 CYBER SECURITY INTERNSHIP

Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap

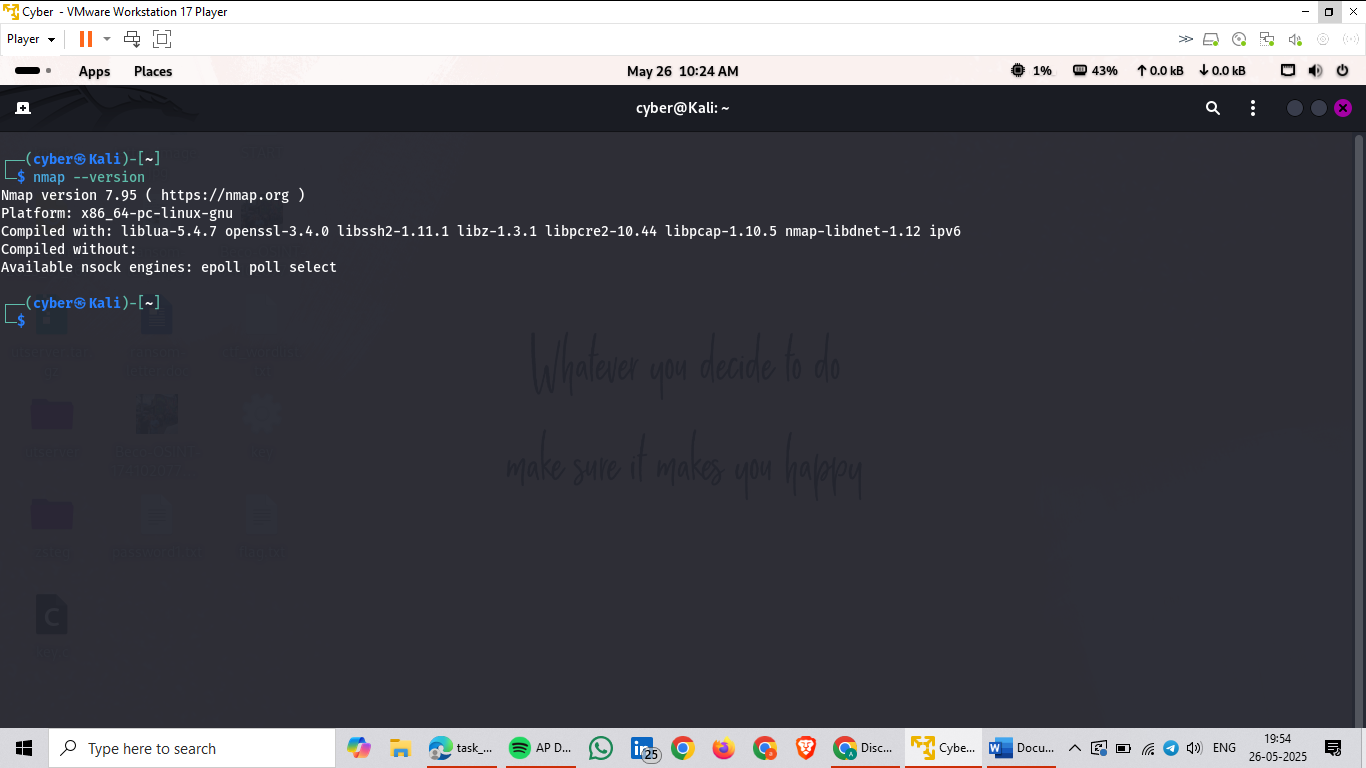
1. Instal Nmap from official website.

I am using **Kali Linux**, Nmap is already **pre-installed**, or can be installed easily via the package manager. Here is how you can proceed directly using Kali:

**1. Check if Nmap is Already Installed**

Open a terminal and run:

Nmap –version



2. **Find Your Local IP Range**

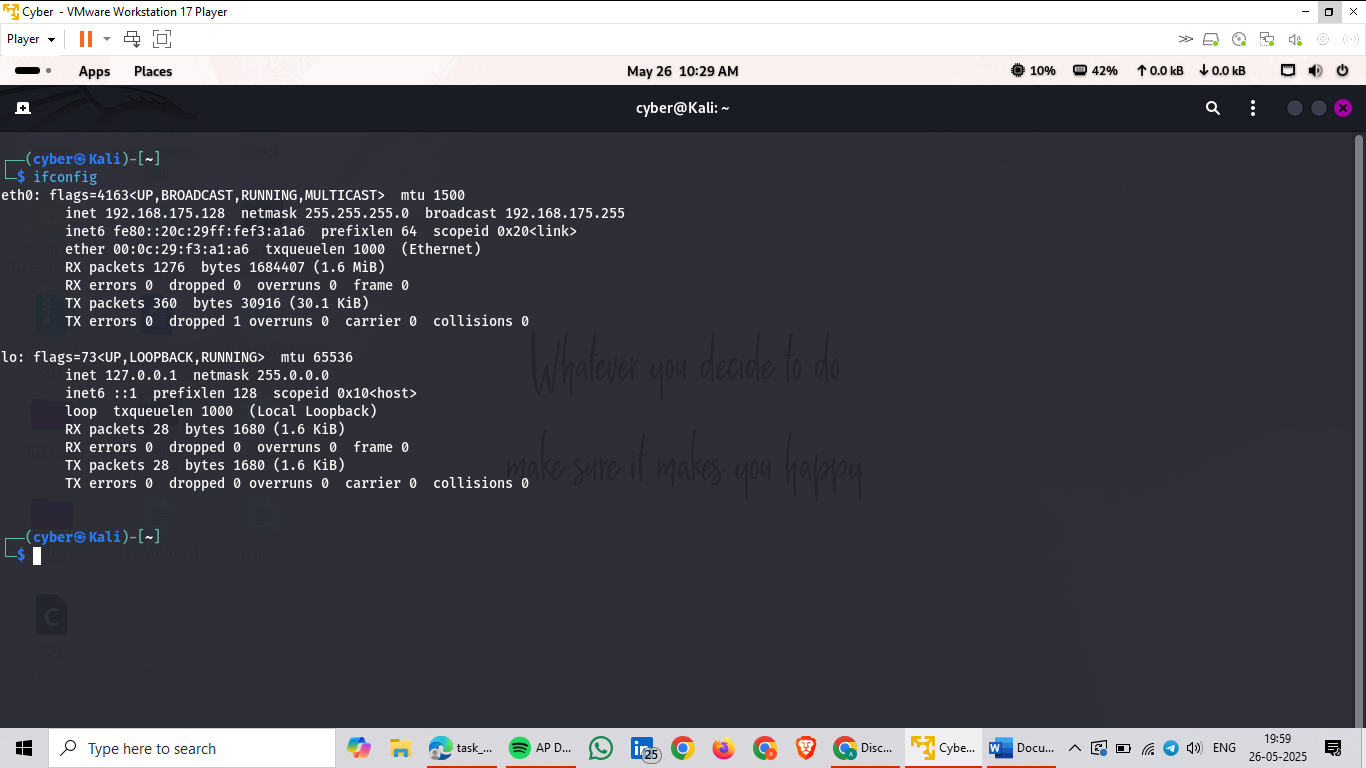
**Open a terminal or command prompt.**

**Run:**

* **Windows: ipconfig**
* **Linux/macOS: ipconfig or ip a**

**Look for your local IP (e.g., 192.168.1.105) and subnet mask (often 255.255.255.0, meaning /24 CIDR).**

**Local IP Change = 192.168.175.128**

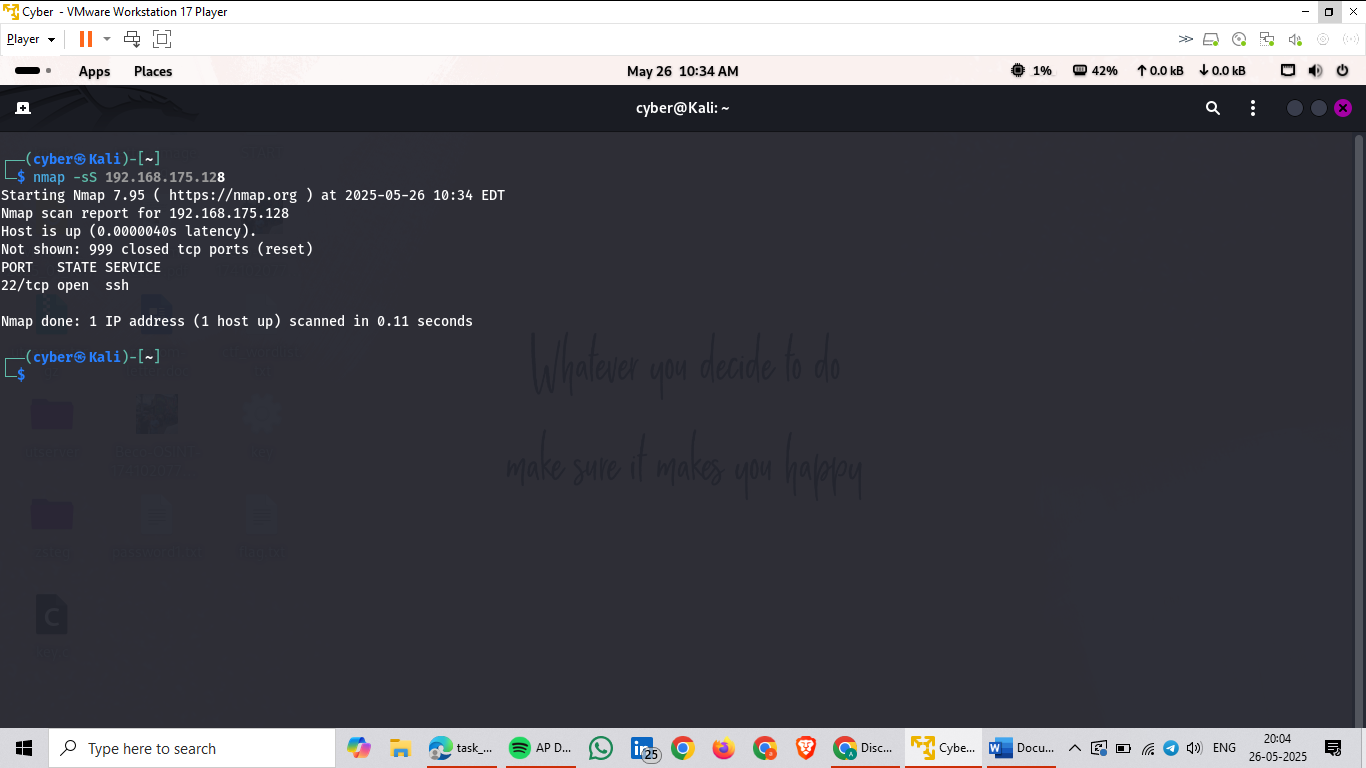
****

**3. Run TCP SYN Scan with Nmap**

**nmap -sS 192.168.175.128/24**

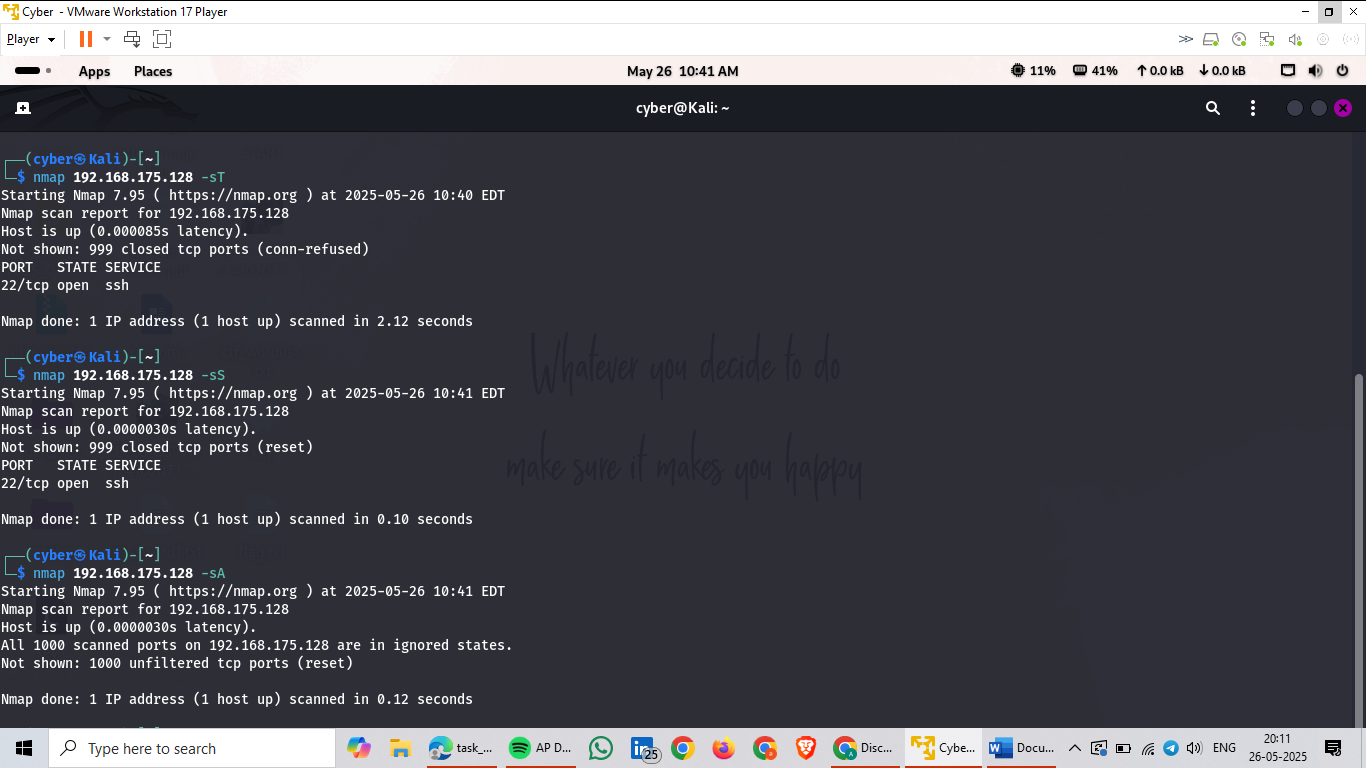
**-sS: Stealth SYN scan (common and fast)**

**Scans all live hosts in the subnet and their open TCP ports.**

****

**4. Note Down IP Addresses and Open Ports**

* **The output will list:**
* **IP addresses of devices found**
* **Open ports and associated services (e.g., port 80 → HTTP)**

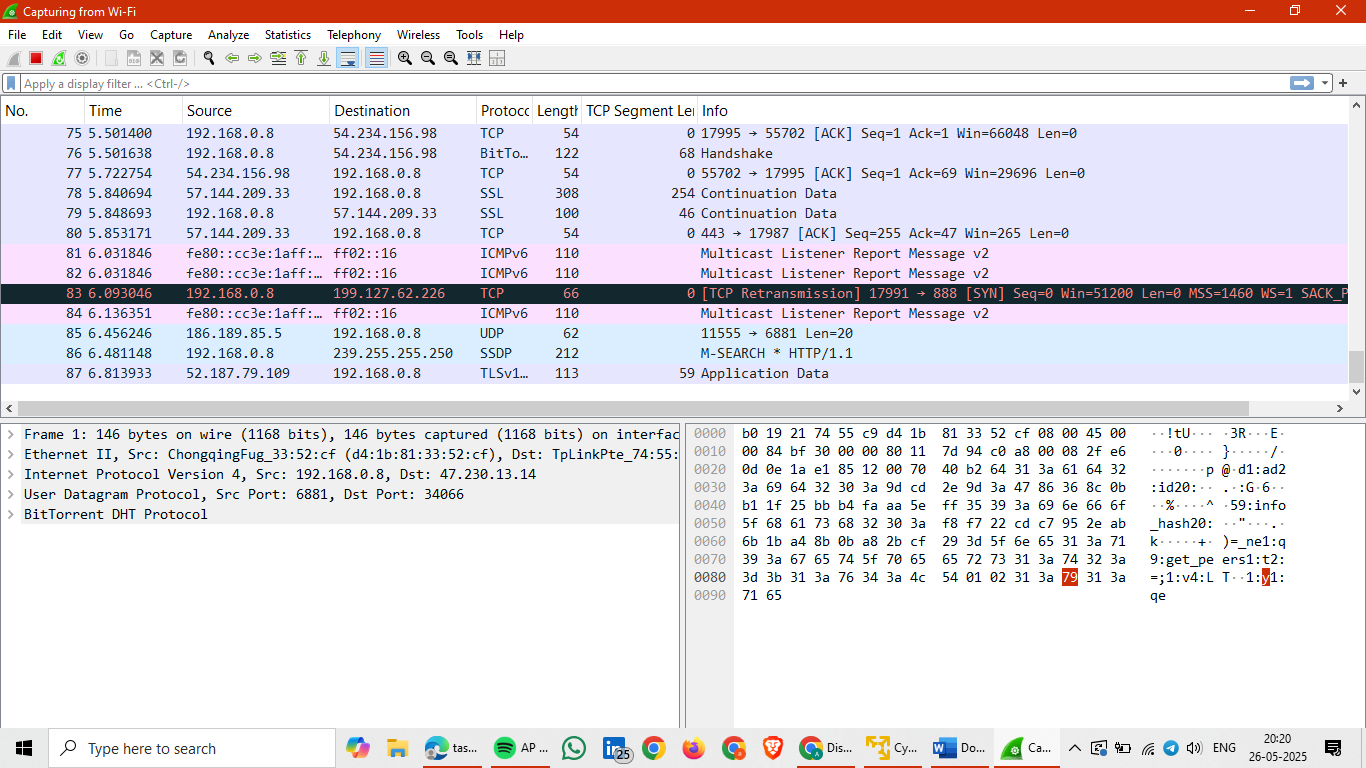
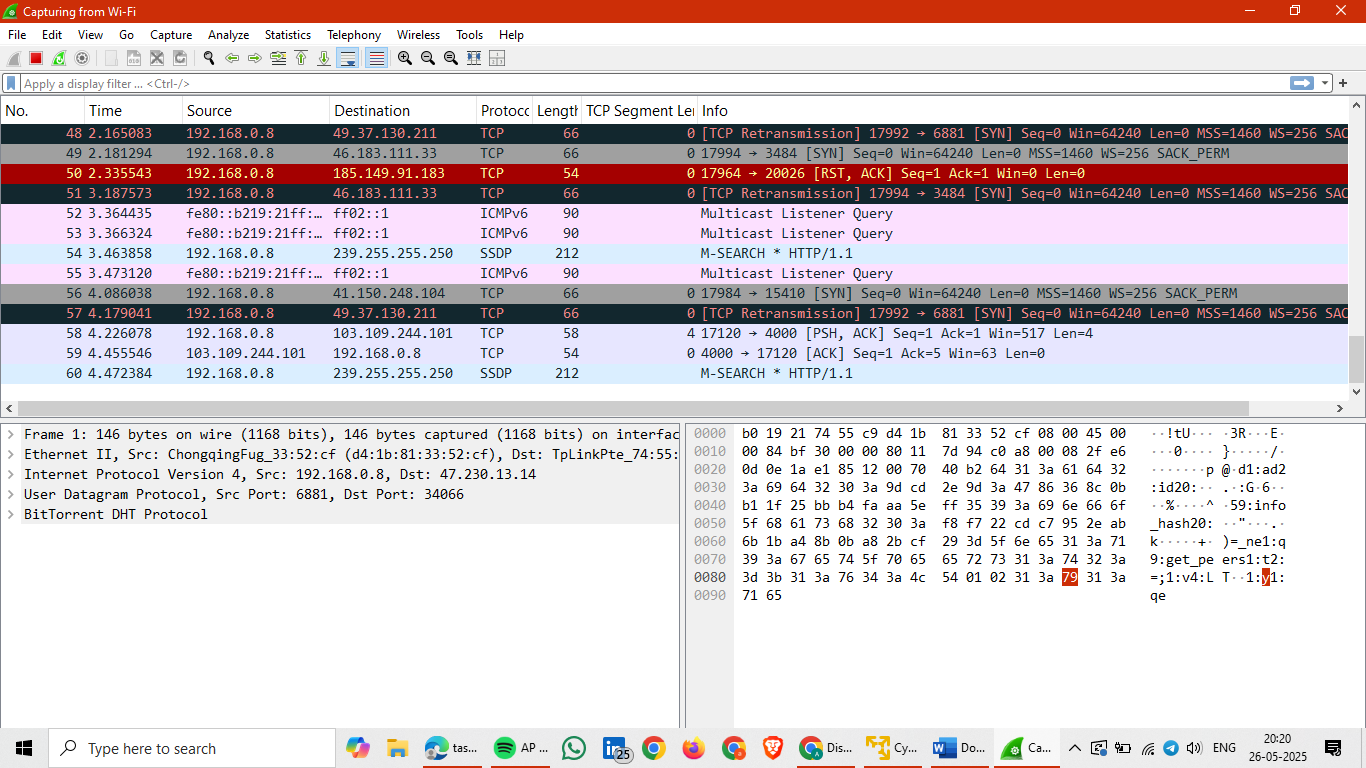
****

**5. (Optional) Analyse with Wireshark**

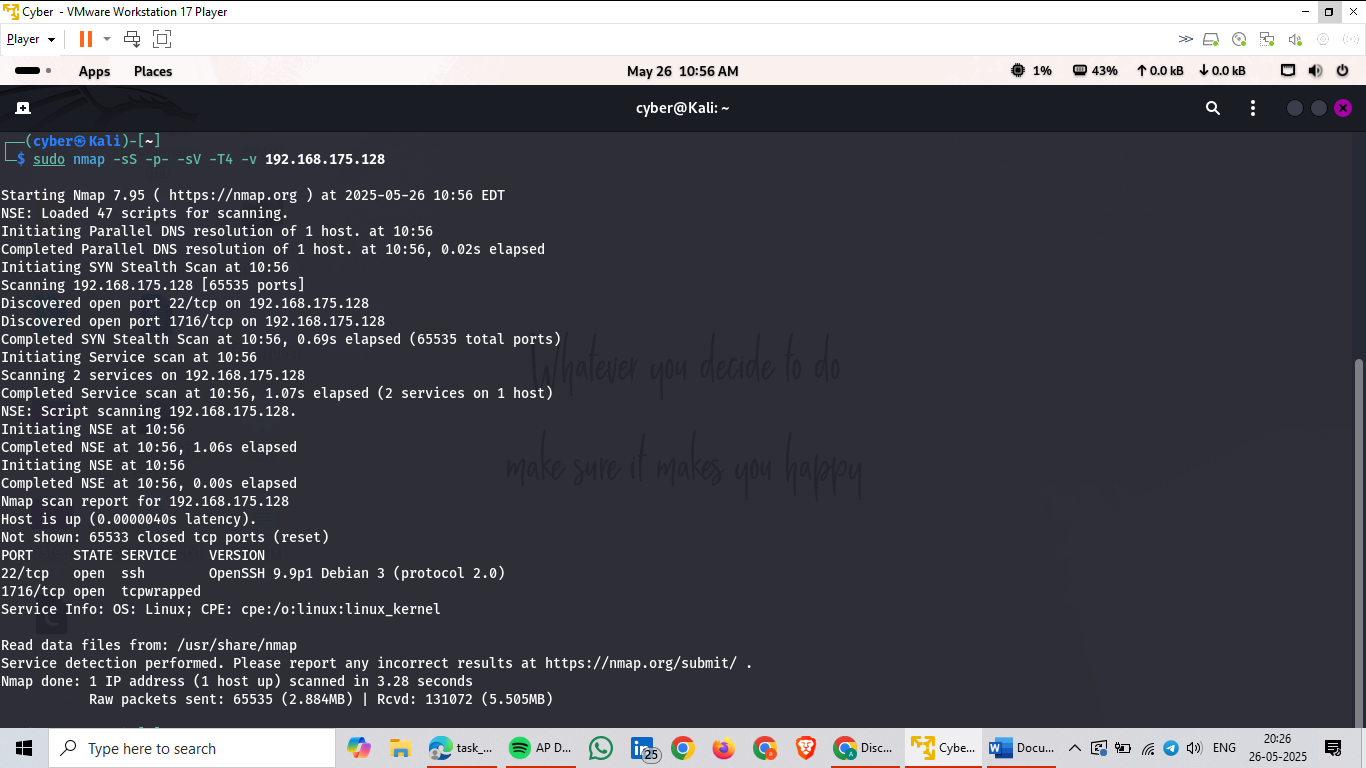
**Open Wireshark before running the scan.**

**Choose your network interface (e.g., eth0, Wi-Fi).**

**Stop capture and use filters like:**

****

6. **Research Common Services**

****

**7. Identify Security Risks**

**What This Means**

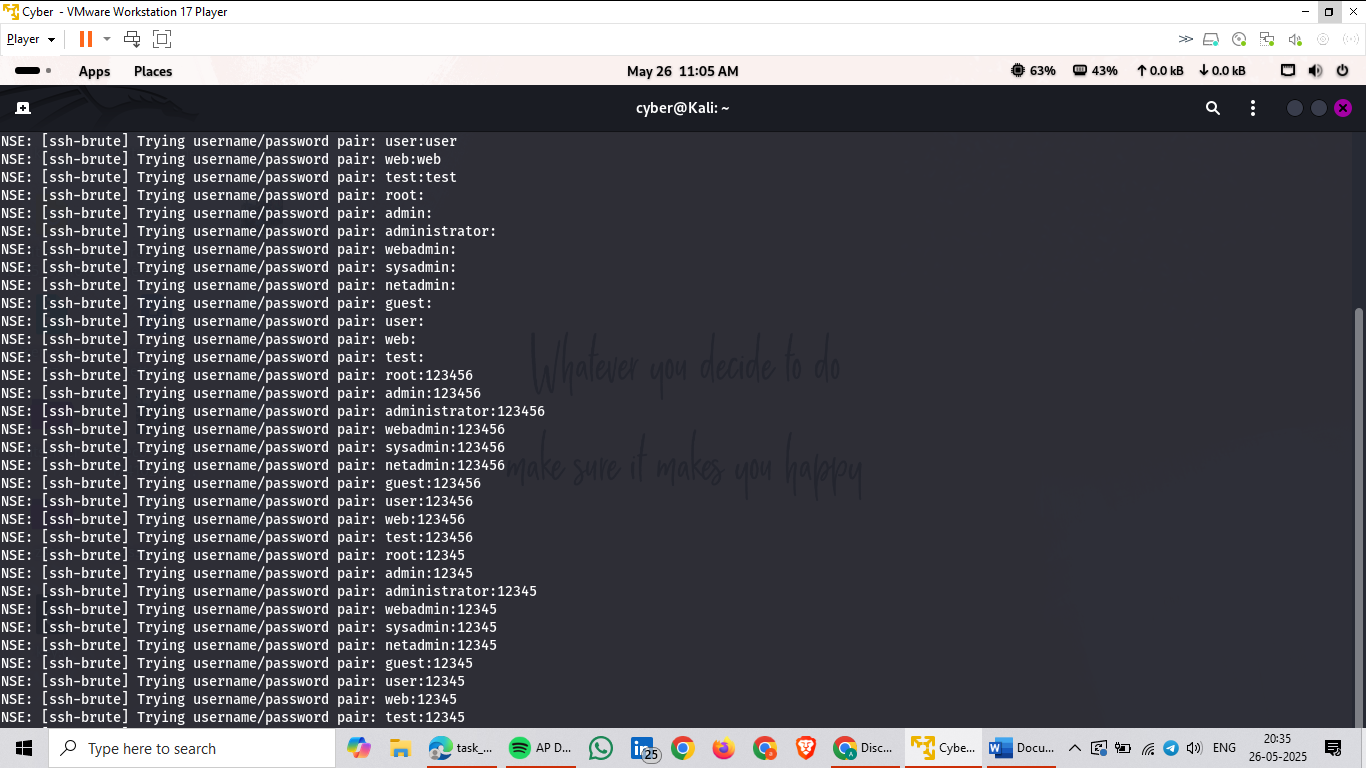
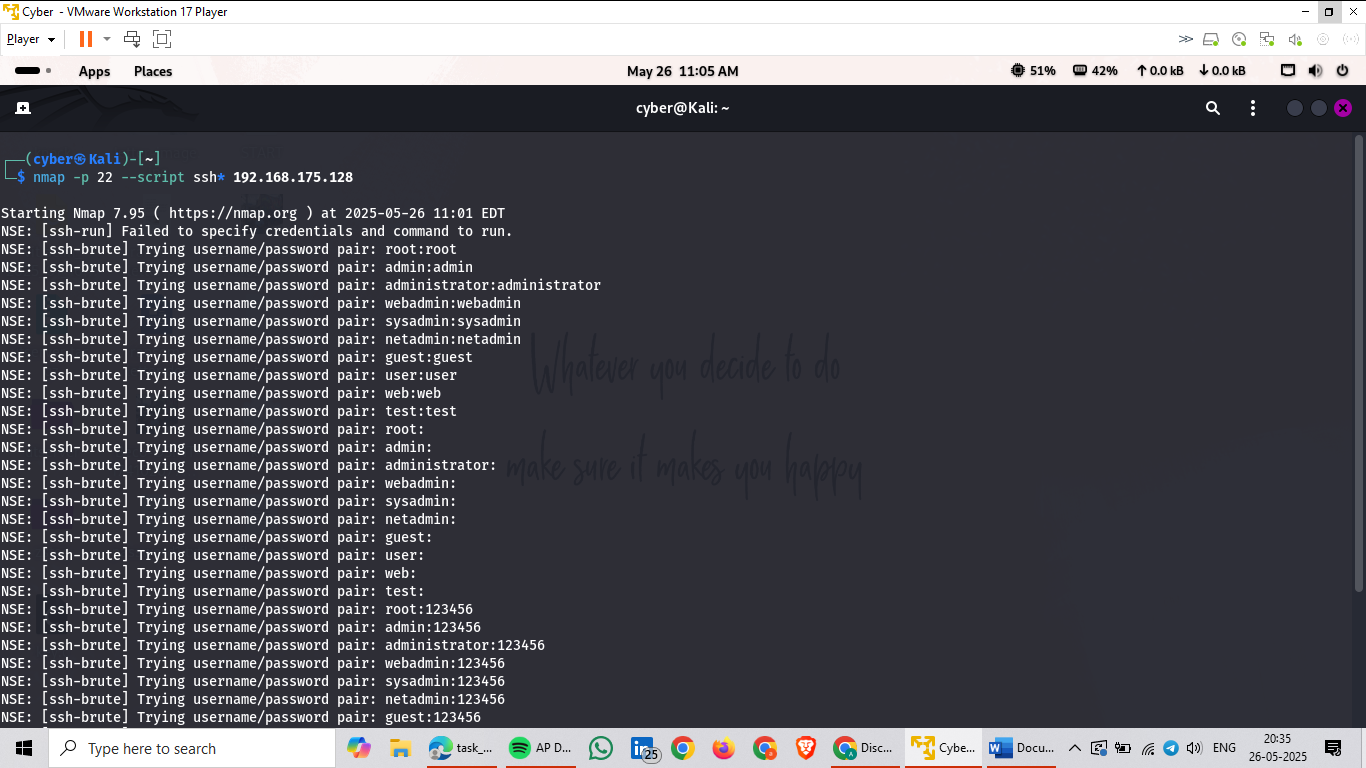
* **Port 22 (TCP): Standard port for SSH (Secure Shell).**
* **OpenSSH 9.9p1 Debian 3: The SSH server software and version running on the device.**
* **Protocol 2.0: Secure version of the SSH protocol.**

**Why SSH Might Be Open**

* **Remote access for system administrators.**
* **Automated remote backups or scripting.**
* **Could be part of a home lab or IoT setup.**

**Run this particular script to get more information**

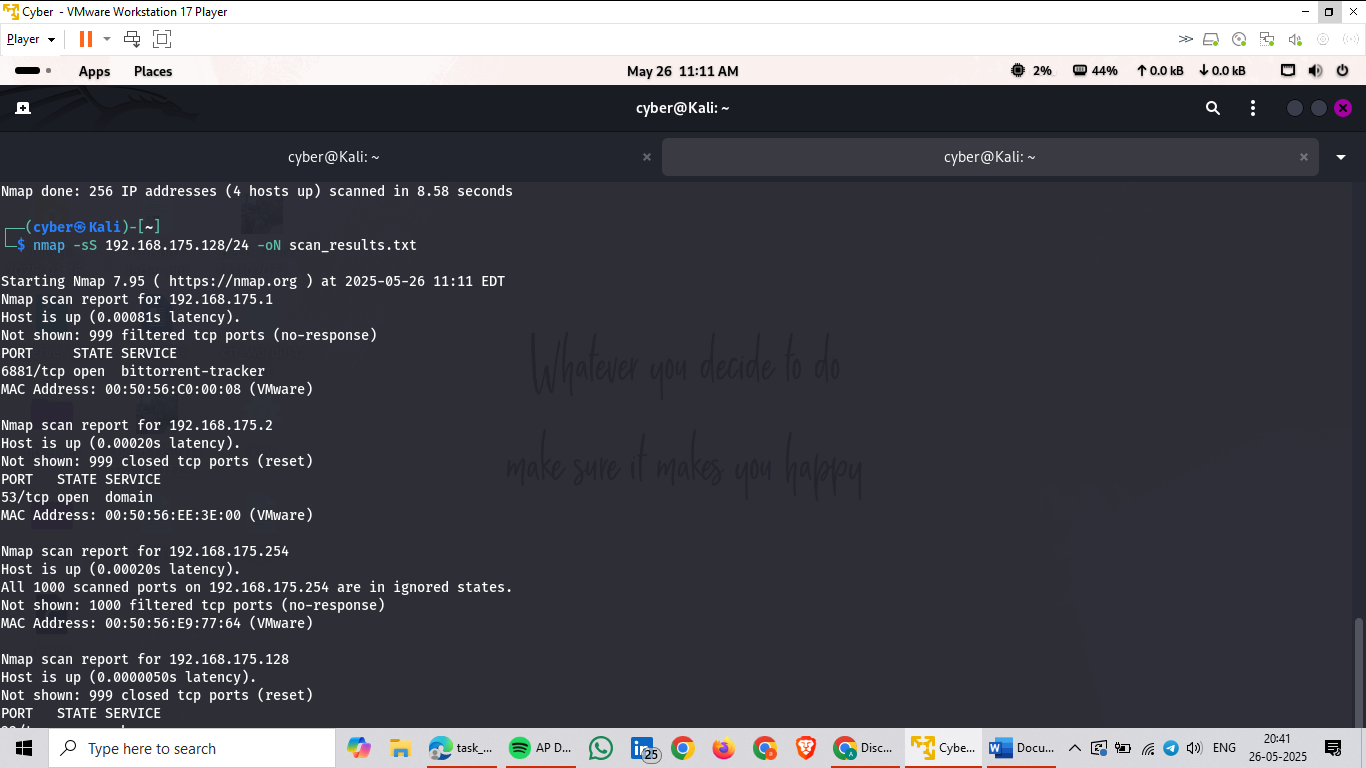
**nmap -p 22 --script ssh\* 192.166.175.128**

****

**8. Save Scan Results**

**nmap -sS 192.168.175.128/24 -oX scan.xml**

**xsltproc scan.xml -o scan.html**

****