Infrastructure Reconnaissance and Automated OSINT via SpiderFoot: A h4cker.org Case Study

Juan Pablo Vega Villamil, *Computer Systems Engineer.*

***Abstract*—This document details the process of information gathering and infrastructure mapping for the domain *h4cker.org*. Utilizing the SpiderFoot OSINT automation framework, critical assets, subdomains, and network configurations were identified. The primary objective was to determine the external attack surface through passive and active enumeration techniques, consolidating findings into a technical relationship graph and statistical data.**

***Index Terms*—OSINT, Reconnaissance, SpiderFoot, Footprinting, Cybersecurity, h4cker.org.**

I. Introduction

RECONNAISSANCE is the initial and most critical phase of any security audit. The goal is to obtain as much public information as possible about a target without intrusively interacting with its systems. In this laboratory, the infrastructure of **h4cker.org** is analyzed to understand its network topology and digital exposure.

II. Methodology and Tools

SpiderFoot was selected as the primary tool, an OSINT framework that integrates over 200 modules to automate footprinting and threat intelligence gathering.

A. Environment Configuration

The service was initialized locally using the Python backend. As shown in Fig. 1, listeners were established on port 5001 to enable the Graphical User Interface (GUI), allowing for centralized management of the scanning modules.

Fig. 1. Terminal initialization and network environment deployment for SpiderFoot.

III. Reconnaissance Execution

A. Target Definition and Scan

To begin data collection, the domain *h4cker.org* was defined as the ”seed.” During this stage (see Fig. 2), specific modules were selected to correlate DNS records, IP address blocks, and associated subdomains. This step is essential for defining the actual scope of the investigation.

Ethical Hacking Laboratory: Reconnaissance Phase. Report generated February 2026.

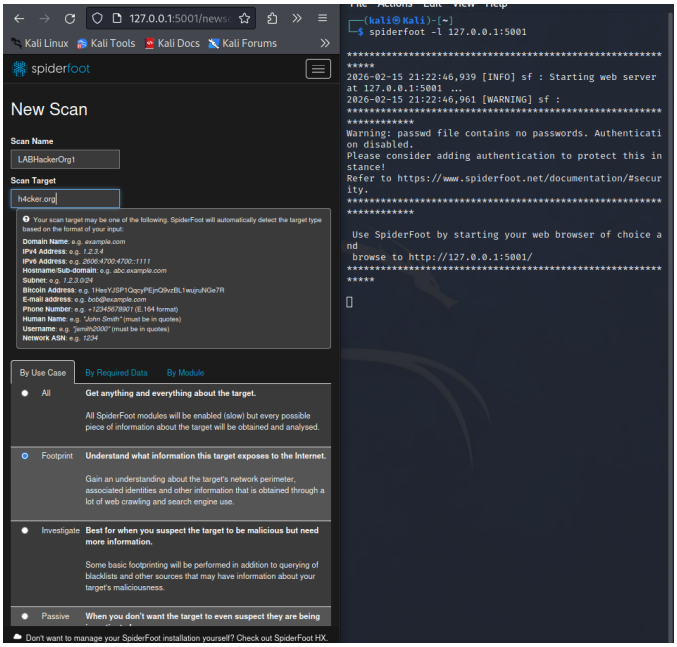

Fig. 2. Scan configuration detailing the target and the activation of correlative modules.

IV. Results and Analysis

The scanning process for the lab ”LABHackerOrg1” reached an ”ABORT-REQUESTED” status after identifying a total of 64 elements, 57 of which were unique. The findings were categorized into several key pillars based on the gathered data types and statistical distribution.

A. Data Distribution and Unique Elements

As illustrated in Fig. 3, the reconnaissance identified a diverse range of data types. Notable percentages of unique elements were found for Internet Names, Co-Hosted Sites, and IP Addresses.

Fig. 3. Statistical distribution of identified unique elements and percentage of findings by data type.

B. Detailed Asset Inventory

A detailed breakdown of the discovered assets is provided in Fig. 4. This includes Affiliate Internet Names, DNS SPF and TXT records, and identified Open TCP Ports.

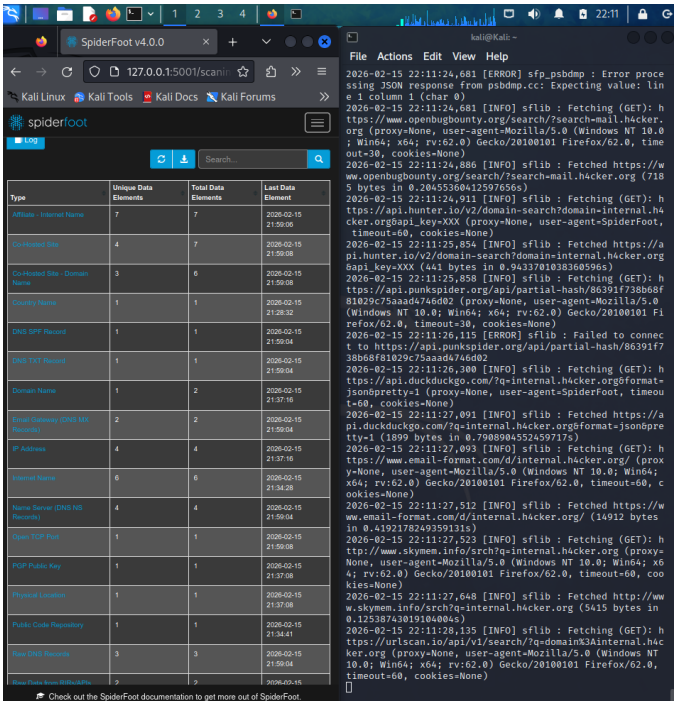

Fig. 4. Tabular summary of detailed findings including data element counts and last identified timestamps.

C. Network Infrastructure and IP Identification

The framework successfully resolved the primary IP addresses associated with *h4cker.org* using the `sfp_dnsresolve` module. The identified IP range includes 185.199.108.153 through 185.199.111.153, as shown in Fig. 5.

Data Element	Source Data Element	Source Module	Identified
185.199.108.153	h4cker.org	sfp_dnsresolve	2026-02-15 21:37:16
185.199.109.153	h4cker.org	sfp_dnsresolve	2026-02-15 21:37:16
185.199.110.153	h4cker.org	sfp_dnsresolve	2026-02-15 21:37:16
185.199.111.153	h4cker.org	sfp_dnsresolve	2026-02-15 21:37:16

Fig. 5. List of identified IP addresses for h4cker.org resolved via DNS enumeration modules.

D. Graph Visualization

The technical relationship graph (Fig. 6) presents the interconnectivity of these findings. This visual analysis allows for the identification of asset density and potential single points of failure or exposure within the infrastructure of *h4cker.org*.

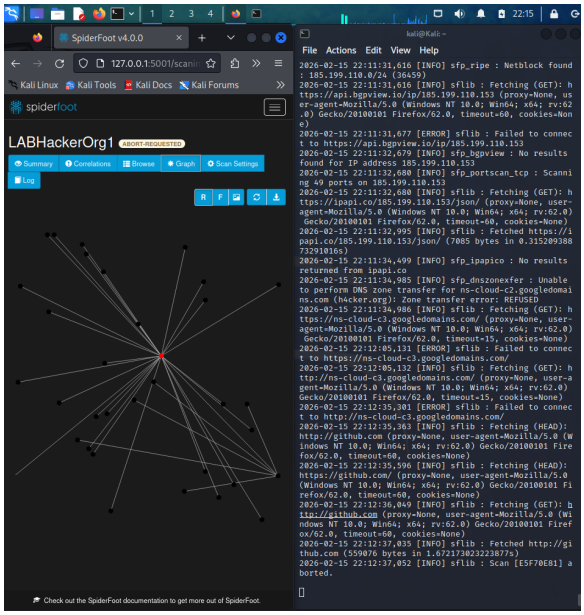

Fig. 6. Technical relationship graph and entities discovered during the reconnaissance phase.

V. Conclusion

Automation through SpiderFoot enables exhaustive mapping in a reduced timeframe. The investigation revealed that

h4cker.org possesses a clearly defined attack surface. Proper management of public records and services, such as the identified open ports and DNS entries, is key to mitigating external reconnaissance vectors.

REFERENCES

[1] SpiderFoot Documentation, “Open Source Intelligence Automation,” [Online]. Available: https://www.spiderfoot.net/documentation/
[2] OWASP, “Information Gathering Guide,” [Online]. Available: https://owasp.org/