

# **Assignment 4 : Penetration Testing**

**Date:** 04-Apr-2025

**Student ID:** 8993413

**Student Name:** Urvi Surti

**Subject:** Software Testing Tools (SENG8031)

# 1. Kali Linux VM Setup :

Oracle VirtualBox Manager

File Machine Help

Tools

kali-linux-2025.1a-virtualbox-amd64

Running

Metasploitable2

Running

New Add Settings Discard Show

General

Name: kali-linux-2025.1a-virtualbox-amd64  
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB  
Processors: 2  
Boot Order: Hard Disk, Optical  
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB  
Graphics Controller: VMSVGA  
Remote Desktop Server: Disabled  
Recording: Disabled

Storage

Controller: IDE  
IDE Secondary Device 0: [Optical Drive] Empty  
Controller: SATA  
SATA Port 0: kali-linux-2025.1a-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound  
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, "VirtualBox Host-Only Ethernet Adapter")

USB

USB Controller: OHCI  
Device Filters: 0 (0 active)

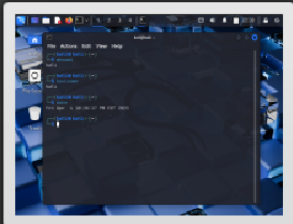
Shared folders

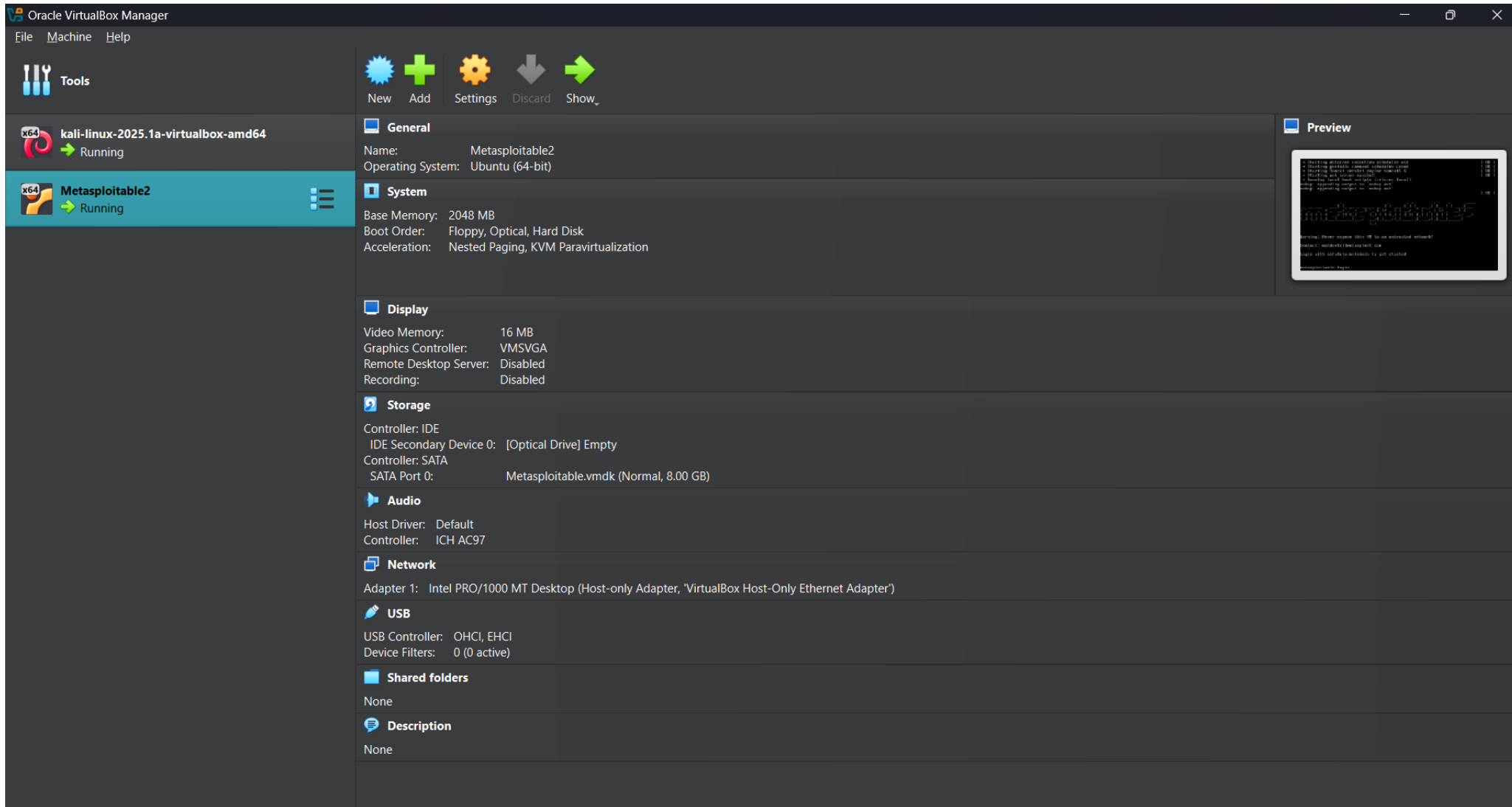
None

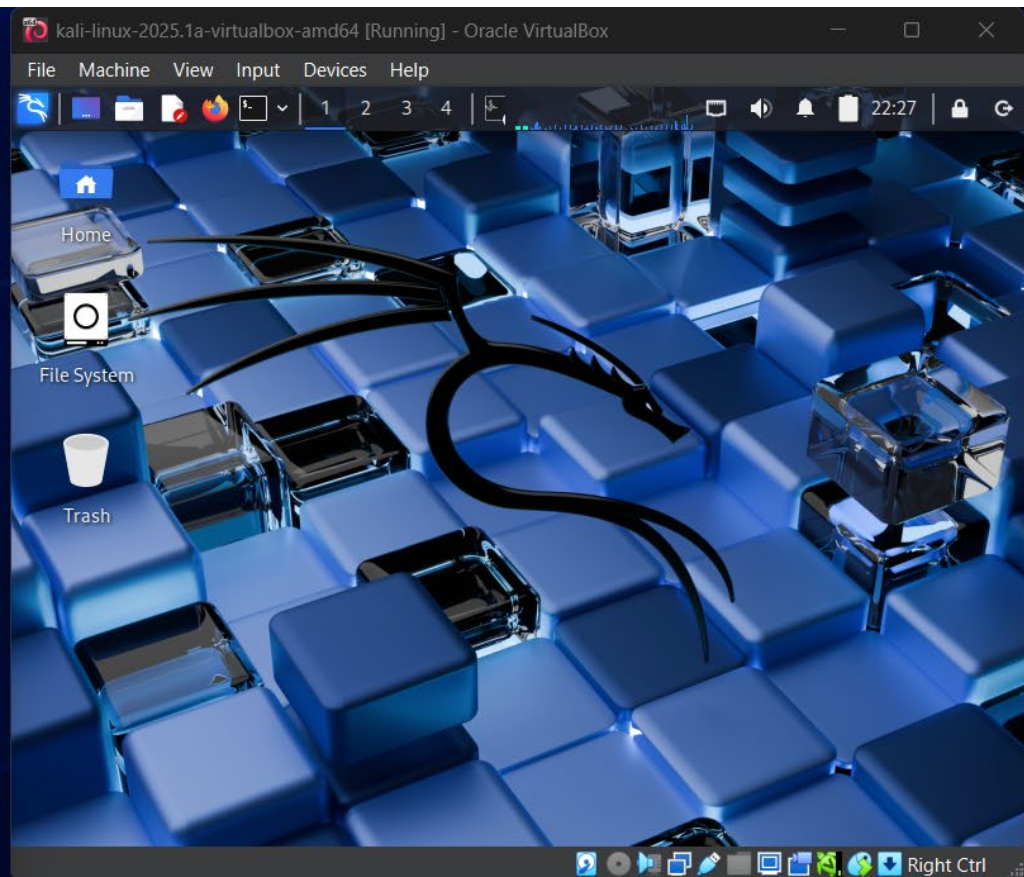
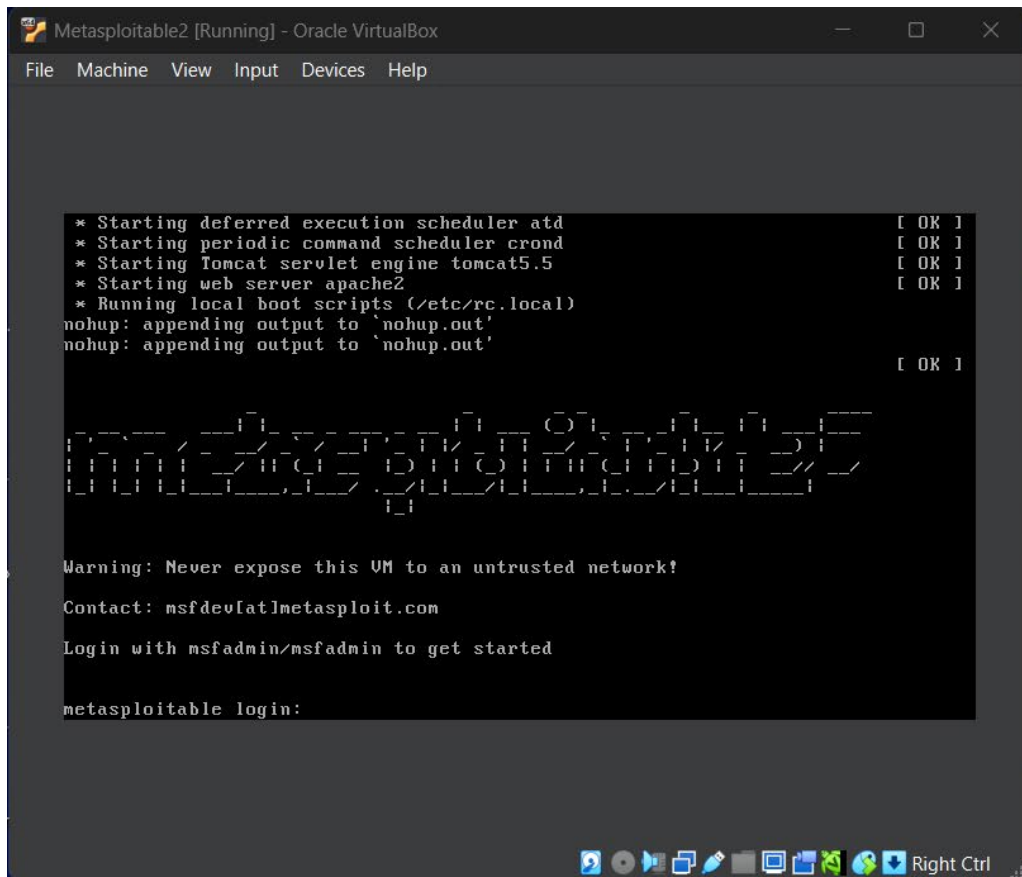
Description

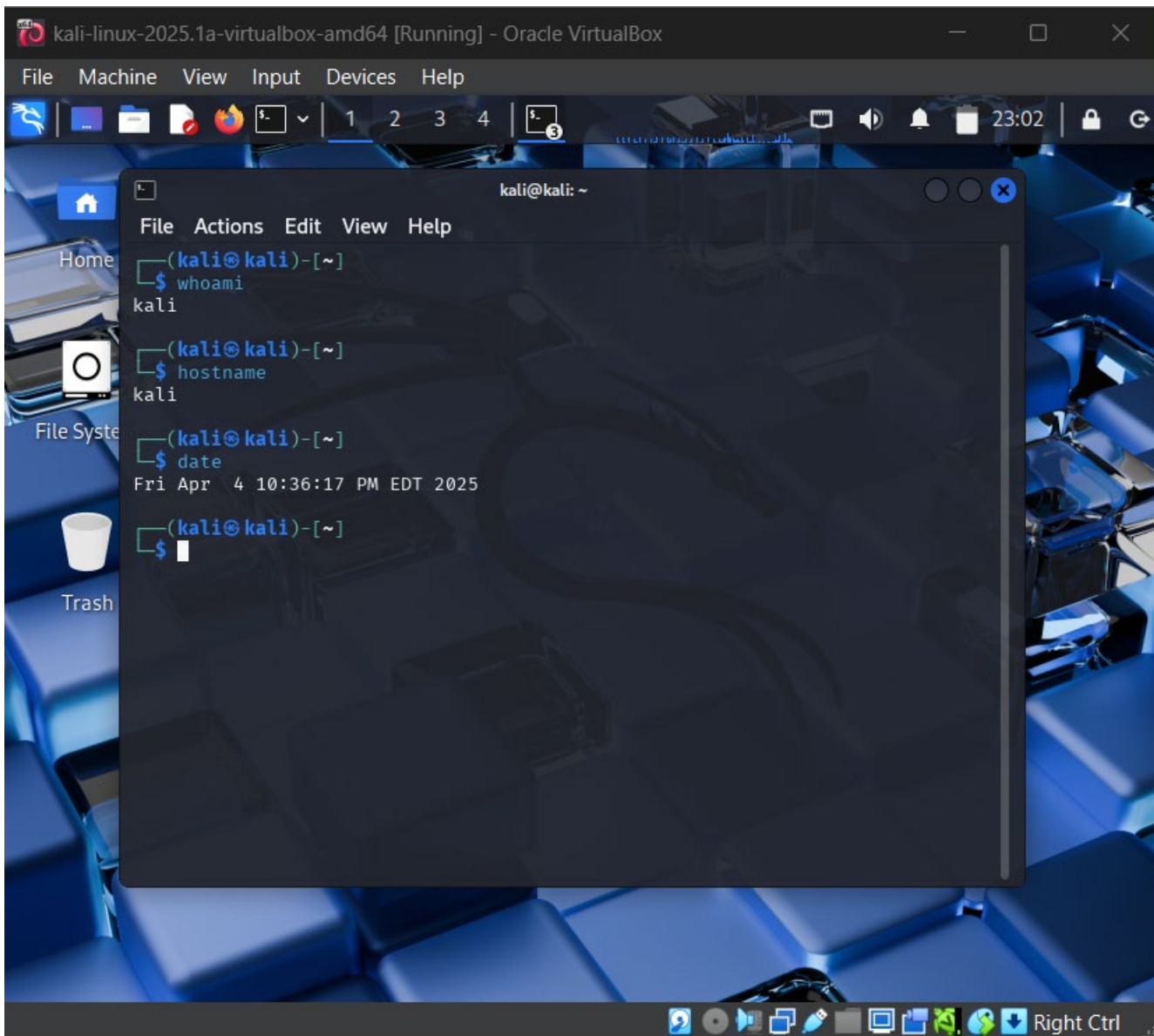
Kali Rolling (2025.1a) x64  
2025-03-07  
-----  
Username: kali  
Password: kali  
(US keyboard layout)

Preview



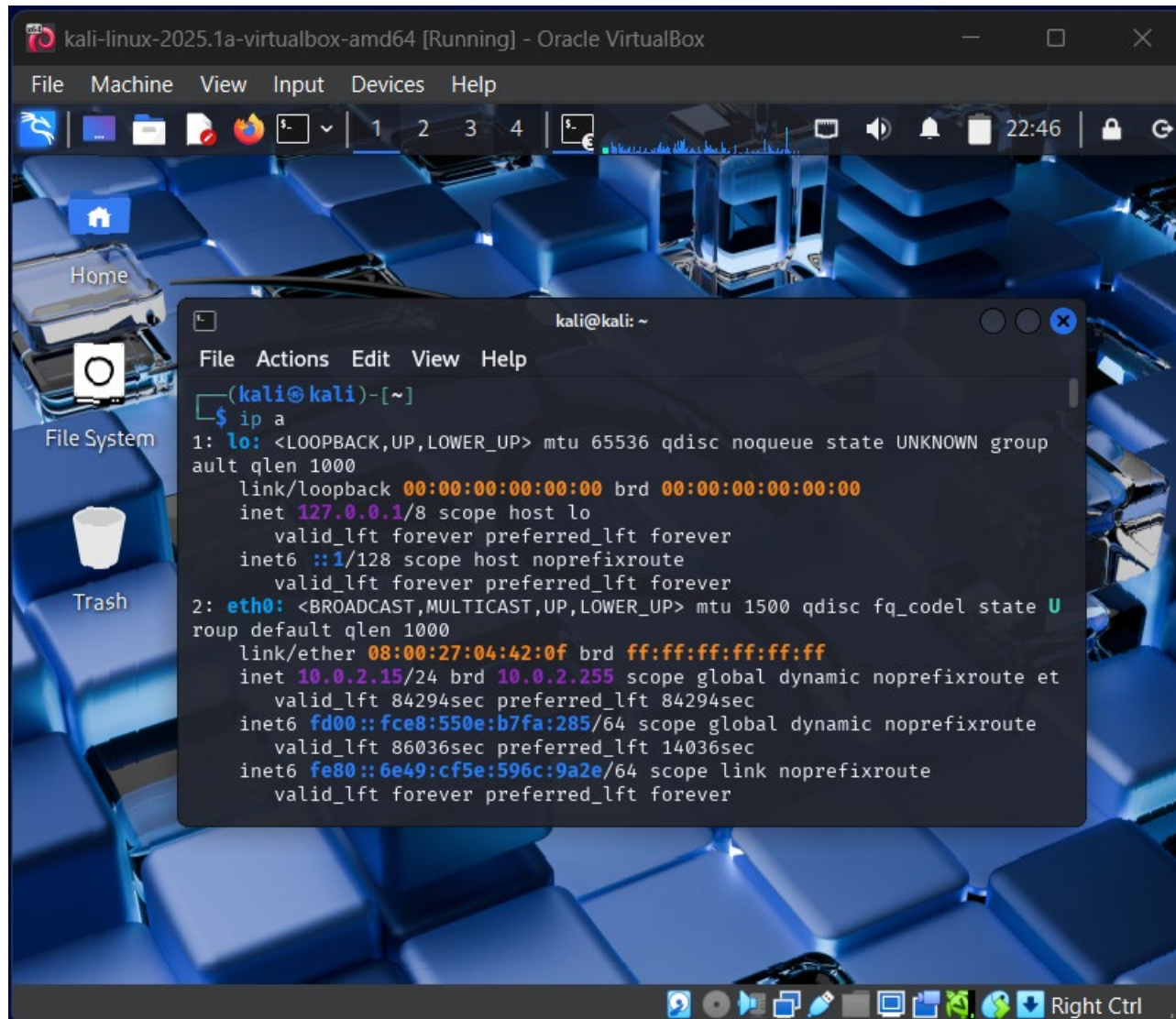








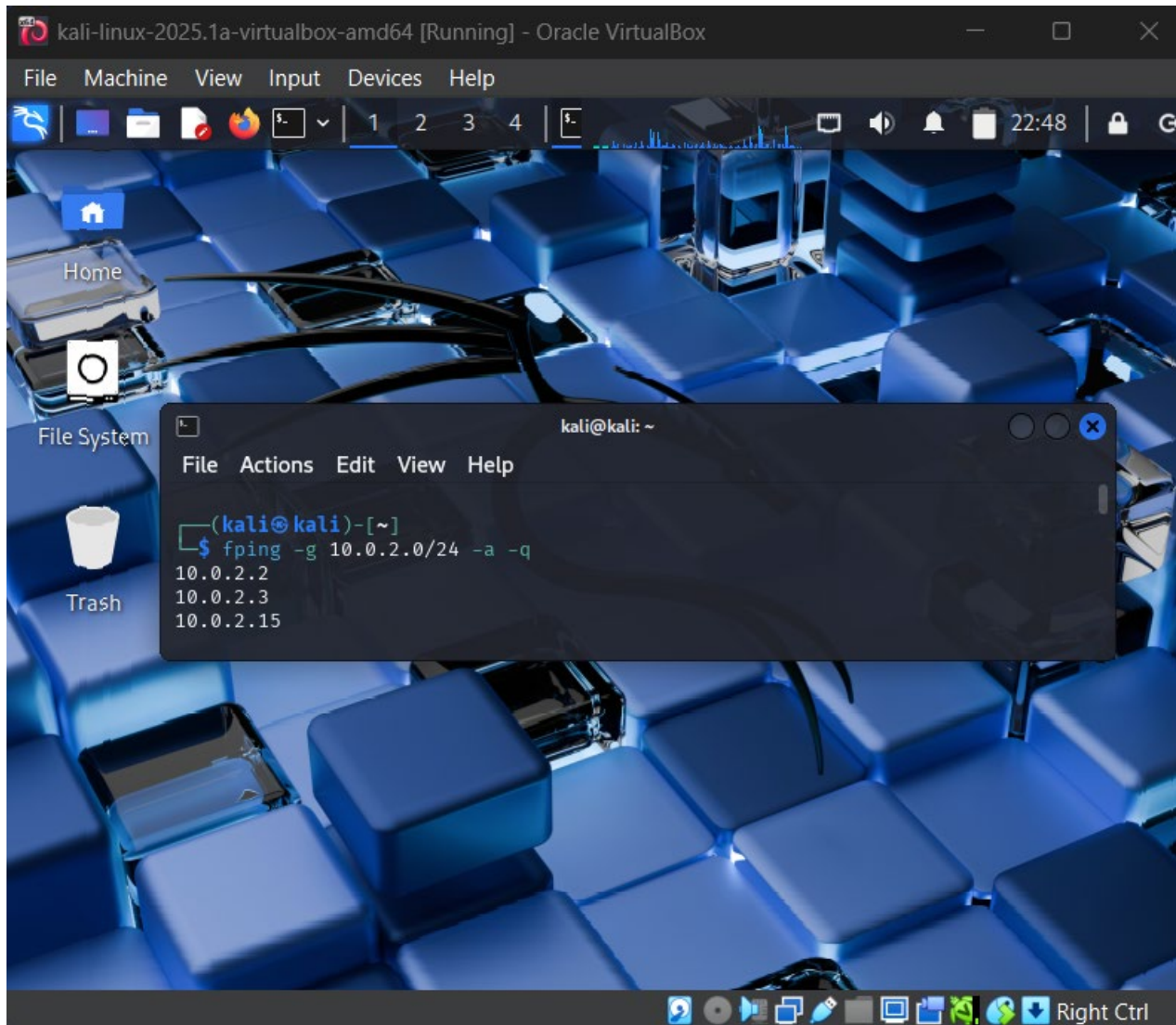
## 2. Finding the IP Address of Kali VM



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The desktop background is a blue keyboard. A terminal window is open, displaying the output of the `ip a` command. The terminal window has a title bar that reads "kali@kali: ~". The output of the command shows the configuration for the loopback interface `lo` and the ethernet interface `eth0`. The IP address for `eth0` is `10.0.2.15`.

```
kali@kali: ~  
File Actions Edit View Help  
~  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group  
    aut 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 noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state U  
    roup default qlen 1000  
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute et  
        valid_lft 84294sec preferred_lft 84294sec  
    inet6 fd00::fce8:550e:b7fa:285/64 scope global dynamic noprefixroute  
        valid_lft 86036sec preferred_lft 14036sec  
    inet6 fe80::6e49:cf5e:596c:9a2e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

### 3. Scanning the Network with fping



kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4 5

22:51

kali@kali: ~

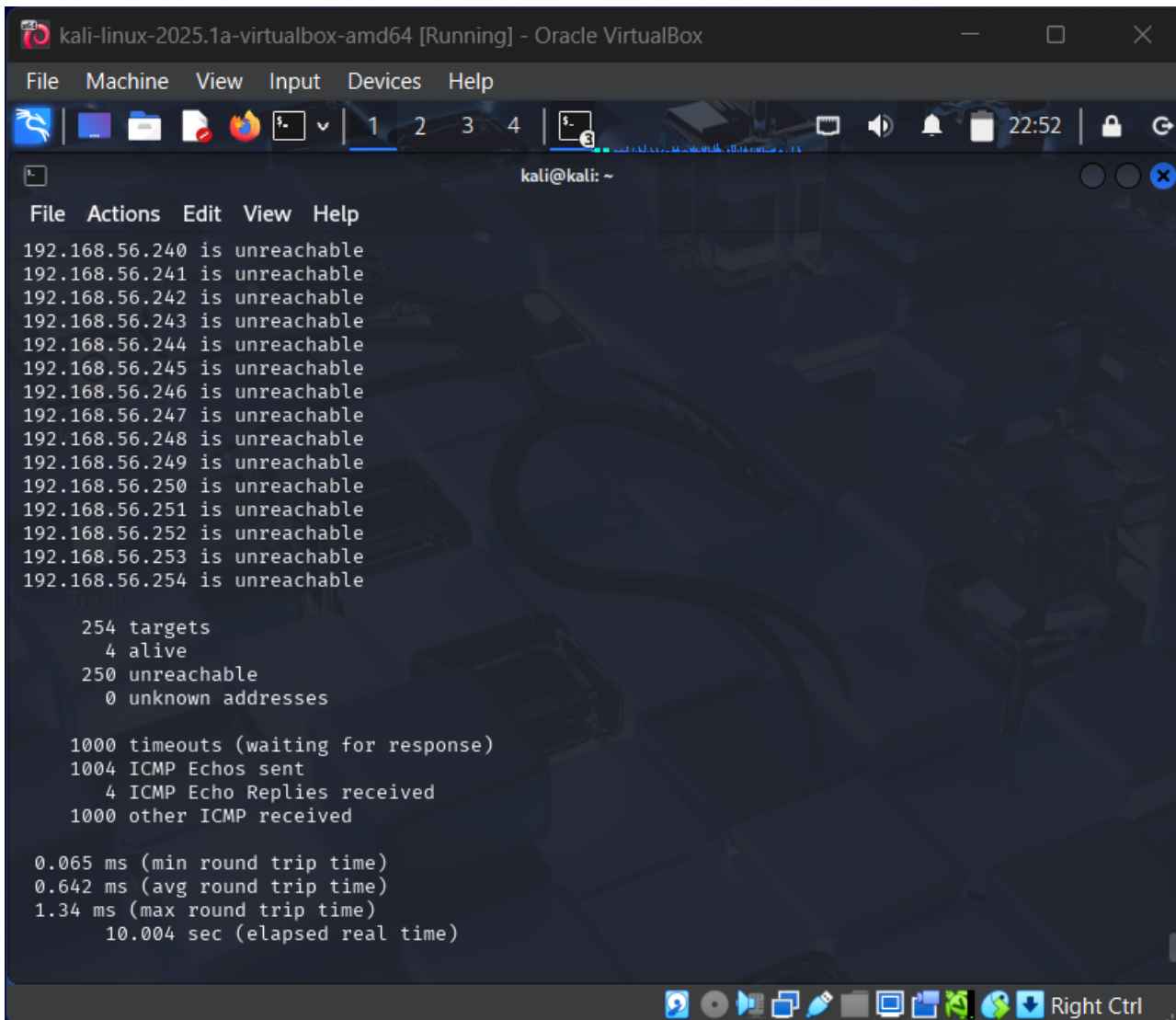
File Actions Edit View Help

0

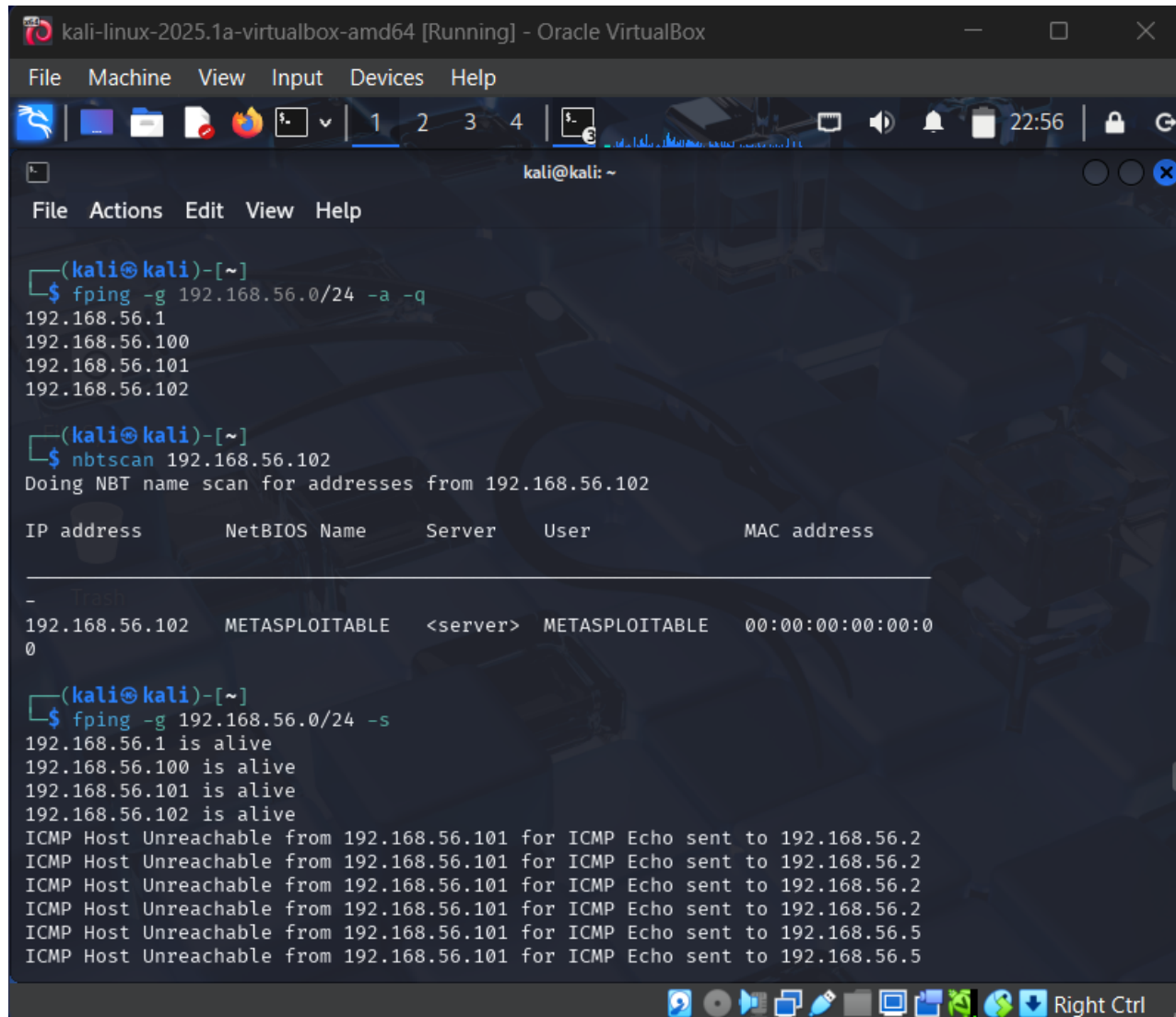
```
(kali@kali)-[~]
$ fping -g 192.168.56.0/24 -s
192.168.56.1 is alive
192.168.56.100 is alive
192.168.56.101 is alive
192.168.56.102 is alive
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.4
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.4
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.4
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.4
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.8
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.8
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.8
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.8
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.7
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.7
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.7
```

Right Ctrl





## 4. Identifying Metasploitable2 with nbtscan

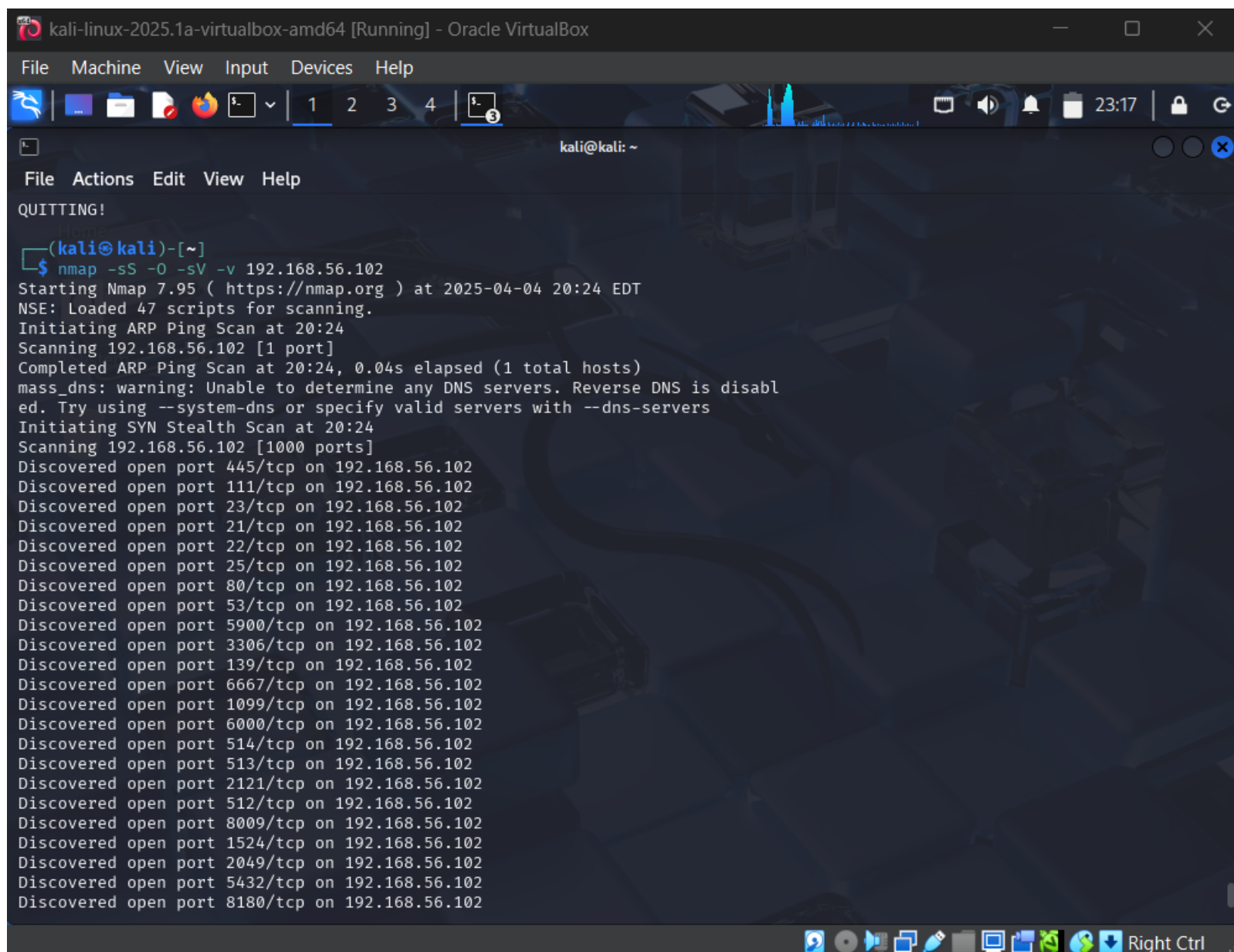


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ fping -g 192.168.56.0/24 -a -q  
192.168.56.1  
192.168.56.100  
192.168.56.101  
192.168.56.102  
  
(kali@kali)-[~]  
$ nbtscan 192.168.56.102  
Doing NBT name scan for addresses from 192.168.56.102  


| IP address     | NetBIOS Name   | Server   | User           | MAC address       |
|----------------|----------------|----------|----------------|-------------------|
| 192.168.56.102 | METASPLOITABLE | <server> | METASPLOITABLE | 00:00:00:00:00:00 |

  
(kali@kali)-[~]  
$ fping -g 192.168.56.0/24 -s  
192.168.56.1 is alive  
192.168.56.100 is alive  
192.168.56.101 is alive  
192.168.56.102 is alive  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.2  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5  
ICMP Host Unreachable from 192.168.56.101 for ICMP Echo sent to 192.168.56.5
```

## 5. Nmap Scan of Metasploitable2



The screenshot shows a Kali Linux terminal window titled "kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VirtualBox". The terminal displays the output of an Nmap scan command: `nmap -sS -O -sV -v 192.168.56.102`. The scan results show that 21 ports are open on the target IP address. The background of the terminal window features a dark, abstract graphic of a cityscape or industrial structure.

```
File Machine View Input Devices Help
File Actions Edit View Help
QUITTING!

(kali@kali)-[~]
$ nmap -sS -O -sV -v 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 20:24 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 20:24
Scanning 192.168.56.102 [1 port]
Completed ARP Ping Scan at 20:24, 0.04s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 20:24
Scanning 192.168.56.102 [1000 ports]
Discovered open port 445/tcp on 192.168.56.102
Discovered open port 111/tcp on 192.168.56.102
Discovered open port 23/tcp on 192.168.56.102
Discovered open port 21/tcp on 192.168.56.102
Discovered open port 22/tcp on 192.168.56.102
Discovered open port 25/tcp on 192.168.56.102
Discovered open port 80/tcp on 192.168.56.102
Discovered open port 53/tcp on 192.168.56.102
Discovered open port 5900/tcp on 192.168.56.102
Discovered open port 3306/tcp on 192.168.56.102
Discovered open port 139/tcp on 192.168.56.102
Discovered open port 6667/tcp on 192.168.56.102
Discovered open port 1099/tcp on 192.168.56.102
Discovered open port 6000/tcp on 192.168.56.102
Discovered open port 514/tcp on 192.168.56.102
Discovered open port 513/tcp on 192.168.56.102
Discovered open port 2121/tcp on 192.168.56.102
Discovered open port 512/tcp on 192.168.56.102
Discovered open port 8009/tcp on 192.168.56.102
Discovered open port 1524/tcp on 192.168.56.102
Discovered open port 2049/tcp on 192.168.56.102
Discovered open port 5432/tcp on 192.168.56.102
Discovered open port 8180/tcp on 192.168.56.102
```

kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

File Actions Edit View Help

```
Discovered open port 2049/tcp on 192.168.56.102
Discovered open port 5432/tcp on 192.168.56.102
Discovered open port 8180/tcp on 192.168.56.102
Completed SYN Stealth Scan at 20:24, 0.07s elapsed (1000 total ports)
Initiating Service scan at 20:24
Scanning 23 services on 192.168.56.102
Completed Service scan at 20:25, 11.08s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.102
NSE: Script scanning 192.168.56.102.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.08s elapsed
Initiating NSE at 20:25
Completed NSE at 20:25, 0.04s elapsed
Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rrexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
```

Right Ctrl

kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

File Actions Edit View Help

513/tcp	open	login	OpenBSD or Solaris rlogind
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:D8:7A:AC (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Uptime guess: 0.006 days (since Fri Apr 4 20:15:49 2025)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=207 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs  
: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds

Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)

Right Ctrl



## 6. Service Analysis and Vulnerability Research

The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VirtualBox". The interface includes a menu bar (File, Machine, View, Input, Devices, Help) and a toolbar with icons for file operations and system settings. Below the toolbar, the terminal window displays the command prompt "kali@kali: ~". The user has entered "msfconsole", which has loaded the Metasploit Framework. A large ASCII art logo for "Metasploit" is displayed. The terminal output shows the version "metasploit v6.4.50-dev" and a summary of available modules: 2495 exploits, 1283 auxiliary, 393 post, 1607 payloads, 49 encoders, 13 nops, and 9 evasion techniques. The Metasploit Documentation URL is provided. The user attempts to use the module "exploit/unix/http/apache\_mod\_cgi\_bash\_env\_exec", but it fails to load. They then set RHOSTS to "192.168.56.102" and TARGETURI to "/", and attempt to run the "exploit" command, which results in an "Unknown command" error. The bottom status bar shows various system icons and the text "Right Ctrl".

## FTP Vulnerability

- I found that the Metasploitable2 machine is running on FTP service. This version has known problem (CVE-2010-4221) that allows a hacker to run their own code on the server and take control. This means that they could get access to the system without logging in properly.
- A hacker can use a tool like **Metasploit** to run this attack. Also, FTP sends usernames and passwords without encryption, so they can be stolen using tools like **Wireshark**.
- To fix this, the server should **stop using FTP**, update to a newer version, or use **SFTP**, which is more secure.
- Reference: <https://nvd.nist.gov/vuln>