

sudo apt update && sudo apt upgrade -y

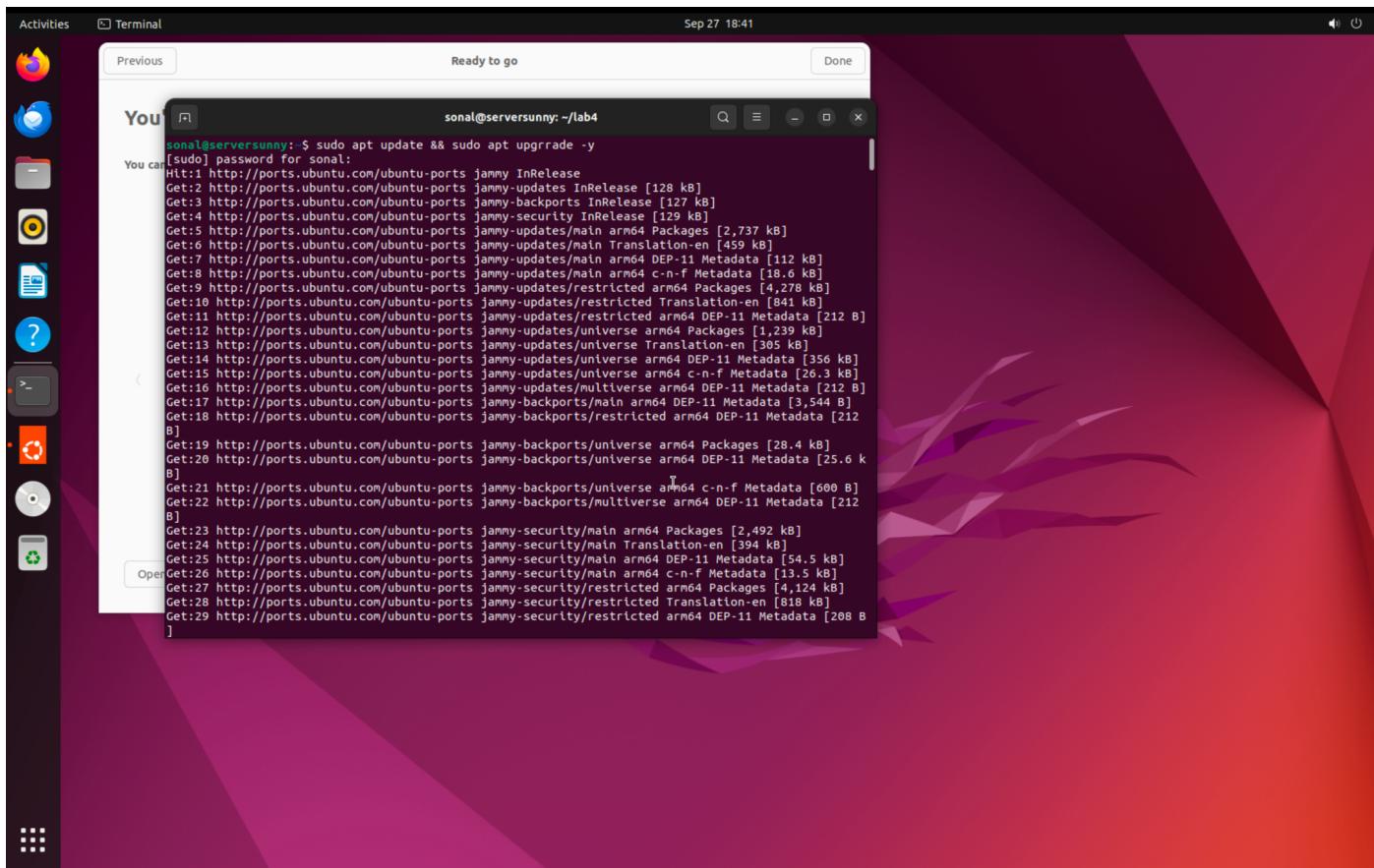
Refreshes Ubuntu's package lists and installs any available updates so the system is current before we start.

mkdir ~/lab4

Creates a working folder in your home directory to keep all Lab 4 files together.

cd ~/lab4

Moves into that folder so any files we create end up in the right place.



```
sonal@serversunny: ~$ sudo apt update && sudo apt upgrade -y
[sudo] password for sonal:
Hit:1 http://ports.ubuntu.com/ubuntu-ports jammy InRelease
Get:2 http://ports.ubuntu.com/ubuntu-ports jammy-updates InRelease [128 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports jammy-backports InRelease [127 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease [129 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 Packages [2,737 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main Translation-en [459 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 DEP-11 Metadata [112 kB]
Get:8 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 c-n-f Metadata [18.6 kB]
Get:9 http://ports.ubuntu.com/ubuntu-ports jammy-updates/restricted arm64 Packages [4,278 kB]
Get:10 http://ports.ubuntu.com/ubuntu-ports jammy-updates/restricted Translation-en [841 kB]
Get:11 http://ports.ubuntu.com/ubuntu-ports jammy-updates/restricted arm64 DEP-11 Metadata [212 B]
Get:12 http://ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 Packages [1,239 kB]
Get:13 http://ports.ubuntu.com/ubuntu-ports jammy-updates/universe Translation-en [305 kB]
Get:14 http://ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 DEP-11 Metadata [356 kB]
Get:15 http://ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 c-n-f Metadata [26.3 kB]
Get:16 http://ports.ubuntu.com/ubuntu-ports jammy-updates/multiverse arm64 DEP-11 Metadata [212 B]
Get:17 http://ports.ubuntu.com/ubuntu-ports jammy-backports/main arm64 DEP-11 Metadata [3,544 kB]
Get:18 http://ports.ubuntu.com/ubuntu-ports jammy-backports/restricted arm64 DEP-11 Metadata [212 B]
]
Get:19 http://ports.ubuntu.com/ubuntu-ports jammy-backports/universe arm64 Packages [28.4 kB]
Get:20 http://ports.ubuntu.com/ubuntu-ports jammy-backports/universe arm64 DEP-11 Metadata [25.6 kB]
]
Get:21 http://ports.ubuntu.com/ubuntu-ports jammy-backports/universe arm64 c-n-f Metadata [600 B]
Get:22 http://ports.ubuntu.com/ubuntu-ports jammy-backports/multiverse arm64 DEP-11 Metadata [212 B]
]
Get:23 http://ports.ubuntu.com/ubuntu-ports jammy-security/main arm64 Packages [2,492 kB]
Get:24 http://ports.ubuntu.com/ubuntu-ports jammy-security/main Translation-en [394 kB]
Get:25 http://ports.ubuntu.com/ubuntu-ports jammy-security/main arm64 DEP-11 Metadata [54.5 kB]
Get:26 http://ports.ubuntu.com/ubuntu-ports jammy-security/main arm64 c-n-f Metadata [13.5 kB]
Get:27 http://ports.ubuntu.com/ubuntu-ports jammy-security/restricted arm64 Packages [4,124 kB]
Get:28 http://ports.ubuntu.com/ubuntu-ports jammy-security/restricted Translation-en [818 kB]
Get:29 http://ports.ubuntu.com/ubuntu-ports jammy-security/restricted arm64 DEP-11 Metadata [208 B]
]
```

sudo apt install nmap -y

Installs Nmap, the network scanner we'll use to discover hosts and services.

nmap -sn 127.0.0.1

Pings the local machine (localhost) to confirm the VM is reachable/up—no port scan, just host discovery.

ip a

Shows your network interfaces and IP addresses; 'ens160' is your VMware network adapter.

```
sonal@serversunny: ~/lab4
```

```
You can use the Up/Down arrow keys to navigate through the command history.
```

```
E: Invalid operation upgrade
```

```
sonal@serversunny: $ mkdir ~/Lab4
```

```
sonal@serversunny: $ cd ~/Lab4
```

```
sonal@serversunny: ~/Lab4$ sudo apt install nmap -y
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
```

```
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

```
sonal@serversunny: ~/Lab4$ nmap -sn 127.0.0.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-27 18:33 UTC
```

```
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.0001s latency).
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

```
sonal@serversunny: ~/Lab4$ lpm a
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
        inet 127.0.0.1/8 scope host lo
```

```
            valid_lft forever preferred_lft forever
```

```
        inet6 ::1/128 scope host
```

```
            valid_lft forever preferred_lft forever
```

```
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
```

```
    link/ether 00:0c:29:3b:6e:53 brd ff:ff:ff:ff:ff:ff
```

```
    altname enp2s0
```

```
    inet 172.16.42.128/24 metric 100 brd 172.16.42.255 scope global dynamic ens160
```

```
        valid_lft 1080sec preferred_lft 1080sec
```

```
        inet6 fe80::20c:29ff:fe3b:6e53/64 scope link
```

```
            valid_lft forever preferred_lft forever
```

```
sonal@serversunny: ~/Lab4$ sudo netstat -tuln
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN

sudo netstat -tuln

Lists TCP/UDP ports that are currently listening. In your case, SSH (22/tcp) and IPP (631/tcp) were open.

sudo lsof -i -P -n

Shows which processes are bound to which network ports (owners/PIDs), without DNS lookups and with numeric ports.

sudo nmap -sV localhost

Scans your own machine to find open ports and attempts to identify the service versions (e.g., OpenSSH, CUPS).

The screenshot shows a Linux desktop environment with a terminal window titled "Ready to go". The terminal displays the following command-line session:

```
sonal@serversunny: ~/lab4
You can run 'man' on a command to get more information.
You can run 'man' on a command to get more information.

sonal@serversunny:~/lab4$ sudo lsof -i -p -n
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd-n 1864 systemd-network 18u IPv4 21397 0t0 UDP 172.16.42.128:68
systemd-r 1866 systemd-resolve 13u IPv4 22253 0t0 UDP 127.0.0.53:53
systemd-r 1866 systemd-resolve 14u IPv4 22254 0t0 TCP 127.0.0.53:53 (LISTEN)
avahi-dae 1877 avahi 12u IPv4 23635 0t0 UDP *:5353
avahi-dae 1877 avahi 13u IPv6 23636 0t0 UDP *:5353
avahi-dae 1877 avahi 14u IPv4 23637 0t0 UDP *:33866
avahi-dae 1877 avahi 15u IPv6 23638 0t0 UDP *:40952
cupsd 1169 root 6u IPv6 22816 0t0 TCP [::1]:631 (LISTEN)
cupsd 1169 root 7u IPv4 22817 0t0 TCP 127.0.1:631 (LISTEN)
sshd 1247 root 3u IPv4 24570 0t0 TCP *:22 (LISTEN)
sshd 1247 root 4u IPv6 24579 0t0 TCP *:22 (LISTEN)
sonal@serversunny:~/lab4$ sudo nmap -sS -O localhost
nmap: unrecognized option '-O'.
See the output of nmap -h for a summary of options.
sonal@serversunny:~/lab4$ sudo nmap -sV localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-27 18:38 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
631/tcp   open  ipp   CUPS 2.4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

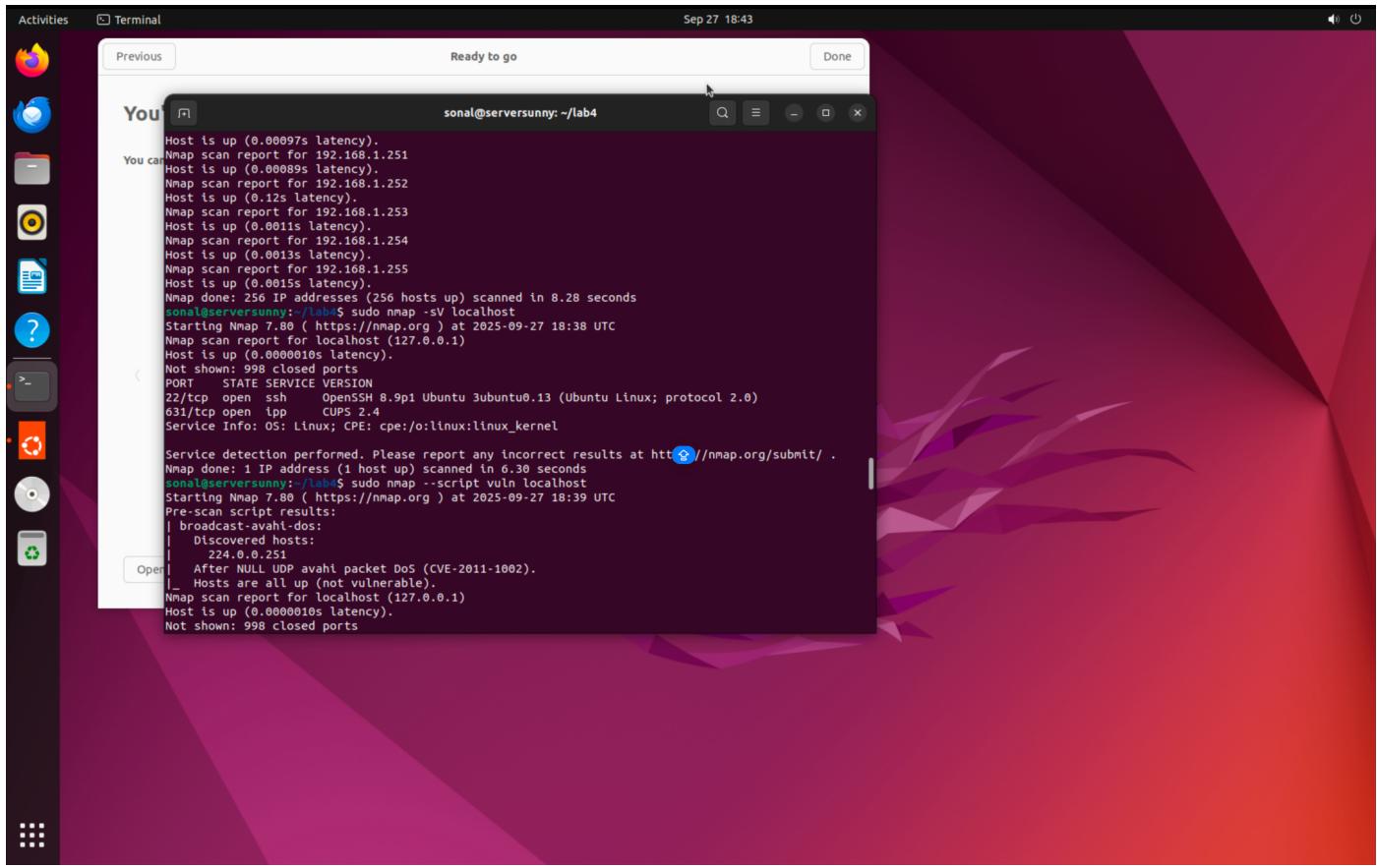
Below the terminal window, a message says "Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 6.33 seconds".

```
sudo nmap -sP 192.168.1.0/24
```

Discovers other devices on your local /24 network using host discovery (this found many live hosts).

```
sudo nmap --script vuln localhost
```

Runs the default ‘vuln’ NSE checks against your machine. Helpful to see if any known, easily testable issues appear.



sudo nmap --script http-enum localhost

If a web service exists, enumerates common web paths; on your box it printed a list of potential admin/backup paths.

sudo tcpdump -i ens160

Starts live packet capture on the VM's main network interface (Ctrl+C to stop).

sudo watch -n 1 netstat -tulnp

Refreshes the listening-ports list every second so you can watch services come and go in real time (Ctrl+C to stop).

sudo ufw status verbose

Shows Ubuntu's firewall (UFW) status and default policies; yours was inactive for this lab.

