**Day 3 - Ethical Hacking Series**

**📌 Topics Covered:**

1. **Google Dorking**
2. **Whois Lookup**
3. **DNS Reconnaissance**
   * host
   * nslookup
   * dig

**📍 1. Google Dorking (Google Hacking Database - GHDB)**

**✅ What is Google Dorking?**

Google Dorking is a technique used by ethical hackers to use advanced search operators on Google to find sensitive data, misconfigured servers, login portals, and exposed documents that are not usually visible.

**🔍 Common Google Dork Operators and Usage**

| **Operator** | **Description** | **Example** |
| --- | --- | --- |
| site: | Restricts search to a specific website | site:example.com |
| filetype: | Searches for specific file formats (PDF, DOCX, etc.) | filetype:pdf site:example.com |
| inurl: | Finds URLs containing certain keywords | inurl:login |
| intitle: | Finds pages with specific words in the title | intitle:"admin login" |
| allintitle: | Searches for pages with all specified words in the title | allintitle:admin login panel |
| intext: | Searches for specific text in the body of web pages | intext:"confidential document" |

**🧪 Realistic Example**

You want to find PDF reports on a university domain:

bash

CopyEdit

filetype:pdf site:ntu.edu.pk

Find exposed login pages:

bash

CopyEdit

inurl:login site:gov.pk

Find text leaks or passwords:

bash

CopyEdit

intext:"password" site:example.com

**📍 2. WHOIS Lookup**

**✅ What is Whois?**

whois is a tool that retrieves **domain registration information**:

* Owner name
* Registrar
* Expiry date
* Contact emails
* Nameservers

**🛠️ Command Syntax**

bash

CopyEdit

whois example.com

**🔍 Example Output:**

yaml

CopyEdit

Domain Name: EXAMPLE.COM

Registrar: XYZ Registrar

Name Server: NS1.EXAMPLE.COM

Updated Date: 2025-01-01

📌 **Note**: Some registrars hide data using privacy protection.

**📍 3. DNS Reconnaissance**

DNS recon helps gather valuable domain infrastructure data like IPs, mail servers, nameservers.

**🔹 A. host Command**

Used to perform DNS lookups.

**🛠️ Syntax:**

bash

CopyEdit

host example.com

host -t ns example.com # Find nameservers

host -t mx example.com # Find mail servers

**✅ Output:**

pgsql

CopyEdit

example.com name server = ns1.example.com

example.com mail is handled by 10 mail.example.com.

**🔹 B. nslookup Command**

Interacts with DNS servers and lets you query for specific record types.

**🛠️ Command Usage:**

bash

CopyEdit

nslookup

> set type=ns

> example.com

This lists **all nameservers** for the domain.

**Additional:**

bash

CopyEdit

> set type=mx

> example.com

**🔹 C. dig Command (Domain Information Groper)**

A powerful DNS lookup tool used in Kali Linux.

**🛠️ Common Commands:**

bash

CopyEdit

dig example.com

dig example.com -t ns # Get nameservers

dig example.com -t mx # Get mail servers

**✅ Sample Output:**

yaml

CopyEdit

;; ANSWER SECTION:

example.com. 3600 IN NS ns1.example.com.

**📦 DNS Record Types (Summary Table)**

| **Record Type** | **Description** |
| --- | --- |
| A | Maps domain to IPv4 address |
| AAAA | Maps domain to IPv6 address |
| CNAME | Alias for a domain |
| NS | Name server of the domain |
| MX | Mail server for handling emails |
| TXT | Misc. info like SPF, verification |
| SOA | Administrative info about domain zone |