Passive Reconnaissance and Information Gathering via Recon-ng: Domain Enumeration and Discovery

Juan Pablo Vega Villamil, *Computer Systems Engineer*

***Abstract*—This report details a passive reconnaissance workflow using the Recon-ng framework to map the digital footprint of the target domain *hackxor.net*. By integrating the HackerTarget and Interesting_Files modules, this laboratory demonstrates the automated identification of subdomains, IP addresses, and sensitive directory structures, resulting in a centralized intelligence database for security assessment.**

***Index Terms*—Recon-ng, HackerTarget, OSINT, Subdomain Enumeration, Passive Reconnaissance, Information Gathering.**

I. Introduction

RECON-NG is a high-velocity web reconnaissance framework that automates OSINT processes. This laboratory focuses on expanding a single seed domain into a comprehensive inventory of hosts and files without direct interaction with the target's primary infrastructure.

II. Methodology and Execution

A. HackerTarget Module Deployment

The initial phase involved loading the *HackerTarget* module to identify publicly listed hostnames. As shown in Fig. 1, the module was initialized and usage information was reviewed before setting the source target to *hackxor.net*.

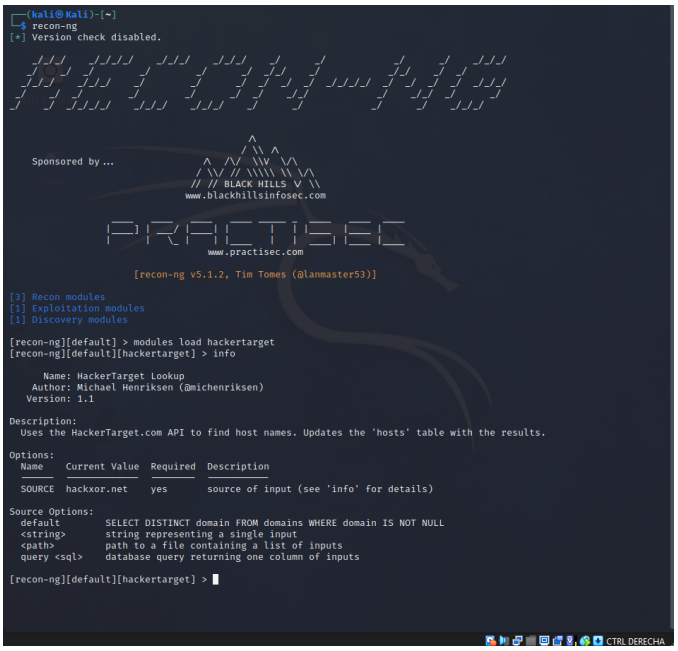

Fig. 1. Loading the HackerTarget module and configuring the target source.

Ethical Hacking Laboratory: Information Gathering Phase. Report generated February 2026.

B. Data Acquisition and Host Discovery

Upon execution of the `run` command (see Fig. 2), the framework performed passive lookups, identifying five total hosts associated with the target domain.

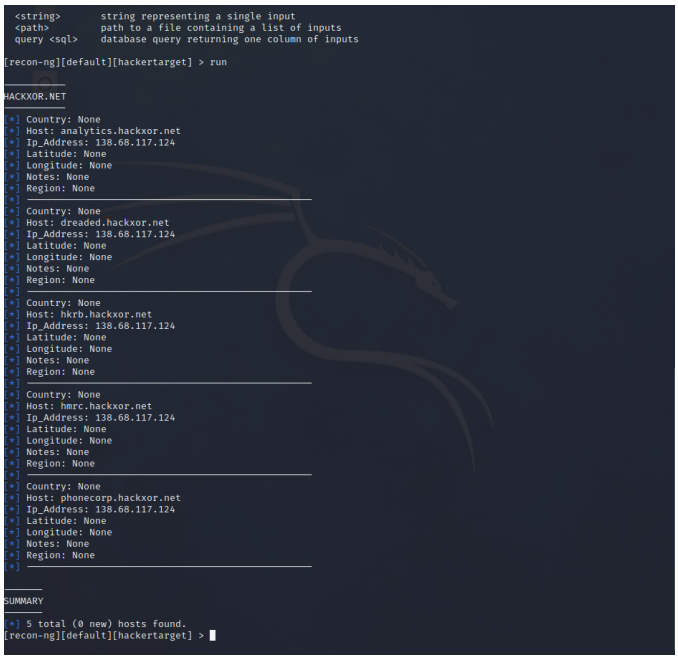

Fig. 2. Execution of the HackerTarget lookup revealing discovered subdomains and IP addresses.

III. Analysis of Discovered Assets

A. Database Consolidation and Host Verification

Recon-ng organizes gathered intelligence into an internal database. The activity was verified using the `dashboard` command (Fig. 3), confirming the successful addition of 5 hosts. Detailed records, including specific IP addresses for each host, were then extracted using the `show hosts` command as seen in Fig. 4.

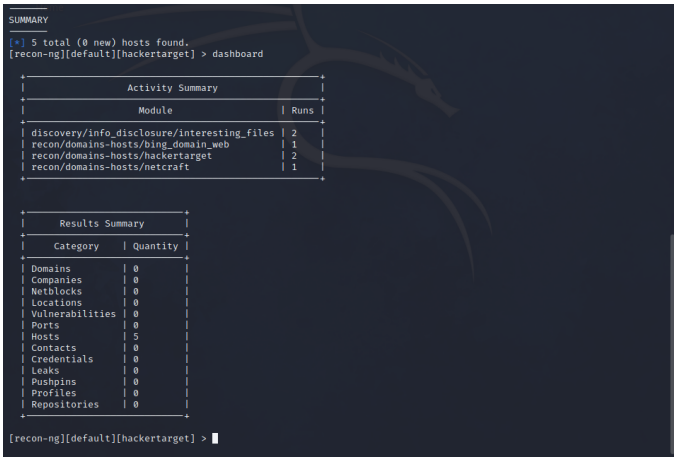

Fig. 3. Activity summary dashboard confirming database updates.

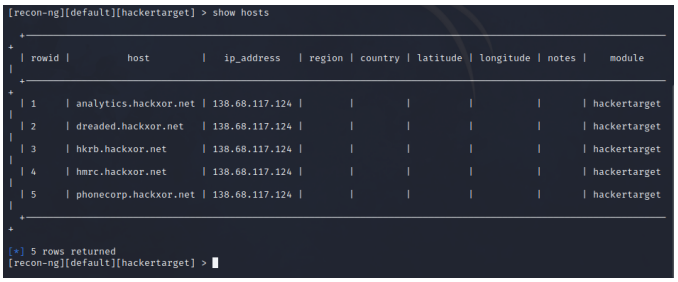

Fig. 4. Detailed view of the 'hosts' table showing resolved IP addresses for hackxor.net.

B. Web-Based Reporting Interface

To facilitate results analysis, the `recon-web` analytics engine was launched. This provides a web-based user interface to visualize the database content, categories of discovery, and module run history in a structured format (Fig. 5).

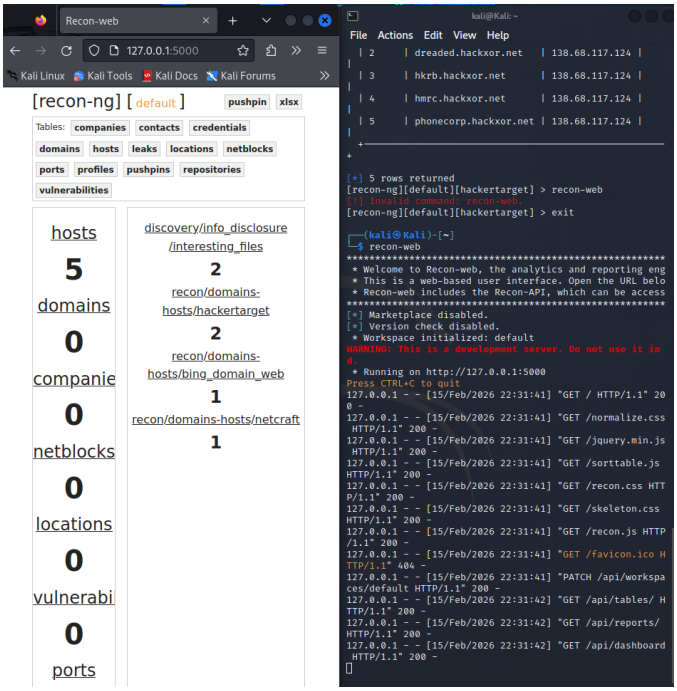

Fig. 5. Recon-web interface displaying the collected intelligence and reconnaissance statistics.

C. Sensitive File Discovery

The final phase utilized the *interesting_files* module against the target. As documented in Fig. 6, the module identified critical files such as `robots.txt`. The results of this discovery were automatically exported to a `.csv` file within the `recon-ng/data` directory for offline documentation.

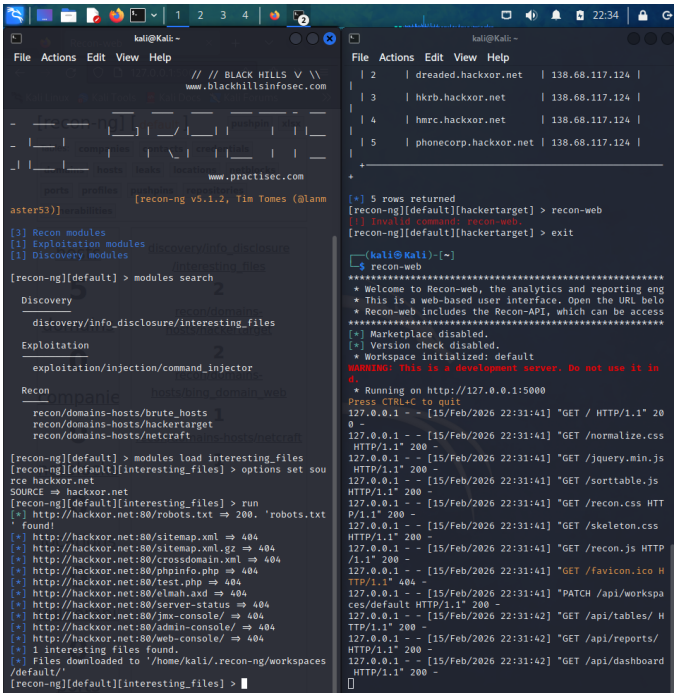

Fig. 6. Execution of the interesting_files discovery module for sensitive directory identification.

IV. Conclusion

The integration of specialized OSINT modules within Recon-ng allowed for a rapid mapping of *hackxor.net*. The discovery of five hosts and associated system files provides a solid foundation for the subsequent vulnerability assessment phases.

References

[1] Recon-ng Framework, "The Recon-ng Documentation," [Online]. Available: https://github.com/lanmaster53/recon-ng

[2] HackerTarget API, "Network Intelligence and IP Discovery," [Online]. Available: https://hackertarget.com/