SPYGLASS TOOL

Introduction

Knowing your digital footprint in today's cybersecurity landscape is important. SpyGlass is a free, open-source Python OSINT tool written for security professionals and ethical hackers. It has the ability to automate the collection of emails, subdomains, open ports, exposed directories, technology stacks, GeoIP data and keyword search. SpyGlass can be used by organizations to see what information about them is publicly visible before it's used by attackers.

Major Threats

- **Sensitive Data Exposure:** Leaked emails, admin panels, or backups [1].
- **Subdomain Enumeration:** Shadow IT and internal system mapping [2].
- **Technology Fingerprinting:** Tech stack exposure, which aids in targeted exploitation.
- **Attack Surface Mapping:** Open ports and attack entry points.
- **Reconnaissance for Hacking:** helps preempt attacks (phishing, brute-force, SQLi, etc.).
- **Keyword Leakage:** Sensitive words like "password" or "admin" revealed in files or code [4].

SpyGlass can exploit: Exposed email addresses, Subdomains, Open ports, exposed directories, technology stacks, GeoIP data, and Keyword Leakages.

Countermeasures

- **Close Unused Ports:** Use firewalls to restrict outside access [2].
- **Monitor and Delete Unused Subdomains:** Disable directory listings and remove unused endpoints [2].
- **Hide Sensitive Files/Emails:** Avoid emailing addresses and config files on public websites.
- **Apply HTTPS/TLS Everywhere:** Encrypt all services to stop sniffing [3].
- **Deploy WAF/IDS:** Install Web Application Firewalls and Intrusion Detection Systems [4].
- **Regular Security Audits:** Scan files prior to publishing; monitor for leaks [5].

Similar Tools

theHarvester:

- Collects emails, subdomains, and hosts from public sources for a given domain.
- Supports a wide range of data sources.
- Simple command-line interface.
- Outputs can be saved in various formats.

Task Analysis: Main Commands

- theHarvester -d example.com -b bing

Finds emails and hosts using Bing as the data source.

- theHarvester -d example.com --shodan

Queries Shodan for open ports on discovered hosts.

- theHarvester -d example.com --screenshot /path/to/folder

Takes screenshots of found subdomains and saves them to a folder.

- theHarvester -d example.com --dns-brute

Performs DNS brute-forcing to find additional subdomains.

Output:

When you run these commands, theHarvester will show you a list of emails, hosts, or subdomains it found. If you use the --shodan option, it will also show any open ports it found using Shodan. You can save all this information into text, HTML, or CSV files.

Recon-ng

- Modular web reconnaissance framework for advanced OSINT.
- Supports scripting, automation, and session management.
- Wide library of modules.
- Highly customizable with workspace support for multiple projects.

Task Analysis: Main Commands

- workspaces create project_name

Starts a new project workspace.

- modules load recon/domains-hosts/hackertarget

Loads a module for subdomain enumeration.

- options set SOURCE example.com

Sets the target domain for the loaded module.

- run

Executes the loaded module and outputs results.

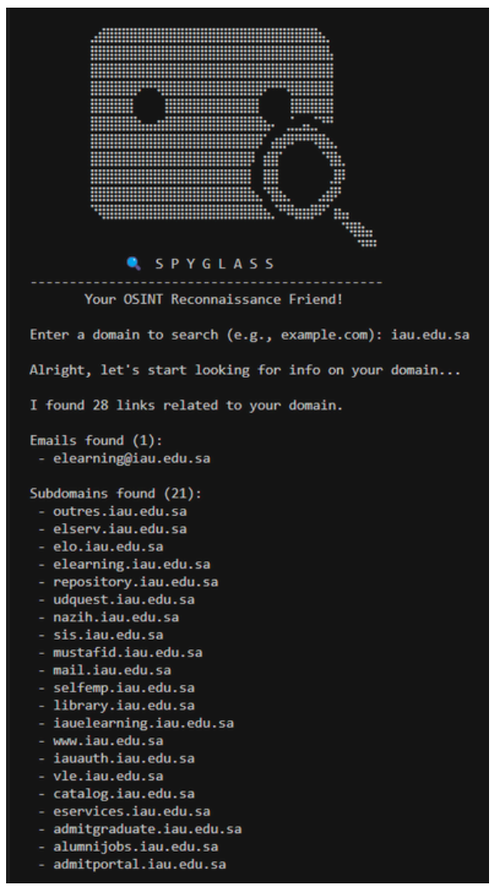
Output:

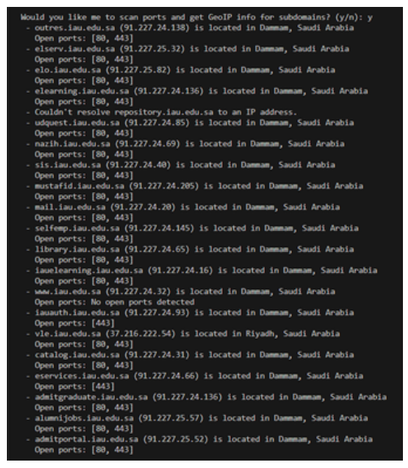
Recon-ng will print the found subdomains or hosts in a table right in your terminal. You can also save these results if you need them. What you see will depend on which Recon-ng module you use.

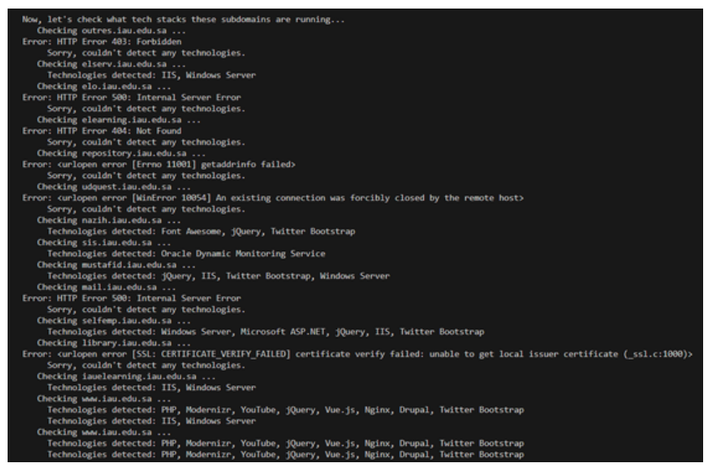
Table 1. Comparison Table

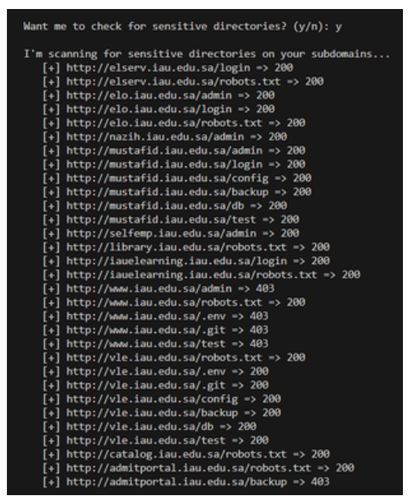
Feature	SpyGlass	theHarvester	Recon-ng
Emails	Yes	Yes	Yes
Subdomains	Yes	Yes	Yes
Directory Scan	Yes	No	With modules
Technology Scan	Yes	No	With modules
Port Scan	Yes	No	With modules
Output Formats	TXT, HTML, CSV	TXT, HTML, CSV	Various
Ease of Use	Friendly	Simple	Advanced

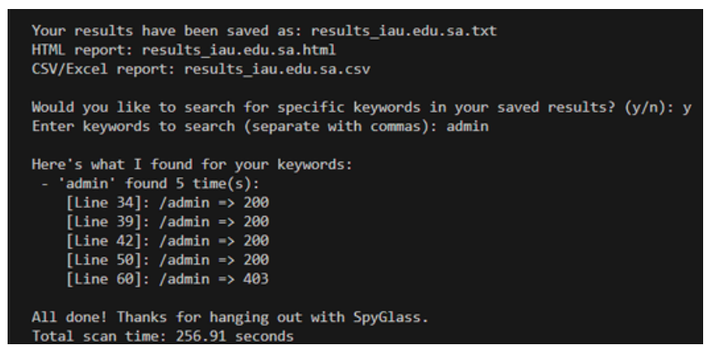
SpyGlass Output











References

[1] Gowranga, "What is Reconnaissance in Cyber Security? Definition, Types & Examples - CCSLA Learning Academy," CCSLA Learning Academy, Feb. 07, 2025. https://www.ccslearningacademy.com/what-is-reconnaissance-in-cyber-security/

[2] "OSINT Framework." https://osintframework.com/

[3] "Welcome to Scapy's documentation! — Scapy 2.6.1 documentation." https://scapy.readthedocs.io/en/latest/

[4] "OWASP Top Ten | OWASP Foundation." https://owasp.org/www-project-top-ten/

[5] X. Yang, Y. Liu, and J. Xie, "Information leakage detection and risk assessment of intelligent mobile devices," Mathematics, vol. 10, no. 12, p. 2011, Jun. 2022, doi: 10.3390/math10122011.

[6] Laramies, "GitHub - laramies/theHarvester: E-mails, subdomains and names Harvester - OSINT," GitHub. https://github.com/laramies/theHarvester

[7] Lanmaster, "GitHub - lanmaster53/recon-ng: Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.," GitHub. https://github.com/lanmaster53/recon-ng