Cybersecurity Internship Program

Task-2: BUILD YOUR PERSONAL CYBERSECURITY LAB

Organization By:

Prepared By: ROHAN ASODIYA

Submission Date: January 2026

Table of Contents

1. Introduction

Cybersecurity practical learning requires a safe and isolated environment. This report documents the creation of a personal cybersecurity laboratory using virtualization technology. The lab consists of an attacker machine (**Kali Linux**) and a vulnerable web application (**DVWA / OWASP Juice Shop**). Proper network segmentation is implemented to ensure that testing remains contained and does not impact the host system or external networks.

2. Objective

The primary goal of this task is to establish a secure, isolated penetration-testing lab for practicing:

- **Vulnerability Assessment:** Identifying weaknesses in systems.
- **Web Application Testing:** Exploiting flaws in web services.
- **Network Scanning:** Discovering active hosts and open ports.
- **Security Tool Proficiency:** Mastering industry-standard tools.

3. Lab Architecture Overview

The lab is designed using a multi-adapter approach to balance connectivity and security.

- **Attacker Machine:** Kali Linux (Debian-based penetration testing suite).
- **Target Machine:** DVWA or OWASP Juice Shop (Deliberately insecure applications).
- **Network Logic:** The Attacker communicates with the Target via a **Host-Only Network**, while the Attacker maintains an external **NAT** connection for repository updates.

4. Prerequisites

Requirement	Recommendation
RAM	**Minimum 8GB (16GB preferred)**
Disk Space	**40–60 GB**
CPU	**Virtualization (VT-x/AMD-V) Enabled**
Host OS	**Windows / Linux / Mac**

5. Tools & Technologies Used

- **Hypervisor:** Oracle VM VirtualBox
- **Operating Systems:** Kali Linux VM
- **Vulnerable Labs:** DVWA
- **Security Tools:** Nmap, Burp Suite, Wireshark

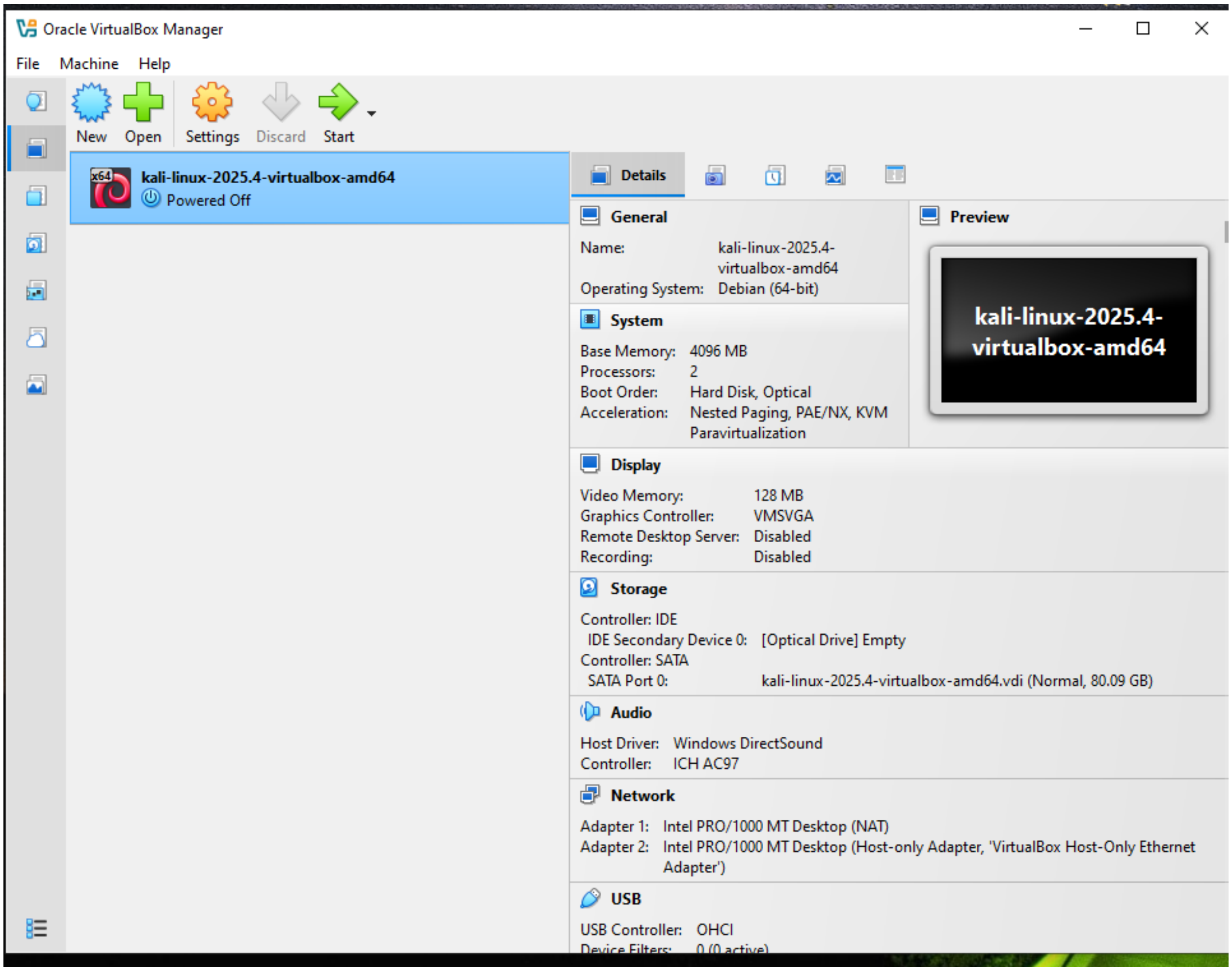
6. Network Configuration

Two network adapters were configured for the Kali Linux environment:

1. **Adapter 1 – NAT:** Provides internet connectivity for downloading tools and security updates.
2. **Adapter 2 – Host-Only:** Creates a private "sandbox" network. This ensures that any exploits or scans are restricted to the virtual environment and cannot reach the local home network.

7. Step-by-Step Implementation

- **Step 1: VirtualBox Installation** – Installed the hypervisor and configured the "VirtualBox Host-Only Ethernet Adapter."



kali-linux-2025.4-virtualbox-amd64
Powered Off

General

Name: kali-linux-2025.4-virtualbox-amd64
Operating System: Debian (64-bit)

System

Base Memory: 4096 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-2025.4-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

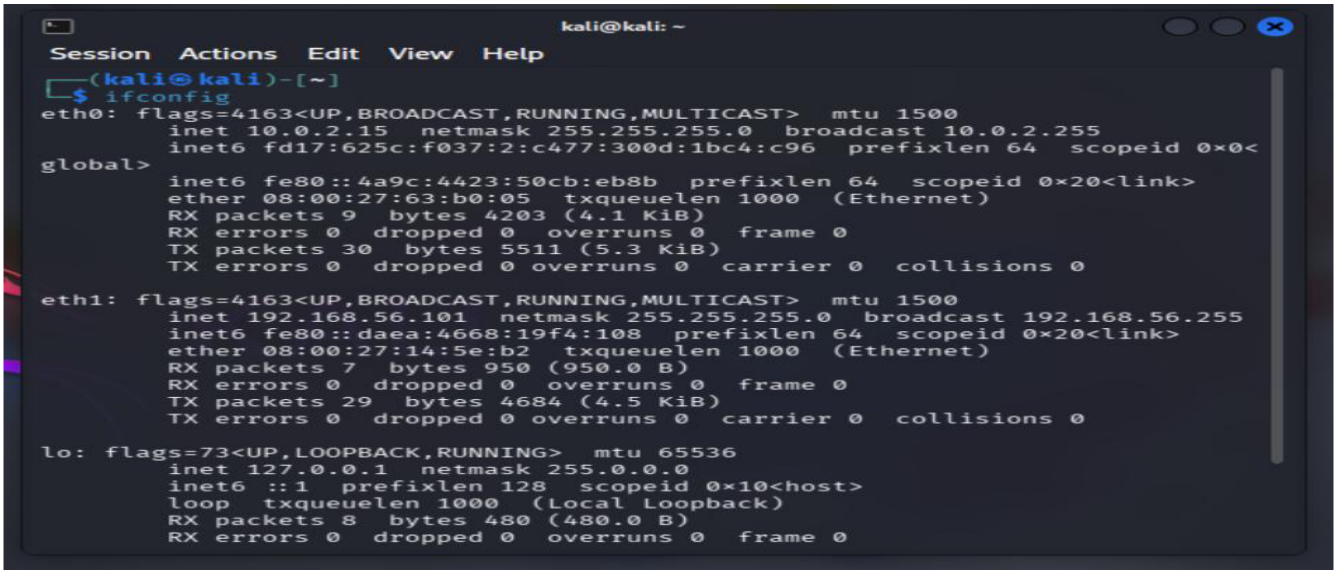
USB

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

- **Step 2: Kali Linux Deployment** – Imported the Kali Linux `.ova` file, assigned 2 CPU cores and 4GB RAM, and attached both network adapters.

- **Step 3: Vulnerable Application Setup** – Deployed the target environment (DVWA) via a standalone VM .

- **Step 4: IP Verification** – Used `ifconfig`(or `ip a`) on both machines to ensure they were on the same Host-Only subnet.

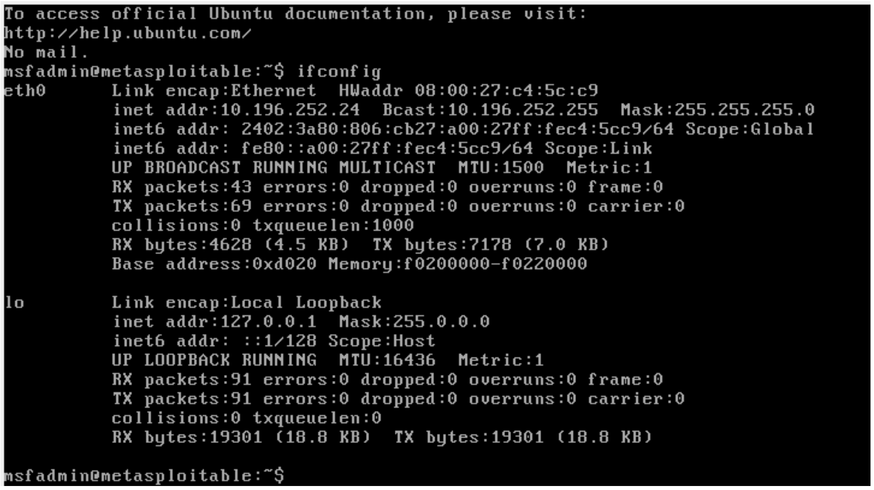


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:c477:300d:1bc4:c96  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::4a9c:4423:50cb:eb8b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 4203 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 5511 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::daea:4668:19f4:108  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:14:5e:b2  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 950 (950.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 4684 (4.5 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

8. Validation & Testing

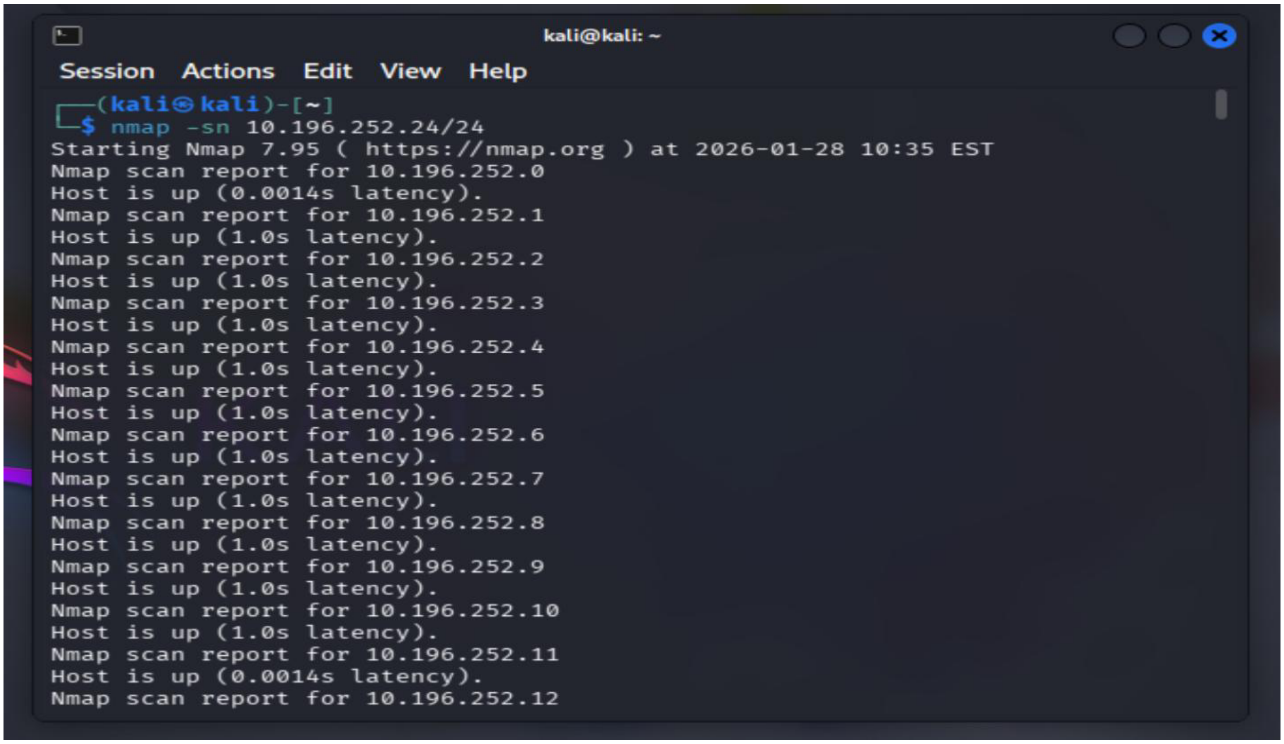
To confirm the lab was operational, the following tests were conducted:

- **Connectivity:** Pinged the target machine from Kali Linux.

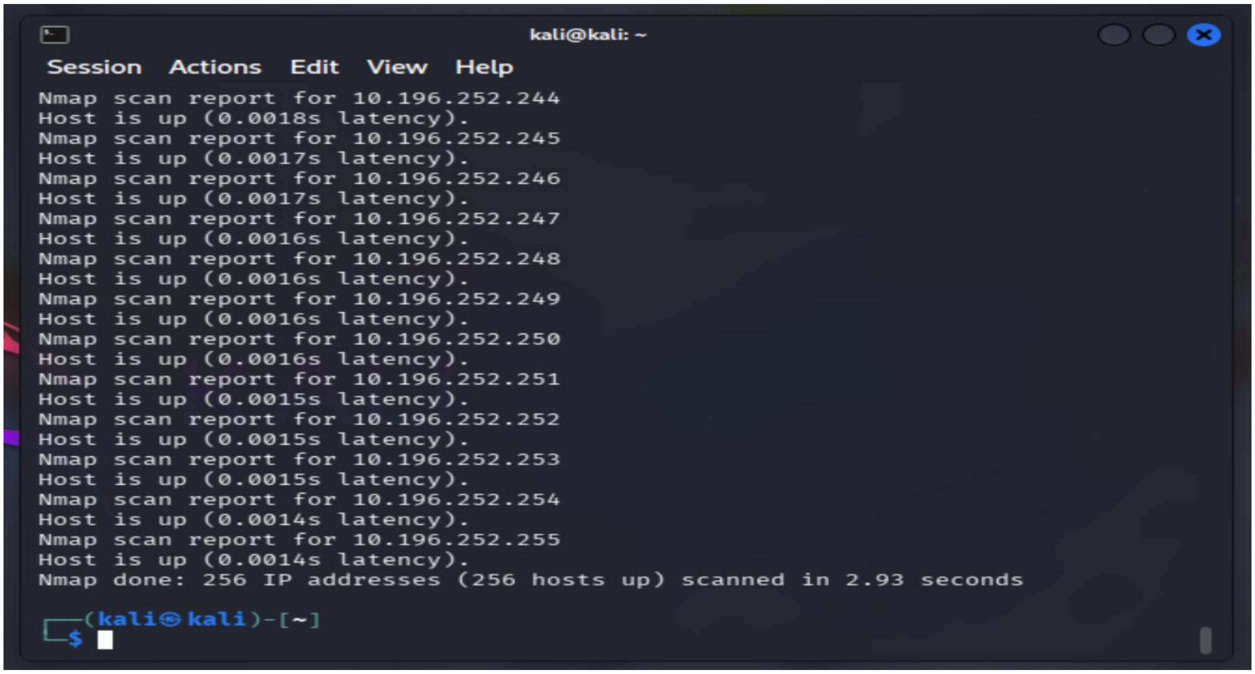


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c4:5c:c9
          inet addr:10.196.252.24  Bcast:10.196.252.255  Mask:255.255.255.0
          inet6 addr: 2402:3a80:806:cb27:a00:27ff:fec4:5cc9/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fec4:5cc9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4628 (4.5 KB)  TX bytes:7178 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

- **Reconnaissance:** Performed a basic `nmap` scan against the target IP.

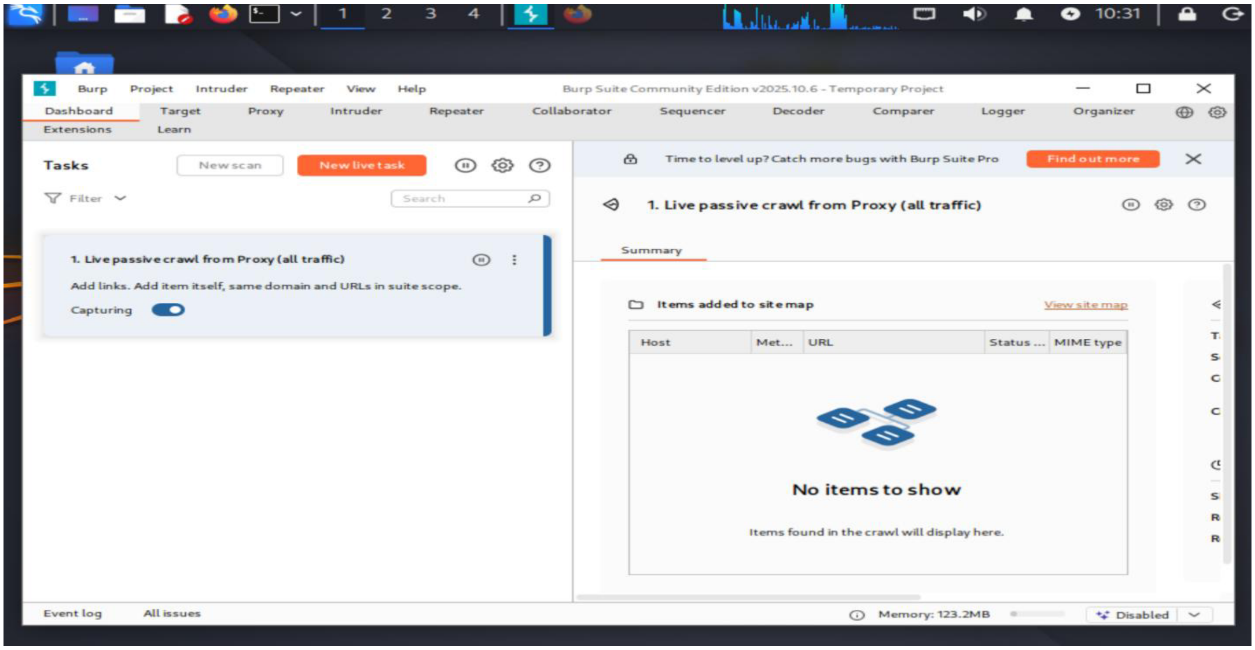


```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.196.252.24/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-28 10:35 EST
Nmap scan report for 10.196.252.0
Host is up (0.0014s latency).
Nmap scan report for 10.196.252.1
Host is up (1.0s latency).
Nmap scan report for 10.196.252.2
Host is up (1.0s latency).
Nmap scan report for 10.196.252.3
Host is up (1.0s latency).
Nmap scan report for 10.196.252.4
Host is up (1.0s latency).
Nmap scan report for 10.196.252.5
Host is up (1.0s latency).
Nmap scan report for 10.196.252.6
Host is up (1.0s latency).
Nmap scan report for 10.196.252.7
Host is up (1.0s latency).
Nmap scan report for 10.196.252.8
Host is up (1.0s latency).
Nmap scan report for 10.196.252.9
Host is up (1.0s latency).
Nmap scan report for 10.196.252.10
Host is up (1.0s latency).
Nmap scan report for 10.196.252.11
Host is up (0.0014s latency).
Nmap scan report for 10.196.252.12
```



```
Nmap scan report for 10.196.252.244
Host is up (0.0018s latency).
Nmap scan report for 10.196.252.245
Host is up (0.0017s latency).
Nmap scan report for 10.196.252.246
Host is up (0.0017s latency).
Nmap scan report for 10.196.252.247
Host is up (0.0016s latency).
Nmap scan report for 10.196.252.248
Host is up (0.0016s latency).
Nmap scan report for 10.196.252.249
Host is up (0.0016s latency).
Nmap scan report for 10.196.252.250
Host is up (0.0016s latency).
Nmap scan report for 10.196.252.251
Host is up (0.0015s latency).
Nmap scan report for 10.196.252.252
Host is up (0.0015s latency).
Nmap scan report for 10.196.252.253
Host is up (0.0015s latency).
Nmap scan report for 10.196.252.254
Host is up (0.0014s latency).
Nmap scan report for 10.196.252.255
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 2.93 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- **Interception:** Configured **Burp Suite** to capture traffic from the vulnerable web app.


1 2 3 4
10:31
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Extensions Learn
Tasks
New scan
New live task
Filter
Search
Find out more
Summary
View site map
Event log
All issues
Disabled

Time to level up? Catch more bugs with Burp Suite Pro

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

1. Live passive crawl from Proxy (all traffic)

Items added to site map

Host	Met...	URL	Status ...	MIME type

No items to show

Items found in the crawl will display here.

Memory: 123.2MB

- **Analysis:** Used **Wireshark** to monitor packet flow between the two machines.

9. Learning Outcomes

- Mastered **Virtual Machine** deployment and resource allocation.
- Understood the critical difference between **NAT and Host-Only** networking.
- Learned how to deploy and manage **vulnerable testing environments**.
- Gained hands-on experience in **basic reconnaissance** and environment hardening.
-

10. Conclusion

This task successfully established a functional and safe personal cybersecurity lab. The setup provides a robust platform for ethical hacking practice without risks to production systems. This environment serves as the foundation for all future penetration testing tasks in this internship.

11. References

- VirtualBox Official Documentation
- Kali Linux Documentation
- OWASP Juice Shop Project
- Damn Vulnerable Web Application (DVWA)