Ethical Hacking lab setup guide

VirtualBox Handout - Kali Linux (NAT + Host-Only) and Metasploitable 2 (Host-Only)

Safety notice

1.Training only: You may scan/exploit Metasploitable 2 in this lab environment only.
2. Never expose Metasploitable: Metasploitable is intentionally vulnerable. It must remain on Host-Only networking only. Do not use Bridged and do not place it on your real LAN.
3. One target: Only target the Host-Only IP address of the Metasploitable VM. Do not scan other IP ranges.
4. No port forwarding: Do not configure port forwarding rules to Metasploitable.
5. If in doubt, stop: If you think Metasploitable is reachable from other devices on your network, power it off and re-check networking.

Quick Start (5-Minute Checklist)

- ☐ Import Kali VM and Metasploitable VM into VirtualBox
- ☐ Kali: Adapter 1 = NAT; Adapter 2 = Host-Only (same Host-Only name as Metasploitable)
- ☐ Metasploitable: Adapter 1 = Host-Only only
- ☐ Boot Metasploitable first, then Kali
- ☐ Find IPs: Kali has two IPs (NAT + Host-Only); Metasploitable has one IP (Host-Only)
- ☐ Ping: Kali -> Metasploitable Host-Only IP
- ☐ Update Kali via NAT and reboot
- ☐ Take snapshots for both VMs (Lab Ready restore points)

1. Purpose and Learning Outcomes

This handout helps you set up a controlled ethical-hacking lab using VirtualBox. The lab is designed so that Kali Linux has internet access for updates (NAT), while the Metasploitable target remains isolated (Host-Only).

Learning outcomes: After completing this lab setup, you will be able to:

- ➔ Explain the difference between NAT and Host-Only networking in VirtualBox.
- ➔ Build a two-interface attacker VM (Kali) with a dedicated isolated attack network.
- ➔ Keep a deliberately vulnerable target (Metasploitable) isolated from real networks.
- ➔ Verify correct IP addressing, routing, and reachability using standard Linux commands.
- ➔ Perform safe, lab-only discovery testing (ping, basic nmap service detection).
- ➔ Create and use snapshots to quickly recover your lab after exercises.

2. Threat Model and Boundaries

A safe lab is built by assuming mistakes happen (wrong adapter selected, wrong IP scanned, vulnerable machine exposed). This section defines what could go wrong and how the design prevents it.

Threat model (what we are defending against):

- ➔ Accidental exposure of Metasploitable to your real network (LAN/Wi-Fi) where others could attack it.
- ➔ Accidentally scanning or attacking non-lab systems due to incorrect targeting.
- ➔ Breaking the lab environment during exercises and losing time rebuilding.

Boundaries (hard rules):

- ➔ Metasploitable uses Host-Only only and has no NAT/Bridged adapter.
- ➔ All scans and attacks target only the Metasploitable Host-Only IP address.
- ➔ No port forwarding to Metasploitable. No bridging. No exposure.
- ➔ Keep the lab private: do not share the VM image files with untrusted parties.

3. Preflight Checklist

Complete these checks before starting. Most failures come from skipping this section.

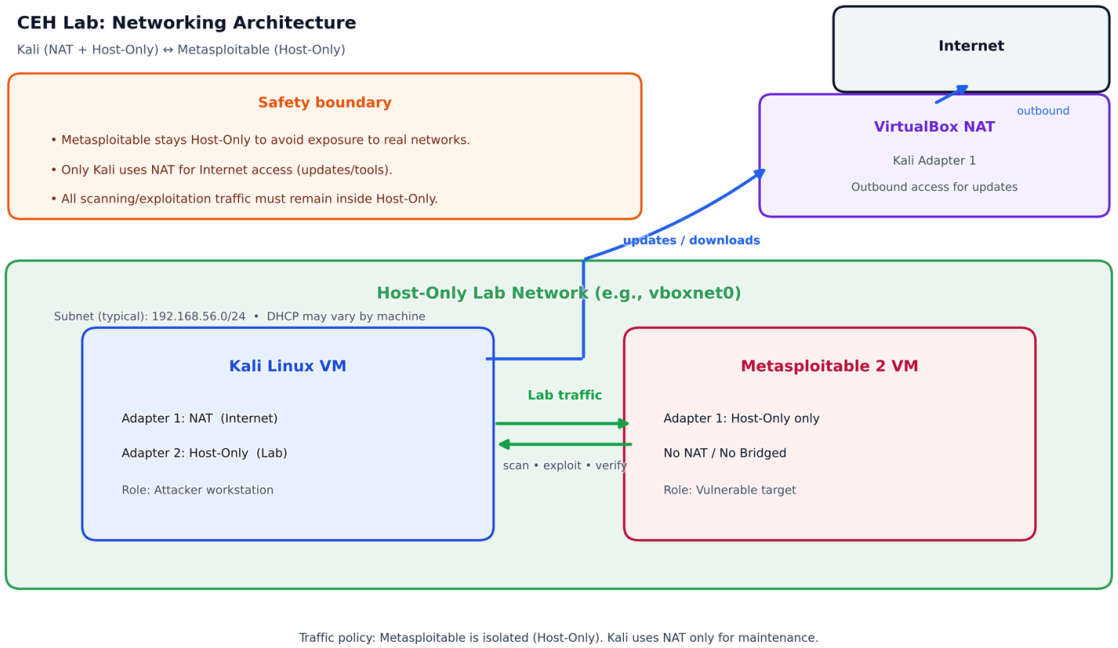
- ☐ Hardware: at least 30 GB free disk space
- ☐ Hardware: at least 6-8 GB RAM available (8+ recommended)
- ☐ BIOS/UEFI: virtualization enabled (Intel VT-x / AMD-V)
- ☐ VirtualBox installed and opens without errors
- ☐ Kali VM image downloaded and extracted (or ISO available)
- ☐ Metasploitable 2 image downloaded and extracted (VMDK present)
- ☐ You understand Metasploitable must remain Host-Only only (no Bridged)
- ☐ You have a stable internet connection for Kali updates

4. Environment Summary

Component	Role	Networking	Internet	Notes
Kali Linux VM	Attacker workstation	Adapter 1: NAT Adapter 2: Host-Only	Yes (via NAT)	Tools, updates, scanning, reporting
Metasploitable 2	Vulnerable target	Adapter 1: Host-Only Adapter 2: Disabled	No	Must remain isolated (no Bridged / no NAT
Host-Only network	Lab-only segment	Shared: Kali Adapter 2 ↔ Meta Adapter 1	No	Traffic stays inside host + VMs
VirtualBox NAT	Outbound internet	Kali Adapter 1 only	Yes	Safe outbound access for Kali (no target exposure)

5. Architecture and Traffic Flow

The lab uses two separate network paths: one for safe internet updates (NAT) and one for isolated lab communication (Host-Only). Metasploitable stays isolated by design.



Traffic rules:

- ➔ Kali (NAT) -> Internet: allowed (updates and downloads).
- ➔ Kali (Host-Only) <-> Metasploitable (Host-Only): allowed (lab scanning/exploitation).
- ➔ Internet/LAN -> Metasploitable: blocked by design (no route, no bridge).

6. Prerequisites

Recommended VM resources (adjust to your computer):

VM	CPU	RAM	Disk	Notes
Kali Linux	4 vCPU (min 2vCPU)	6 GB (min 4 GB)	30+ GB	Needs headroom for tools and updates
Metasploitable 2	1 vCPU	1 GB	Existing VMDK	Lightweight target

Downloads (official sources):

VirtualBox
https://www.virtualbox.org/wiki/Downloads
Kali Linux (VirtualBox images)
https://cdimage.kali.org/kali-2025.4/kali-linux-2025.4-virtualbox-amd64.7z
Kali import guide
https://www.kali.org/docs/virtualization/import-premade-virtualbox/
Metasploitable 2
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Metasploitable 2 setup guide (online)
https://www.geeksforgeeks.org/linux-unix/how-to-install-metasploitable-2-in-virtualbox/

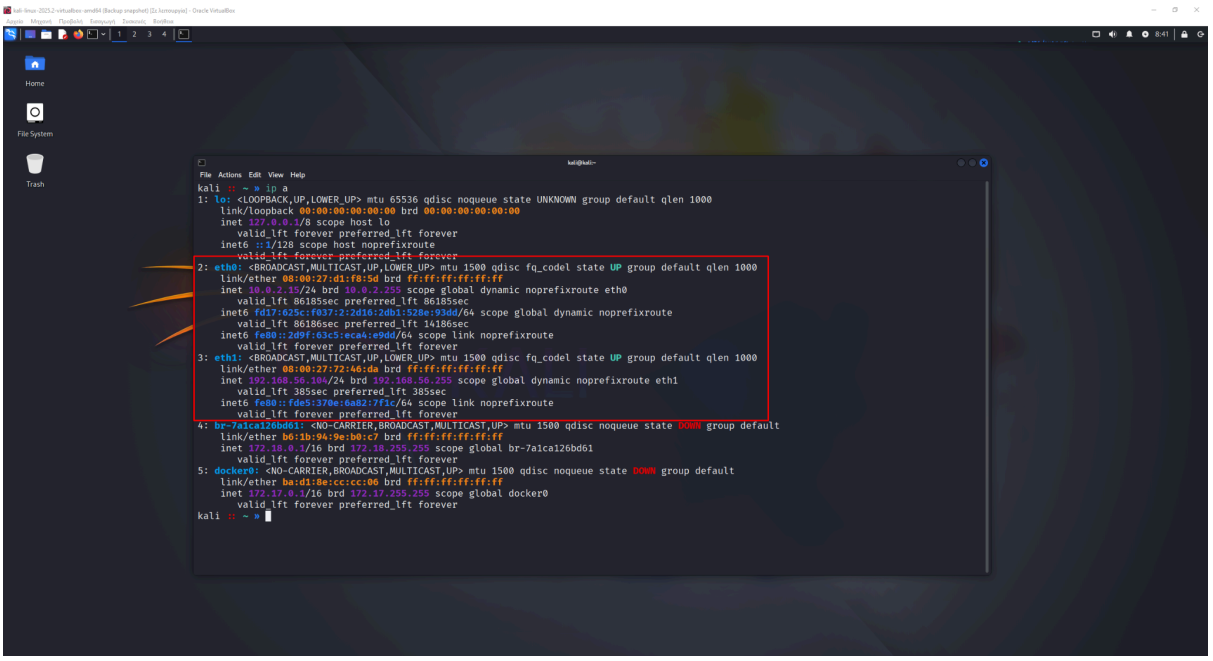
7. Setup and Run (Step-by-Step)

Follow these steps in order. Do not skip checkpoints.

1) Import Kali into VirtualBox

- ➔ Download the Kali VirtualBox image and extract it (7-Zip/WinRAR).
- ➔ Open VirtualBox -> Machine -> Add.
- ➔ Select the Kali .vbox file (or import .ova if provided).
- ➔ Start the VM and log in.

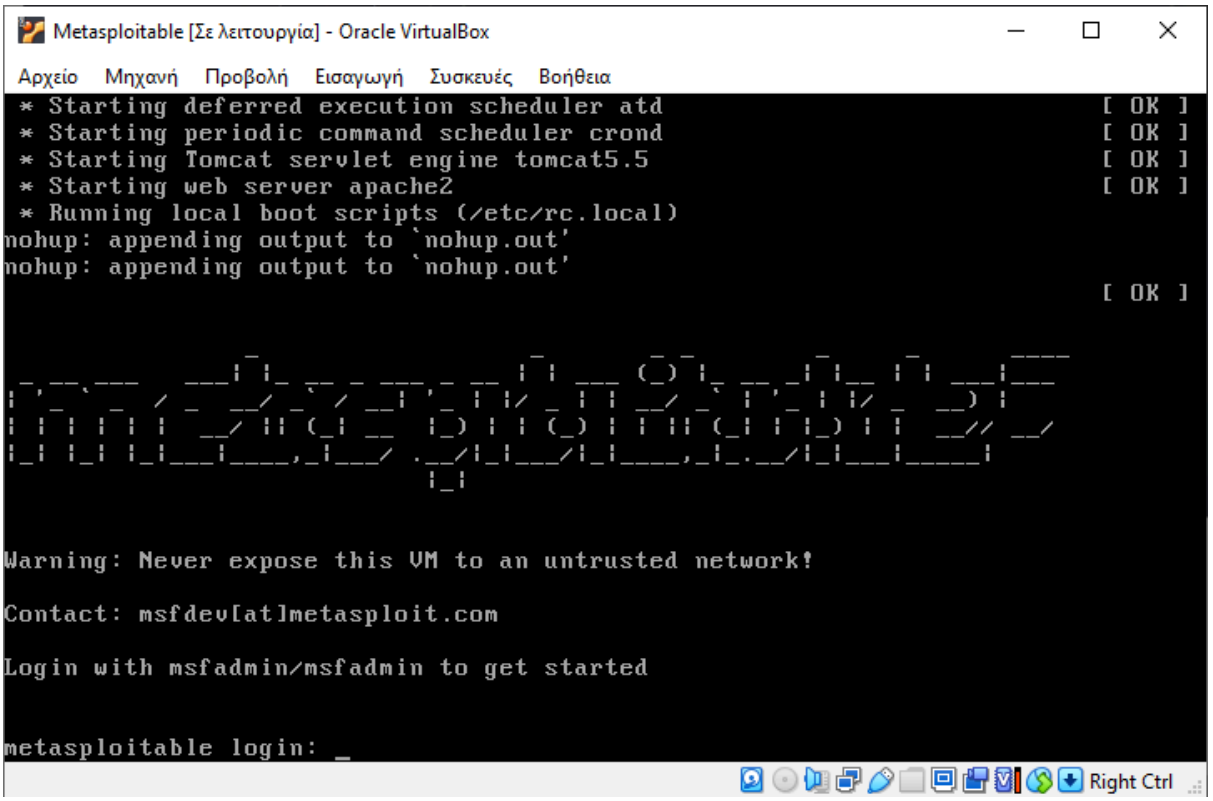
Common default credentials for prebuilt Kali images: username: kali | password: kali
Checkpoint: Kali boots successfully and you can open a terminal.



2) Create Metasploitable 2 VM (Attach Existing VMDK)

- ➔ Download Metasploitable 2 and extract the archive.
- ➔ In VirtualBox click New.
- ➔ Name: Metasploitable2; Type: Linux; Version: Ubuntu (32-bit or 64-bit depending on the image).
- ➔ When asked for a disk, choose 'Use an existing virtual hard disk file' and select the extracted .vmdk.
- ➔ Finish and start the VM.

Default credentials: username: msfadmin | password: msfadmin
Checkpoint: Metasploitable reaches the login prompt.



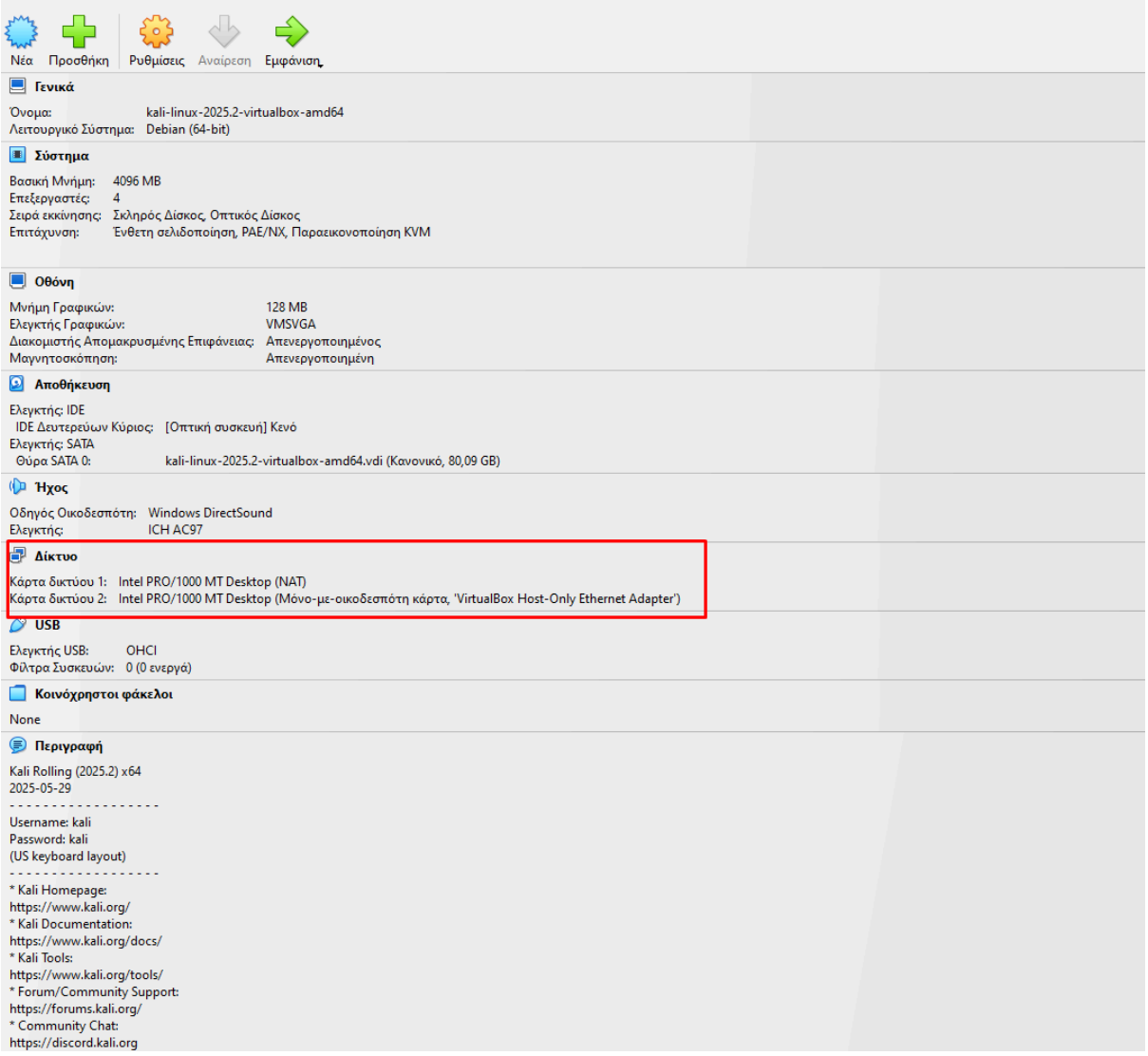
3) Configure Networking (Exact Required Configuration)

You will configure adapters directly in each VM's Network tab. You do not need to manually create a Host-Only adapter as a separate step. Just select the available Host-Only network from the dropdown (commonly named vboxnet0 if other provided by default).

Kali VM - Network settings

- ➔ VirtualBox -> select Kali -> Settings -> Network.
- ➔ Adapter 1: Enable; Attached to = NAT; Cable connected = On.
- ➔ Adapter 2: Enable; Attached to = Host-only Adapter; Name = select the Host-Only network (e.g., vboxnet0); Cable connected = On.

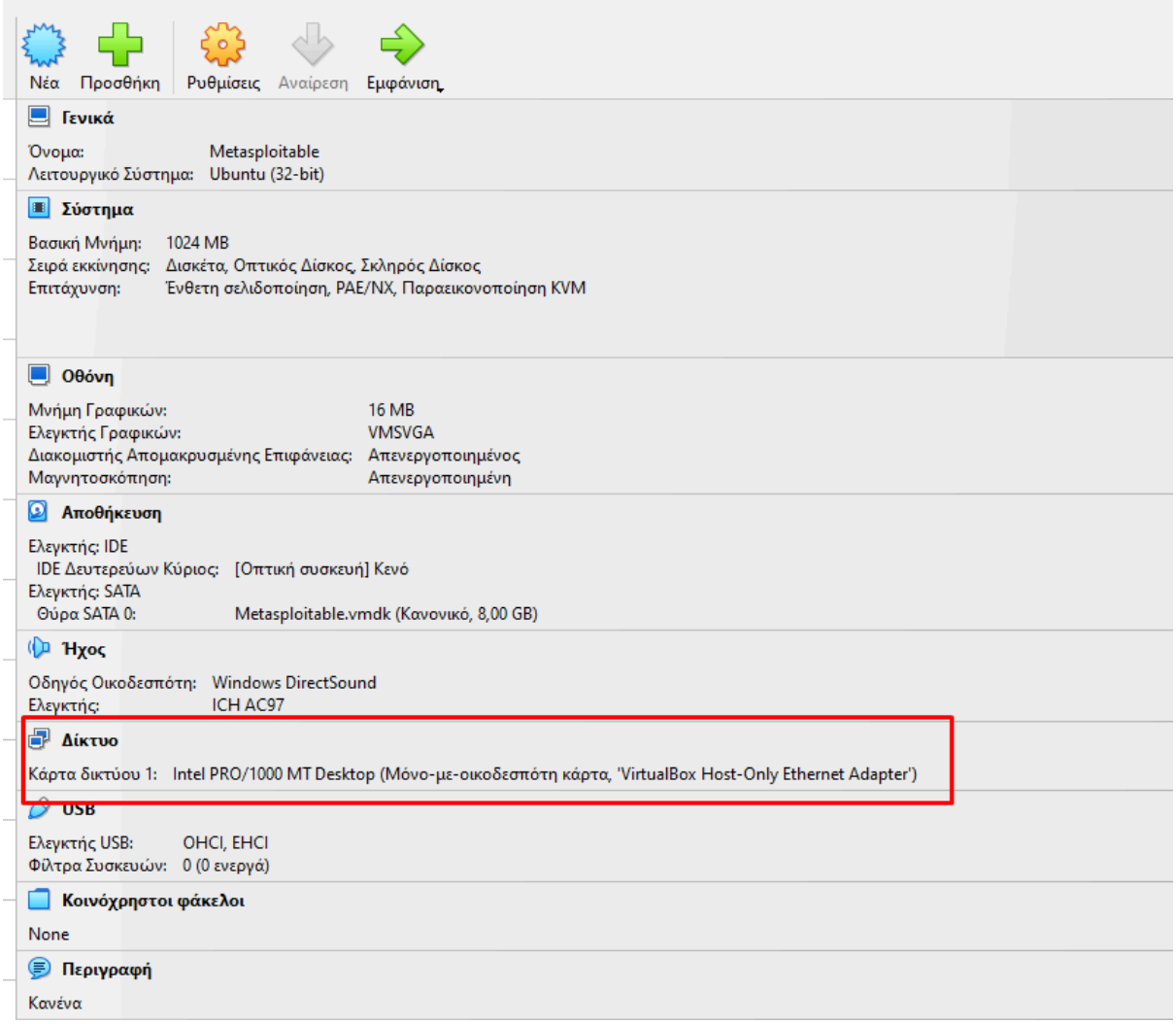
Checkpoint: Kali has exactly two enabled adapters: NAT (Adapter 1) + Host-Only (Adapter 2).



Metasploitable 2 VM - Network settings

- ➔ VirtualBox -> select Metasploitable2 -> Settings -> Network.
- ➔ Adapter 1: Enable; Attached to = Host-only Adapter; Name = same Host-Only network as Kali
- ➔ Adapter 2; Cable connected = On.
- ➔ Adapter 2: Disabled.

Checkpoint: Metasploitable has Host-Only only (no NAT, no Bridged).



Important: Host-Only dropdown empty?

If the Host-only Adapter 'Name' dropdown is empty on your machine, VirtualBox has no Host-Only network available. In that case, you must create one (VirtualBox Tools -> Host Network Manager -> Create) and then return to the VM settings.

Boot Order

- ➔ Start Metasploitable first (target).
- ➔ Start Kali second (attacker).
- ➔ Wait 30-60 seconds after boot so DHCP can assign addresses

8. Validation Tests

Do these tests before class. If any test fails, fix it before proceeding

Identify Kali IPs (NAT vs Host-Only)

Run on kali

```
ip a
ip route
ip route | grep default
```

Expected:

- ➔ One interface has a NAT IP (often 10.0.2.x).
- ➔ One interface has a Host-Only IP (often 192.168.56.x).
- ➔ The default route typically points to the NAT gateway (often 10.0.2.2).

Identify Metasploitable Host-Only IP

Run on Metasploitable

```
ifconfig
# or
ip addr
```

Expected:

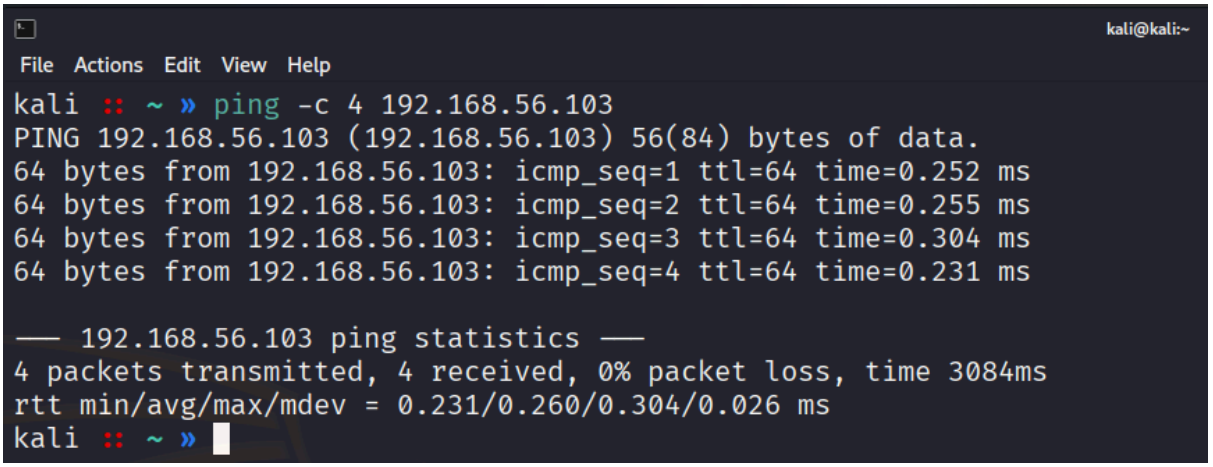
- ➔ Metasploitable has exactly one IP on the Host-Only subnet (often 192.168.56.x).

Ping Test (Kali -> Metasploitable

Run on Kali

```
ping -c 4 [METASPLOITABLE_HOST_ONLY_IP]
```

Expected: replies received (0% packet loss).



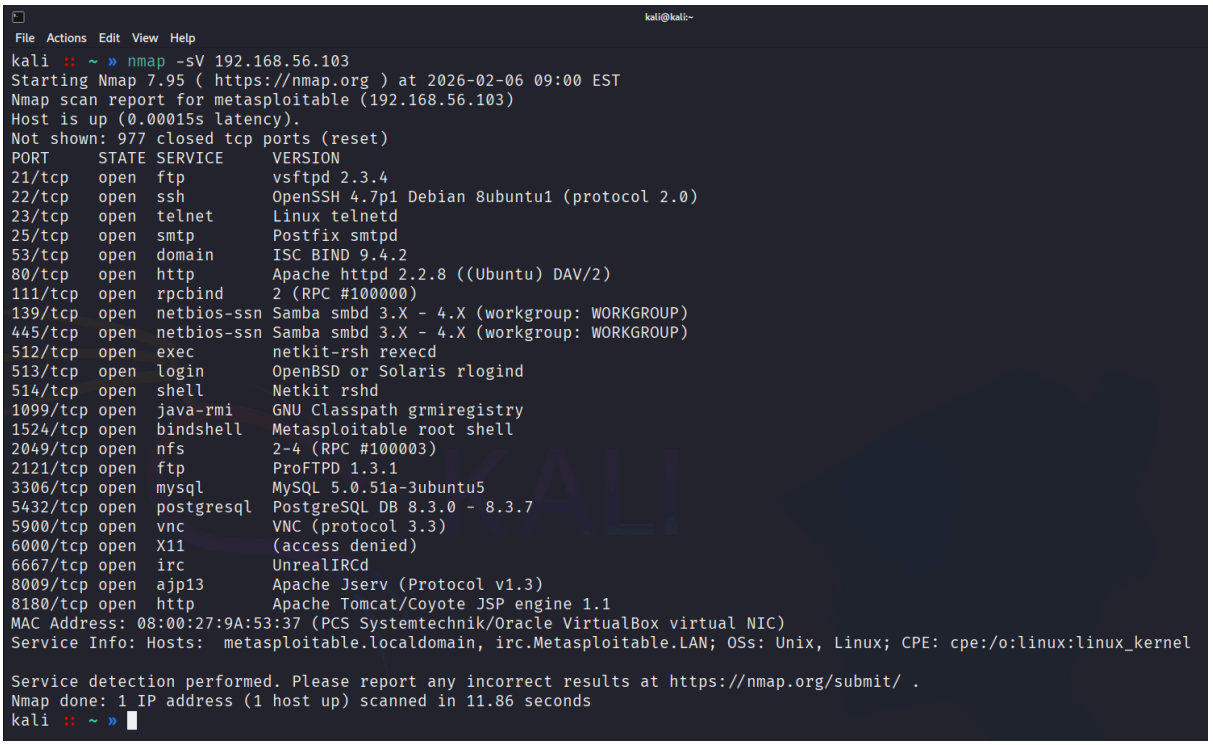
Light Service Discovery (Lab-Only)

This confirms that services are reachable. Only run this against the Metasploitable Host-Only IP.

Run on Kali

```
nmap -sV [METASPLOITABLE_HOST_ONLY_IP]
```

Expected: multiple open ports/services are listed (Metasploitable is intentionally vulnerable).



9. Update Kali (Class-Ready Baseline)

Update Kali after your networking validation confirms NAT is working. Updating ensures tools and packages match the lab exercises and reduces errors during class.

Confirm internet access (NAT), Update packages, Reboot and re-validate

Run on kali

```
ping -c 2 1.1.1.1
ping -c 2 google.com

sudo apt update

sudo reboot
# After reboot:
ip a
ping -c 2 [METASPLOITABLE_HOST_ONLY_IP]
```

10. Reset, Restore, and Cleanup

Snapshots are your safety net. Take them once the lab is validated and Kali is updated.

Take snapshots (recommended)
- VirtualBox -> select VM -> Snapshots -> Take.
- Name suggestions:
- - Kali - Updated + Lab Ready
- - Metasploitable - Clean + Lab Ready

Restore after a lab breaks something
- Power off the VM (do not save the state if it is unstable).
- Snapshots -> select your Lab Ready snapshot -> Restore.
- Re-run: ip a and ping tests before continuing.

Safe cleanup (if you need to remove the lab)
- Power off both VMs.
- VirtualBox -> right click VM -> Remove.
- Optionally delete VM files to free disk space.
- Keep your downloads if you want to reinstall quickly later