sudo apt update && sudo apt upgrade -y

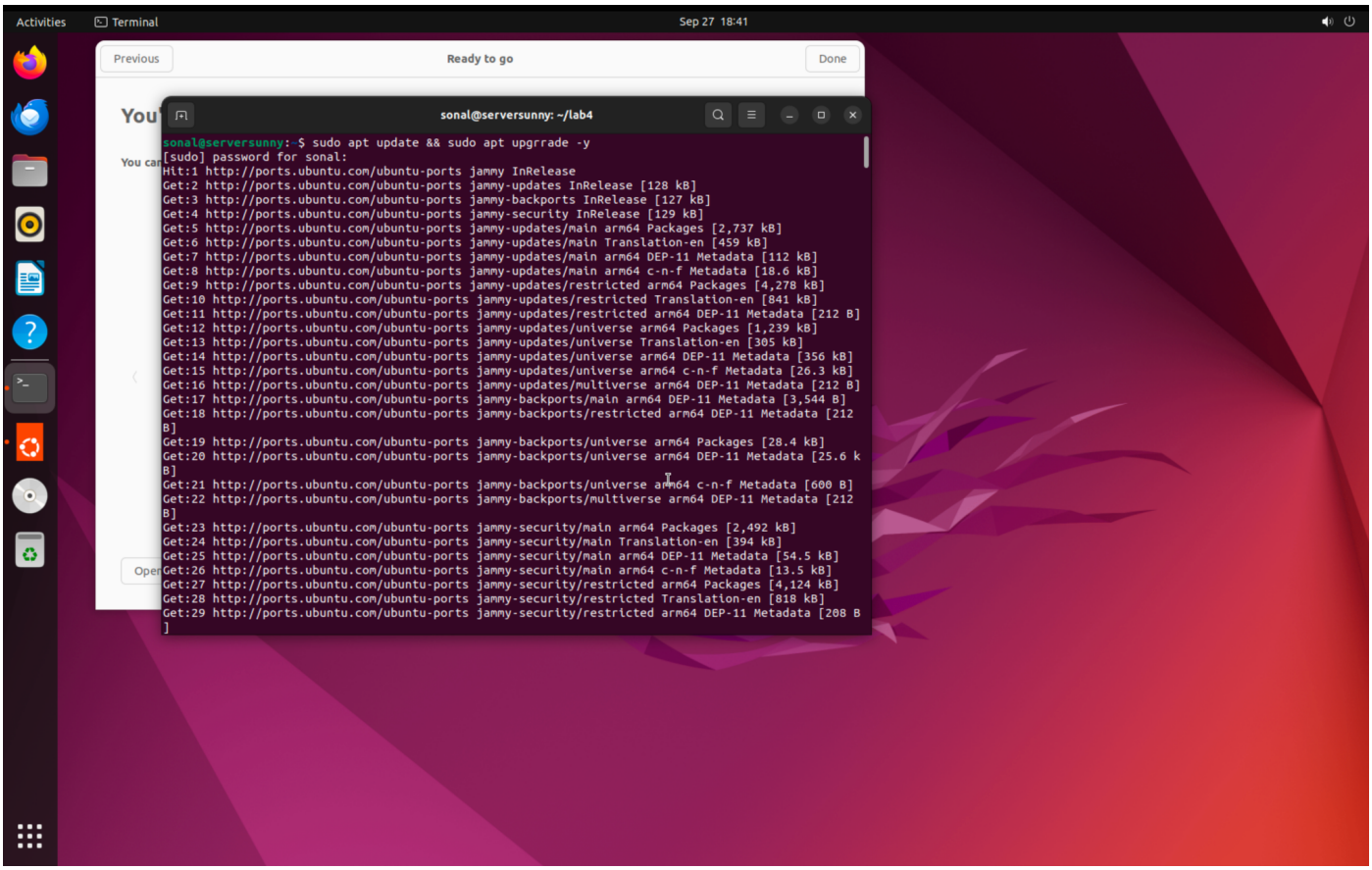
Refreshes Ubuntu's package lists and installs any available updates so the system is current before we start.

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.



sudo apt install nmap -y

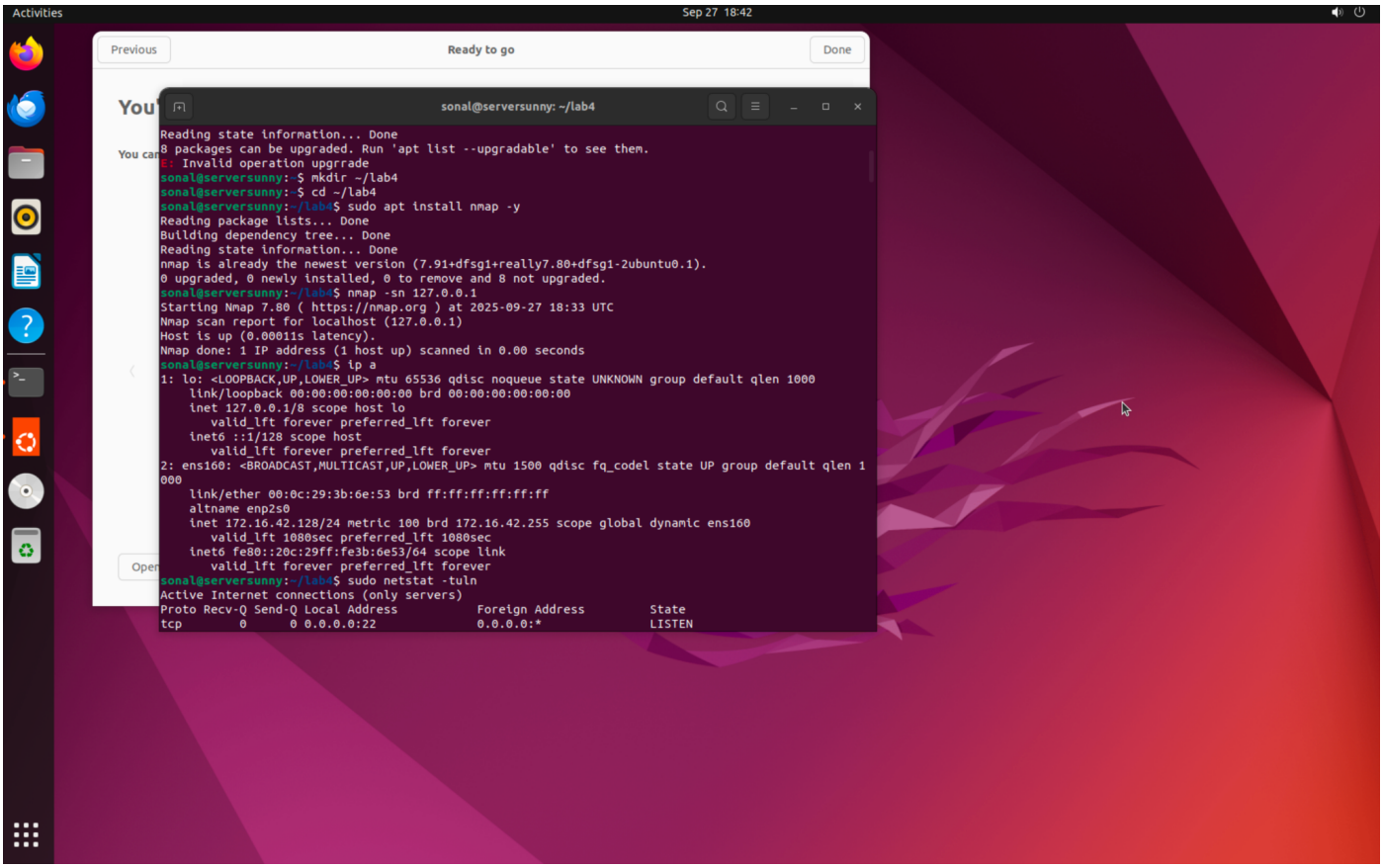
Installs Nmap, the network scanner we'll use to discover hosts and services.

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.



sudo netstat -tuln

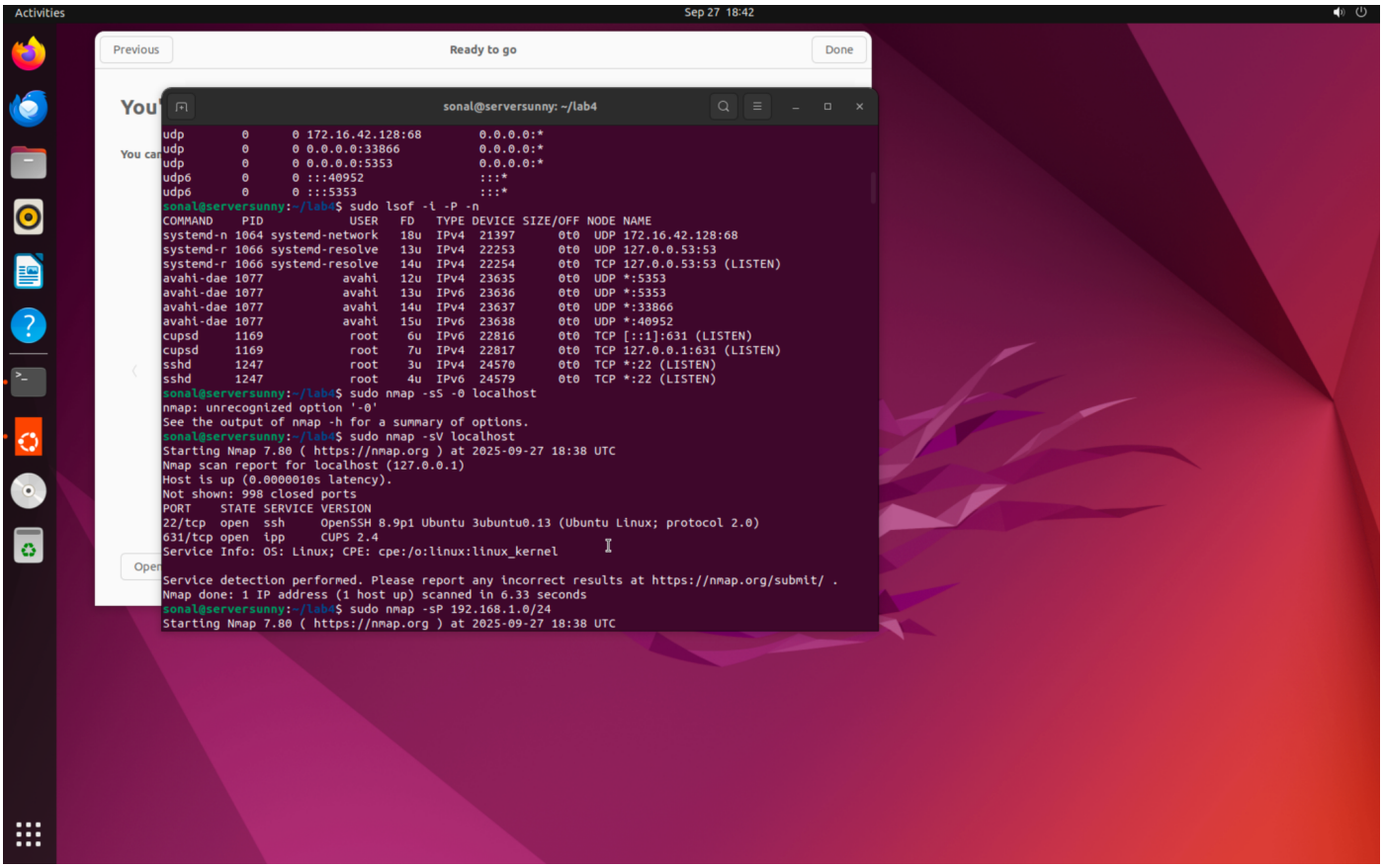
Lists TCP/UDP ports that are currently listening. In your case, SSH (22/tcp) and IPP (631/tcp) were open.

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).

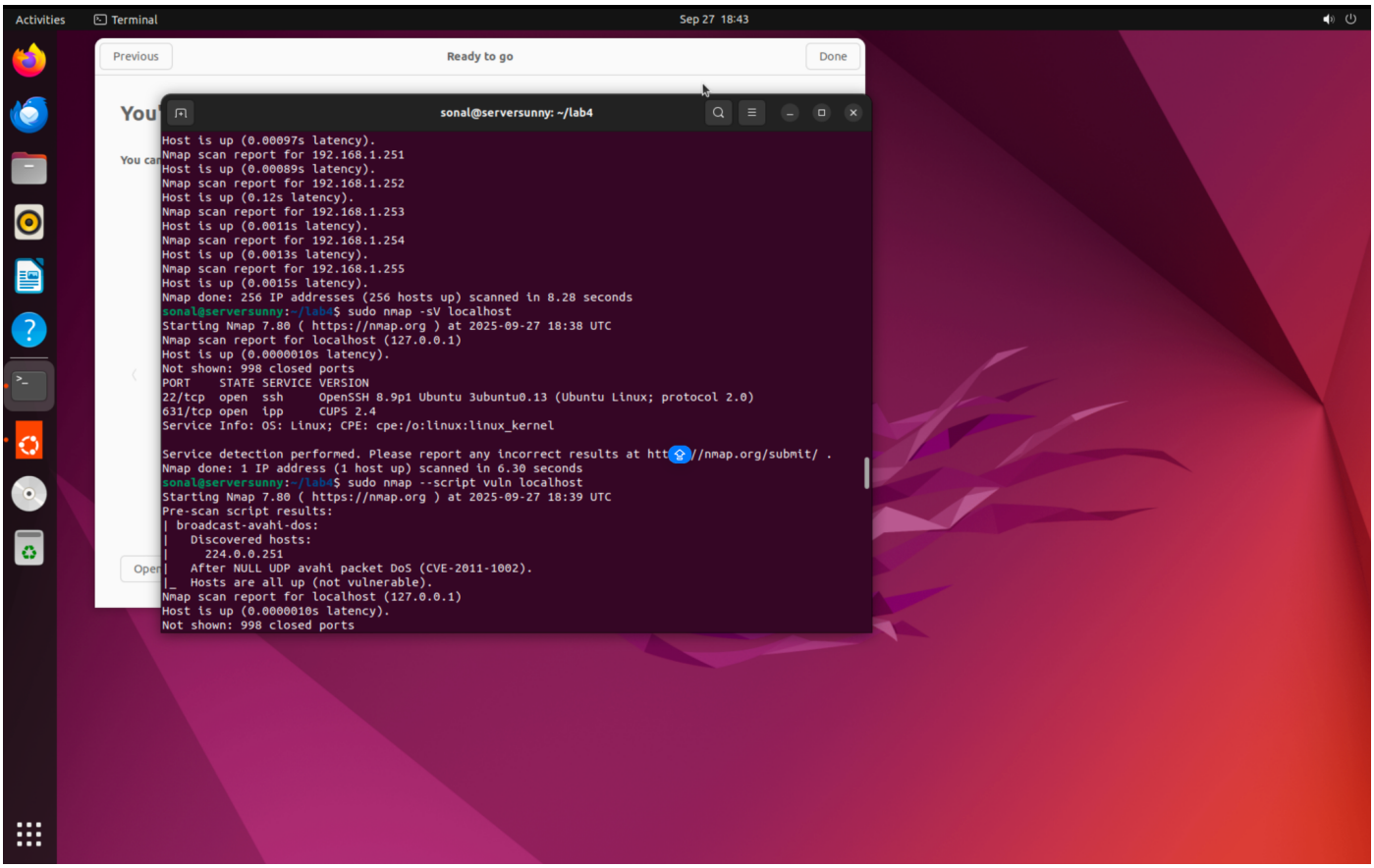


sudo nmap -sP 192.168.1.0/24

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

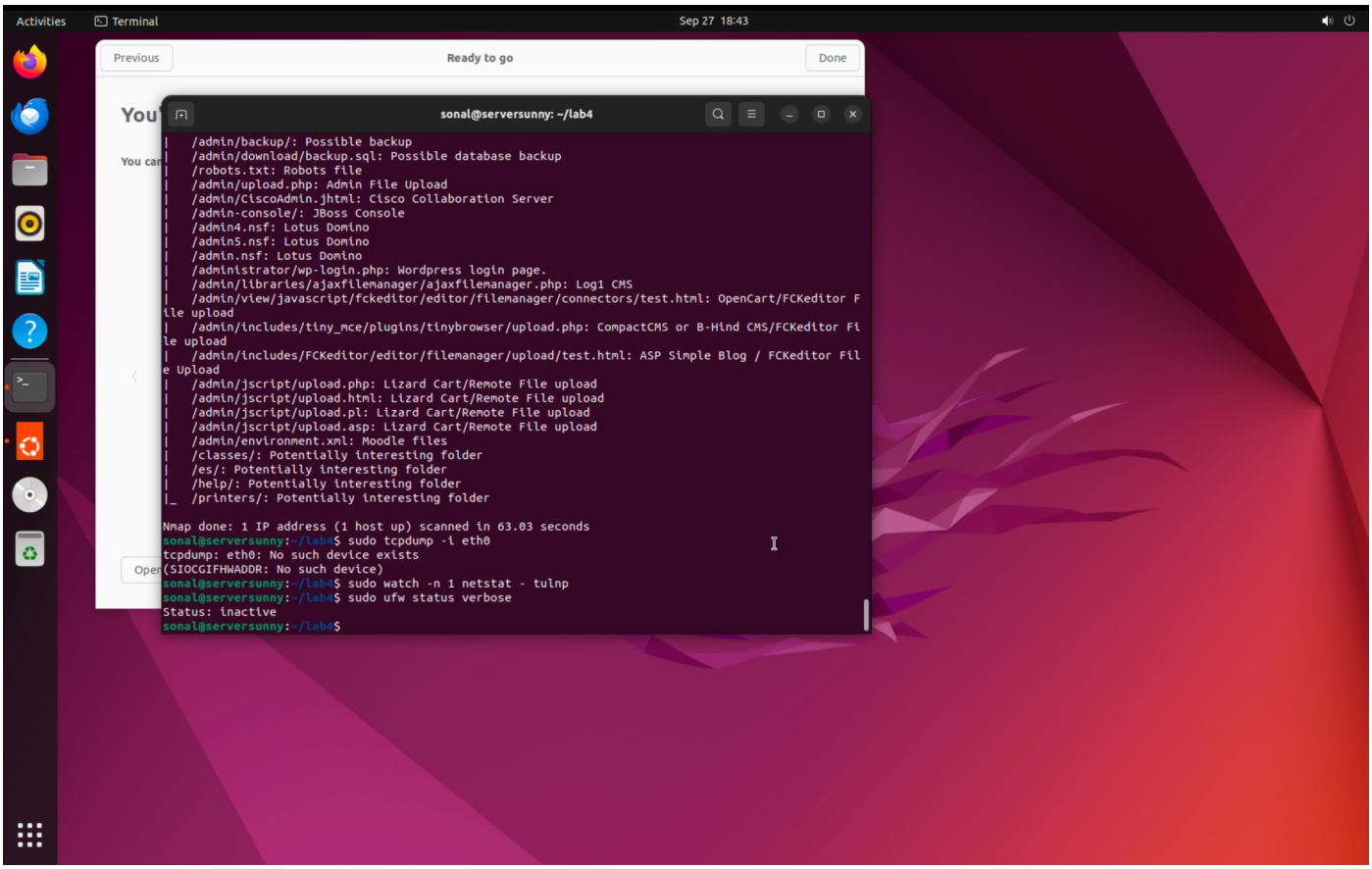
Starts live packet capture on the VM's main network interface (Ctrl+C to stop).

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.


Activities
Terminal
Sep 27 18:43
Previous
Ready to go
Done
sonal@serversunny: ~/lab4
| /admin/backup/: Possible backup
| /admin/download/backup.sql: Possible database backup
| /robots.txt: Robots file
| /admin/upload.php: Admin File Upload
| /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
| /admin-console/: JBoss Console
| /admin4.nsf: Lotus Domino
| /admin5.nsf: Lotus Domino
| /admin.nsf: Lotus Domino
| /administrator/wp-login.php: Wordpress login page.
| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.php: Lizard Cart/Remote File upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
| /admin/jscript/upload.pl: Lizard Cart/Remote File upload
| /admin/jscript/upload.asp: Lizard Cart/Remote File upload
| /admin/environment.xml: Moodle files
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
|_ /printers/: Potentially interesting folder
Nmap done: 1 IP address (1 host up) scanned in 63.03 seconds
sonal@serversunny:~/lab4$ sudo tcpdump -i eth0
tcpdump: eth0: No such device exists
(SIOCGIFHWADDR: No such device)
sonal@serversunny:~/lab4$ sudo watch -n 1 netstat - tulnp
sonal@serversunny:~/lab4$ sudo ufw status verbose
Status: inactive
sonal@serversunny:~/lab4$