3.1.4 **OSINT Tools Laboratory Report**

Lab Title: Using OSINT Tools for Penetration Testing

Date: August 5, 2025

Student: Carol Macharia 66

Course:

**Executive Summary**

This laboratory exercise provided hands-on experience with foundational Open Source Intelligence (OSINT) tools and techniques used in penetration testing. The lab demonstrated that a significant amount of actionable intelligence can be gathered from publicly available sources, revealing the digital footprint and potential attack surface of an organization. Key activities included exploring the OSINT Framework, performing automated reconnaissance with **SpiderFoot**, executing modular scans with **Recon-ng**, and discovering sensitive file disclosures. The findings underscore the critical role of OSINT in the initial phases of a security assessment and highlight the need for organizations to actively manage their public information exposure.

**Lab Objectives**

The primary objectives of this lab were successfully met:

1. **Examine OSINT resources** and frameworks to understand the landscape of available tools.
2. **Use SpiderFoot** for broad, automated intelligence gathering against a target domain.
3. **Investigate Recon-ng's** modular framework for targeted, organized reconnaissance.
4. **Find interesting files** to identify potential information disclosure vulnerabilities.
5. Understand how to map the **digital footprint** and data exposure of a target.

**Part 1: OSINT Resources and Frameworks**

The initial phase involved exploring web-based OSINT resources that serve as directories and search aggregators.

1. **OSINT Framework (osintframework.com)**: This resource provides a comprehensive, tree-structured visualization of OSINT tools, categorized by the type of information sought (e.g., Username, Domain Name, Email Address). It serves as an excellent starting point for identifying the right tool for a specific intelligence-gathering task.
2. **WhatsMyName (whatsmyname.app)**: This tool was used to check for the existence of specific usernames across hundreds of websites and social media platforms. The results can be filtered and exported, making it efficient for mapping the online presence of target individuals.
3. **SMART (smart.myosint.training)**: An aggregated resource tool that searches a community-curated collection of OSINT bookmarks. This proved useful for discovering lesser-known or specialized tools by searching for terms like "usernames".

**Key Findings: Value of Account Enumeration**

Username searching and account enumeration are highly valuable in penetration testing. As demonstrated in the lab, these techniques can identify accounts associated with enterprise personnel on various sites. This information is critical as it can reveal personal details, interests, and affiliations that can be leveraged in sophisticated **social engineering attacks**. Furthermore, if any of these external accounts are compromised, it could lead to password reuse attacks against corporate systems.

**Part 2: SpiderFoot Automated OSINT Scanner**

SpiderFoot is a powerful, automated OSINT tool that queries over 200 sources to gather intelligence on a target.

**Setup and Scan Configuration**

SpiderFoot was launched from the Kali terminal, and its web interface was accessed locally.

* **Launch Command**: spiderfoot -l 127.0.0.1:5001
* **Web UI**: http://127.0.0.1:5001

A **Footprint** scan was initiated against the target h4cker.org. This scan type is designed to map a target's network perimeter and associated identities using extensive web crawling and search engine queries. Other available scan types include *Passive* (for stealth), *Investigate* (for suspected malicious targets), and *All* (most comprehensive).

**Module and API Analysis**

SpiderFoot's capabilities are driven by its modules. Many modules are enhanced by integrating API keys, which often requires free registration with the respective services.

| Information Type | Scanner/Module Name | API Key Required? | Comments |
| --- | --- | --- | --- |
| Account Discovery | Account Finder (sfp\_accounts) | No | Searches over 200 sites like Reddit and eBay. |
| Email Discovery | Hunter.io | Yes (Free Plan) | Enumerates email addresses associated with a domain. |
| Web Technologies | Builtwith | Yes (Free Plan) | Identifies the software and technologies used by a website. |
| Geolocation | ipapi.com (sfp\_ipapicom) | Yes (Free Plan) | Provides geolocation data for IP addresses. |
| Data Breach Info | IntelligenceX (sfp\_intellx) | Yes (Free) | Searches for data leaks and breaches. |

After a 30-minute scan, SpiderFoot collated a wide array of data on h4cker.org, including subdomains, associated email addresses, and potential data leaks identified by the sfp\_intellx module, which linked to the original leaked information.

**Part 3: Recon-ng Modular Framework**

Recon-ng is a command-line framework for web-based reconnaissance, notable for its modularity and structured workflow using workspaces.

**Workspace and Module Management**

Workspaces allow for the isolation of projects, preserving module configurations and results separately for each engagement.

* **Initial State**: Recon-ng starts without any modules installed.
* **Marketplace**: Modules are installed from the marketplace, a GitHub repository of community-developed tools.
* **Key Commands**:

workspaces create test: Creates and switches to a new workspace.

marketplace install [module\_name]: Installs a module.

modules load [module\_name]: Loads a module into the current context.

options set [option] [value]: Configures the loaded module.

run: Executes the module.

**Comparative Host Discovery**

The hackertarget and bing\_domain\_web modules were installed and run against the target hackxor.net to discover subdomains, which Recon-ng classifies as "hosts".

1. **HackerTarget Module**:

**Module**: recon/domains-hosts/hackertarget

**Configuration**: options set SOURCE hackxor.net

**Results**: Discovered **9 hosts**.

1. **Bing Module**:

**Module**: recon/domains-hosts/bing\_domain\_web

**Configuration**: options set SOURCE hackxor.net

**Results**: Discovered **6 hosts**.

This discrepancy highlights the importance of using multiple modules for comprehensive coverage, as different data sources yield different results. The findings were viewed using the dashboard and show hosts commands, as well as the recon-web graphical interface.

**Part 4: Interesting Files Discovery**

To find potentially sensitive files, the interesting\_files module in Recon-ng was used.

**Module**: discovery/info\_disclosure/interesting\_files

**Purpose**: Scans a domain for files that could lead to information disclosure, such as log files, backup archives, configuration files, and documentation.

**Execution**: The module was loaded, the SOURCE was set to hackxor.net, and the scan was executed. The module successfully identified several files, including robots.txt, and generated a CSV report of its findings.

Discovering such files can expose sensitive information about web server configurations, application logic, and potentially credentials, creating significant security risks.

**Reflection and Conclusions**

This lab effectively demonstrated the power and utility of modern OSINT tools.

1. **Workspace Benefits**: The Recon-ng workspace feature is invaluable for organizing penetration testing engagements. It isolates data, tools, and configurations on a per-client or per-project basis, ensuring that results are not co-mingled and that workflows are repeatable.
2. **Modular Framework Advantages**: The modular architecture of tools like Recon-ng and SpiderFoot simplifies reconnaissance. By configuring options within a module's context, the execution command is simplified to run. This modularity also allows for easy extension and customization of the tool's capabilities.

In conclusion, this exercise affirmed that a wealth of information is publicly accessible to a determined adversary. The tools explored are not only essential for ethical hackers to identify weaknesses but also serve as a reminder for organizations to be vigilant about their digital footprint. Effective security posture management must include regular OSINT assessments to understand and mitigate the risks posed by publicly available information.

**Appendices**

**Appendix A: Command Reference**

**SpiderFoot Commands:**

bash

spiderfoot -l 127.0.0.1:5001 *# Start web interface*

spiderfoot -M | grep [term] *# Search modules via command line*

**Recon-ng Commands:**

bash

recon-ng *# Start framework*

workspaces create [name] *# Create workspace*

marketplace search [term] *# Search modules*

marketplace install [module] *# Install module*

modules load [module] *# Load module*

options set [option] [value] *# Set option*

run *# Execute module*

dashboard *# View results summary*

show [data\_type] *# Display specific data*

**Appendix B: Useful Resources**

* OSINT Framework: <https://osintframework.com/>
* WhatsMyName: <https://whatsmyname.app/>
* SMART Tool: <https://smart.myosint.training/>
* Recon-ng Marketplace: <https://github.com/lanmaster53/recon-ng-marketplace>
* SpiderFoot Documentation: <https://www.spiderfoot.net/documentation/>

**Appendix C: Ethical Considerations**

All reconnaissance activities performed in this laboratory were conducted against:

* Explicitly authorized targets (hackxor.net, h4cker.org)
* Educational/training environments
* With proper permissions and within legal boundaries