Vulnerablility Asessment Scan Report on a Unix Server Using Spiderfoot

IP Address: 192.168.0.170

Prepared by: Femi A. Ojo

Date: 6th March, 2025

Table of Contents

Introduction

This report presents the findings of a penetration testing scan performed on a Unix machine with the IP address 192.168.0.170 The assessment was conducted using three security reconnaissance tools: Nmap, SpiderFoot, and Recon-ng. Each tool was used to gather different security-related information about the target system.

The goal of this scan is to identify open ports, services, vulnerabilities, and possible security risks that could be exploited by attackers. This document provides detailed results from each tool, along with relevant screenshots and findings.

Objective

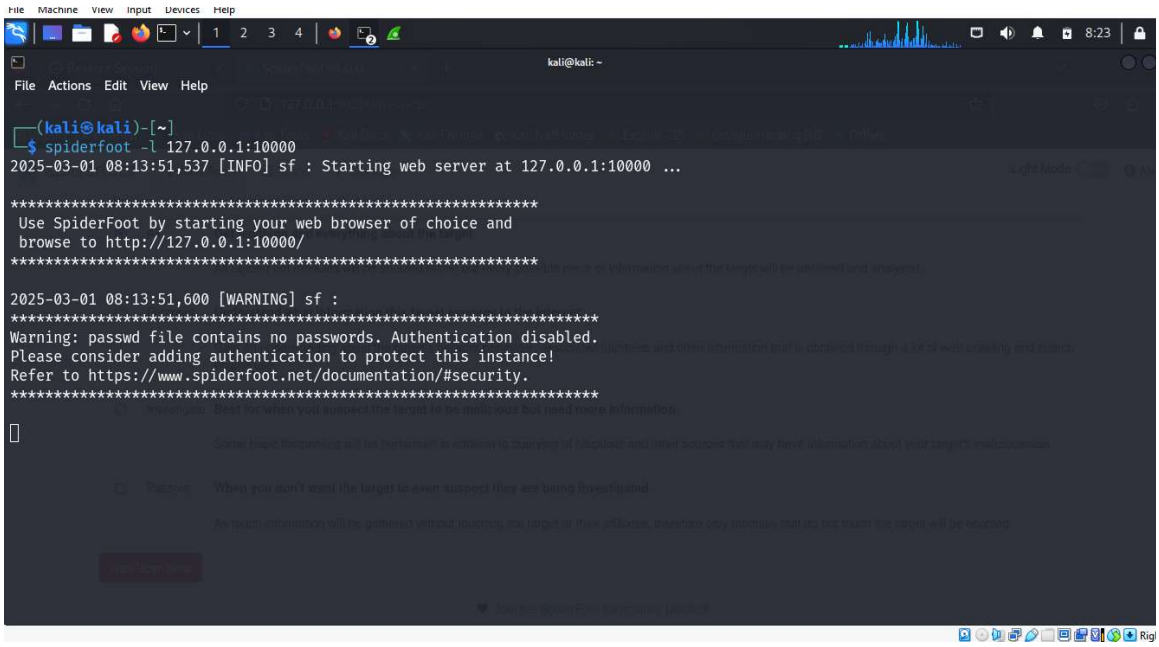
Spiderfoot (OSINT) was used to scan the Unix machine to detect open ports, running services, and vulnerabilities.

Spiderfoot Scan Report

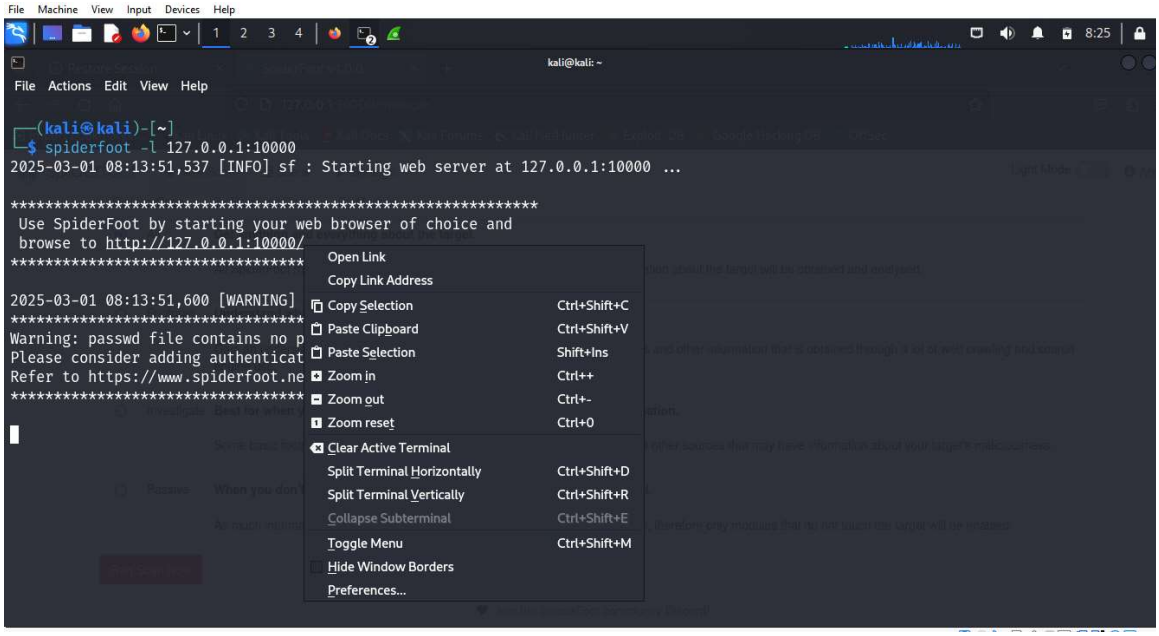
Scan Command Used

Spiderfoot uses Modules to run it scan, We need to start spiderfoot on our localhost by using the command line below.

spiderfoot -l 127.0.0.1: 10000



This start on a GUI interface where you can easily run your scan, by default it's gives you a link all you have to do is to right click and click on open link.



Breaking it Down:

After this it will redirect you to a GUI interface

- **spiderfoot** → Calls the **Spiderfoot** tool, which is used for network scanning and security auditing.
- **192.168.0.170** → The target IP address being scanned.

How It Helps in a Vulnerability Scan:

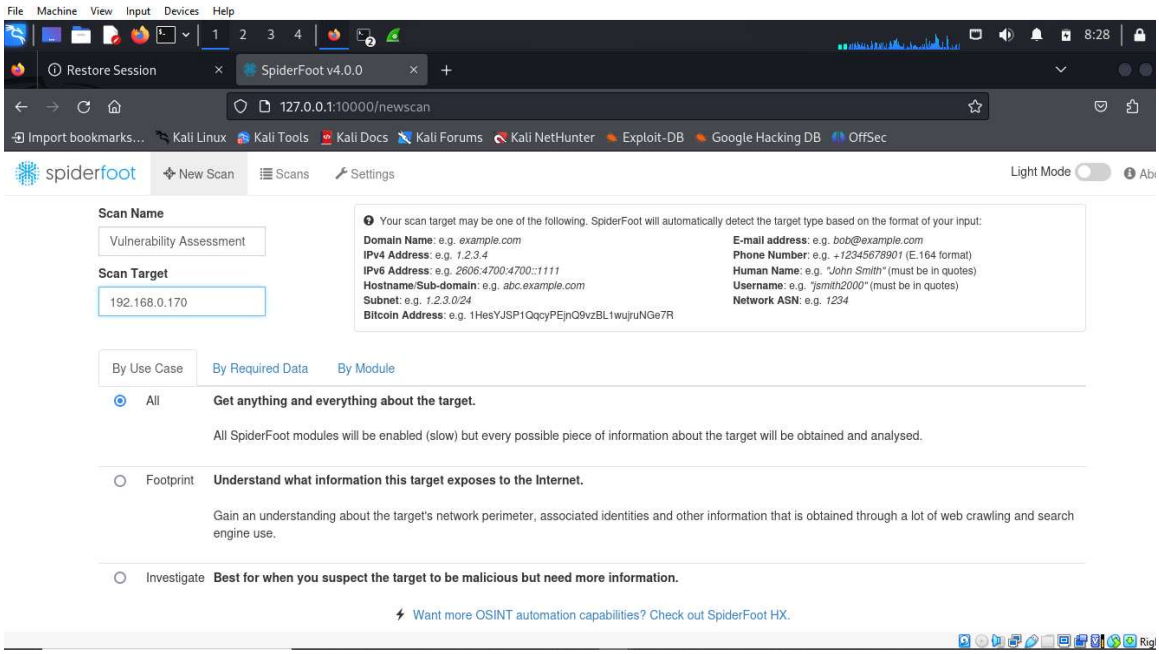
- **Identifies Open Ports** → Shows which services are running and where vulnerabilities might exist.
- **Detects Running Services & Versions** → Helps find outdated or misconfigured services.
- **Finds OS & System Info** → Useful for fingerprinting a system to tailor attacks or defenses.
- **Performs Traceroute** → Helps map out the network for possible attack paths.

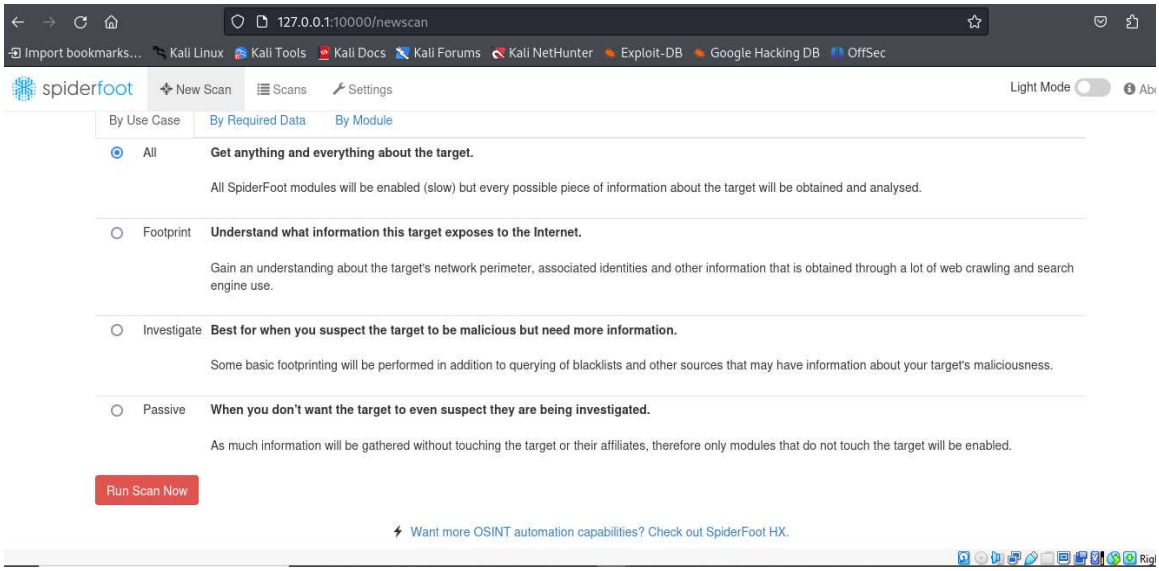
Findings from Nmap Scan on 192.168.0.170

General Information:

- **Target IP:** 192.168.0.170
- **Host is up:** 0.00093s latency

- **Operating System:** Linux 2.6.9 - 2.6.33
- **Network Distance:** 1 hop
- **MAC Address:** 08:00:27:3A:27:F4 (Oracle VirtualBox virtual NIC)
- **Hostname:** metasploitable.localdomain





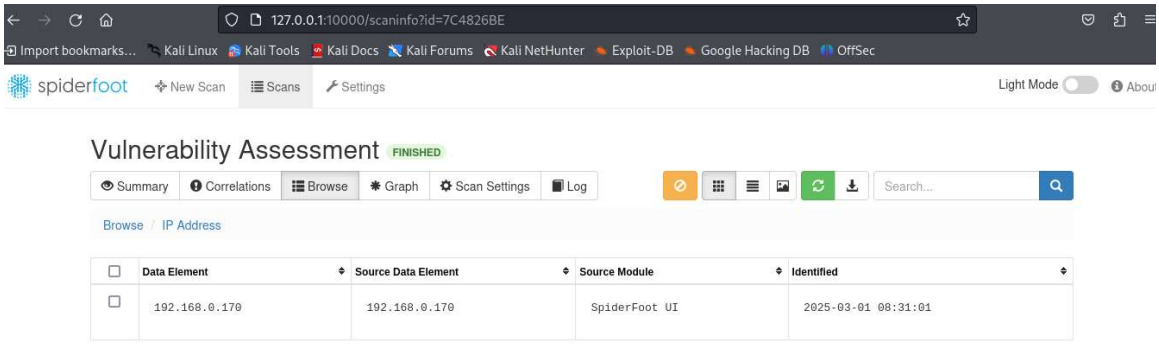
Give your scan a NAME, input the targert IP(192.168.0.170) Remember spiderfoot runs on modules. After this click on run scan now.

This start to run scan on the IP address of the target and gives us result in a well formated

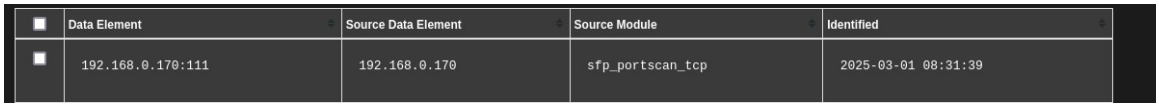
manner.

IP ADDRESS:

- **Data Element(192.168.0.170)**
    - **Source Data Element:** 192.168.0.170
    - **Source Module:** Spiderfoot UI
    - **Identified:** 2025-03-06 08:31:01



- **Open Port and Services**
    - Port 111 (192.168.0.170:111)
    - **Source Data Element :192. 168.0.170**
    - Source Module: sfp_portscan_tcp
    - Identified: 2025-03-06 08:31:01



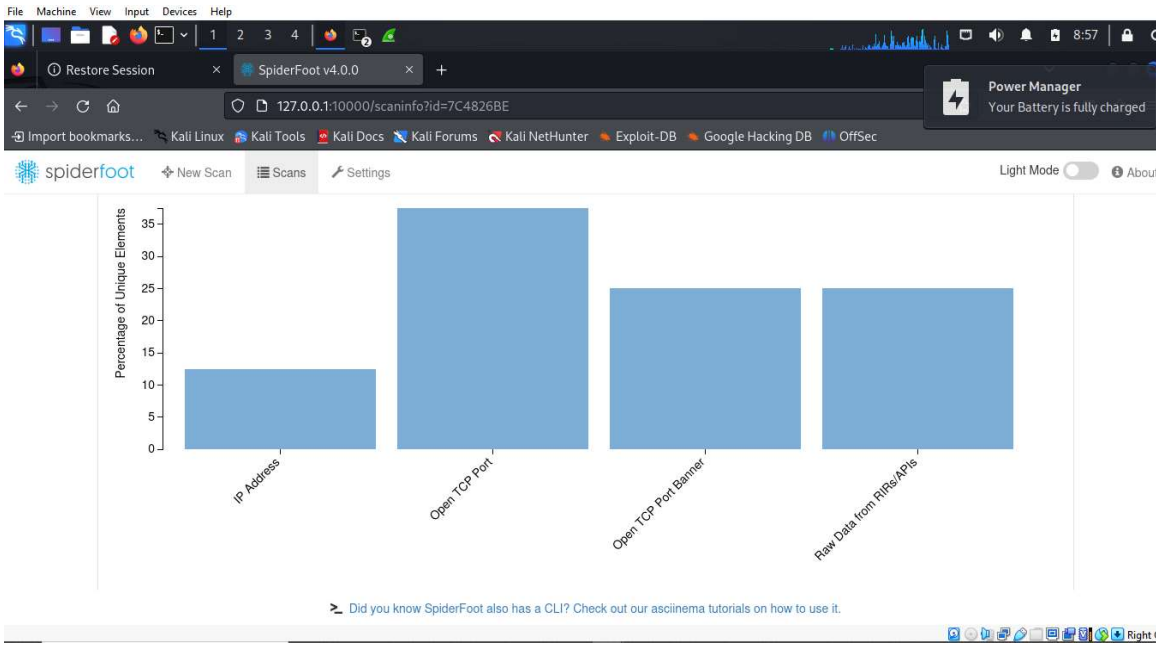
- **Port 22 (192.168.0.170:22)**
    - **Source Data Element:** 192.168.0.170
    - **Source Module :sfp_portscan_tcp**
    - Identified: 2025-03-06 08:31:01

☐	192.168.0.170:22	192.168.0.170	sfp_portscan_tcp	2025-03-01 08:31:39

- **Port 3306 (192.168.0.170:3306)**
    - **Source Data Element:** 192.168.0.170
    - **Source Module :sfp_portscan_tcp**
    - Identified: 2025-03-06 08:31:01

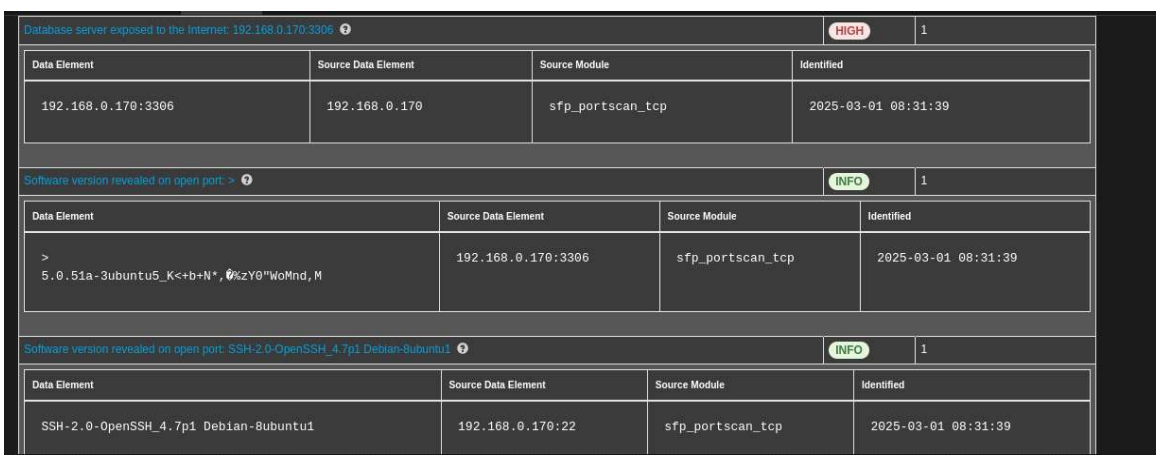
☐	192.168.0.170:3306	192.168.0.170	sfp_portscan_tcp	2025-03-01 08:31:39

- **Graphical Representation of Scan**
    - **IP Address**
    - **Open TCP port**
    - Open TCP port baner
    - Raw Data from RIRs/APIs



- **Correlations**

Observations that arise from SpiderFoot's analysis of the data, highlighting interesting information from the scan.



Database server exposed to the Internet: 192.168.0.170:3306 — HIGH — 1

Data Element	Source Data Element	Source Module	Identified
192.168.0.170:3306	192.168.0.170	sfp_portscan_tcp	2025-03-01 08:31:39

Software version revealed on open port: > — INFO — 1

Data Element	Source Data Element	Source Module	Identified
> 5.0.51a-3ubuntu5_K<+b+N*,[illegible]%zY0"WoMnd,M	192.168.0.170:3306	sfp_portscan_tcp	2025-03-01 08:31:39

Software version revealed on open port: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 — INFO — 1

Data Element	Source Data Element	Source Module	Identified
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1	192.168.0.170:22	sfp_portscan_tcp	2025-03-01 08:31:39

Analysis & Recommendations:

- **Disable anonymous FTP access** or upgrade vsftpd to a secure version.
- **Upgrade OpenSSH to the latest version** to patch known vulnerabilities.

- **Disable Telnet** and use SSH for secure remote access.
- **Upgrade SMTP service** and restrict VRFY to prevent user enumeration.
- **Upgrade BIND DNS** to the latest secure version to mitigate cache poisoning risks.
- **Update Apache HTTP Server** to avoid known exploits.
- **Harden Samba configuration** and ensure the latest security patches are applied.
- **Upgrade MySQL and PostgreSQL** to mitigate SQL injection risks.
- **Secure VNC with strong authentication** or disable it if not needed.
- **Update Apache Tomcat** and remove default credentials.
- **Disable or restrict distccd** to prevent remote code execution vulnerabilities.

Conclusion:

This scan indicates that the target system is highly vulnerable, running several outdated services with known exploits. Immediate security patches and mitigations are recommended to secure the system from potential attacks.