

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.

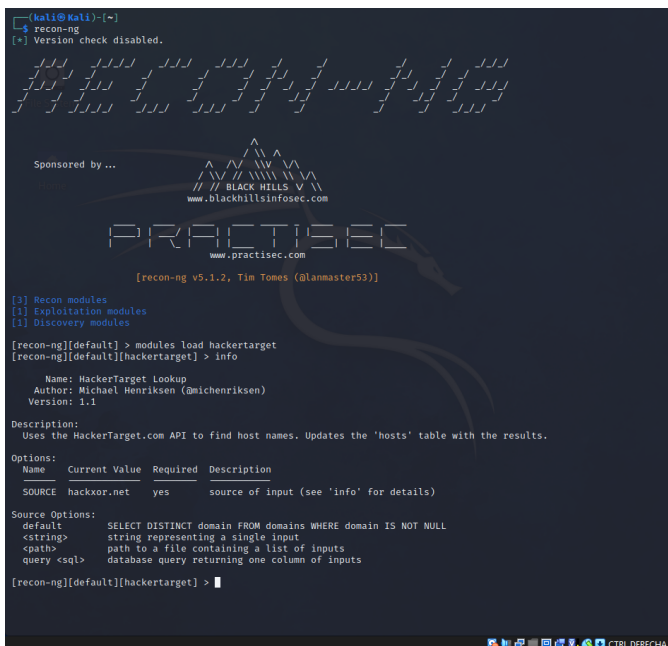
I. INTRODUCTION

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*.



```

[anti@kali:~]$ recon-ng
[*] Version check disabled.

Sponsored by ...
// BLACK HILLS //
www.blackhillsinfosec.com

PRACTISEC
www.practiseccom

[recon-ng v5.1.2, Tim Tones (@lanmaster53)]

[?] Recon modules
[!] Exploitation modules
[!] Discovery modules

[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  -----
  SOURCE    hackxor.net      yes       source of input (see 'info' for details)

Source Options:
  default  SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string> string representing a single input
  <path>   path to a file containing a list of inputs
  query <sql> database query returning one column of inputs

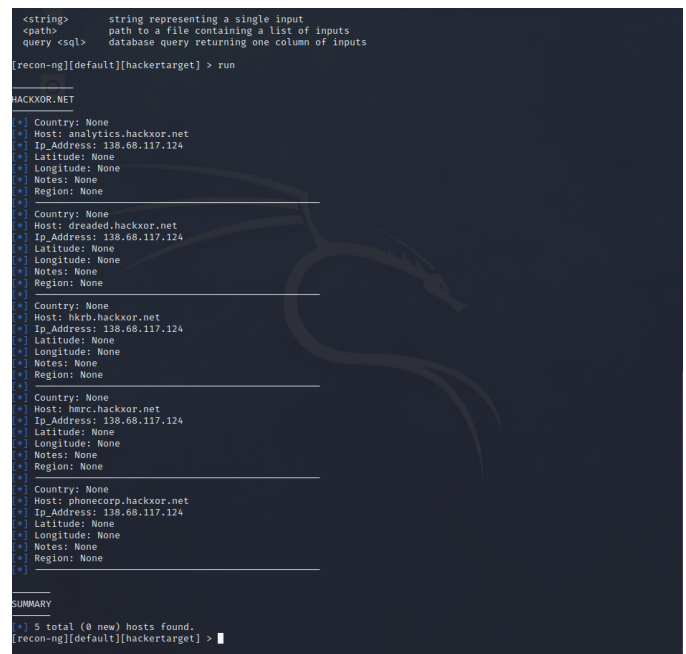
[recon-ng][default][hackertarget] >
  
```

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.



```

[recon-ng][default][hackertarget] > run

HACKXOR.NET

[*] Country: None
[*] Host: analytics.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

[*] Country: None
[*] Host: drealed.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

[*] Country: None
[*] Host: hkrb.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

[*] Country: None
[*] Host: hmrc.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

[*] Country: None
[*] Host: phonecorp.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

SUMMARY
[*] 5 total (0 new) hosts found.
[recon-ng][default][hackertarget] >
  
```

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.

```

SUMMARY
[*] 5 total (0 new) hosts found.
[recon-ng][default][hacktarget] > dashboard

```

Activity Summary		
Module	Runs	
discovery/info_disclosure/interesting_files	2	
recon/domains-hosts/bing_domain_web	1	
recon/domains-hosts/hacktarget	2	
recon/domains-hosts/netcraft	1	

Results Summary		
Category	Quantity	
Domains	0	
Companies	0	
Netblocks	0	
Locations	0	
Vulnerabilities	0	
Ports	0	
Hosts	5	
Contacts	0	
Credentials	0	
Leaks	0	
Pushpins	0	
Profiles	0	
Repositories	0	

```

[recon-ng][default][hacktarget] >

```

Fig. 3. Activity summary dashboard confirming database updates.

```

[recon-ng][default][hacktarget] > show hosts

```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	analytics.hackxor.net	138.68.117.124						hacktarget
2	dreaded.hackxor.net	138.68.117.124						hacktarget
3	hkrb.hackxor.net	138.68.117.124						hacktarget
4	hmrc.hackxor.net	138.68.117.124						hacktarget
5	phonecorp.hackxor.net	138.68.117.124						hacktarget

```

[*] 5 rows returned
[recon-ng][default][hacktarget] >

```

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.

```

[recon-ng][default][hacktarget] > modules load interesting_files
[recon-ng][default][interesting_files] > options set source hackxor.net
[recon-ng][default][interesting_files] > run
[*] http://hackxor.net:80/robots.txt => 200. 'robots.txt' found!
[*] http://hackxor.net:80/sitemap.xml => 404
[*] http://hackxor.net:80/sitemap.xml.gz => 404
[*] http://hackxor.net:80/crossdomain.xml => 404
[*] http://hackxor.net:80/pipinfo.php => 404
[*] http://hackxor.net:80/test.php => 404
[*] http://hackxor.net:80/elmah.axd => 404
[*] http://hackxor.net:80/server-status => 404
[*] http://hackxor.net:80/jmx-console/ => 404
[*] http://hackxor.net:80/web-console/ => 404
[*] 1 interesting files found.
[*] Files downloaded to /home/kali/.recon-ng/workspaces/default/
[recon-ng][default][interesting_files] >

```

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/>