CYBERSECURITY LAB REPORT
Task 2 – Build Your Own Personal Lab

Author – Akanksha Mane
Date – 15/12/2025

1. INTRODUCTION

With the rapid increase in cyber threats, hands-on practical knowledge has become a critical requirement for anyone pursuing a career in cybersecurity. This report documents the successful design, implementation, and validation of a personal cybersecurity practice lab built in a safe and isolated environment. The lab is designed to support future learning in areas such as vulnerability assessment, web application penetration testing, exploitation practice, and basic incident response.

The lab environment consists of an attacker machine (Kali Linux) and a deliberately vulnerable target application (DVWA / OWASP Juice Shop) deployed using virtualization technology. Proper network segmentation using NAT and Host-Only adapters ensures complete isolation from the host system and the external internet, preventing any accidental real-world impact.

This report explains the architecture, tools used, step-by-step setup process, validation methods, challenges faced, and learning outcomes achieved during the task.

---

2. OBJECTIVE OF THE TASK

The primary objectives of this task are:

- To create a secure and isolated cybersecurity lab on a personal computer
- To understand and apply virtualization concepts using VMware
- To deploy an attacker system (Kali Linux) with proper resource allocation
- To deploy an intentionally vulnerable web application for testing purposes
- To implement network segmentation using NAT and Host-Only networking
- To validate connectivity and tools readiness using industry-standard security tools

Achieving these objectives provides a strong foundation for advanced cybersecurity tasks in the future.

---

3. SCOPE OF THE LAB ENVIRONMENT

The scope of this lab includes:

- Virtual machine setup and configuration
- Basic networking concepts (NAT vs Host-Only)
- Safe attack target communication within an isolated subnet
- Initial exposure to common security testing tools such as:
  - ❖ Nmap
  - ❖ Burp Suite
  - ❖ Wireshark

Out of scope, items include real-world exploitation, denial-of-service attacks, or testing against external systems.

---

4. SYSTEM REQUIREMENTS & PREREQUISITES

4.1. Hardware Requirements

- RAM – Minimum 2 GB (4GB preferred)
- Disk Space – 40 to 60 GB free
- CPU – Virtualization enabled

4.2. Software Requirements

- VMware – Virtualization platform
- Kali Linux VM – Attacker machine
- DVWA – Vulnerable target application

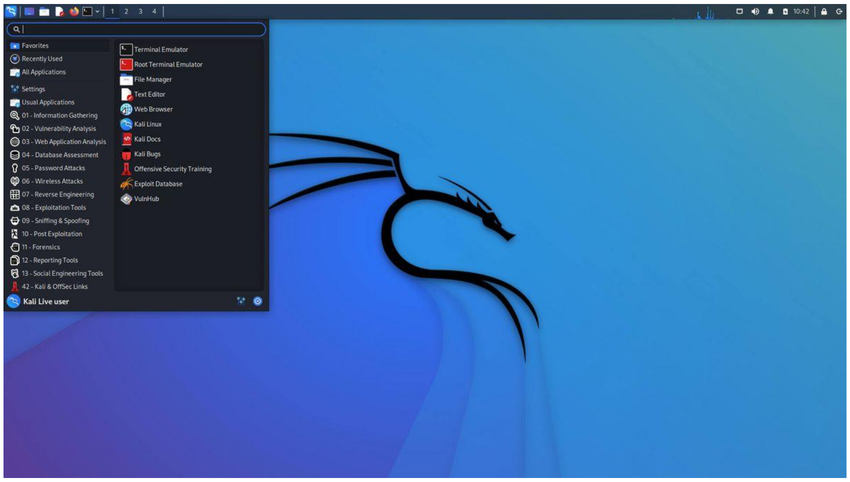
All software was obtained from official sources to ensure integrity and security

---

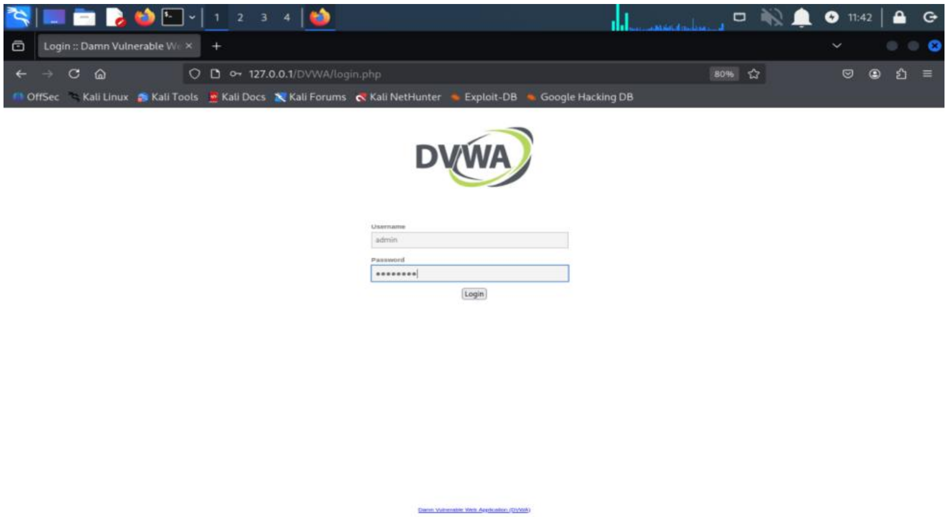
5. LAB ARCHITECTURE & DESIGN

5.1. Architecture Overview

1. Kali Linux (Attacker)



2. Vulnerable Web Application (Target)
   Both machines are hosted on the same physical system using virtualization



127.0.0.1/DVWA/login.php

Username
admin

Password
••••••••

5.2. Network Segmentation Design

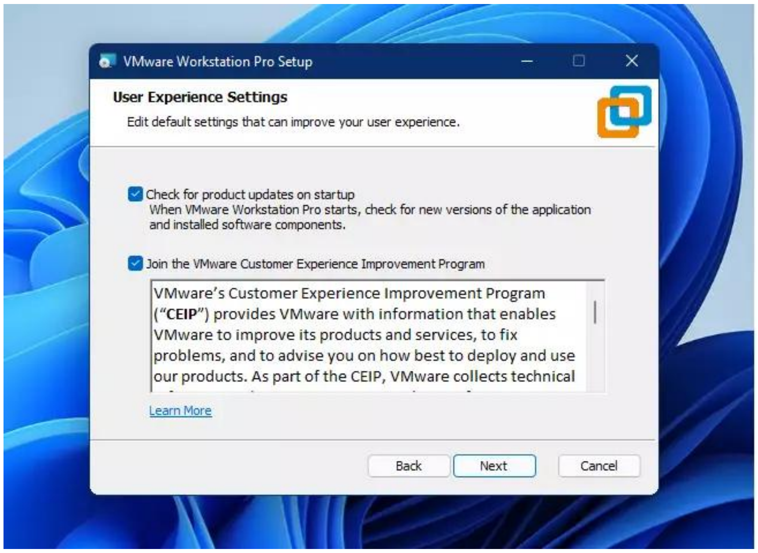
Two network adapters are used:

- ❖ NAT Adapter
  - Provides limited internet access for updates
  - Prevents inbound access from external networks
- ❖ Host-Only Adapter
  - Enables communication only between VMs and the host
  - Used for attack simulations and testing

This dual adapter setup ensures security, isolation and functionality

6. STEP-BY-STEP IMPLEMENTATION

6.1. Installation for Virtualization Software



User Experience Settings

Edit default settings that can improve your user experience.

☑ Check for product updates on startup
When VMware Workstation Pro starts, check for new versions of the application and installed software components.

☑ Join the VMware Customer Experience Improvement Program

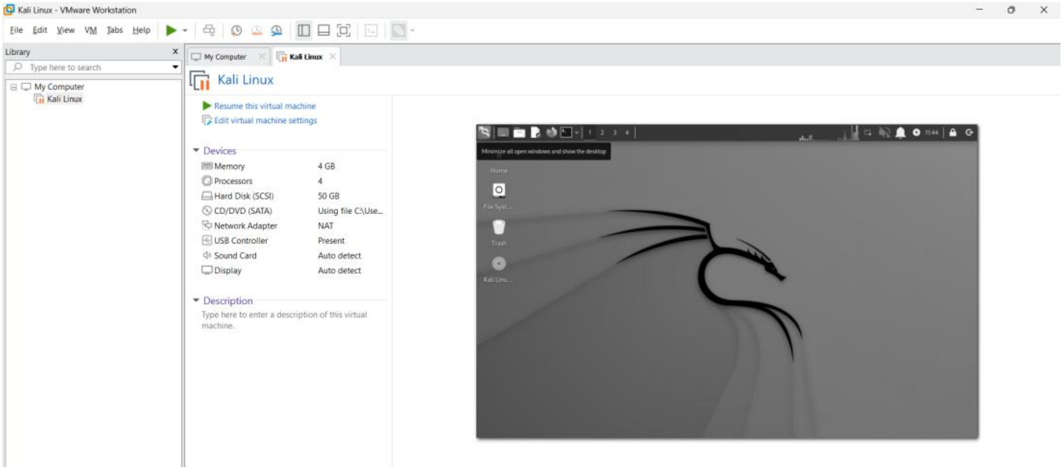
VMware's Customer Experience Improvement Program ("**CEIP**") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical

VMware was installed on the host system. During setup:

- Host-only network was created
- Default NAT configuration was enabled
- Virtualization support was verified in BIOS

This step enabled the host system to run multiple isolated operating systems simultaneously.

6.2. Deployment of Kali Linux (Attacker Machine)


Kali Linux - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
Kali Linux
My Computer
Kali Linux
Kali Linux
Resume this virtual machine
Edit virtual machine settings
Devices

Memory	4 GB
Processors	4
Hard Disk (SCSI)	50 GB
CD/DVD (SATA)	Using file C:\Use...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description
Type here to enter a description of this virtual machine.

Kali Linux was deployed using a prebuilt virtual machine image.

Configuration Details:

- CPUs: 2
- RAM: 4 GB
- Storage: Preallocated virtual disk

Network Configuration:

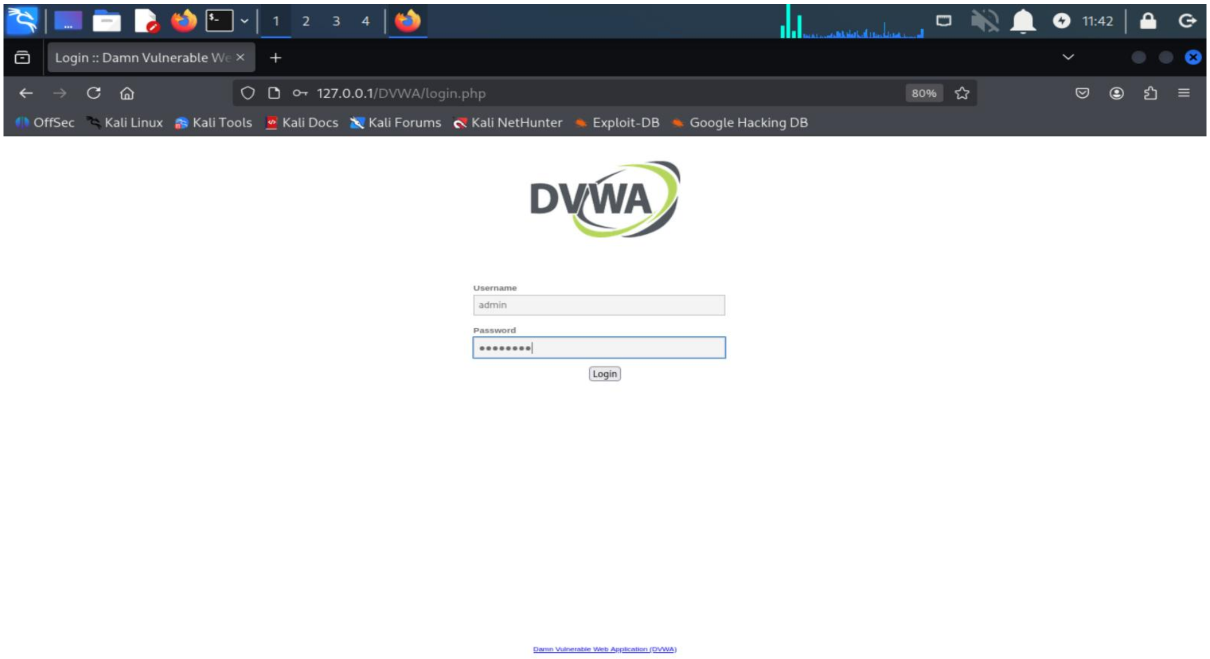
- Adapter 1: NAT
- Adapter 2: Host-Only

After Booting:

- Default credentials were changed
- Network interfaces were verified
- System updates were applied

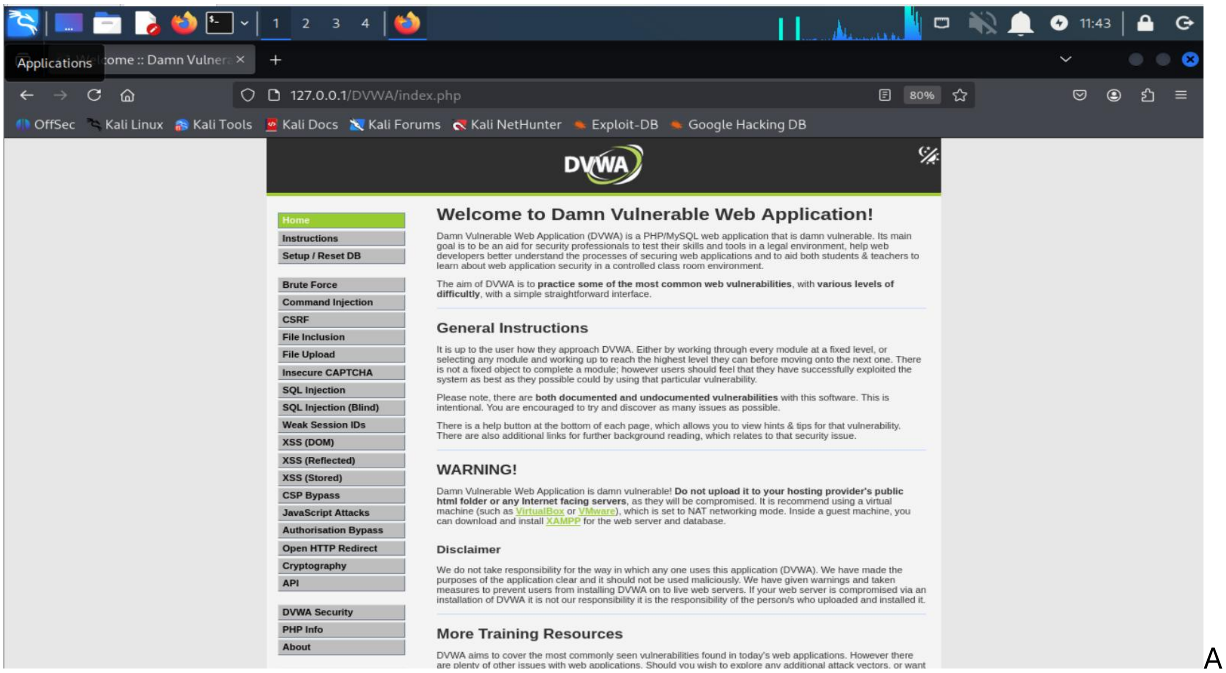
Kali Linux provides a comprehensive suite of penetration testing tools required for the lab.

6.3. Deployment of Deployment of Vulnerable Target Application



Username
admin

Password
••••••••



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want

A

Two options were considered:

- Damn Vulnerable Web Application (DVWA)
- OWASP Juice Shop

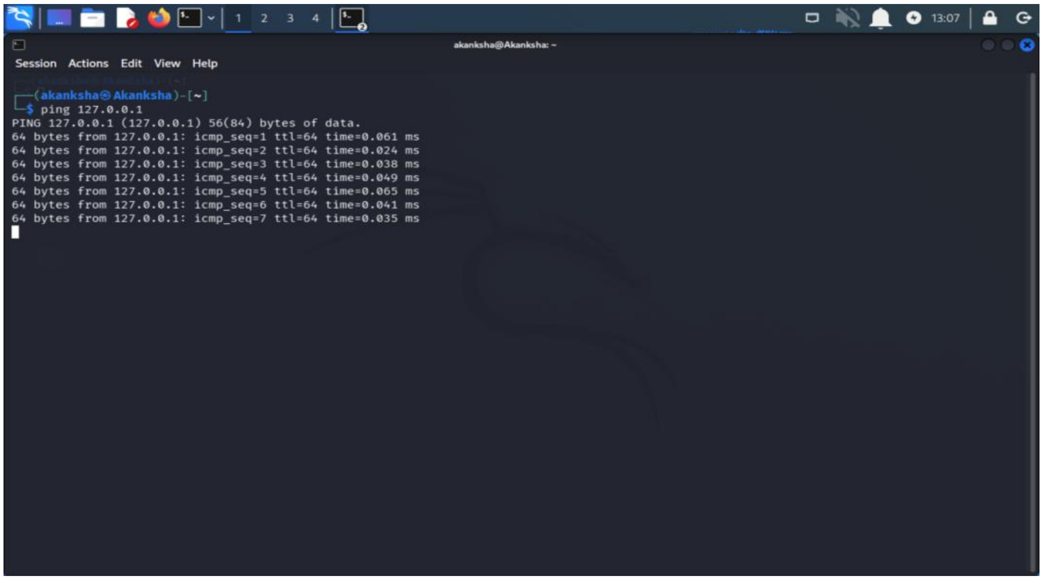
For this lab, the vulnerable application was deployed locally using LAMP stack (for DVWA)
Key Feature of the Target:

- Intentionally insecure configurations
- Contains common vulnerabilities such as:
  - ❖ SQL Injection
  - ❖ Cross-Side Scripting (XSS)
  - ❖ Broken Authentication

This application was assigned a Host-Only IP address to allow controlled access from Kali Linux

7. NETWORK CONFIGURATION & VALIDATION

7.1. Connectivity Testing



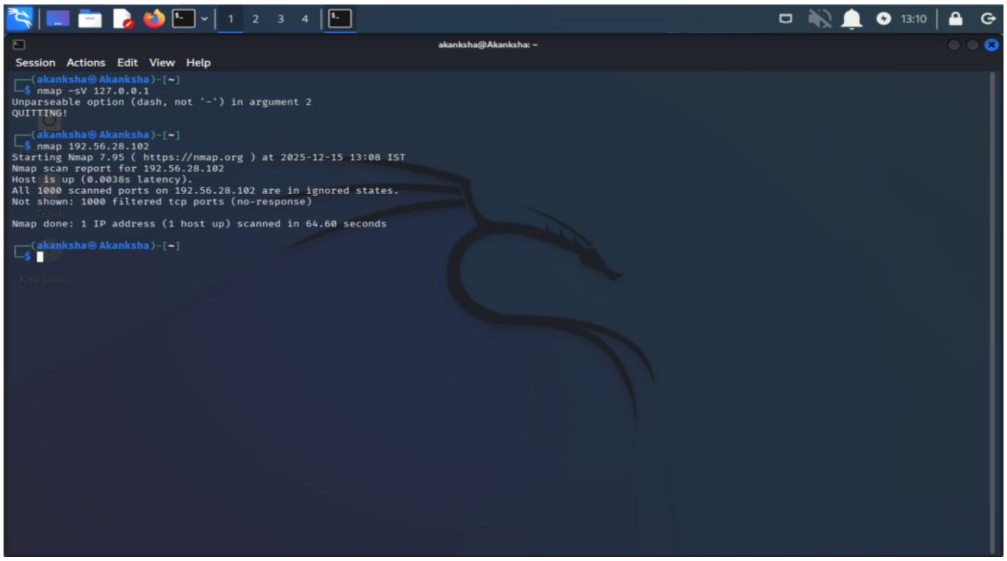
```
┌──(akanksha㉿Akanksha)-[~]
└─$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.035 ms
```

Basic connectivity was tested using:

- ping 127.0.0.1

Successful responses confirmed proper network configuration

7.2. Nmap Scanning



```
┌──(akanksha㉿Akanksha)-[~]
└─$ nmap –sV 127.0.0.1
Unparseable option (dash, not '-') in argument 2
QUITTING!

┌──(akanksha㉿Akanksha)-[~]
└─$ nmap 192.56.28.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 13:08 IST
Nmap scan report for 192.56.28.102
Host is up (0.0038s latency).
All 1000 scanned ports on 192.56.28.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 64.60 seconds

┌──(akanksha㉿Akanksha)-[~]
└─$ 
```

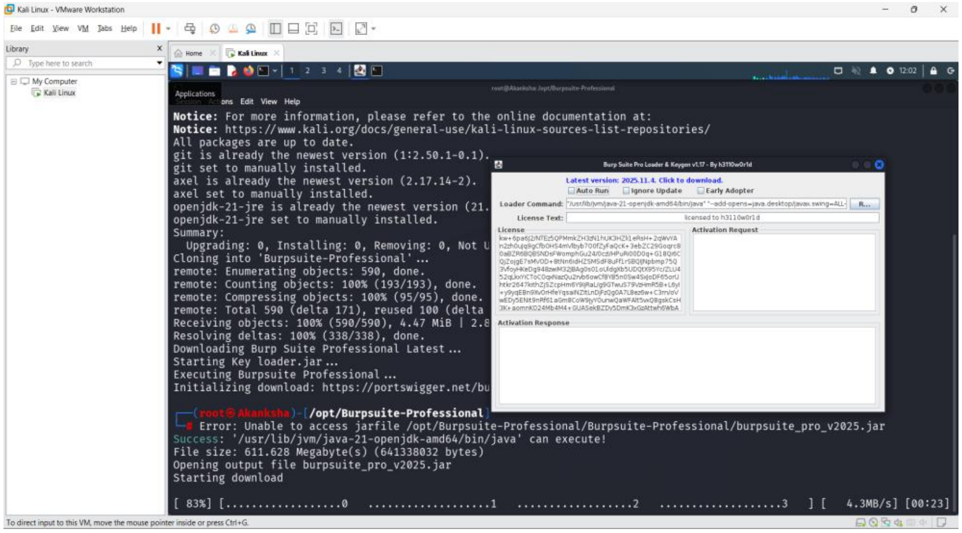
Nmap used to identify open ports and running services on the target machine. Example scan:

- nmap –sV 127.0.0.1

This validated that the vulnerable web service was accessible and detectable from the attacker machine

8. TOOL VALIDATION & USAGE

8.1. Burp Site


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux
Home
Kali Linux
1 2 3 4
12:02
Applications
Session Actions Edit View Help
root@Akanksha: /opt/Burpsuite-Professional
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Notice: For more information, please refer to the online documentation at:
Notice: https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
All packages are up to date.
git is already the newest version (1:2.50.1-0.1).
git set to manually installed.
axel is already the newest version (2.17.14-2).
axel set to manually installed.
openjdk-21-jre is already the newest version (21.
openjdk-21-jre set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not U
Cloning into 'Burpsuite-Professional'...
remote: Enumerating objects: 590, done.
remote: Counting objects: 100% (193/193), done.
remote: Compressing objects: 100% (95/95), done.
remote: Total 590 (delta 171), reused 100 (delta
Receiving objects: 100% (590/590), 4.47 MiB | 2.8
Resolving deltas: 100% (338/338), done.
Downloading Burp Suite Professional Latest...
Starting Key loader.jar...
Executing Burpsuite Professional...
Initializing download: https://portswigger.net/bu

┌──(root㉿Akanksha)-[/opt/Burpsuite-Professional]
└─# Error: Unable to access jarfile /opt/Burpsuite-Professional/Burpsuite-Professional/burpsuite_pro_v2025.jar
Success: '/usr/lib/jvm/java-21-openjdk-amd64/bin/java' can execute!
File size: 611.628 Megabyte(s) (641338032 bytes)
Opening output file burpsuite_pro_v2025.jar
Starting download

[ 83%] [...................0  ...................1  ...................2  ...................3  ] [  4.3MB/s] [00:23]
```

Burp Suite Pro Loader & Keygen v1.17 - By h3110w0r1d

Latest version: 2025.11.4. Click to download.

☐ Auto Run ☐ Ignore Update ☐ Early Adopter

Loader Command: "/usr/lib/jvm/java-21-openjdk-amd64/bin/java" "--add-opens=java.desktop/javax.swing=ALL-

License Text: licensed to h3110w0r1d

License

```
kw+6pa6j2/NTEz5QPMmkZH3zN1hUK3HZk1eRsH+2qWvYA
n2zh0ujq9gCfb0HS4mVlbyb7O0fZyFaQcK+3ebZC29Gogrc8
0aBZR6BQBSNDsFWomphGu24/0czl/HPuRi00D0q+G18Qi6C
QjZojgE7sMVOD+8tNn6idHZSMSdF8uFf1rSBQtNpbmp75Q
3VfoyHKeDg948zwM32jBAg0s01oUldgXb5UDQtX95Yc/ZLU4
52qLkxYiCToC0qxNazQu2rvb6owCf8YB5n0Sw4SxjoDF65orU
htkr2647kthZjSZcpHm6Y9ljRaL/g9GTwuS79VzHmR5B+L6yl
+y9yqEBn9XvOrHfeYqsaiNZItLnDjFzQg0A7L8ez6w+C3m/oV
wEDy5ENt9nRf61aGm8CoW9jyY0urwQaWFAlt5vxQ8gskCsH
3K+aomnK024Mb4M4+GUASekBZDy5DmK3xGzAttwh6WbA
```

Activation Request

Activation Response

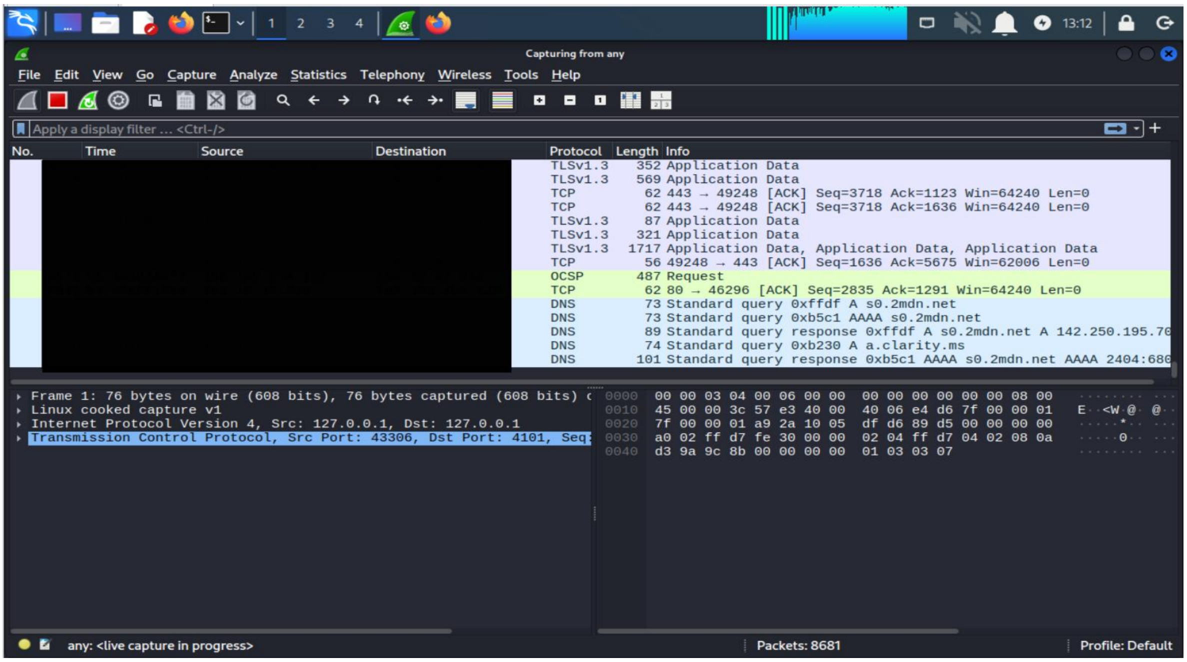
Burp Suite was configured as a proxy in the browser

Functions validated:

- Intercepting HTTP requests
- Viewing parameters and headers
- Analyzing application behavior

This confirmed readiness for web application testing

8.2. Wireshark


1 2 3 4
13:12
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time   Source   Destination   Protocol  Length Info
[redacted]
                                    TLSv1.3    352 Application Data
                                    TLSv1.3    569 Application Data
                                    TCP         62 443 → 49248 [ACK] Seq=3718 Ack=1123 Win=64240 Len=0
                                    TCP         62 443 → 49248 [ACK] Seq=3718 Ack=1636 Win=64240 Len=0
                                    TLSv1.3     87 Application Data
                                    TLSv1.3    321 Application Data
                                    TLSv1.3   1717 Application Data, Application Data, Application Data
                                    TCP         56 49248 → 443 [ACK] Seq=1636 Ack=5675 Win=62006 Len=0
                                    OCSP       487 Request
                                    TCP         62 80 → 46296 [ACK] Seq=2835 Ack=1291 Win=64240 Len=0
                                    DNS         73 Standard query 0xffdf A s0.2mdn.net
                                    DNS         73 Standard query 0xb5c1 AAAA s0.2mdn.net
                                    DNS         89 Standard query response 0xffdf A s0.2mdn.net A 142.250.195.70
                                    DNS         74 Standard query 0xb230 A a.clarity.ms
                                    DNS        101 Standard query response 0xb5c1 AAAA s0.2mdn.net AAAA 2404:680
```

```
› Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) c
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 43306, Dst Port: 4101, Seq:
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ···
0010  45 00 00 3c 57 e3 40 00  40 06 e4 d6 7f 00 00 01   E··<W·@· @···
0020  7f 00 00 01 a9 2a 10 05  df d6 89 d5 00 00 00 00   ·····*·· ····
0030  a0 02 ff d7 fe 30 00 00  02 04 ff d7 04 02 08 0a   ·····0·· ····
0040  d3 9a 9c 8b 00 00 00 00  01 03 03 07               ········ ····
```

any: <live capture in progress> Packets: 8681 Profile: Default

Wireshark was used to monitor Host-Only network traffic

Key Observations:

- Captured HTTP packets
- Identified source and destination IPs
- Verified isolation from external traffic

This reinforced understanding of network-level visibility

9. CHALLENGES FACED

Several precautions were taken:

- No bridged networking was used
- Target applications were never exposed to the internet
- Attacks were limited strictly within the lab

These measures ensured ethical and legal compliance

10. LEARNING OUTCOMES

Though this task, the following skills were developed:

- Understanding virtualization and VM management
- Configuring isolated lab networks
- Deploying vulnerable applications safely
- Using reconnaissance and interception tools
- Buildings a strong foundation for penetration testing

11. CONCLUSION

The successful completion of this task demonstrates the ability to design and implement a secure, isolated cybersecurity lab environment. This lab provides a practical foundation for advanced cybersecurity learning and experimentation while maintaining ethical and safety standards. The environment is scalable, reusable, and suitable for long-term skill development.

12. REFERENCES

- VirtualBox Documentation
- Kali Linux Official Documentation
- OWASP Juice Shop Project

- DVWA Project
- Burp Suite Documentation
- Wireshark Documentation