Penetration Testing Project (Part 1): Lab Setup, Reconnaissance, and Enumeration

Prepared by: Saboor Ali
Date: May 4, 2025

Overview

To simulate a real-world penetration testing environment by setting up a local lab, conducting network and service discovery, and performing vulnerability assessments using open-source tools.

Phase 1: Lab Environment Setup & Fundamentals

Objective: Set up a safe lab environment and get familiar with Kali Linux and essential commands.

- **Tools Used**: Kali Linux, VMware Workstation, Metasploitable 2, OWASP BWA
- **Key Concepts**:
    - Virtualization
    - Linux terminal basics
    - Networking setup (bridged adapters, static IPs)

---

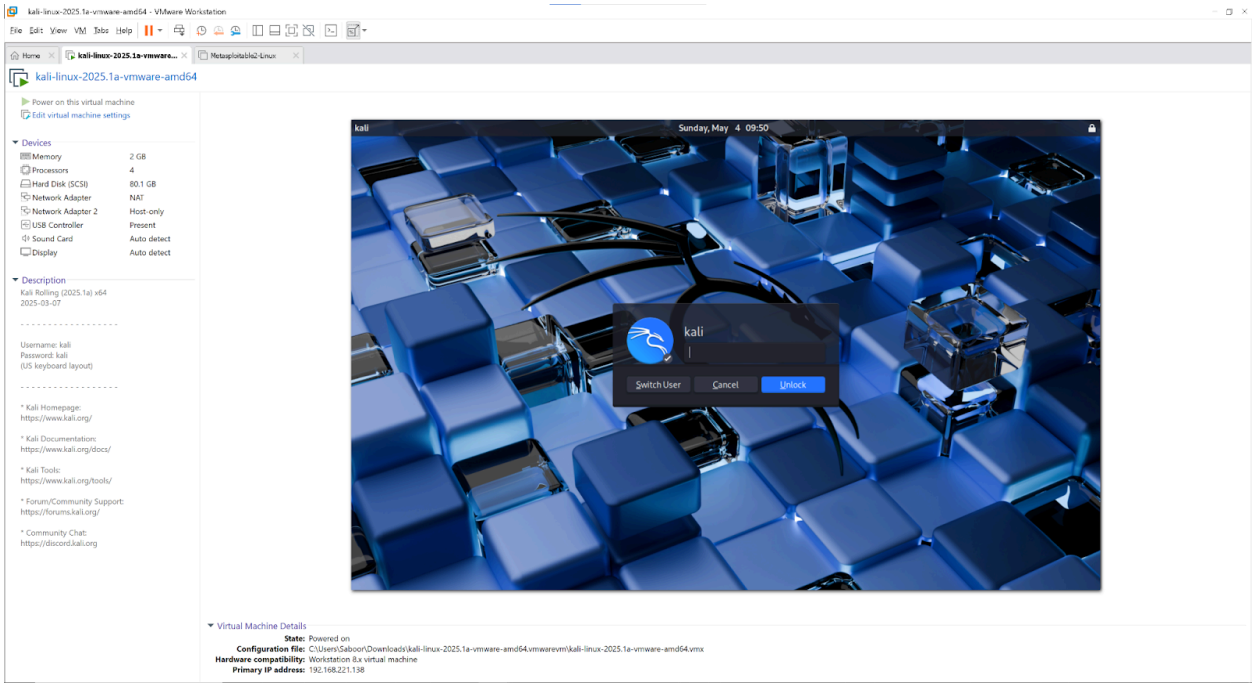
1. Setting up Kali Linux (Prebuilt Image)

- **VM Used**: Kali Linux prebuilt VM (kali-linux-2025.1a-vmware-amd64)

  https://cdimage.kali.org/kali-2025.1c/kali-linux-2025.1c-vmware-amd64.7z
- **Virtualization Platform**: VMware Workstation / VMware Player
- **VM Configuration**:
    - RAM: 8GB
    - CPU: 2 Cores
    - Storage: 80GB
    - Network Adapter: NAT:
    - Network Adapter 2: Host-only

Steps Followed:

1. Downloaded the Kali Linux VMware image from the official Kali Linux website.
2. Unzip the .7z file and open VM into VMware using the `.vmx` file.
3. Adjusted the system configuration (RAM, CPU, and storage) based on the available system resources.
4. Launched the VM and verified that it booted successfully into Kali Linux.



---

2. System Updates

Ran the following command to ensure the Kali system was up-to-date:

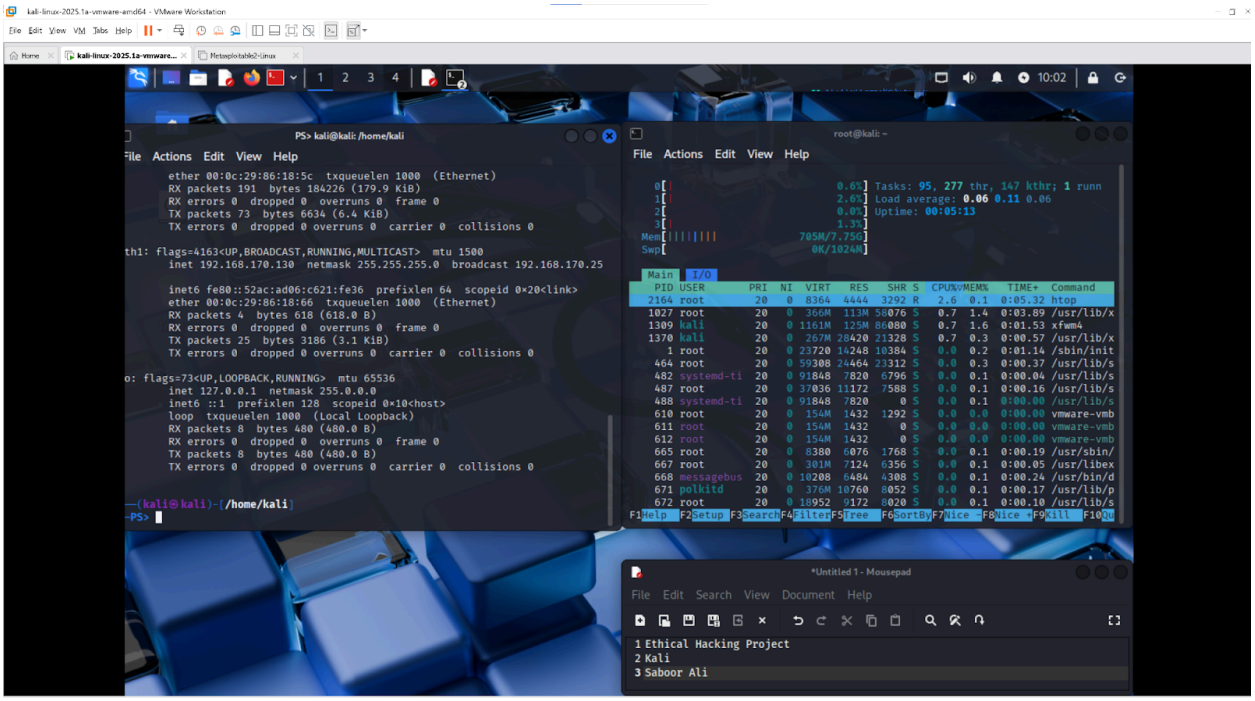
```
sudo apt update && sudo apt upgrade
```

This ensured all the software packages and repositories in Kali Linux were up-to-date for security and functionality.

---

3. Tools Explored

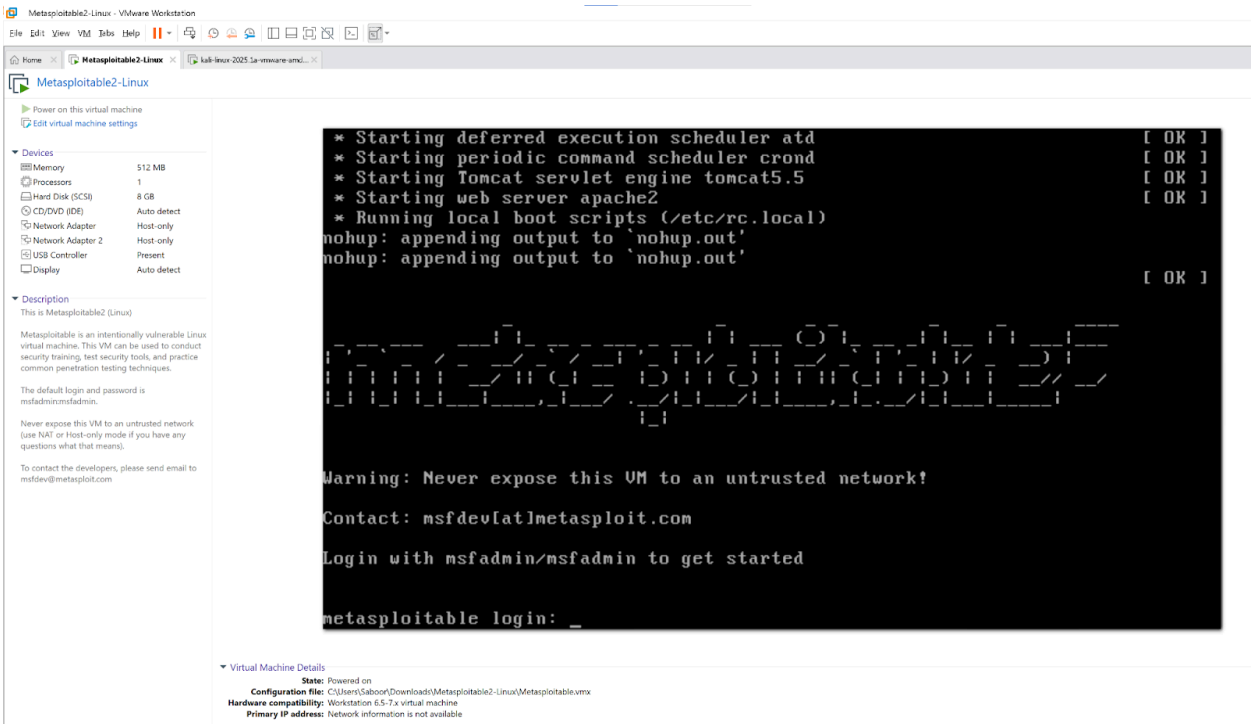
- **gnome-terminal**: Default terminal interface in Kali Linux.
- **htop**: Tool for system resource monitoring.
- **ifconfig / ip a**: Used to check network interface configurations.



4. Setting Up Metasploitable 2

Metasploitable 2 was set up as a vulnerable target system in VMware with the following configuration:

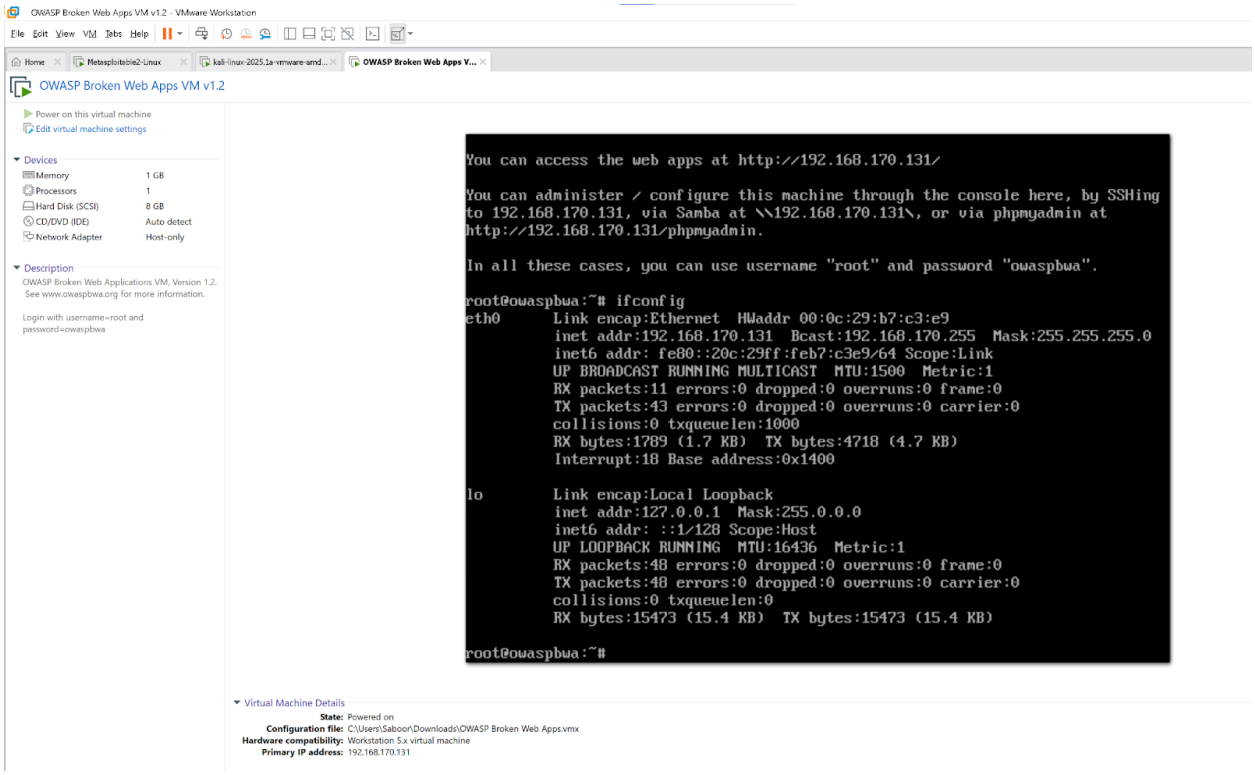
- **IP Address**: 192.168.170.128
- **Network Configuration**: Host-only, so all lab VMs are on the same network.



5. Setting Up OWASP BWA (DVWA)

OWASP BWA (Broken Web Applications) was imported into VMware as a prebuilt virtual machine. It contains intentionally vulnerable web applications such as **DVWA** (Damn Vulnerable Web Application), **Mutillidae**, and more.

- **VM Settings**:
    - **Network Adapter**: Host-only (same network as Kali)
    - **IP Address**: Static (e.g., `192.168.170.131`)
    - **OS**: Ubuntu-based with LAMP stack preconfigured



Phase 2: Network Scanning & Enumeration

Objective:

Discover devices and gather information from the network using active and passive reconnaissance techniques.

Tools Used:

- **Netdiscover**
- **Nmap**
- **Greenbone Vulnerability Management (GVM)**

1. Discover Devices on Local Area Network (LAN)

Tool Used: `netdiscover`

This tool was used to discover active devices on the local network.

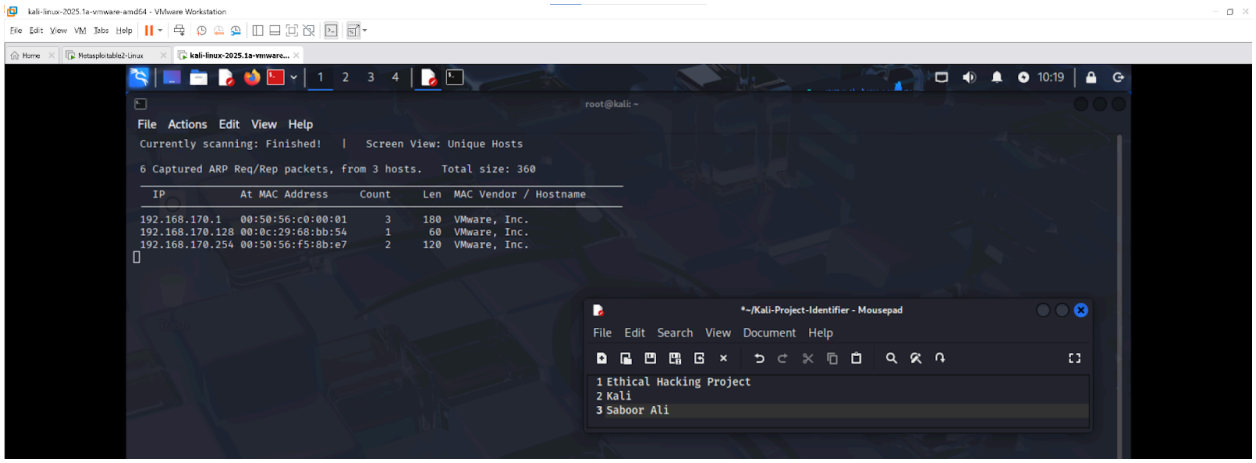
Command:

```
netdiscover -r 192.168.170.0/24
```

Explanation:
This command scans the `192.168.170.0/24` network range and lists all devices on the network, including IP and MAC addresses.

Observations:

- Discovered multiple devices on the LAN.
- Successfully identified **Metasploitable 2** at IP `192.168.170.128`.



2. Nmap Scans

2.1 Basic Nmap Scan

Used Nmap to perform a basic service version scan on Metasploitable 2 (IP: 192.168.170.128).

Command:

```
nmap -sS -sV -T4 192.168.170.128
```

Explanation:

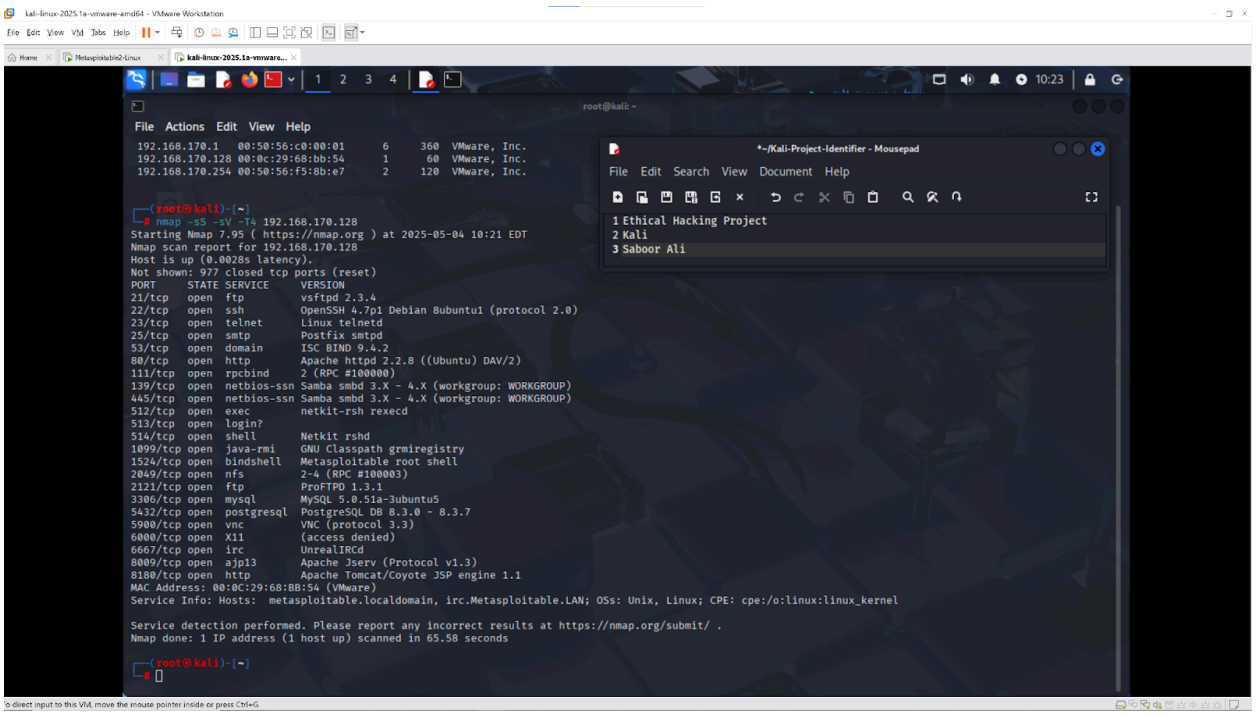
- `-sS`: Performs a TCP SYN scan
- `-sV`: Attempts to determine service versions
- `-T4`: Speeds up the scan (aggressive timing)

Output Observations:

Identified the following open ports on Metasploitable 2:

- `21/tcp` – FTP
- `22/tcp` – SSH
- `23/tcp` – Telnet
- `80/tcp` – HTTP

Other services were also detected, indicating a vulnerable system.



2.2 Aggressive Nmap Scan

Command:

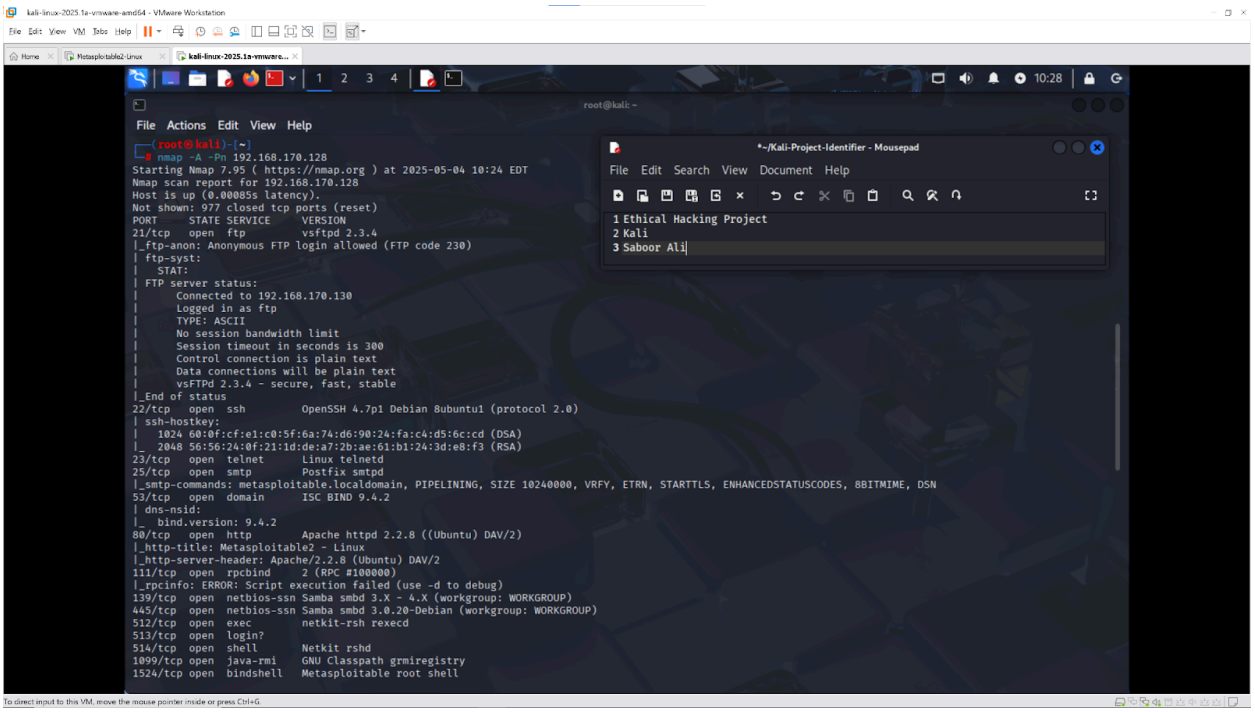
```
nmap -A -Pn 192.168.170.128
```

Explanation:

- `-A`: Enables OS detection, version detection, script scanning, and traceroute.
- `-Pn`: Skips host discovery; assumes the host is up.

Observations:

- Revealed detailed service information and OS fingerprinting.
- Detected potentially exploitable services such as outdated versions of FTP, HTTP, and SMB.



---

3. Vulnerability Assessment with GVM (Greenbone Vulnerability Management)

GVM (formerly known as OpenVAS) is an open-source framework used for scanning systems and identifying known vulnerabilities. It integrates vulnerability scanning, result management, and reporting in a centralized interface.

3.1 Installing GVM on Kali Linux

Command used:

```
sudo apt install gvm
sudo gvm-setup
sudo gvm-check-setup
```

Explanation:

- Installed the GVM framework.
- Initialized feed downloads (Network Vulnerability Tests).
- Ensured scanner and services were correctly configured.

3.2 Starting GVM and Logging In

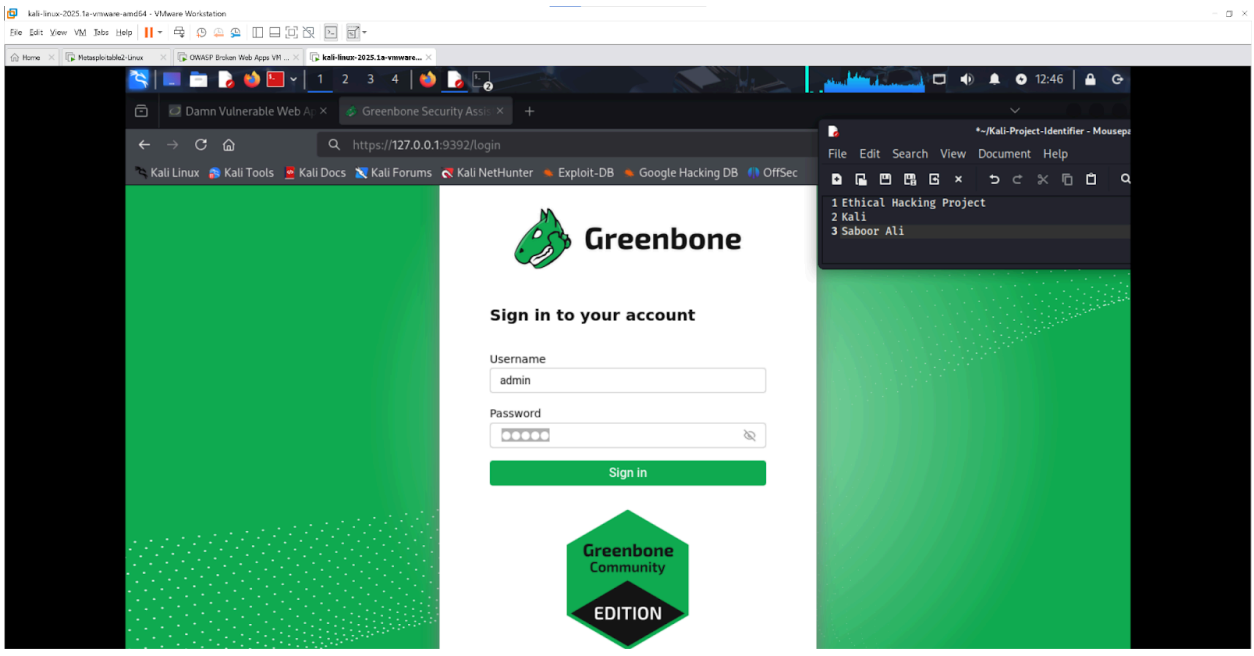
Command:

```
sudo gvm-start
```

Access:

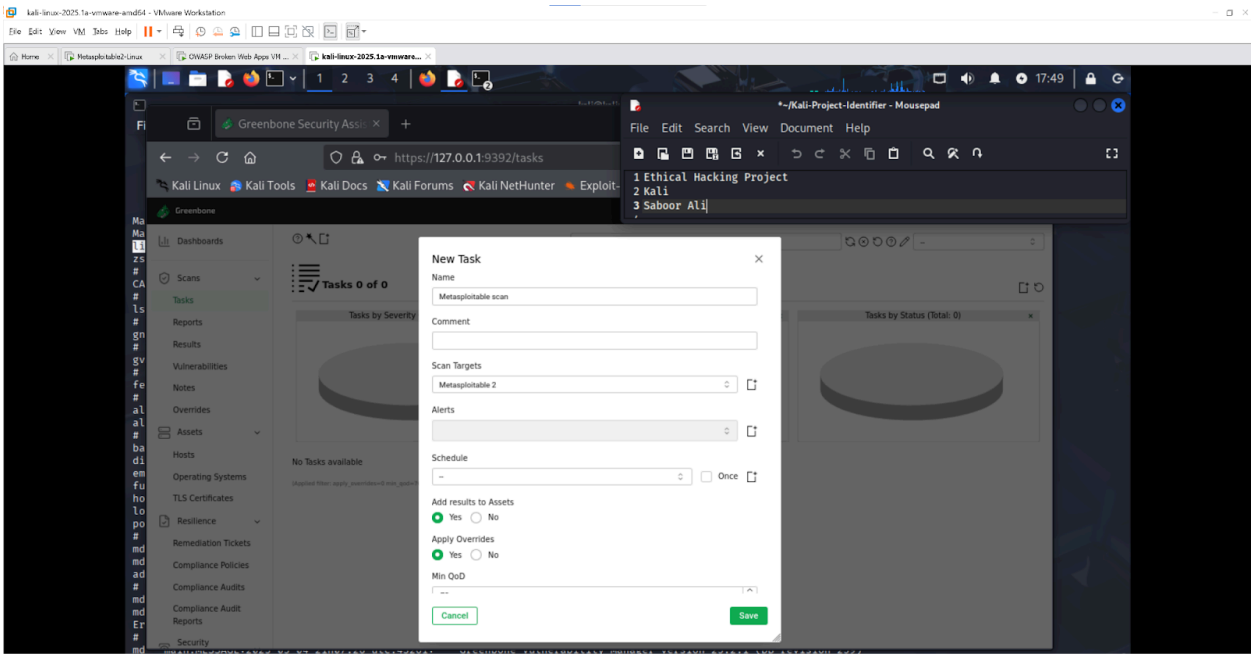
Opened browser and navigated to: https://127.0.0.1:9392

Logged in using credentials generated during setup.



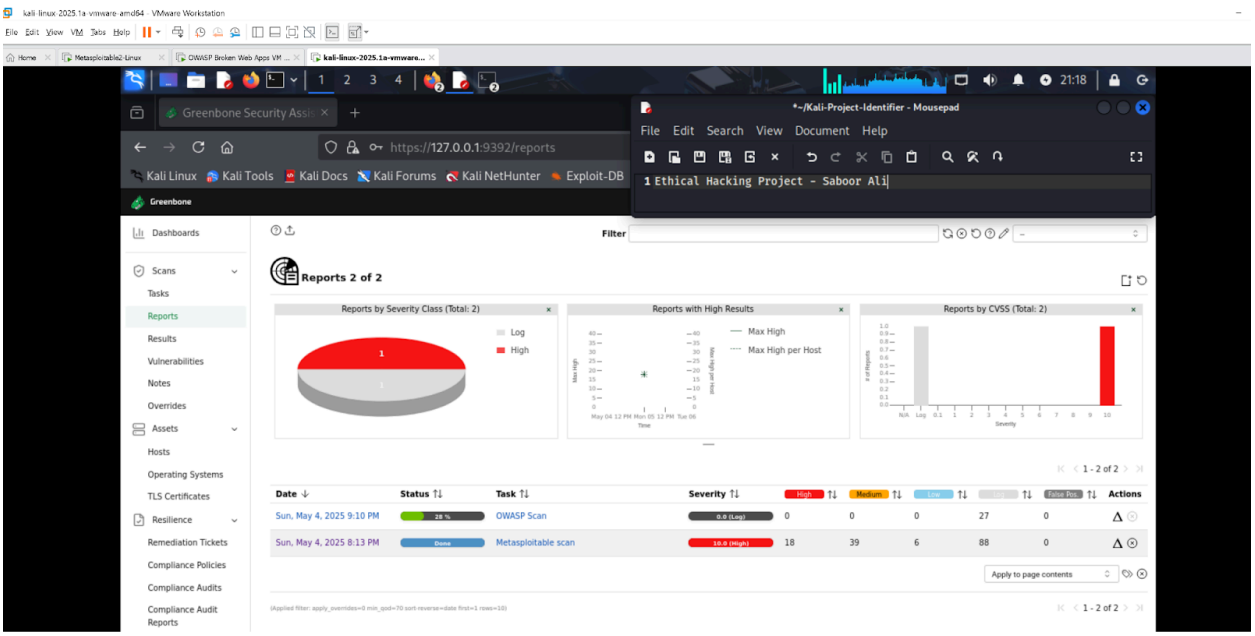
3.3 Scanning Metasploitable 2 with GVM

- Created a new target with IP: `192.168.170.128`
- Launched a full and fast scan
- Waited for the scan to complete and reviewed the results

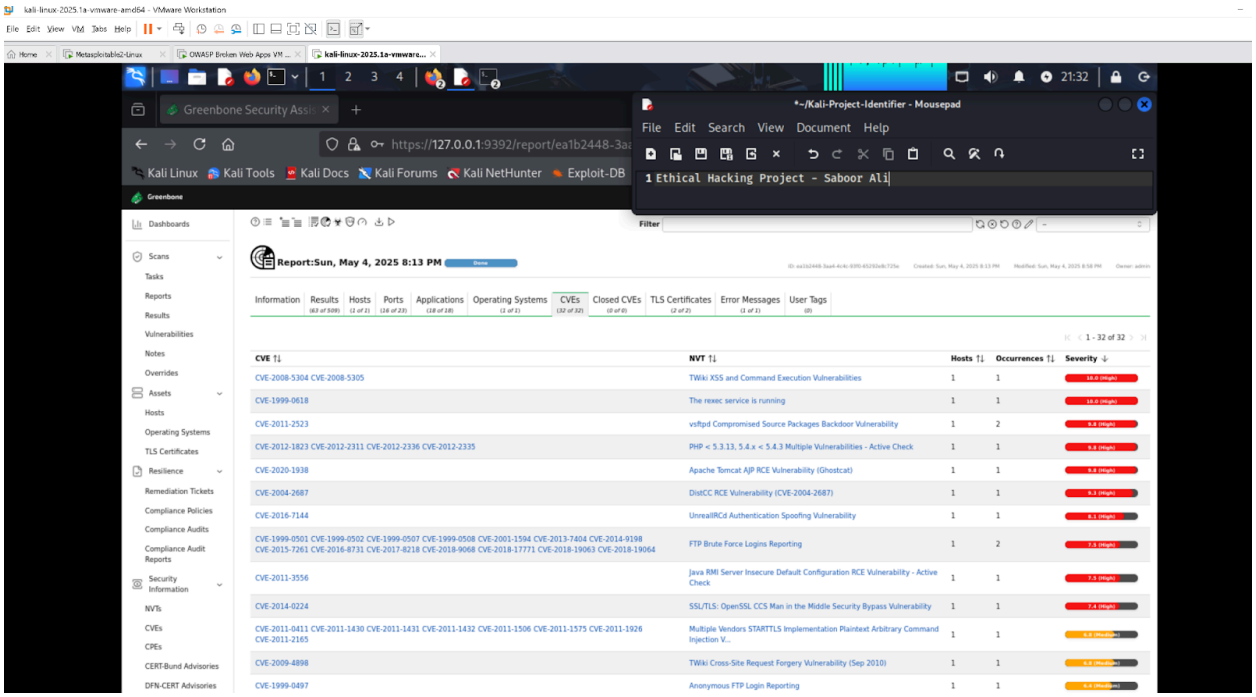


3.4 Vulnerability Assessment Results

The vulnerability assessment conducted using Greenbone Vulnerability Management (GVM) on host `192.168.170.128` revealed 63 vulnerabilities, with 16 vulnerabilities scoring a CVSS v3 base score of 9.0 or higher, indicating a critical security risk to the system. The affected services span multiple open ports and protocols, and include both remote code execution (RCE) vulnerabilities and misconfigurations exposing the host to potential compromise.



3.5 Targeting Vulnerable Services on Metasploitable 2

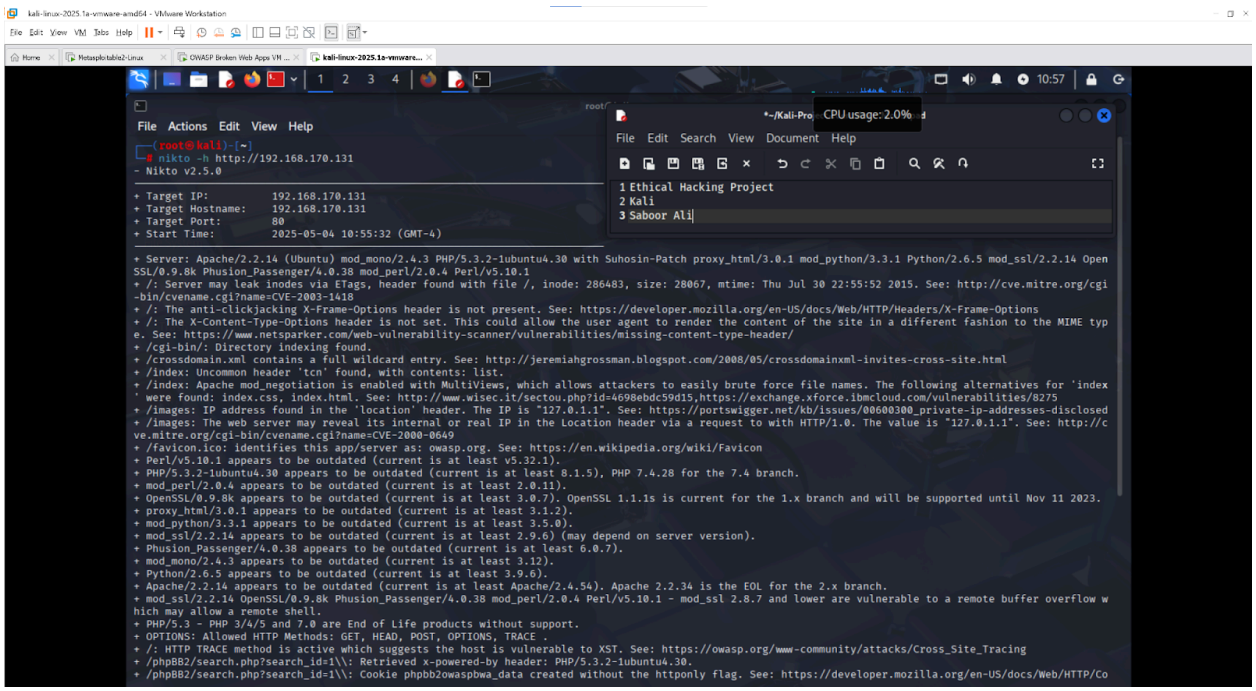


3.6 Vulnerability Scanning with Nikto

Nikto is a web vulnerability scanner that detects common misconfigurations and outdated software.

Command Used:

```
nikto -h http://192.168.170.131
```



4. Enumeration Overview

In this section, I performed a detailed enumeration to identify open services, gather system information, and discover potential vulnerabilities on both Metasploitable 2 and OWASP BWA. This phase builds on the information gathered during the initial network scanning.

4.1 Metasploitable 2 Enumeration

Based on Nmap and GVM findings for Metasploitable 2, this is a concise list of the easiest and most commonly exploited vulnerabilities that are often flagged and actively exploitable via Metasploit:

Service	Port	Vulnerability	CVE	Exploit Name in Metasploit
vsftpd	21	Backdoor Command Execution	CVE-2011-2523	`exploit/unix/ftp/vsftpd_234_backdoor`
Telnet / Linux (root shell)	23	Default Credentials	N/A (misconfig)	`auxiliary/scanner/telnet/telnet_login`
DistCC	3632	Remote Command Execution	CVE-2004-2687	`exploit/unix/misc/distcc_exec`
Samba	139, 445	Remote Code Execution	CVE-2007-2447	`exploit/multi/samba/usermap_script`
MySQL	3306	Auth Bypass with root/no pass	N/A (misconfig)	`auxiliary/scanner/mysql/mysql_login`
Tomcat Manager	8180	Weak creds → RCE via WAR	CVE-2009-3843	`exploit/multi/http/tomcat_mgr_upload`
UnrealIRCd	6667	Backdoored version RCE	CVE-2010-2075	`exploit/unix/irc/unreal_ircd_3281_backdoor`
PhpMyAdmin	80	Exposed login page, common creds	Various	`auxiliary/scanner/http/phpmyadmin_login`
PHP CGI Argument Injection	80	Remote Code Execution	CVE-2012-1823	`exploit/multi/http/php_cgi_arg_injection`
Apache 2.2.8	80	Multiple known exploits	e.g. CVE-2009-1891	Varies by module (mod_negotiation, mod_ssl, etc.)

4.2 OWASP BWA Enumeration

Based on Nikto findings for the OWASP BWA (Broken Web Applications) VM, this is a concise list of the easiest and most commonly exploited vulnerabilities identified during the assessment. These vulnerabilities are frequently targeted in penetration testing and can be actively exploited to gain unauthorized access or execute malicious actions.

Finding	Risk Level	CVE / Reference	Description / Exploitability	Recommended Fix
Outdated Apache/2.2.8 (Ubuntu)	🔴 High	CVE-2017-9798, CVE-2011-3368	Multiple known vulnerabilities (RCE, DoS, path traversal)	Upgrade to Apache 2.4.54+
Outdated PHP/5.2.4	🔴 High	CVE-2014-3515, CVE-2012-0830	Multiple RCE and info disclosure flaws	Upgrade to PHP 8.x
phpinfo.php exposed	🔴 High	CWE-552	Reveals server paths, loaded modules, configs	Remove file or restrict access
phpMyAdmin exposed	🔴 High	CVE-2009-1151	Brute-force, XSS, privilege escalation possible	Restrict IP or use auth
Directory Indexing Enabled (/doc/, /icons/, /test/)	🔴 High	CVE-1999-0678	Allows file listing and potential download of sensitive files	Disable `Indexes` in Apache config
TRACE Method Enabled	🔴 High	OWASP XST	Can be exploited for Cross Site Tracing (XST) to steal cookies	Set `TraceEnable Off` in Apache config
wp-config.php# file exposed	🔴 High	CWE-538	WordPress DB credentials exposed	Remove file or deny access in `.htaccess`

🟡 Medium to Low-Risk Issues

Finding	Risk Level	CVE / Reference	Description / Exploitability	Recommended Fix
Missing X-Frame-Options	🟡 Medium	CWE-1021	Clickjacking risk	Add `X-Frame-Options: DENY` header

Missing X-Content-Type-Options	🟡 Medium	CWE-16	MIME sniffing → XSS	Add `X-Content-Type-Options: nosniff`
Apache mod_negotiation (MultiViews)	🟡 Medium	IBM X-Force 8275	Brute-force filename attacks	Disable `MultiViews`
ETag inode leak via phpMyAdmin/ChangeLog	🟡 Medium	CVE-2003-1418	Info leak via ETag headers	Disable ETags or restrict file access
Junk HTTP Methods Accepted	🟡 Medium	CWE-693	Indicates poor input validation or unexpected behavior	Restrict methods to GET/POST/HEAD

---

5. Analysis of Enumeration Findings

Based on the enumeration results, the most critical and easily exploitable services have been identified:

- **Metasploitable 2:**
    - FTP (vsftpd 2.3.4) – Backdoor (CVE-2011-2523)
    - Telnet – Default credentials
    - Samba (CVE-2007-2447)
    - DistCC (CVE-2004-2687)
    - UnrealIRCd (CVE-2010-2075)
- **OWASP BWA:**
    - Apache (Multiple CVEs)
    - phpMyAdmin (Exposed)
    - DVWA (SQL Injection, XSS)

These services will be prioritized in the exploitation phase.