Passive Reconnaissance Practice Lab

This lab focuses on gathering publicly available information about **Pentest.TV** using passive reconnaissance techniques. The tools used are preconfigured in your Kali Linux environment.

Objectives

1. Extract domain registration and DNS information for pentest.tv.
2. Identify publicly visible subdomains and related infrastructure.
3. Gather indexed data like emails, metadata, and technology stack information.

Lab Workflow

Task 1: Perform WHOIS Lookup

Gather registration details for pentest.tv:

```
#whois pentest.tv
```

Objective: Identify registrar, nameservers, and domain status.

Task 2: Query DNS Records

Use dig and nslookup to query DNS information.

- Query DNS records for pentest.tv:

```
#dig pentest.tv any
#nslookup -type=any pentest.tv
```

Objective: Map DNS structure and identify records such as A, NS, and MX.

Task 3: Enumerate Subdomains

Use amass to passively enumerate subdomains.

```
#amass enum -passive -d pentest.tv
```

Objective: List subdomains and map potential attack vectors.

Task 4: Gather Emails and Metadata

Use theHarvester to collect emails and metadata from public sources.

```
#theHarvester -d pentest.tv -b all
```

Objective: Identify email addresses, hostnames, and related domains.

Task 5: Analyze Website Technologies

Run whatweb to analyze the technologies used on pentest.tv.

```
#whatweb https://pentest.tv
```

Objective: Understand the website's technology stack, including CMS, web server, and frameworks.

Task 6: Perform Search Engine Dorking

ON your local computer, use Google advanced search queries to discover sensitive data:

```
site:archive.org "admin"
intitle:"index of" site:archive.org
site:archive.org filetype:pdf
```

Objective: Locate hidden pages, indexed files, or exposed information.