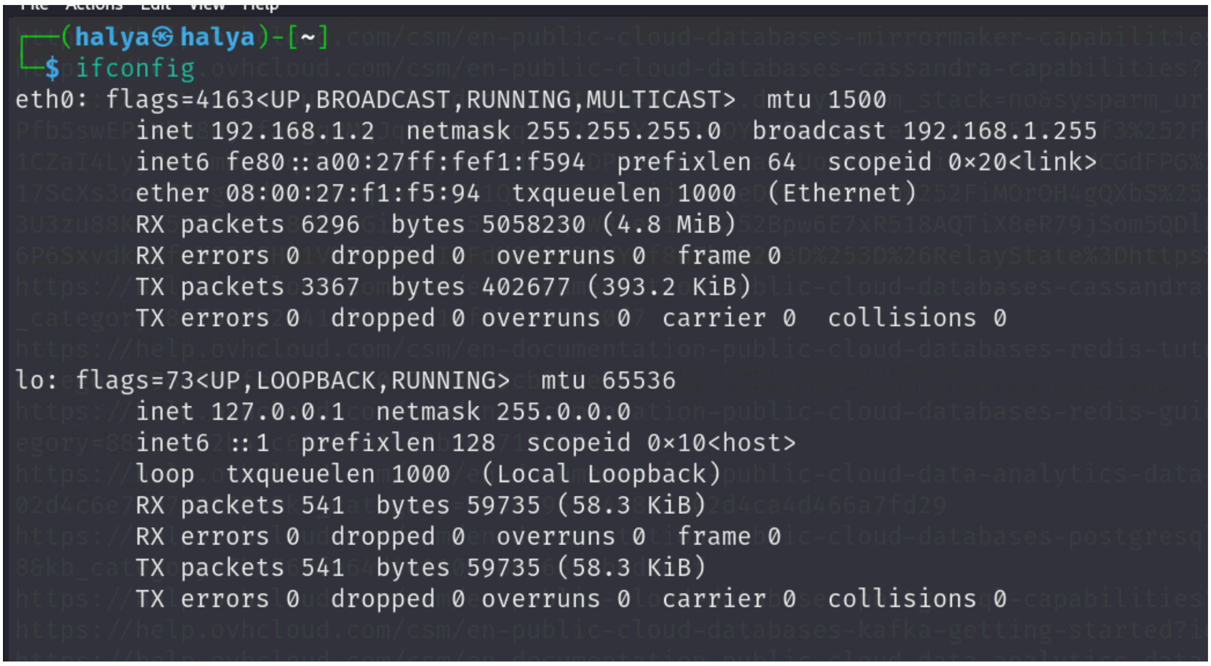
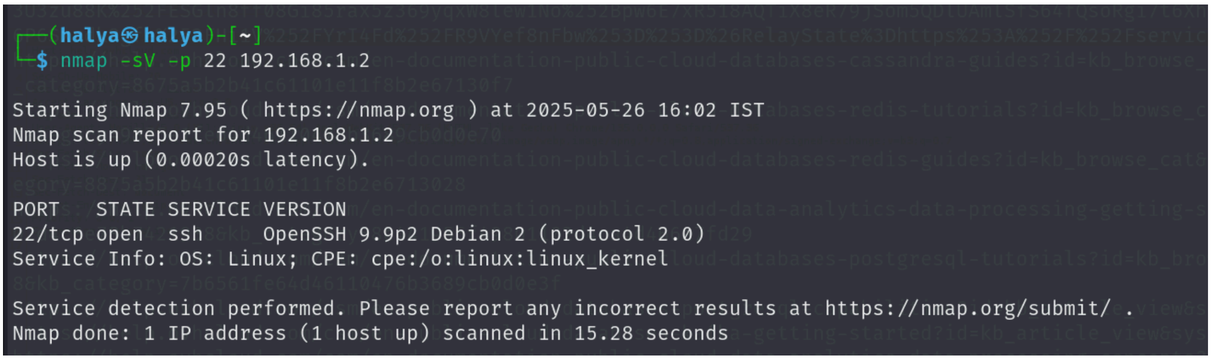
Nmap Scan Report:



```
┌──(halya㉿halya)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fef1:f594  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f1:f5:94  txqueuelen 1000  (Ethernet)
        RX packets 6296  bytes 5058230 (4.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3367  bytes 402677 (393.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 541  bytes 59735 (58.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 541  bytes 59735 (58.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Scan Date: 26-May-2025
Scan Time: 15:44 IST
Tool Used: Nmap v7.95
Scan Command: nmap -sS -p 192.168.1.2



```
┌──(halya㉿halya)-[~]
└─$ nmap -sV -p 22 192.168.1.2

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 16:02 IST
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.9p2 Debian 2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.28 seconds
```

Objective of the Scan

The goal of this scan was to identify open TCP ports and running services on host 192.168.1.2 using a TCP SYN scan. This is a common method for evaluating a host's network exposure and assessing potential security risks associated with its open ports.

Scan Methodology

Scan Type: TCP SYN Scan (-sS)

- Also known as a stealth scan, it sends SYN packets and waits for a response.
- If a SYN-ACK is received, the port is open.
- If an RST is received, the port is closed.
- **Target:** Single IP 192.168.1.2
- **Reason:** Understand which services are exposed on the local network.

Target Host Information

Attribute	Value
IP Address	192.168.1.2
Host Status	Up
Response Latency	0.00011 seconds
Detected Ports	1 open port
Closed Ports	999 TCP ports

Scan Results Summary

Port	Protocol	State	Service	Version
22	TCP	open	SSH	OpenSSH 9.9p2 Debian 2

Additional Information:

- **OS Detected:** Linux
- **CPE Identifier:** cpe:/o:linux:linux_kernel

Analysis of SSH Version

- **OpenSSH Version:** 9.9p2
- **Distribution:** Debian-based system

Positives:

- OpenSSH 9.9p2 is a **relatively recent version**, released in **2024**, suggesting the system is updated.
- Protocol 2.0 is the **secure version** of SSH

Still Important to Confirm:

- Whether the service **allows password authentication** or is limited to **key-based**.
- Whether **root login** is disabled in /etc/ssh/sshd_config.

- If any **public exposure** of the port exists (e.g., NAT/router port forwarding).
- Whether **fail2ban** or similar protections are enabled against brute-force attempts.

Updated Security Recommendations

Updated Security Recommendations (Bullet Format)

- Use key-based SSH authentication instead of password-based logins.
- Disable root login by setting PermitRootLogin no in the SSH configuration file (/etc/ssh/sshd_config).
- Configure a firewall to allow SSH access only from trusted IP addresses or networks.
- Change the default SSH port (e.g., from 22 to 2222) to reduce automated scan attempts (optional, but helps reduce noise).
- Enable logging and monitor logs for SSH activity and failed login attempts (e.g., /var/log/auth.log).
- Protect against brute-force attacks using tools like fail2ban or SSHGuard.
- Regularly update the OpenSSH service and the underlying Debian-based system to patch security vulnerabilities.

Conclusion

The host 192.168.1.2 is running **OpenSSH 9.9p2 on a Debian-based Linux system**. The service appears up-to-date, but its exposure and configuration should be reviewed to minimize risk.

The next logical steps are:

- SSH into the host (if authorized) and review /etc/ssh/sshd_config
- Confirm authentication methods
- Check for any misconfigurations
- Continue enumerating the host or network if this is part of a broader audit