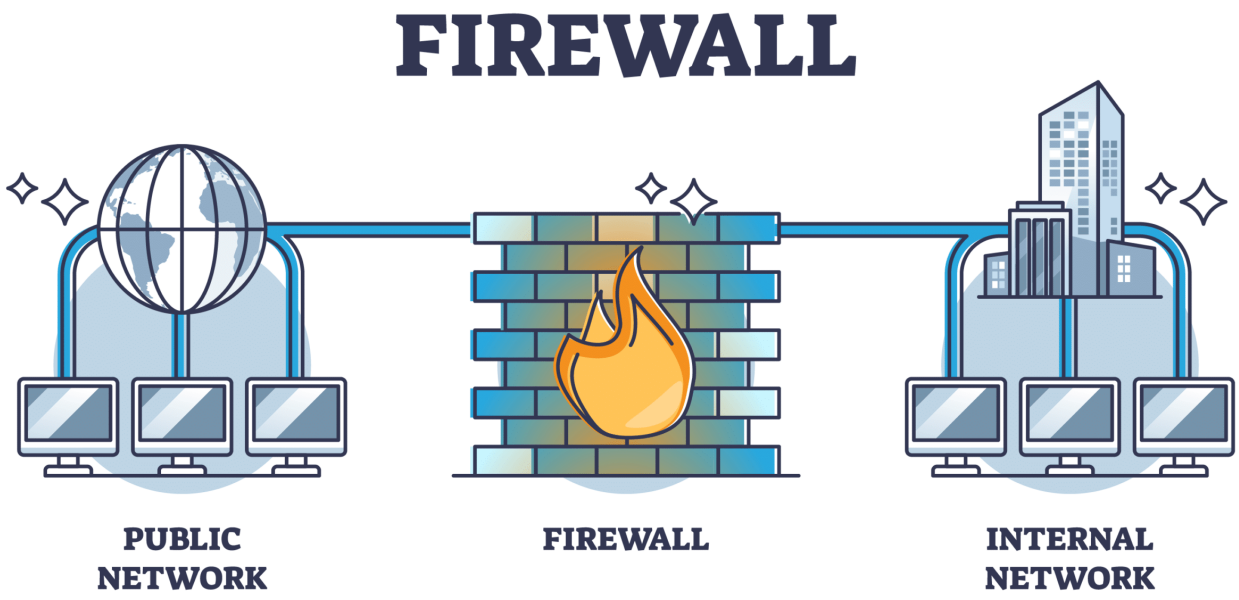
- **Host Machine:** The host machine is the real, physical computer you are using. It provides the actual hardware CPU, RAM, storage, and network that gets shared with virtual machines. Example: Your Windows 10 laptop running VirtualBox is the host.
- **Guest Machine:** The guest machine is the virtual machine (VM) running inside the host. It has its own virtual CPU, memory, storage, and operating system, but all of it is simulated by the host. Example: A Debian Linux VM you installed inside VirtualBox is the guest.

7. What is Debian?

Debian is a free, open-source Linux operating system known for its stability, security, and huge software repository. It's one of the oldest and most respected Linux distributions, and many other popular systems like Ubuntu, Kali Linux, and Linux Mint are built from Debian.

Debian is widely used for servers, cybersecurity labs, development environments, and learning Linux because it's reliable, well-documented, and completely community-driven. When you install Debian, you get the Linux kernel along with thousands of packages for tools, software, and utilities. It's also commonly used in VirtualBox or VMware for IT and networking practice because it runs fast and doesn't use a lot of system resources.

8. What is a firewall?



A firewall is a security tool that protects a computer or network by controlling what traffic is allowed in or out. It acts like a digital security guard, checking each incoming or outgoing connection and deciding whether to

allow or block it based on rules. Firewalls help prevent hackers, malware, and unauthorized access from reaching your devices or network.

Firewalls can be hardware devices (like those used in routers or business networks) or software programs (like Windows Firewall). They filter traffic using rules such as IP addresses, ports, protocols, and application behavior. In short, a firewall creates a protective barrier between a trusted internal network and the untrusted outside world (like the internet) to keep systems safe.

9. What is SSH?

SSH (Secure Shell) is a secure network protocol used to remotely access and manage computers over an unsecured network like the internet. It creates an encrypted connection, which means everything you type passwords, commands, data is protected from anyone trying to spy on it.

With SSH, you can open a command-line session on another computer (usually a server or a Linux machine) and control it as if you were sitting right in front of it. It’s commonly used by system administrators, developers, and IT students for managing servers, running commands, transferring files, and doing remote troubleshooting.

10. What is an IP Address?

An IP address (Internet Protocol address) is a unique number assigned to every device on a network so it can be identified and communicate with other devices. It works like a home address, but for computers—allowing data to know exactly where to go. When you browse the internet, send emails, or connect to Wi-Fi, your device uses its IP address to send and receive information. There are two main types: IPv4 (like 192.168.1.1) and IPv6 (like 2606:4700:4700::1111). Without IP addresses, devices wouldn’t be able to find each other or exchange data across networks or the internet.

11. What is a network mask?

A network mask (also called a subnet mask) is a number that divides an IP address into two parts: the network portion and the host portion. It tells devices which part of the IP identifies the network and which part identifies the specific device on that network.

Example: IP address: 192.168.1.25 Subnet mask: 255.255.255.0 This mask means:

255.255.255 = the network part

0 = the host part

So all devices with IPs starting with 192.168.1.x are on the same network.

12. What is a port? (in the context of networking/computers)

In networking, a port is a virtual doorway on a computer that allows specific types of network traffic to enter or leave. It doesn’t refer to a physical plug it's a software based channel used so multiple applications can use the network at the same time without mixing their data.

Every port is identified by a number (0–65535). Examples:

Port 80 → HTTP (web browsing)

Port 443 → HTTPS (secure web browsing)

Port 22 → SSH

Port 25 → Email (SMTP)

When your computer communicates over the internet or a network, it uses these port numbers so data goes to the correct application. So in simple terms, a port is like a mailbox slot on a computer that routes specific kinds of network traffic to the right program

13. What is port forwarding?

Port forwarding is a networking technique that allows devices outside your home network like the internet to access a specific device or service inside your private network. It works by telling your router to take incoming traffic on a certain port number and send it to a specific internal IP address.

15. What is localhost? (in the context of networking/computers)

Localhost is a special networking term that refers to the computer you are currently using. When you type “localhost” into a browser or terminal, your device automatically directs the connection back to itself using the loopback IP address 127.0.0.1. This allows your computer to test network services, web servers, and applications locally without using the internet or connecting to other devices. Developers and IT students use localhost to safely experiment, run servers, and troubleshoot network issues because it keeps all communication internal to the machine.

16. What does this ip address represent 127.0.0.1?

127.0.0.1 is the loopback IP address, which means it always points back to your own computer. When you use this address, you're telling your device to send network traffic to itself instead of going out to the internet or another machine.

14. What is Git?

Git is a version control system that helps you track changes to files usually code over time. It lets you save versions of your work, go back to earlier versions, and collaborate with others without overwriting each other’s work. Developers use Git to manage projects, fix bugs, create branches for new features, and merge changes safely.

Git stores snapshots of your files, keeps a history of every modification, and makes it easy to work on a project from multiple computers or with a team. It’s fast, secure, and works offline. Platforms like GitHub, GitLab, and Bitbucket use Git to host repositories so people can share and collaborate on code.

15. What is GitHub?

GitHub is an online platform that hosts Git repositories, making it easier to store, share, and collaborate on code projects. While Git is the tool that tracks changes on your computer, GitHub is the website where you can upload those projects so others can view them, contribute, or work with you.

GitHub provides features like issue tracking, pull requests, project management tools, wikis, and automated workflows. Developers use it to work on open source projects, store personal code, build portfolios, and collaborate with teams across the world. It also acts as a cloud backup for your repositories.

Concepts I did not understand

- **Port forwarding**: is a technique that routes incoming traffic on a specific port of your router to a particular device within your private network.
- **SSH**: is a secure protocol used to remotely access and control another computer through an encrypted connection.