Lab Manual 3 : Reconnaissance & OSINT

Passive Information Gathering using WHOIS, DNS Lookups, and Metadata Extraction

---

Objective

To collect publicly available information about a target domain using passive reconnaissance methods such as WHOIS lookups, DNS record enumeration, and website metadata analysis.

Theory

In **Vulnerability Assessment and Penetration Testing (VAPT)**, the first stage is **reconnaissance** — gathering as much information about a target as possible before attempting any exploitation.
Passive reconnaissance focuses on collecting data without directly interacting with the target in a way that could alert them.

Key Concepts:

- **WHOIS Lookup**: Reveals registration details, owner information, and domain life cycle.
- **DNS Records**: Provide details about the infrastructure, such as IP addresses, mail servers, and security settings.
- **Website Metadata**: Offers insights into the site's structure, purpose, and sometimes technologies used.
- **Passive Reconnaissance**: Safe, legal, and uses publicly available sources.

Tools Required

- Google Colab (Python environment)
- WHOIS lookup tools/libraries
- DNS query utilities
- HTML parsing libraries
- Internet connection

Lab Setup

1. Open Google Colab from https://colab.research.google.com
2. Create a new notebook.
3. Install required Python libraries for WHOIS, DNS, and HTML parsing.
4. Select a target domain for analysis (e.g., india.gov.in, iitb.ac.in, tcs.com).

Procedure

1. **Identify the Target Domain**
    - Choose a domain you have permission to analyze or a public domain for passive reconnaissance.
2. **Perform WHOIS Lookup**
    - Retrieve details like registrar, registration date, expiration date, and name servers.
3. **Perform DNS Record Enumeration**
    - Collect A, MX, NS, and TXT records for the target domain.
    - Note down all the findings in a table format.
4. **Analyze Website Metadata**
    - Access the target's homepage and extract the page title, meta descriptions, and keywords.
5. **Document Findings**
    - Record the collected information in a structured observation table.

Observation Table Format

Parameter	Example Output
Registrar	RESERVED-Internet Assigned Numbers Authority
Creation Date	1995-08-14 04:00:00
Expiration Date	2025-08-13 04:00:00
Name Servers	['A.IANA-SERVERS.NET', 'B.IANA-SERVERS.NET']
A Record	23.192.228.80 23.192.228.84
MX Record	0
Title	Example Domain
Meta Description	--

Result

Thus we successfully scanned a website

Precautions

- Only perform reconnaissance on domains where it is legally allowed.
- Avoid any form of active scanning or exploitation without explicit permission.
- Handle any collected data responsibly and ethically.

Viva Questions

1. Differentiate between active and passive reconnaissance.
2. Explain the importance of WHOIS data in VAPT.
3. What information can you gather from DNS TXT records?
4. Why is metadata extraction useful for penetration testers?
