Cybersecurity and Ethical Hacking

Lab setup, Networking, Demo on Tools

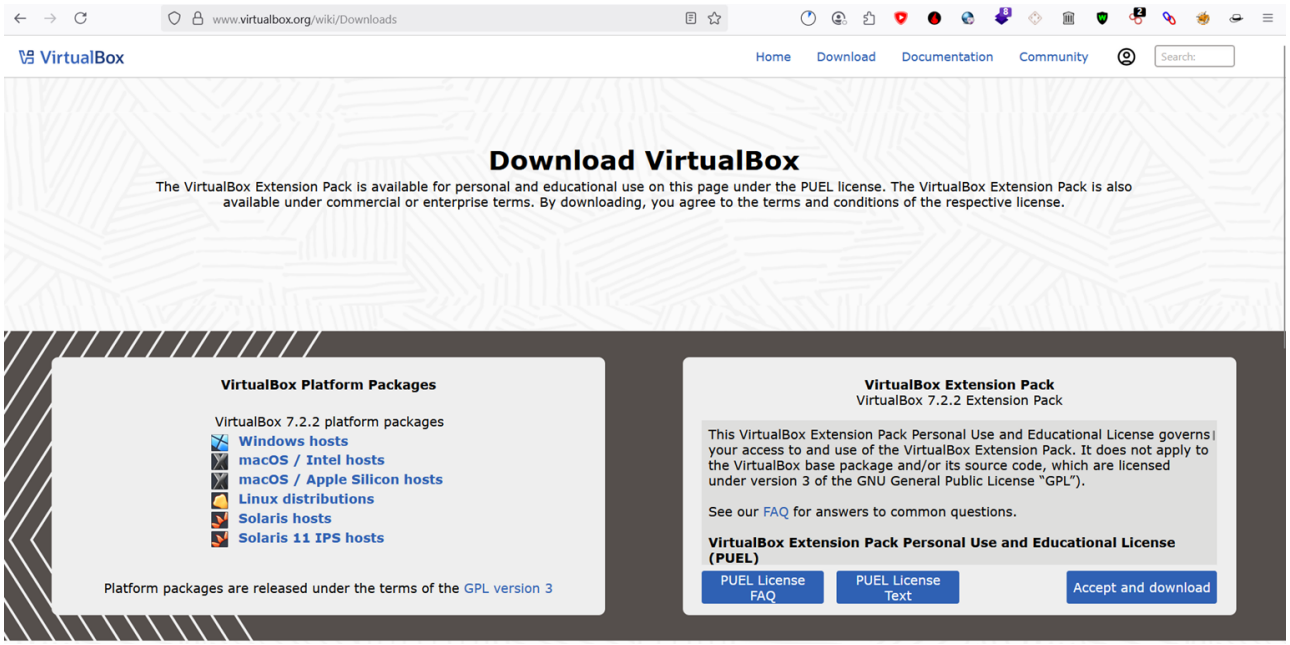
Lab setup :

Host OS:

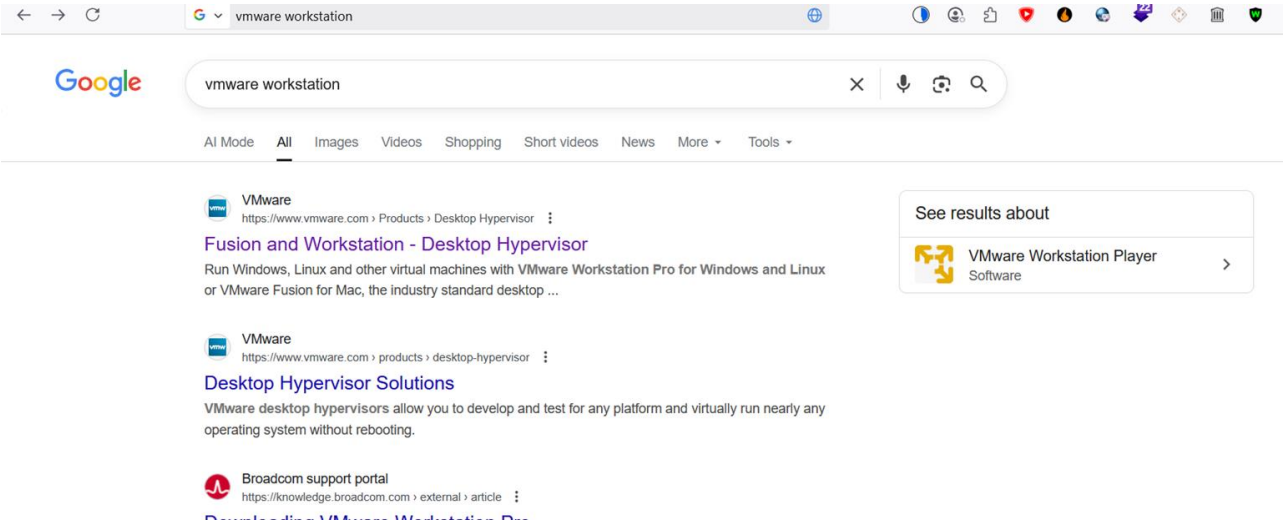
- Virtualization: VirtualBox/VMware (version)
- Kali image: <filename, version>
- Metasploitable image: <filename, version>
- Network setup: (Host-only, NAT, Bridged). Include IP addressing scheme.

2. Installation steps Vmware/VirtualBox

- Download Vmware/VirtualBox
- https://www.virtualbox.org/wiki/Downloads



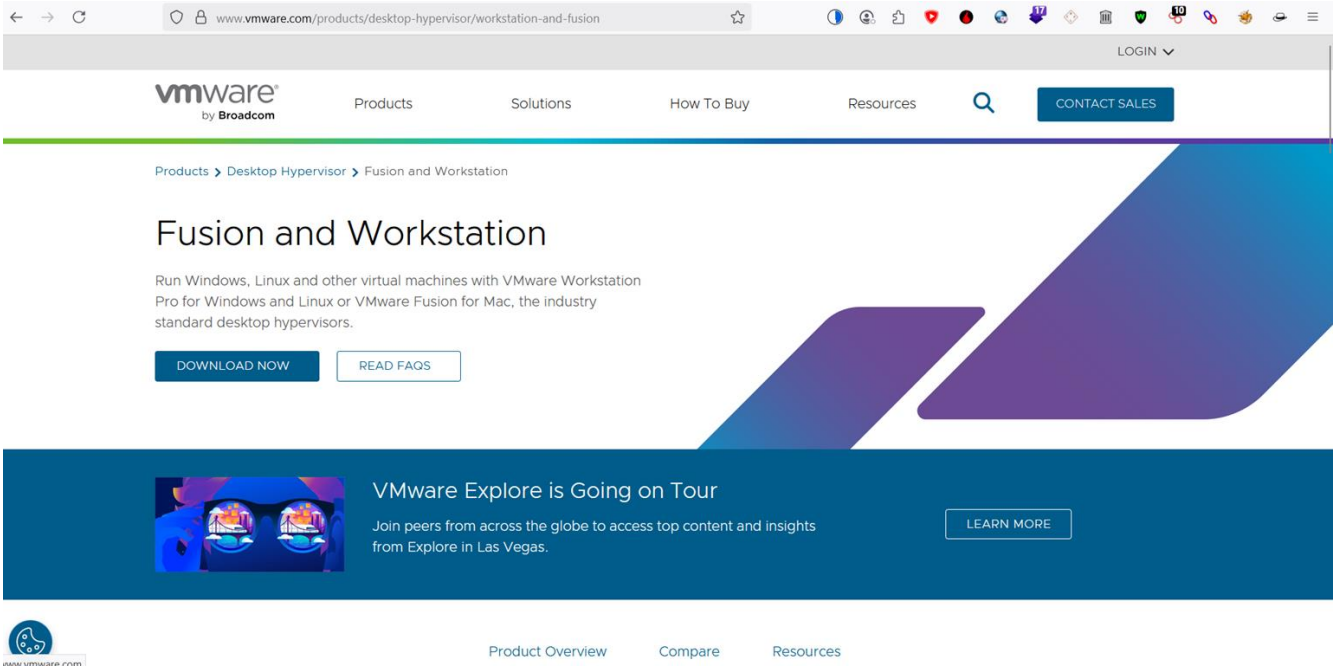
- Above method is how to dowload virtual box this method is how to download Vmware



❿

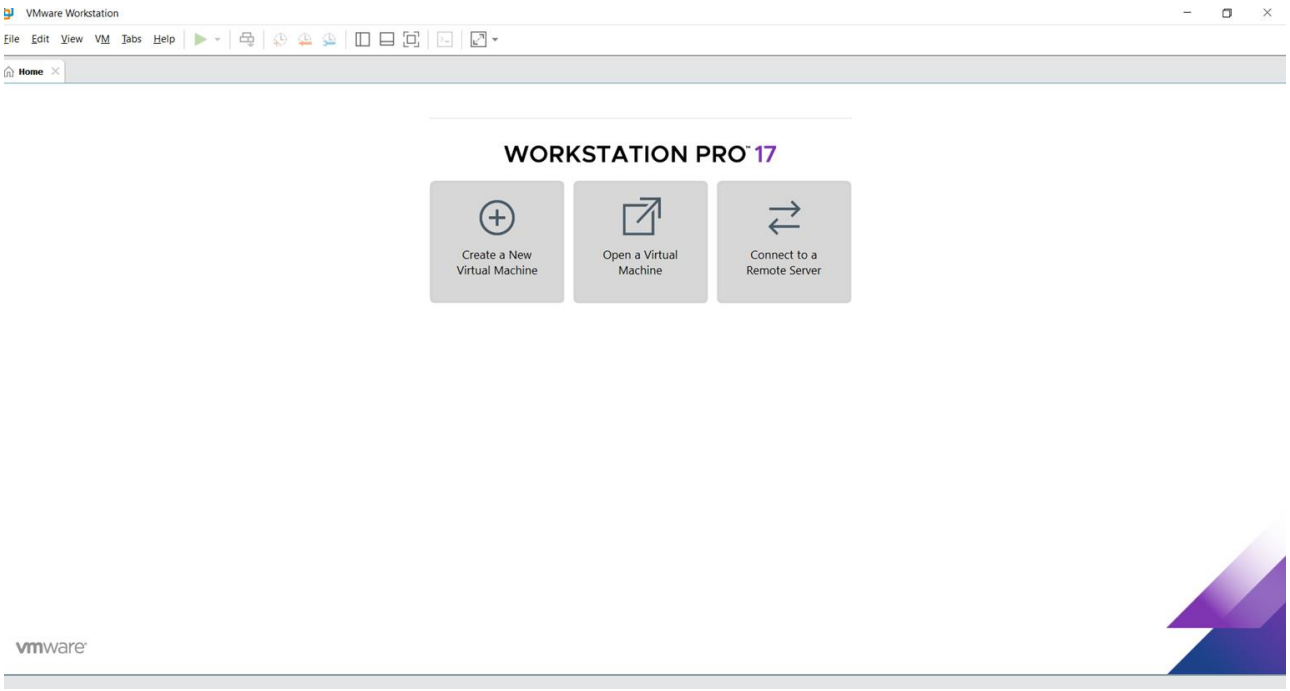
❿ Search Vmware in google.com and try to download and install in your machine

❿



❿ After Downloading the Vmware install in it on your machine it’s look like this down image

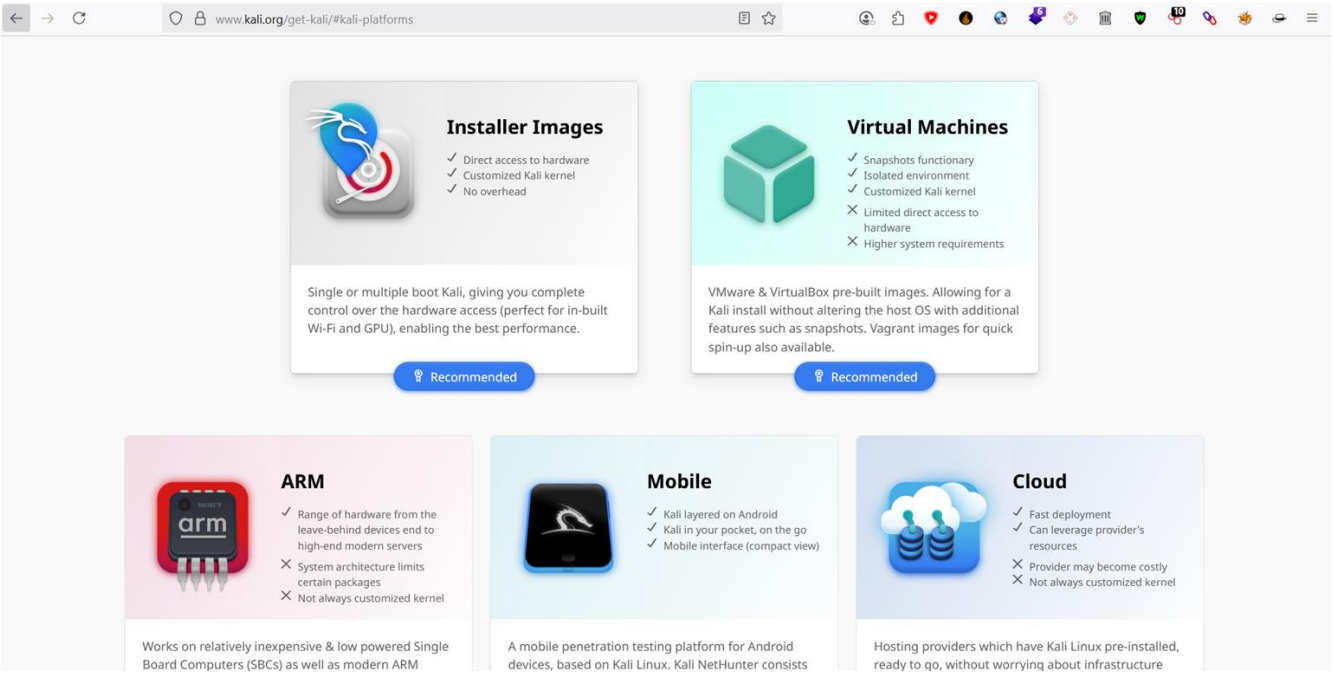
❿ I choose Vmware because its looks goods



❿

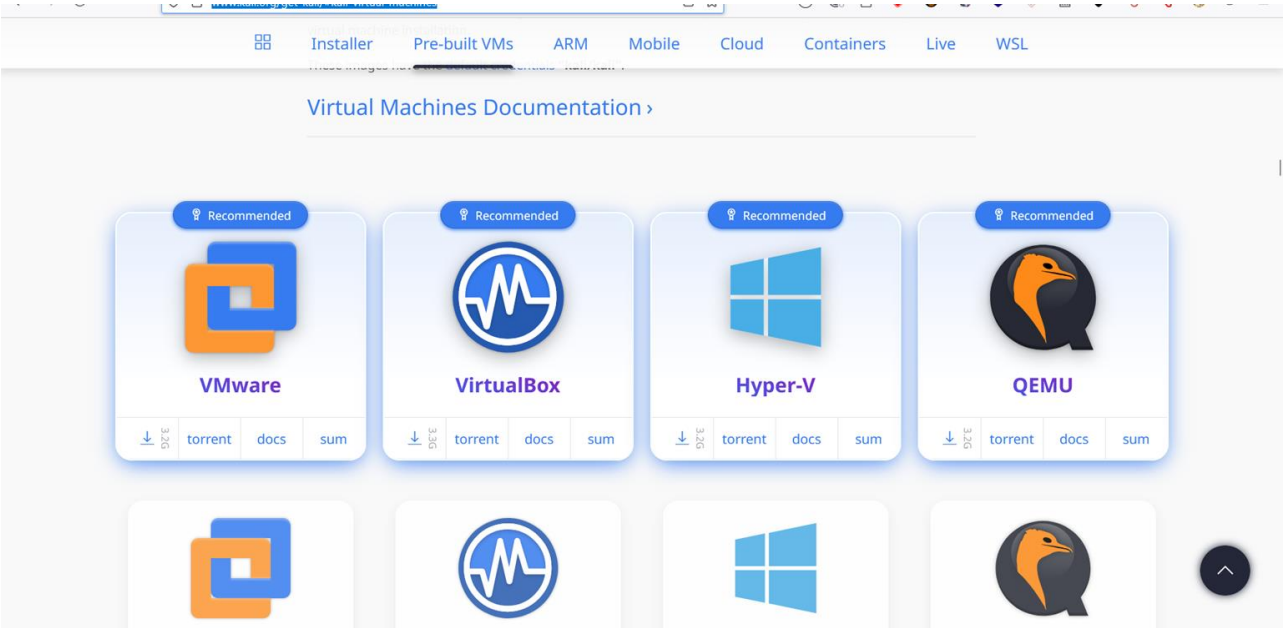
3. Installation Steps (brief)

❿ Download kali linux in here : https://www.kali.org/get-kali/#kali-virtual-machines

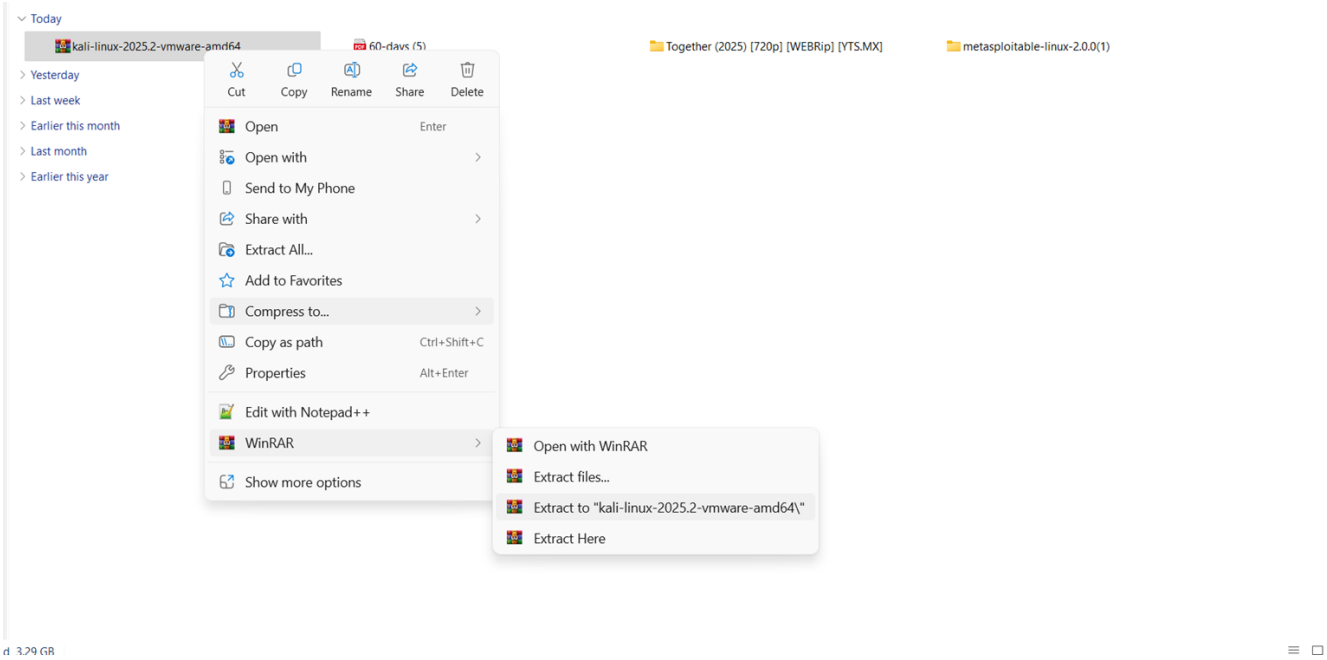


❿ Click on Virtual machine

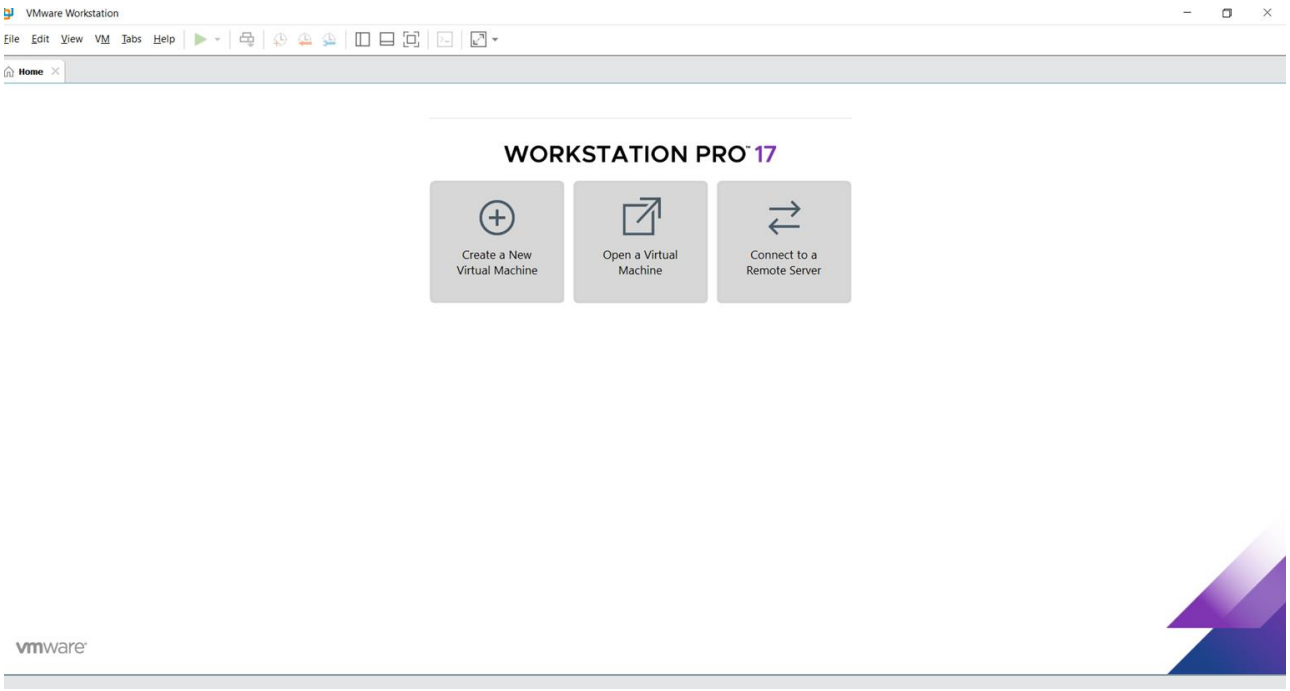
❿ Download the VM ware OS because in os we have to adjust everything in WM ware os it automatically choose every thing like dynamic



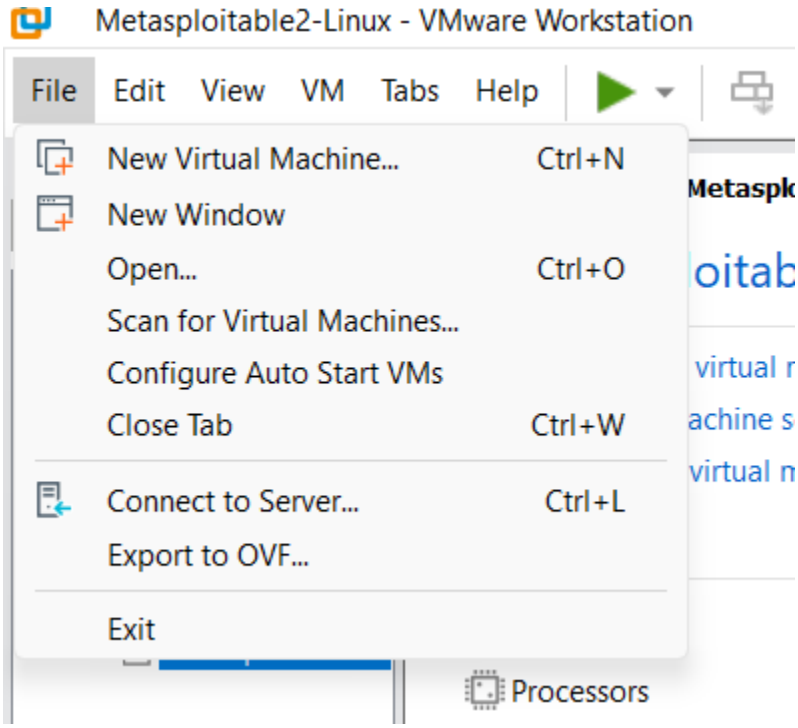
❿ After downloaded the os software with the file using winrar or with other extracter



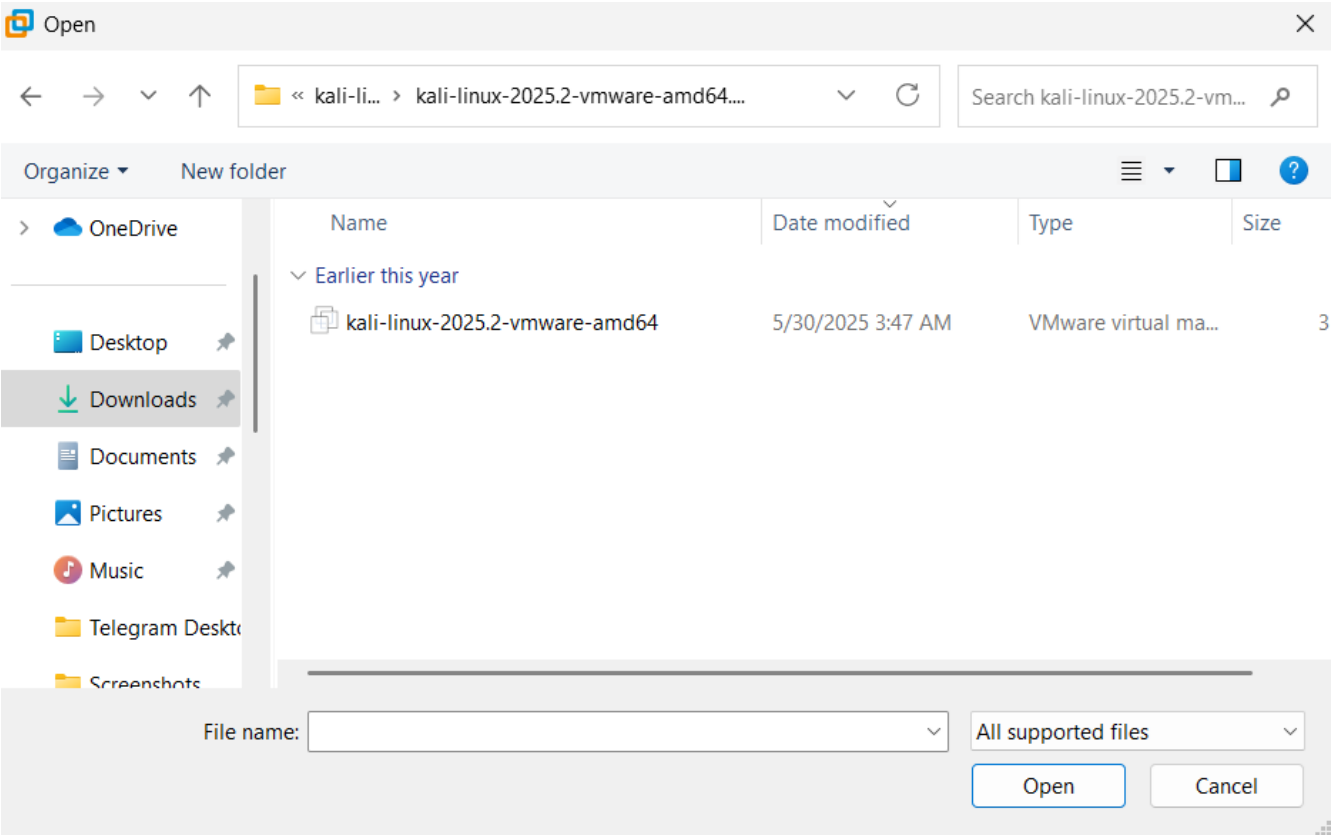
❿ after extracted open VM ware and right corner above click on file and it will show the show the menu click on open go to download open the file the you've extracted and import and VM ware dynamically adjust every based RAM and CPU and memory space everything


VMware Workstation
File Edit View VM Tabs Help
Home
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware

❿


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Scan for Virtual Machines...
Configure Auto Start VMs
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Export to OVF...
Exit
Processors

❿



❿ As I told you it will dynamically adjust everything as it won because orgnisation created that way things VM ware Kali Linux

Kali Rolling (2025.2) x64

2025-05-29

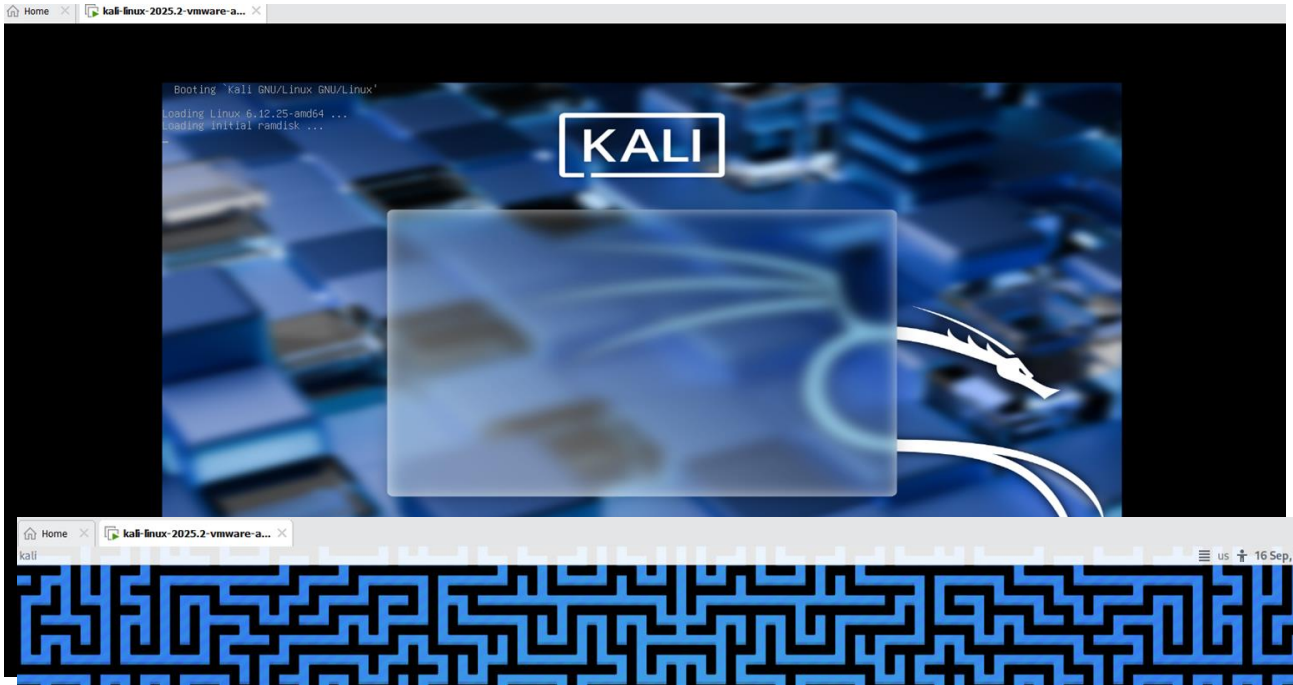
- - - - - - - - - - - - - - - - - -

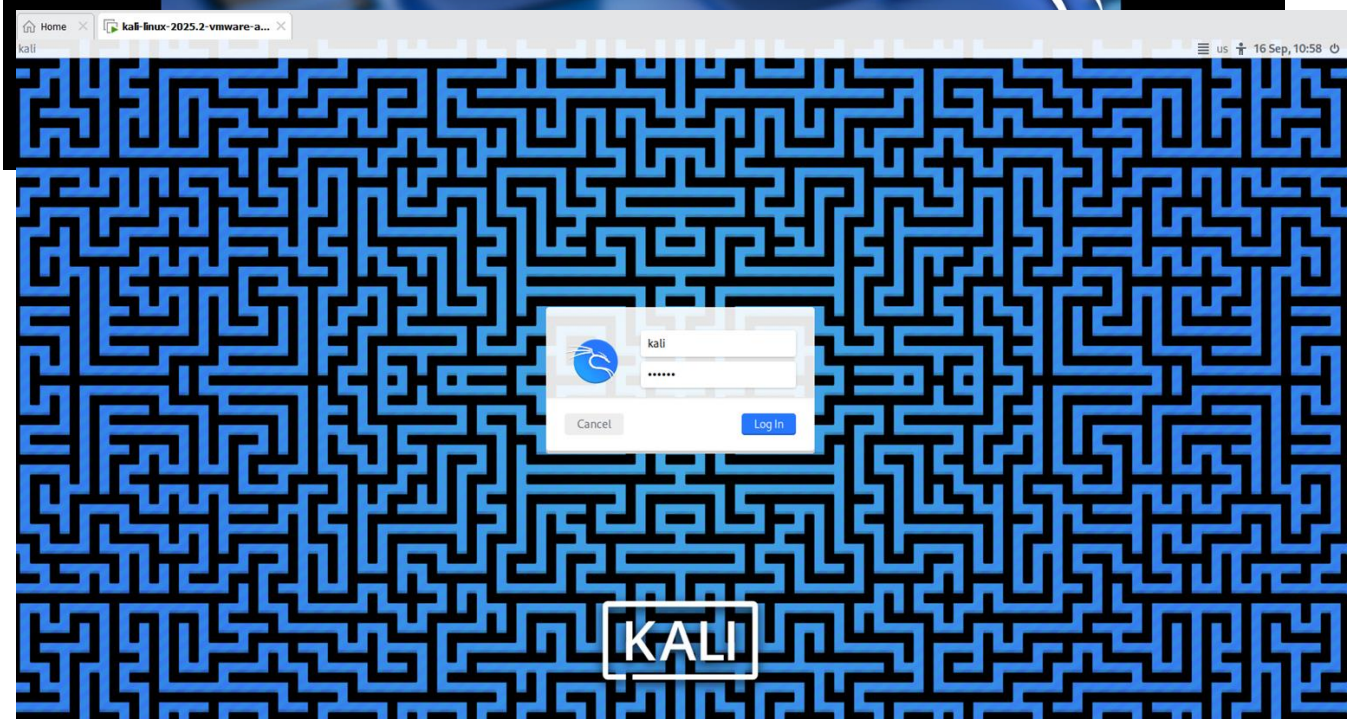
Username: kali

Password: kali

(US keyboard layout)

❿ Click on power on the machine and it will boot the kali linux os once it boosted it will show the login page and Username and Password is : kali


Home
kali-linux-2025.2-vmware-a...
Booting `Kali GNU/Linux GNU/Linux'
Loading Linux 6.12.25-amd64 ...
Loading initial ramdisk ...
KALI


Home
kali-linux-2025.2-vmware-a...
kali
us
16 Sep, 10:58
kali
Cancel
Log In
KALI

- This is the way that we can install kali linux without getting any error on other things in next thing we'll install vulnerable os which is Metasploitable2 the machine is created for where ethical hacker can hack and test how things are working and practice purpose developed by

Installing Metasploitable2 (breif)

- Download the Software here : https://sourceforge.net/projects/metasploitable/

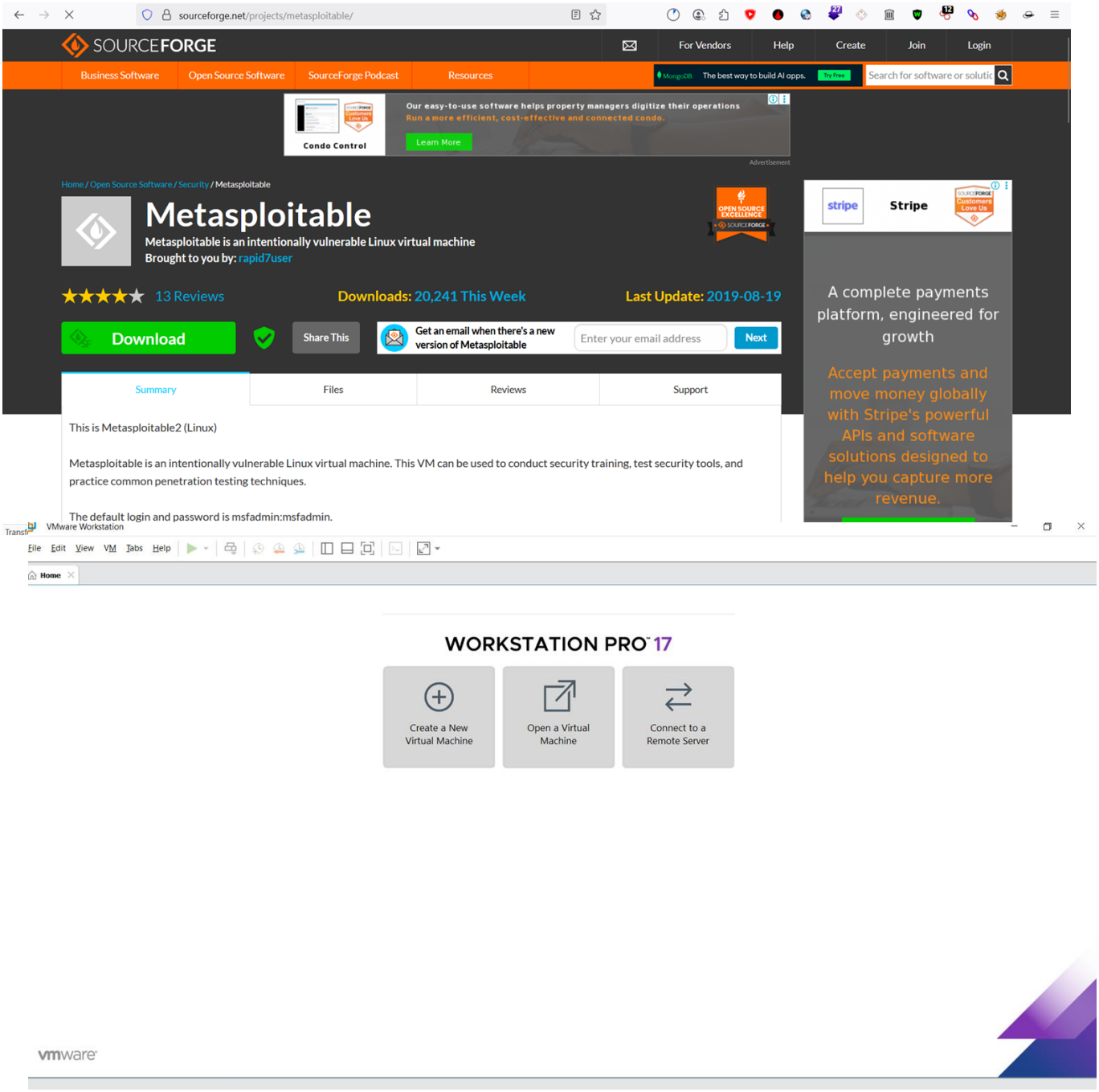
after download extract the file and import that file to VM ware click open

- This is Metasploitable2 (Linux)

  Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

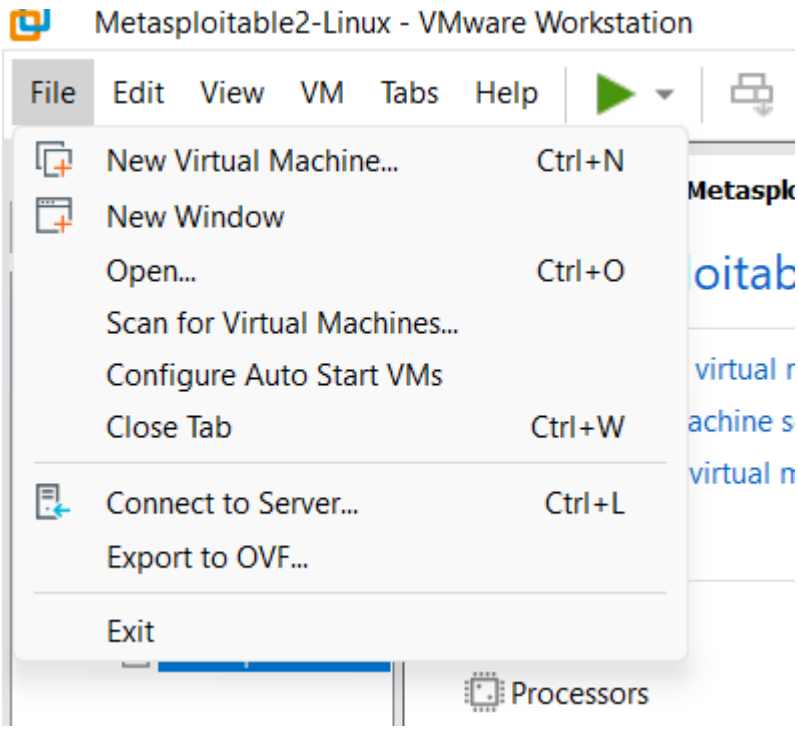
  The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means



open the VMware after in right corner above click of file it will show the menu file click of file

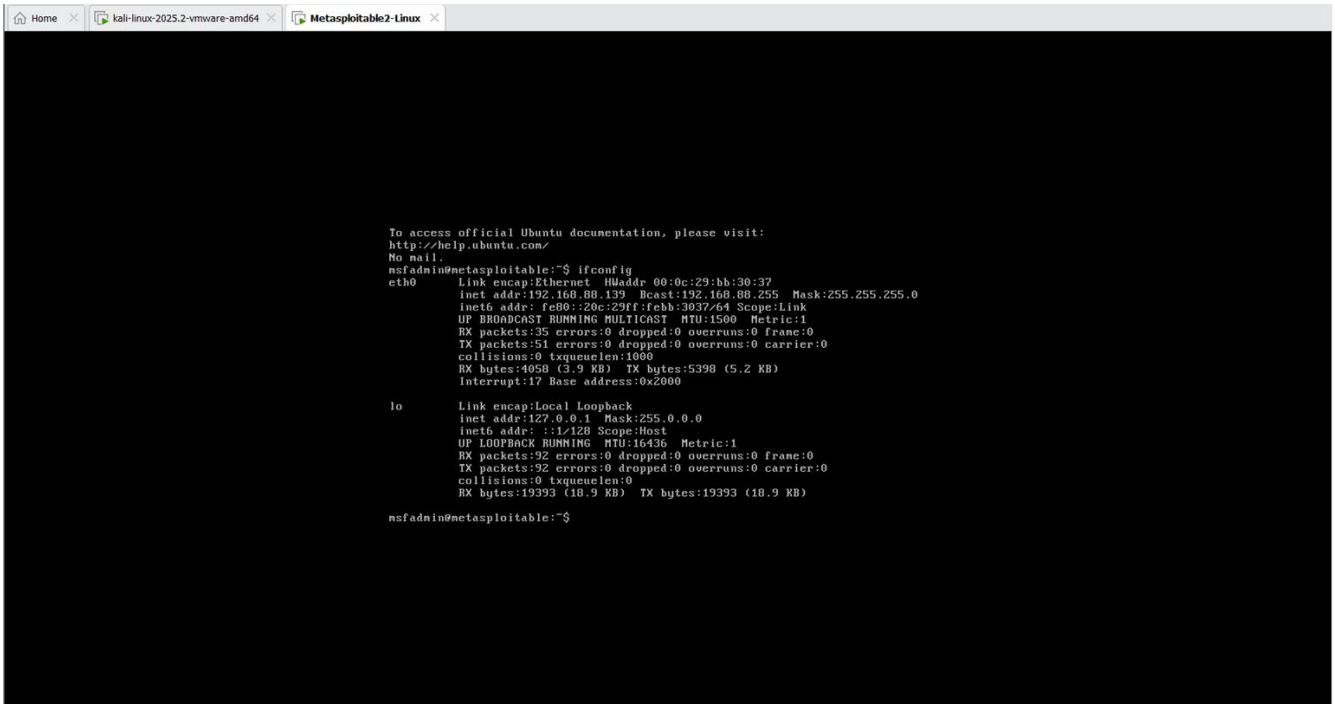
go and select the you've extracted the Metasploitable2 choose the file upload the software and open it will dynamically allocate the process and RAM and Memory space and everything it's needed



❿

❿ Click power on the virtual machine and when its booted use login credential as msfadmin:msfadmin

❿



❿

NETWORKING:

❿ Networking is where two system interconnected each to make communication and share **resources**

❿ This can be done Wired or Wireless

OSI - (Open system interconnection)

- OSI is open system interconnection it has 7 layer how each layer interconnected each to share information though each layer
  - OSI Model (7 Layers)

1. **Physical** – Transmits raw bits over cables or wireless signals.
2. **Data Link** – Ensures error-free transfer between two directly connected nodes.
3. **Network** – Handles logical addressing and routing of data (IP).
4. **Transport** – Provides reliable or fast delivery using TCP/UDP.
5. **Session** – Manages starting, maintaining, and ending communication sessions.
6. **Presentation** – Translates, encrypts, or compresses data for applications.
7. **Application** – Interfaces directly with the user through apps and services

TCP/IP

TCP/IP Model (4 Layers)

1. **Network Interface (Link Layer)** – Deals with hardware addressing and data transfer over the local link.
2. **Internet** – Defines IP addressing and routes packets across networks.
3. **Transport** – Ensures complete and reliable data delivery with TCP/UDP.
4. **Application** – Provides services like HTTP, FTP, SMTP, DNS for users.

DNS ,HTTP,HTTPS

DNS (Domain Name System) is like the **phonebook of the internet** – it converts human-readable domain names (e.g., `www.google.com`) into machine-readable IP addresses (e.g., `142.250.183.110`) so browsers and applications can locate servers and communicate with them

DNS Zone

- A **DNS zone** is a part of the domain namespace that is managed by a specific organization or administrator.
- It contains information about one or more domains.
- Example: `example.com` zone may include records for `www.example.com`, `mail.example.com`, etc.

DNS Zone Transfer

- A process of **copying DNS records from a primary (master) DNS server to a secondary (slave) DNS server**.
- Ensures **redundancy, backup, and load balancing**.
- Types:
  - **AXFR (Full Zone Transfer):** Transfers the entire zone file.
  - **IXFR (Incremental Zone Transfer):** Transfers only changes made since the last update.

If misconfigured, attackers can use **zone transfer** to enumerate all DNS records of a domain (serious security risk).

Common DNS Record Types

Record	Purpose
A	Maps a domain name to an IPv4 address.
AAAA	Maps a domain name to an IPv6 address.
CNAME	Alias – points one domain to another domain name.
MX	Mail Exchange – specifies mail servers for email delivery.
NS	Nameserver – shows which servers are authoritative for the zone.
SOA	Start of Authority – contains zone info (primary server, admin email, serial number, refresh timings).
PTR	Pointer record – reverse DNS lookup (IP → domain).
TXT	Holds arbitrary text (e.g., SPF, DKIM, verification data).
SRV	Defines services (like SIP, XMPP).

- **HTTP (HyperText Transfer Protocol)** → Transfers web pages and data between browser and server.

- **HTTPS (HyperText Transfer Protocol Secure)** → Secure version of HTTP that encrypts data using SSL/TLS.

IP ADDRESSING,NAT,SUBNETTING

↘ IP Addressing

An **IP Address** is like the "home address" of a device on a network. It tells where data should be sent and where it comes from.

- **IPv4**: 32-bit address, written as 4 numbers (0–255), e.g., `192.168.1.10`
- **IPv6**: 128-bit address, written in hexadecimal, e.g., `2001:0db8:85a3::8a2e:0370:7334`

Two parts in an IP address:

- **Network ID** → Identifies the network (like a street name)
- **Host ID** → Identifies the device on that network (like a house number)

Example:

`192.168.1.10/24`

- Network ID = `192.168.1.0`
- Host range = `192.168.1.1 - 192.168.1.254`
- Broadcast = `192.168.1.255`

2. Subnetting

Subnetting means dividing a large network into smaller ones (sub-networks).

Why? → To manage IPs efficiently, improve performance, and add security.

Subnet Mask

A subnet mask decides how many bits are for **Network ID** and how many for **Host ID**.

- Example: `/24` means **24 bits for network** and **8 bits for hosts**.
  - Mask: `255.255.255.0`
  - Hosts possible: `2^8 - 2 = 254` (subtract 2 for network & broadcast).

CIDR Notation

Instead of writing full masks, we write `/x` (number of network bits).

- `/8` → 16 million hosts (very big, e.g., `10.0.0.0/8`)
- `/16` → 65,534 hosts (e.g., `172.16.0.0/16`)
- `/24` → 254 hosts (e.g., `192.168.1.0/24`)

Example:

- You have `192.168.1.0/24` and want 4 smaller networks.
- Borrow 2 bits from host part → `/26` (255.255.255.192).
- Each subnet has 64 addresses (62 usable hosts).

3. NAT (Network Address Translation)

NAT allows multiple devices in a private network to share a single public IP to connect to the internet.

- **Private IP ranges** (not routable on internet):
  - `10.0.0.0 - 10.255.255.255`
  - `172.16.0.0 - 172.31.255.255`
  - `192.168.0.0 - 192.168.255.255`

- **How NAT works:**
    - Your PC (192.168.1.10) → NAT router → Internet with public IP (say, 103.45.67.89).
    - NAT keeps a table to match internal requests with external responses.

Types of NAT:

- **Static NAT** → 1 private IP mapped to 1 public IP.
- **Dynamic NAT** → Many private IPs mapped to a pool of public IPs.
- **PAT (Port Address Translation)** → Many private IPs share **one public IP** (most common).

3.Cryptography Basics

Symmetric vs Asymmetric Encryption

- **Symmetric Encryption** : Same key is used for **both encryption and decryption**.
    - Fast, good for large data.
    - Example: AES.
    - Problem: Key must be securely shared.
- **Asymmetric Encryption** : Uses **public key** to encrypt and **private key** to decrypt.
    - Slower, but solves key sharing issue.
    - Example: RSA.

Hashing (MD5, SHA256)

- **Hashing** converts data into a fixed-length string.
- It's **one-way** (cannot be reversed).
- **MD5** : 128-bit, fast but broken (collisions found).
- **SHA-256** : 256-bit, stronger and widely used.

Digital Certificates & SSL/TLS

- **Digital Certificate** = Electronic ID card for a website, issued by a **Certificate Authority (CA)**.
- **SSL/TLS** uses certificates + encryption to secure web traffic (HTTPS).
    - Ensures **confidentiality** (data encrypted),
    - **integrity** (no tampering),
    - **authenticity** (you're really talking to the right server)

Hands-on with OpenSSL (Encrypt/Decrypt Messages)

Step 1: Create a key

openssl genrsa -out private.pem 2048
openssl rsa -in private.pem -pubout -out public.pem

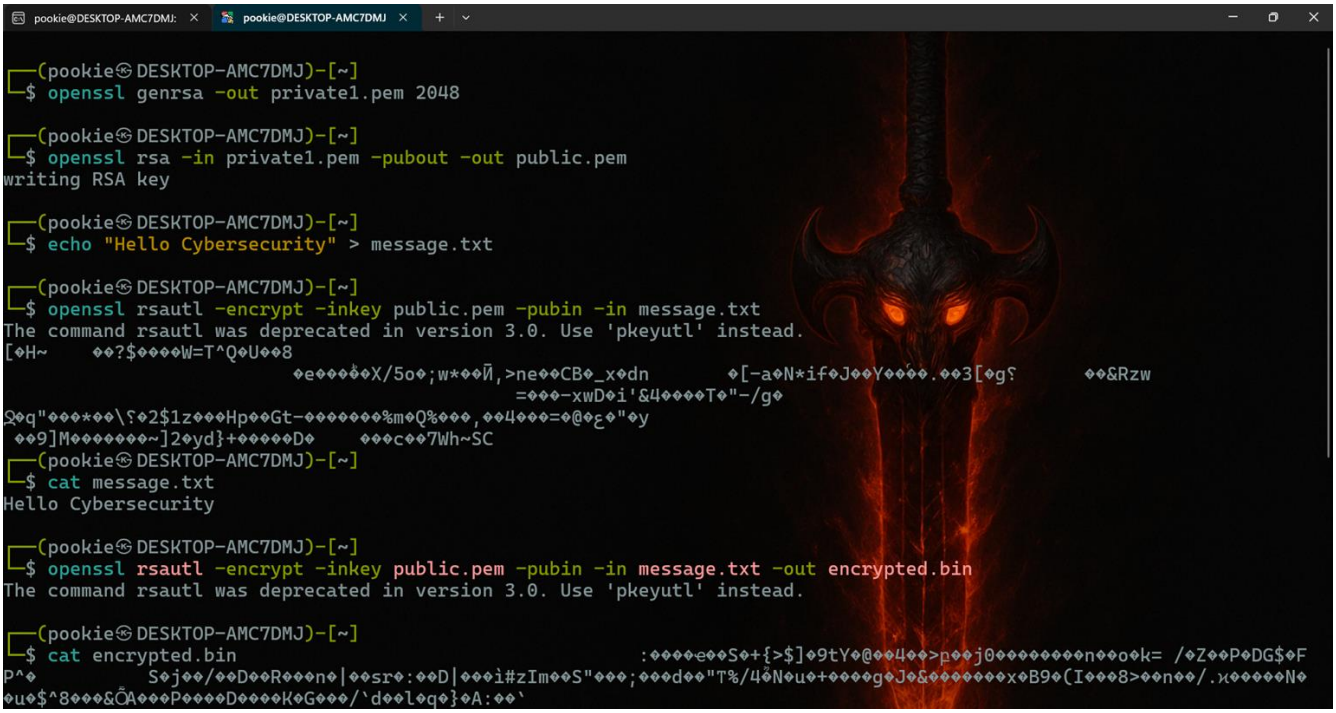
Step 2: Encrypt a message with Public Key

echo "Hello, Cybersecurity" > message.txt
openssl rsautl -encrypt -inkey public.pem -pubin -in message.txt -out encrypted.bin

Step 3: Decrypt with Private Key

openssl rsautl -decrypt -inkey private.pem -in encrypted.bin -out decrypted.txt

cat decrypted.txt



```
┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$ cat encrypted.bin                                   :◆◆◆◆e◆◆S◆+{>$]◆9tY◆@◆◆4◆◆>p◆◆j0◆◆◆◆◆◆◆◆n◆◆o◆k= /◆Z◆◆P◆DG$◆F
P^◆          S◆j◆◆/◆◆D◆◆R◆◆◆n◆|◆◆sr◆:◆◆D|◆◆◆ì#zIm◆◆S"◆◆◆;◆◆◆d◆◆"T%/4◆N◆u◆+◆◆◆◆g◆J◆&◆◆◆◆◆◆◆◆x◆B9◆(I◆◆◆8>◆◆n◆◆/.x◆◆◆◆◆N◆
◆u◆$^8◆◆◆&ÕA◆◆◆P◆◆◆◆D◆◆◆◆K◆G◆◆◆/`d◆◆l◆q◆}◆A:◆◆`
┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$ openssl rsautl -decrypt -inkey private1.pem -in encrypted.bin -out decrypted.txt
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$ cat decrypted.txt
Hello Cybersecurity

┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$

┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$
```