



Custom Reconnaissance Tool Development

ITSolera internship

AUTHOR: SUHAILA ADEL ALI

DATE: 13TH JUNE 2025

TOOL NAME: ITSOLERA RECON SCANNER

INTERNSHIP PROGRAM: ITSOLERA CYBER DEPARTMENT – SUMMER INTERNSHIP 2025

Table of Contents

Executive Summary	2
Technical Details	3
Key Features	2
• Modular CLI Interface	2
• Execution Method.....	2
• Passive Recon Modules	2
• Active Recon Modules.....	2
Output Summary	3
Screenshots & Evidence	5
Conclusion	7

Executive Summary

This report documents the development and execution of a custom reconnaissance tool, ITSOLERA Recon Scanner, created for the ITSOLERA Cyber Department Internship.

It is a custom-built reconnaissance and information gathering tool developed as part of the ITSOLERA Cyber Department Summer Internship program. Designed in Python, the tool combines passive and active reconnaissance techniques to streamline and automate the initial phase of a cybersecurity assessment. This tool simplifies the reconnaissance process by automating data collection from various open sources and direct probes. It is designed for penetration testers, security analysts, and ethical hackers to quickly gather intelligence on a target domain during the early stages of an engagement.

This is the GitHub link of the project: <https://github.com/Suhaila2Adel/Reconnaissance-Automated-Tool>

Key Features

- **Modular CLI Interface**

Each feature can be executed independently using command-line flags, enabling flexible workflows and targeted operations.

- **Execution Method**

The tool was executed using specific CLI flags to activate modules (through the terminal).

```
python main.py example.com --whois --dns --subdomains --ports  
--dirs -vulns
```

- **Passive Recon Modules**

- **WHOIS Lookup:** Extracts domain registration and ownership details.
- **DNS Enumeration:** Retrieves A, MX, TXT, and NS records.
- **Subdomain Enumeration:** Gathers subdomains using sources like crt.sh and HackerTarget.

- **Active Recon Modules**

- **Port Scanning:** Uses nmap to detect open TCP ports and services.
- **Directory & File Enumeration:** Probes for common files and paths using HTTP requests.

- **Basic Vulnerability Scanning:** Identifies exposed sensitive files and misconfigurations.

Technical Details

- **Language:** Python 3.12
- **Libraries used:** whois, dnspython, requests, nmap, yaml, argparse
- **Platform:** PyCharm, Windows 11
- **Tool structure:** main.py + providers/ modules

Task1ITSolera/

```
├── main.py
├── providers/
│   ├── __init__.py
│   ├── whois_lookup.py
│   ├── dns_enum.py
│   ├── crtsh.py
│   ├── hackertarget.py
│   ├── active_recon.py
│   ├── port_scan.py
│   ├── dir_enum.py
│   └── vul_scan.py
```

- **Configuration:** sources.yaml for API toggles
- **Output:** appears in the terminal and this detailed pdf report for the selected target.

Output Summary

- **Target:** Hilton.io
I got this target from HackerOne platform, a real-world bug bounty platform.
- **Open Ports:** No open ports found
- **Subdomains Found:**
 - api-s.hilton.io
 - api-t.hilton.io
 - api.hilton.io
 - apicmgmt-prv.hilton.io
 - apim.pep-s.hilton.io
 - apim.pep.hilton.io
 - developer.hilton.io
 - m.hilton.io
 - m.stg.hilton.io
 - m.test.hilton.io

Custom Reconnaissance Tool Development- Task 1

- pep-s.hilton.io
- pep.hilton.io
- **Vulnerabilities:** No vulnerabilities found
- **Directory and File Enumeration:** No significant directories or files found

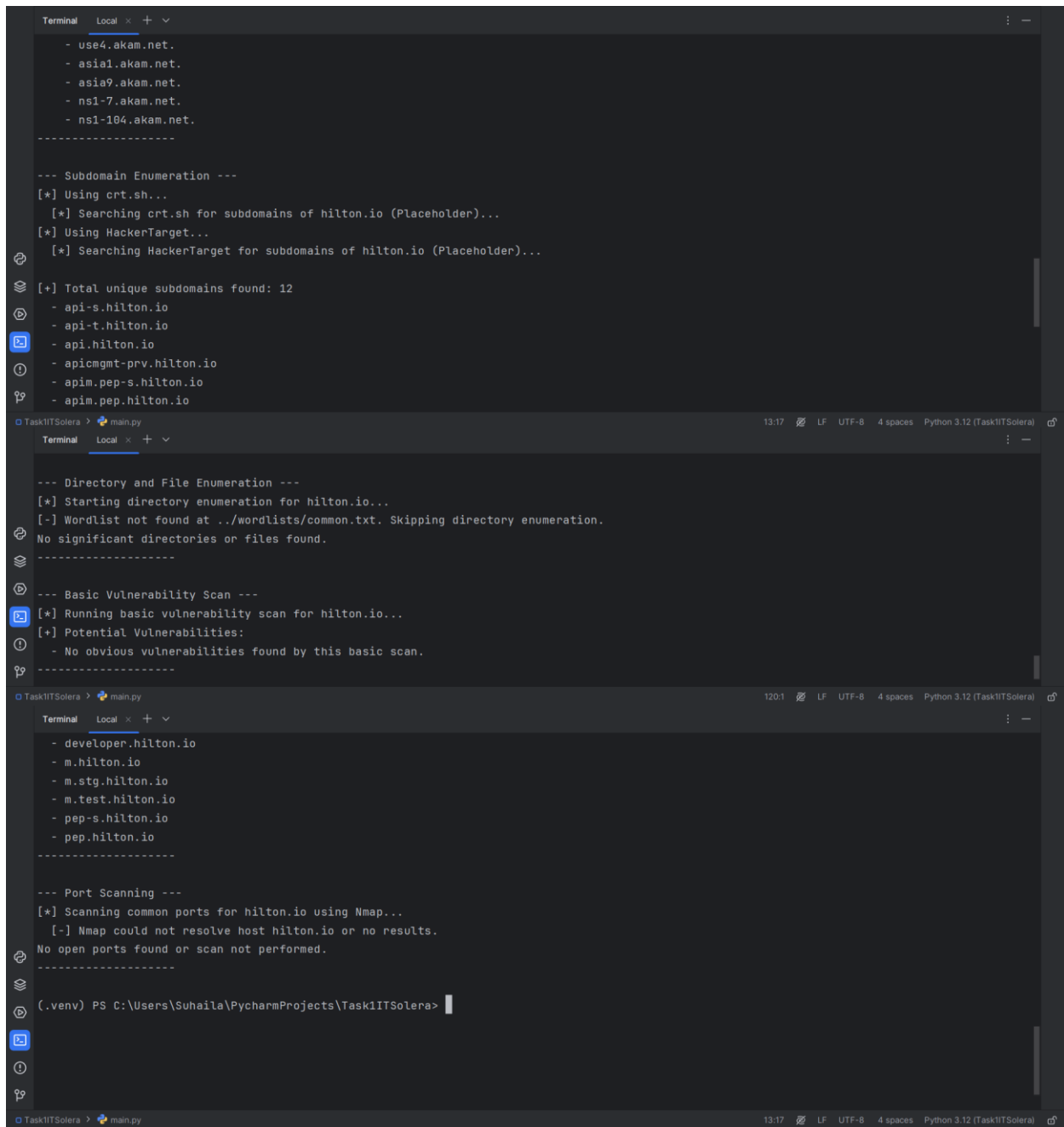
Screenshots & Evidence

```
(.venv) PS C:\Users\Suhaila\PycharmProjects\Task1ITSolera> python main.py hilton.io --whois --dns --subdomains --ports
[*] Starting reconnaissance for: hilton.io

--- WHOIS Lookup ---
[*] Performing WHOIS lookup for hilton.io (Placeholder)...
{
  "domain_name": "hilton.io",
  "domain__id": "66b712fd6ebe4b26b36841d5e7bc32b3-DONUTS",
  "registrar": "MarkMonitor, Inc.",
  "registrar_id": "292",
  "registrar_url": "http://www.markmonitor.com",
  "status": [
    "clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited",
    "clientTransferProhibited https://icann.org/epp#clientTransferProhibited",
    "clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited",
    "clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)",
    "clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)",
    "clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)"
  ],
  "registrant_name": "Hilton Worldwide Manage Limited",
  "registrant_state_province": "Hertfordshire",
  "registrant_country": [
    "GB",
    "UK"
  ],
  "name_servers": [
    "eur5.akam.net",
    "asia1.akam.net",
    "eur6.akam.net",
    "use1.akam.net",
    "asia9.akam.net",
    "ns1-7.akam.net",
    "use4.akam.net",
    "ns1-104.akam.net"
  ],
  "creation_date": [
    "2003-06-22 01:00:00",
    "2003-06-22 01:00:00+00:00"
  ],
  "expiration_date": "2026-06-21 01:00:00",
  "updated_date": [
    "2025-05-25 09:02:17",
    "2025-05-20 09:02:01+00:00"
  ]
}

--- DNS Enumeration ---
[*] Enumerating DNS records for hilton.io (Placeholder)...
A Records:
No records found
MX Records:
No records found
TXT Records:
- "sc2zh0xfh17msqr6lx4v83fzh8kvvx9g"
NS Records:
- eur5.akam.net.
- eur6.akam.net.
- use1.akam.net.
```

Custom Reconnaissance Tool Development- Task 1



```
Terminal Local x + v
- use4.akam.net.
- asia1.akam.net.
- asia9.akam.net.
- ns1-7.akam.net.
- ns1-104.akam.net.
-----

--- Subdomain Enumeration ---
[*] Using crt.sh...
[*] Searching crt.sh for subdomains of hilton.io (Placeholder)...
[*] Using HackerTarget...
[*] Searching HackerTarget for subdomains of hilton.io (Placeholder)...

[+] Total unique subdomains found: 12
- api-s.hilton.io
- api-t.hilton.io
- api.hilton.io
- apicmgt-prv.hilton.io
- apim.pep-s.hilton.io
- apim.pep.hilton.io

Task1ITSolera > main.py 13:17 LF UTF-8 4 spaces Python 3.12 (Task1ITSolera)

Terminal Local x + v

--- Directory and File Enumeration ---
[*] Starting directory enumeration for hilton.io...
[-] Wordlist not found at ../wordlists/common.txt. Skipping directory enumeration.
No significant directories or files found.
-----

--- Basic Vulnerability Scan ---
[*] Running basic vulnerability scan for hilton.io...
[+] Potential Vulnerabilities:
- No obvious vulnerabilities found by this basic scan.
-----

Task1ITSolera > main.py 12:01 LF UTF-8 4 spaces Python 3.12 (Task1ITSolera)

Terminal Local x + v

- developer.hilton.io
- m.hilton.io
- m.stg.hilton.io
- m.test.hilton.io
- pep-s.hilton.io
- pep.hilton.io
-----

--- Port Scanning ---
[*] Scanning common ports for hilton.io using Nmap...
[-] Nmap could not resolve host hilton.io or no results.
No open ports found or scan not performed.
-----

(.venv) PS C:\Users\Suhaila\PycharmProjects\Task1ITSolera>
```

Conclusion

The **ITSOLERA Recon Scanner** effectively consolidates essential reconnaissance tasks into a single, modular, and automated Python tool. Through its command-line interface, the tool enables targeted passive and active information gathering — including WHOIS lookups, DNS enumeration, subdomain discovery, ports scanning and basic vulnerability checks.

By leveraging reliable OSINT sources and tools such as crt.sh, HackerTarget, and Nmap, the scanner provides actionable insights that are critical in the early phases of penetration testing and red team operations. It also enhances productivity by generating structured reports with timestamps and module-specific results.

The modularity of the tool allows for easy extensibility and selective execution of recon modules, which is especially beneficial for scalable, real-world assessments. The logging feature adds another layer of professionalism and control, enabling analysts to trace tool behavior and debug effectively.

This project demonstrates both technical capability and practical awareness of cybersecurity workflows. It meets the deliverables outlined by the internship and lays the groundwork for future enhancements.