Deliverable 1: Projects Requirements

Questions

What is a web server? (In the context of software Ex. Apache)

A web server (like Apache) is a software program that delivers web pages to people when they visit a website.

- It stores, processes, and sends web pages(like HTML, images, or videos) to your web browser when you type a web address.
- In the case of Apache, it runs on a computer(server) and listens for requests from browsers using HTTP or HTTPS protocol.

What are some different web server applications? Include definitions, project's website/where to download it, which operating system is available for and its latest version.

1. **Apache HTTP Server**

   - ***Definition***: A widely-used open source web server known for its flexibility and extensive module support
   - Download: https://httpd.apache.org/download.cgi
   - **Operating Systems**: Linux, Windows, macOS
   - Latest Version: 1.29.2 (Released on October 7, 2025)

2. **NGINX**

   - ***Definition***:A high-performance web server and reverse proxy server designed for scalability and speed.
   - Download: https://nginx.org/en/download.html
   - ***Operating Systems***: Linux, Windows, macOS
   - Latest Version:1.29.2 (Released on October 7, 2025)

3. ***LiteSpeed Web Server***

   - ***Definition***: A commericial web server known for its speed and security features, often used in high-traffic environments.
   - Download: https://www.litespeedtech.com/products/litespeed-web-server/download
   - ***Operating Systems***: Linux, macOS, Windows
   - Latest Version:6.3.4 (Released on August 1, 2025)

What is virtualization?

- Virtualization is the process of creating virtual versions of something, like a computer system, storage, or network, so that multiple operating systems can run on a single physical machine at the same time.

What is virtualbox?

- VirtualBox is a software program that lets you run virtual computers inside your real computer (host)

- Think of VirtualBox like a special manager that divides the house(Your computer) into separate apartments(virtual machines),letting other operating systems like Linux or Windows live there at the same time.

- Each virtual machines has its own CPU, Memory, and storage but it still share the resources of your real computer.

- VirtualBox can be used to safely test new software, try different operating systems, or experiment without affecting main computer.

What is a virtual machine?

- A virtual machine is a software based computer that runs inside physical computer. It can have its own operating system, files, programs, and settings but it exists only as software.
  - Virtual machine machine uses a piece of software called a ***hypervisor*** (like VirtualBox) to share your (host) computer's physical resources like CPU, memory, and storage.
  - Even if it runs on the same hardware, each machine act s like a independent system.
  - Can run multiple VMs at once, and they wont interfere with each other.
  - Perfect for testing,learning, or running different operating systems with out changing host setups.

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

Host Machine

Host machine is the actual physical computer - the one that can physically be touched.

- It runs the main operating system (Windows,macOs, Linux) and has the real hardware (CPU, Ram, stoage).

- The job of host is to run the virtualization software (like VirtualBox) and share its resources with the virtual machines.

- Example:

  - A windows laptop with VirtualBox installed. The laptop is the `host machine`

The host provides parts of its memory, CPU, and disk space to any virtual computers (guests) created.

Guest Machine

The guest machine is the virtual computer that runs inside the host machine.

- It acts just like a regular computer but is completely software-based.

- Each guest machine can have its own operating system, settings, and programs, and it doesn't affect the host directly.

- Example: If created a Linux virtual machine inside VirtualBox on Windows computer. The Linux system is the `guest machine`
- The guest machine uses parts of the host's memory and storage to run, but it behaves like a independent computer.

What is Debian?

Debian is a free and open source operating system that is based on the Linux Kernel. It's a type of Linux operating system, which means it's an alternative to Windows or macOS.

- Debian is built and maintained by a large community of developers who work together to make it secure, reliable, and easy to update.
- What's included with debian is thousands of free software packages like web browsers, text ediors, and office tools that can be installed with a simple command.

What is a firewall?

A firewall is a security system (either software,hardware, or both) that montiors and controls network traffic deciding what data is allowed to enter or leave computer or network.

- Can think of a firewall as a security guard for a computer or network.
- Every time data tries to come in or go out like when visiting a website or downloading something, the firewall check if it's safe or suspicious.
- If the data looks safe, it's allow through; if it looks dangerous like a hacker attack or virus, it's blocked.
- Firewall protects system from unauthorized access, malware, and hackers trying to connect to your network.
- Firewalls can be software-based which means installed on the computer or hardware-based which built into routers or network devices.

What is SSH?

SSH (Secure Shell) is a network protocol that allows you to securely connect to another computer or server over the internet or a local network.

- It lets you control that remote system as if you were sitting right in front of it.
- SSH uses encryption, which means the data sent between the computer and the remote one is locked and protected so no one can read or steal it whiles it while it's being transmitted.
- Once connected, can run commands, transfer files, and configure systems remotely
- Can think of SSH as a secure tunnel that lets you safely log in and control another computer from anywhere in the world.

Example : A company IT staff uses SSH to log into a remote web server to update file or restart services without needing to physically touch the machine.

What is an IP Address?

An IP Address is a unique number assigned to every device that connects to a network or the internet. Its acts like a home address for your computer or phone, allowing other devices to find it and send data to it.

- Every device that connect to the internet like phone, laptop, gaming console needs an IP address so it can communicate with other devices.
- When visiting a website, your computer uses IP address to send and receive information
- Without IP addresses, computers wouldnt know where to send data, just like a mailman cant deliver a letter without an address.
- IP addresses are assigned by the `Internet Service Provider(ISP)` when you connect to the internet.

What is a network mask?

A network mask is a number that helps divide an IP address into two parts:

1. The `Network part` - which identifies the overall network.
2. `The Host Part` - which identifies the indiviual device (computer, phone, etc.) within that network.

- Can think of IP address like a full street address
  - The **network part** is like the street name which tell which specific house on that street.
  - The **host part** is like your house number which tells which specific house on the street.
- Network Mask acts like a filter that tell computers which portion of IP address belong to the network and which belongs to the host.
- It helps organize and manage networks by preventing confusion when multiple devices are connected.
- For example :
  - If a computer's IP address is `192.168.1.10`
  - The `192.168.1` part is network
  - The `.10` is the device (host) on that network.

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

A port is like a door or channel on a computer that allows data to enter or leave.

- a port helps computers and devices communicate over a network or the internet by directing data to the right program or service.
- For example:
  - When visiting a website, the computer uses port 80 or 443 to connect to the web server.
  - Can also think of the computer as a apartment building.
    - The IP address is the building street address
    - The port number is the apartment

What is port forwarding?

Port forwarding is a network feature that allows outside devices on the internet connect to a specific computer or service inside your private home network.

How it works?

- It works by forwarding (sending) data that comes into your router on a specific port number to a specific device (computer, game console, or server) inside your home network.

Port forwarding is commonly used when hosting a web server, game server, or a remote desktop connection and want other to connect to it from outside the home network.

- Can think of it as telling the router where to send specific visitors based on which door (port number) they knock on.

For example: `1. Setting up a web server on the computer using port 80.`

- You configure the router to forward to port 80 to your computer's local IP address (192.168.1.10)
- Now, anyone visiting your public IP address will reach the web server

`2. Hosting an online game on your PC`

- The game uses port 25565 for minecraft.
- You set up port forwarding on the router so friends can connect to your computer over the internet and join your game.

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

Localhost is a special name that means "this computer"

In networking, it refers to your own computer's loopback network connection which is a built in way for your device to communicate with itself using the IP address 127.0.0.1

- When you type localhost into a web browser, you are not going to the internet. You are connecting back to your own computer
    - Mostly used to test websites, servers, or applications locally before making them public.

`Note for reminder` - Local Host mean own computer. Talking to self. Computer connect to itself to test or run programs locally.

Example

1. If installing a web server like Apache on the computer, when you type `http://localhost` in the browser, it opens the website stored on your own computer. That allows you test the website safely before anyone else can see it.

What does this ip address represent 127.0.0.1?

The IP address 127.0.0.1 represent your own computer, also known as `localhost`

- It is a special address that allows your computer to communicate with itself for testing and internal network functions.
- When you send data to 127.0.0.1 it does not go out the internet or any external network. Instead, it stays withing your own computer.
- Useful for systems admins because it lets them test web servers, databases, or applications safely without needing another device or internet connection.

Example - If installing a web server like Apache on the computer and open a browser to `http://127.0.0.1`, you are viewing the website that exists only on the machine not the internet.

`127.0.0.1` is a your computer "home address in networking. It means "this machine" "me"

What is Git?

Git is a version control system.

- Meaning a special type of software that help you track, manage, and save changes to files over time, especially when working on projects like code, documents, or websites.
- It's like a save history for projects.
- Allows multiple people to work on the same project without overwriting each other's work.
- Any changes made you can commit it. commit it means saves a new version that can be reviewed later.
- If something breaks or mistakes made, you can roll back to an older version easily.

Example : If building a website and make a mistake in the code.Because you can save progress with Git, you can go back to an earlier version that worked correctly no work is lost.

What is GitHub?

GitHub is a website and cloud platform that helps people store,share, and collaborate on projects that use Git version control.

Concepts I did not understand

1. **What are `systemd` and `systemctl`**

What is `systemd`?

- When a Linux computer turns on, something has to to:
    - Start background programs (**web servers**, databases, etc)
    - Keep them running
    - Restart them if they crash
- That "something" is called an **init system**
- `systemd` is the modern init system used by most Linux distributions,
- **Example**: Think of `sytemd ` as the manager of all backgrounds apps on your server.
    - It decides what starts,when it starts and what happens if it fails.

What is `systemctl`?

`systemctl` is the command you use to talk to `systemd`

- With **systemctl** you can:

- - Start/stop/restart services (programs)
- - Enable/disable them at boot
- - Check their status
- - See what’s running on the system
- - Edit how services are defined

Example If **systemd** is the manager, systemctl is the remote control you use to give it orders.

Unit = thing systemd manages (file ends in .service, .target, etc.).

Service unit (something.service) = background program (web server, db, etc.).

Basic service commands

`sudo systemctl start NAME.service` - **start now** `sudo systemctl stop NAME.service` - **stop now** `sudo systemctl restart NAME.service` - **stop + start** `sudo systemctl reload NAME.service` - **reload config (no restart)** `sudo systemctl reload-or-restart NAME.service`

Check service status

`sudo systemctl status NAME.service` - detailed status + logs `systemctl is-active NAME.service` - active/inactive (exit 0 = active) `systemctl is-enabled NAME.service` - enabled/disabled `systemctl is-failed NAME.service` - failed/unknown/inactive (exit 0 = failed)

Enable Boot/Disable at Boot

`sudo systemctl enable Name.service` - start automatically at boot `sudo systemctl disable Name.service` - dont start at boot.

2. Understanding Virtual Machine Networking

VM is like a house inside another house.

Your real computer = the big house Your virtual machine = the small house inside it Networking modes = how the small house connects to the outside world

Different network modes decide:

- Can the VM access the internet?
- Can you access the VM from your real computer?
- Can other computers access the VM?
- Can VMs talk to each other?

The Different Network Modes :

1. **Not Attached** Definition:The VM has a network plug, but nothing is plugged in

Example: Like having a Tv but no cable or Wifi hooked up

Result: VM cant access anything and nothing can access the VM

2. **NAT (Network Address Translation)**

Definition: The VM uses your real computer's internet like a kid using their parent's WiFi hotspot.

Example: The VM is hiding behind your computer. It cant go out to the internet, but nobody from the outside can "see" it or reach it.

Result: VM can access the internet, Other computers cannot access you VM, Good for safety,Bad for hosting a web server.

3. **NAT (Network Address Translation)**

Defintion: Similar to NAT, but multiple VMs can talk to each other too.

Example: Think of it as a group of kids sharing one parent's hotspot. They can:

- Use the internet
- Talk to each other But outsiders still cannot talk to them.

Result:

- VMs can talk to the internet
- VMS can talk to each other
- Outside world still cant reach them

4. **Bridged Networking | *Most useful for running servers***|

Definition: Your VM acts like a regular computer on your home network.

Example: Your VM gets its own address on the network — like having its own phone number. Anyone in your house WiFi can call it.

Result:

- Other computers can reach your VM

- VM behaves like a real machine

- Perfect for hosting a web server

This is the easiest way to make the VM reachable from other devices.

5. **Internal Network** - The VM can only talk to other VMs on the same "internal network.

6. **Host-Only Network** - A private network between:

- your real computer (host)
- the VM
- No internet Good for things that only need to talk to the host.

7. **Cloud Networking** - Lets your VM connect to a cloud service's network. Super niche,mostly for advanced setups.

When running a virtual machine, it needs a way to connect to the internet or your home network

Two main ways to connect it:

1. Bridge Adapter (The easier way)

- Can think of it like plugging the virtual machine directly into your router.
- Your Vm gets it own IP address just like any normal computer or phone on your Wi-Fi.

- It behaves like a separate physical computer on your home network.

Why it's easy? You literally just switch the network setting in virtualbox to bridge and boom.

Some computers or routers don't allow this mode.Some network cards (hardware inside your laptop/PC) don't support bridging.Some routers block it for security.If your router or network card won't allow it, the VM basically gets ignored or kicked off the network.

2. NAT with Port Forwarding

- This is like your VM hides behind your actual computer when going online
- Instead of having its own address, it uses your computer's internet connection.

But if you want to access something inside the VM(like a website hosted on it), you have to set up "port forwarding."This kinda of like telling your computer, *If someone knocks on the front door asking for web traffic, send that traffic to the VM.*