

# **Vulnerability Assessment Scan Report on a Unix Server Using Spiderfoot**

**IP Address: 192.168.0.170**

**Prepared by: Femi A. Ojo**

**Date: 6<sup>th</sup> March, 2025**

## Table of Contents

Introduction .....	3
Objective .....	4
Spiderfoot Scan Report .....	5
Findings from Spiderfoot Scan on 192.168.0.170 .....	5
Analysis & Recommendation .....	10
Conclusion .....	10

## 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

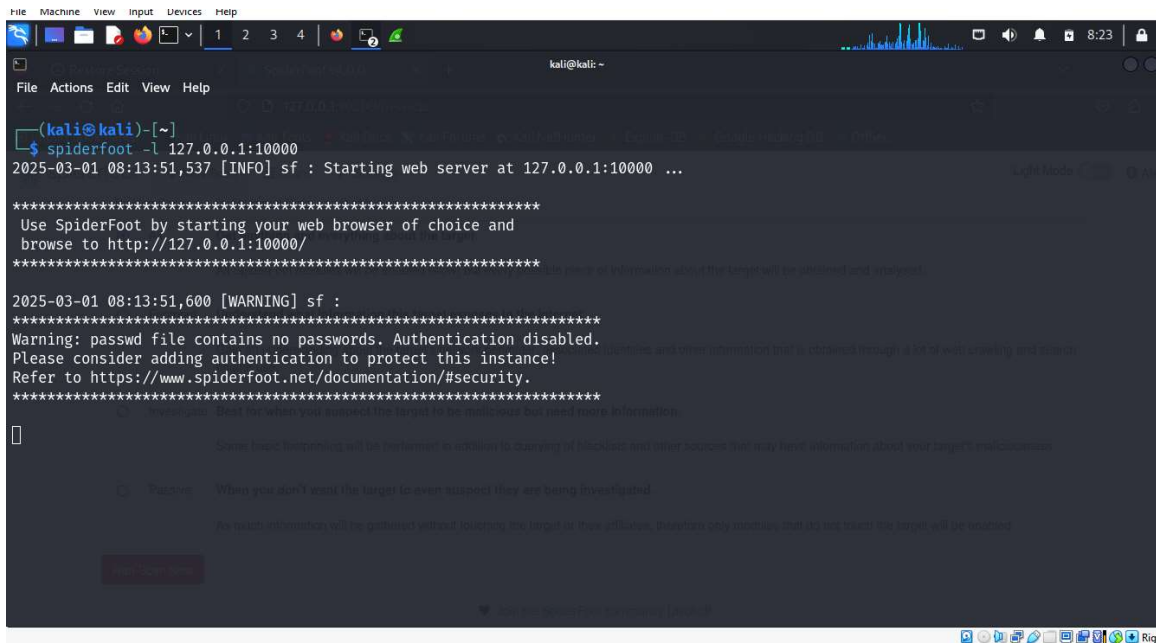
Spiderfoot (OSINT) was used to scan the Unix machine to detect open ports, running services, and vulnerabilities.

# 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**



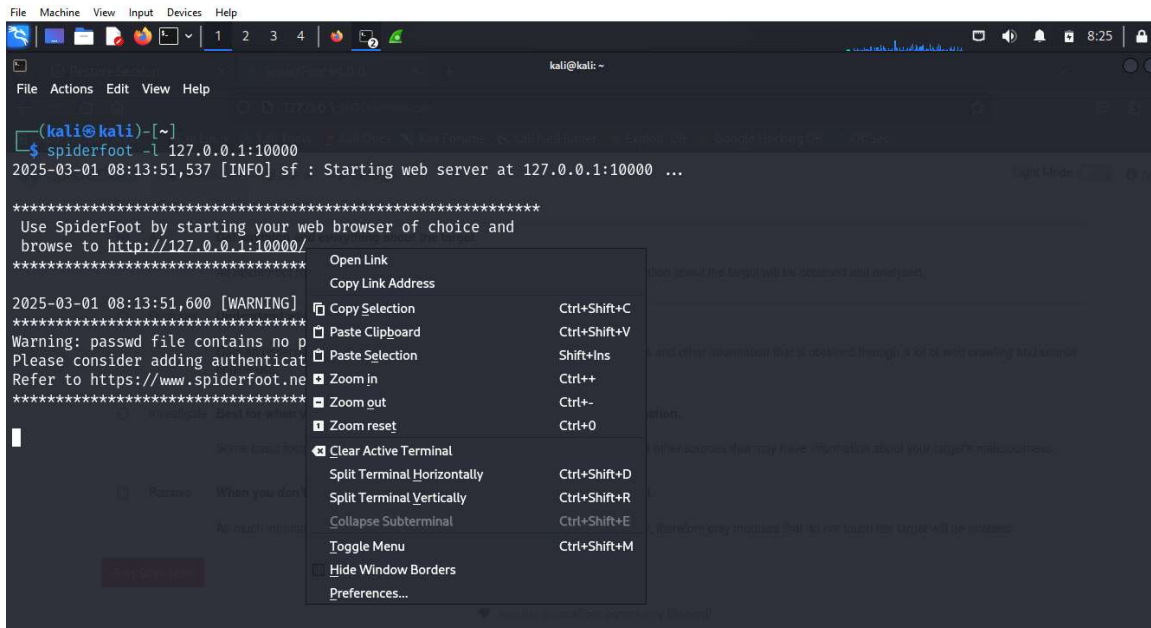
```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ spiderfoot -l 127.0.0.1:10000
2025-03-01 08:13:51,537 [INFO] sf : Starting web server at 127.0.0.1:10000 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:10000/
*****

2025-03-01 08:13:51,600 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****

[ ]
Some basic information will be gathered in addition to scanning of IP/hosts and other sources that may have information about your target's infrastructure.
When you don't want the target to even suspect they are being investigated.
No extra information will be gathered without knowing the target or their affiliates. Sources may indicate that the target will be located.
```

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

File Machine View Input Devices Help

SpiderFoot v4.0.0

127.0.0.1:10000/newscan

Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

spiderfoot New Scan Scans Settings Light Mode

**Scan Name**  
Vulnerability Assessment

**Scan Target**  
192.168.0.170

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. example.com	E-mail address: e.g. bob@example.com
IPv4 Address: e.g. 1.2.3.4	Phone Number: e.g. +12345678901 (E.164 format)
IPv6 Address: e.g. 2606:4700:4700::1111	Human Name: e.g. "John Smith" (must be in quotes)
Hostname/Sub-domain: e.g. abc.example.com	Username: e.g. "jsmith2000" (must be in quotes)
Subnet: e.g. 1.2.3.0/24	Network ASN: e.g. 1234
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vZBL1wujruNGe7R	

By Use Case By Required Data By Module

☒ All **Get anything and everything about the target.**  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐ Footprint **Understand what information this target exposes to the Internet.**  
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate **Best for when you suspect the target to be malicious but need more information.**  
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ Passive **When you don't want the target to even suspect they are being investigated.**  
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

[Want more OSINT automation capabilities? Check out SpiderFoot HX.](#)

Run Scan Now

Give your scan a NAME, input the target 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 formatted

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

127.0.0.1:10000/scaninfo?id=7C4826BE

Import bookmarks...Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

spiderfootNew ScanScansSettingsLight ModeAbout

Vulnerability AssessmentFINISHED

SummaryCorrelationsBrowseGraphScan SettingsLog

SummaryGridListImageRefreshDownloadSearch...

Browse / IP Address

	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	192.168.0.170	192.168.0.170	SpiderFoot UI	2025-03-01 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

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	192.168.0.170:111	192.168.0.170	sfp_portscan_tcp	2025-03-01 08:31:39



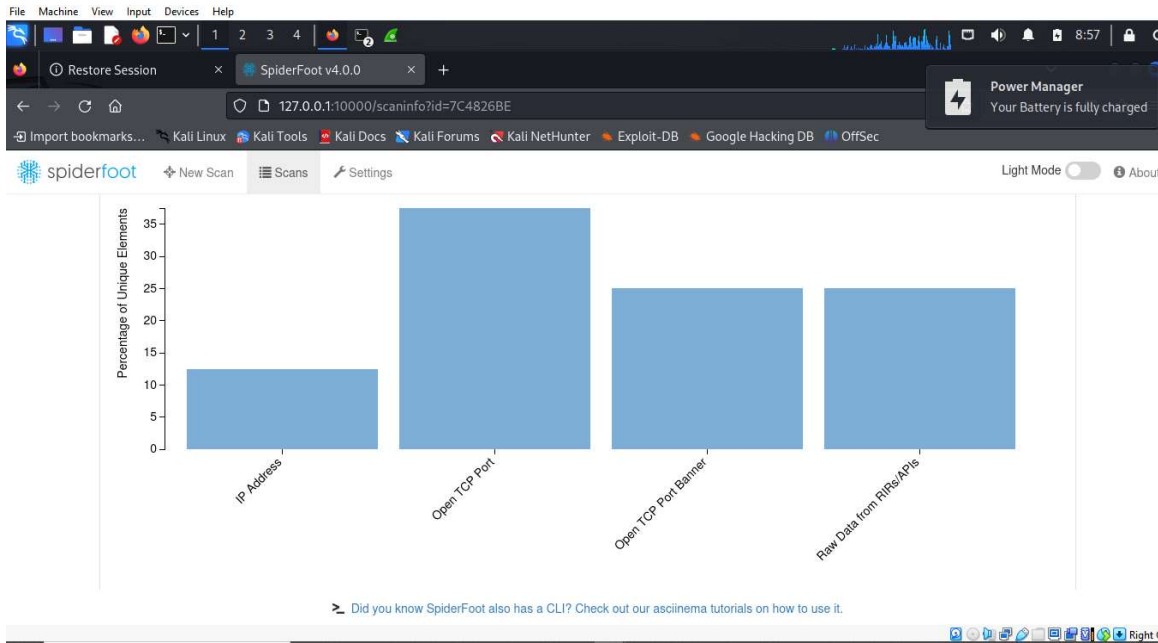
- **Port 22 (192.168.0.170:22)**
  - **Source Data Element:** 192.168.0.170
  - **Source Module :**sfp\_portscan\_tcp
  - **Identified:** 2025-03-06 08:31:01

	■	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_Kc+b+N*,0%zY9"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.