Welcome to Cybersecurity and Ethical hacking

Sha jalal
Cybersecurity Expert and Ethical Hacker
Dept. Of Computer Science and Engineering (CSE) , University Of Chittagong

Introduction to Reconnaissance

- ✓ **Definition:**

  The process of gathering information about a target before attacking.

- ✓ **Goal:**

  Understand the environment and identify weak points.

- ✓ **Types:**
  - ❖ Passive Reconnaissance
  - ❖ Active Reconnaissance

Passive vs Active Reconnaissance

Feature	Passive Reconnaissance	Active Reconnaissance
Definition	No direct interaction with target	Direct interaction with target
Tools Used	WHOIS, Google, social media	ping, nslookup, port scanners
Risk Level	Low (stealthy)	High (may trigger alerts)
Example	Reading public DNS records	Scanning open ports

WHOIS Lookup

✓ **Purpose:** Obtain domain ownership details.

✓ **Here are the 10 important points from the WHOIS output:**

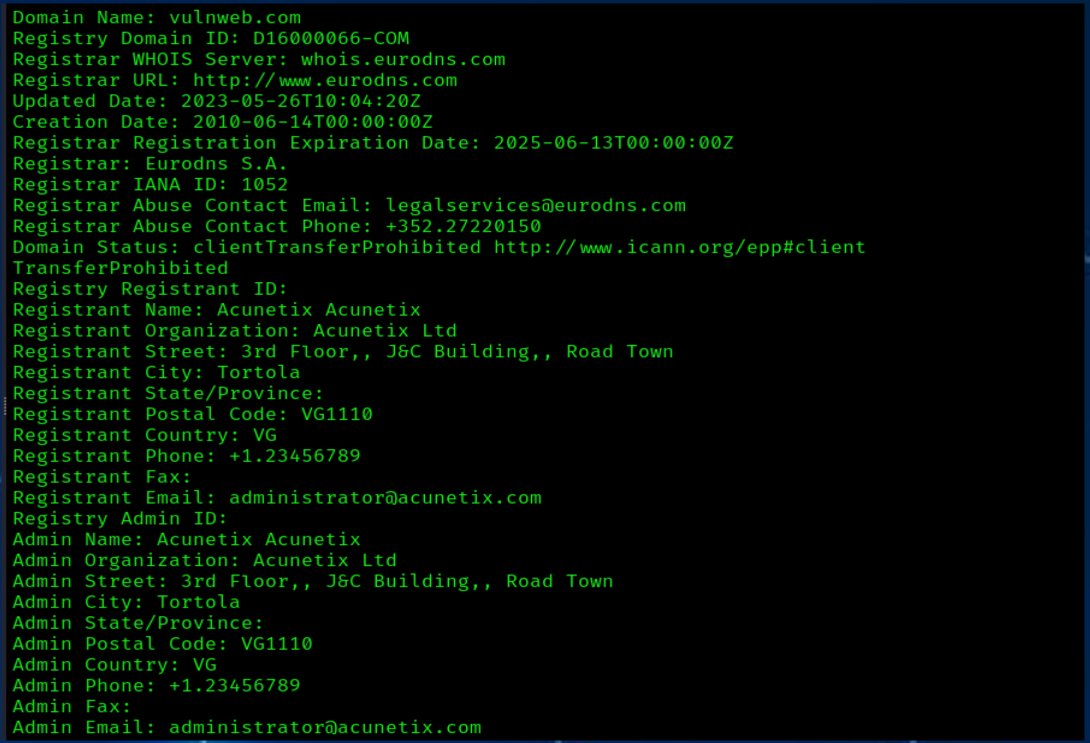
- ❖ **Domain Name**
- ❖ **Registry Domain ID**
- ❖ **Registrar Information**
- ❖ **Creation, Update, and Expiration Dates**
- ❖ **Domain Status**
- ❖ **Name Servers**
- ❖ **DNSSEC**
- ❖ **Registrant, Admin & Tech Contact**
- ❖ **Registrar Abuse Contact**
- ❖ **Legal Notice and Terms of Use**

WHOIS Lookup

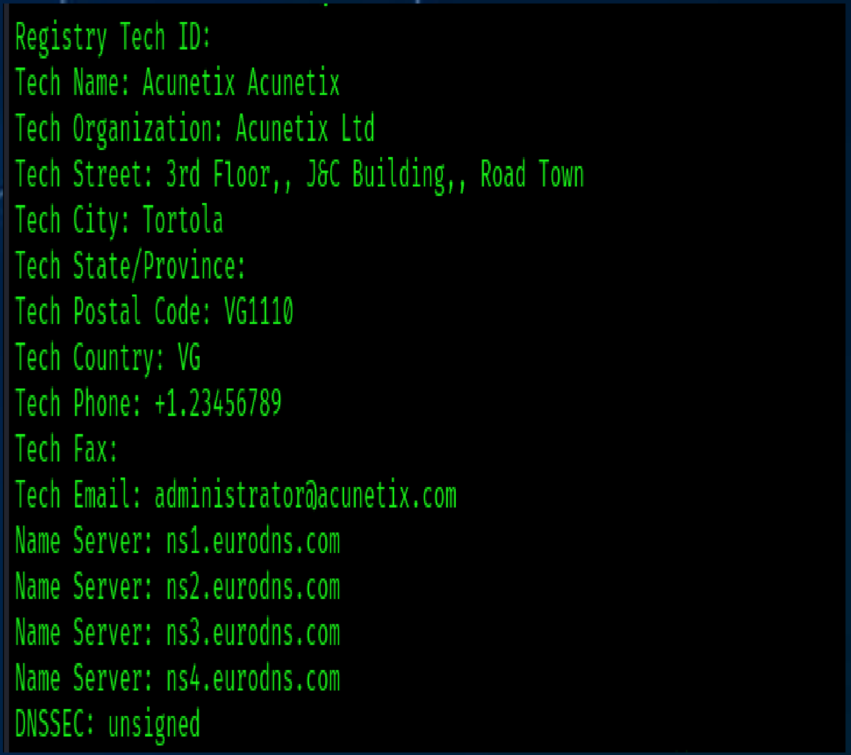
- ✓ **Command:**

```
whois vulnweb.com
```

- ✓ **Output:**



```
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#client
TransferProhibited
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
```



```
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
```

DNS Recon Tools – nslookup and dig

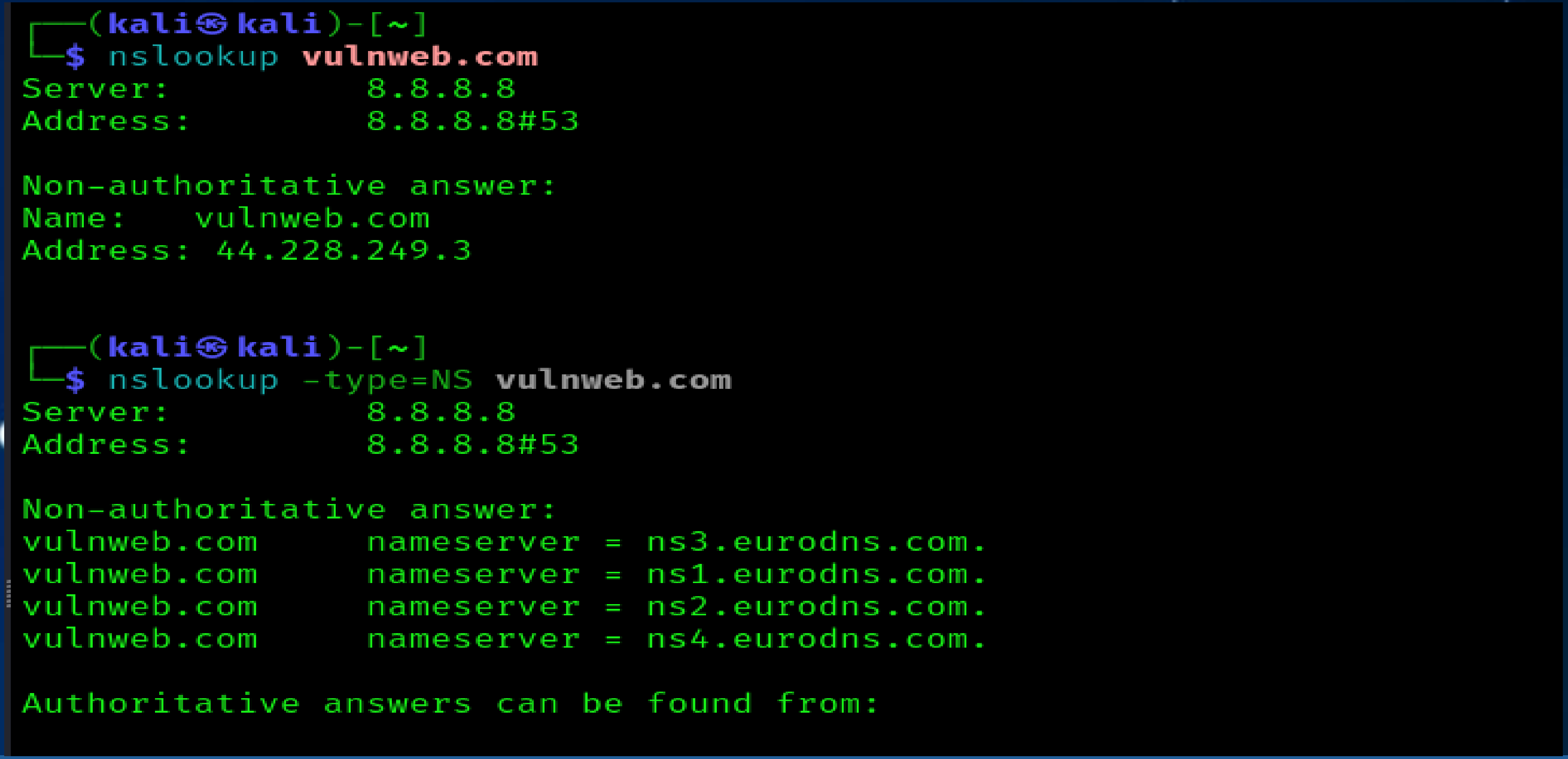
- **nslookup:**
  - Queries DNS to obtain domain-related record
  - Can resolve domain names to IPs.
- **dig** (Domain Information Groper):
  - More advanced than nslookup
  - Retrieves A, MX, TXT, and other DNS records.
- **Use:.**
  - Mapping a domain's structure

Nslookup(name Server Lookup)

- ✓ **Command:**

```
nslookup vulnweb.com
```

- ✓ **Output:**



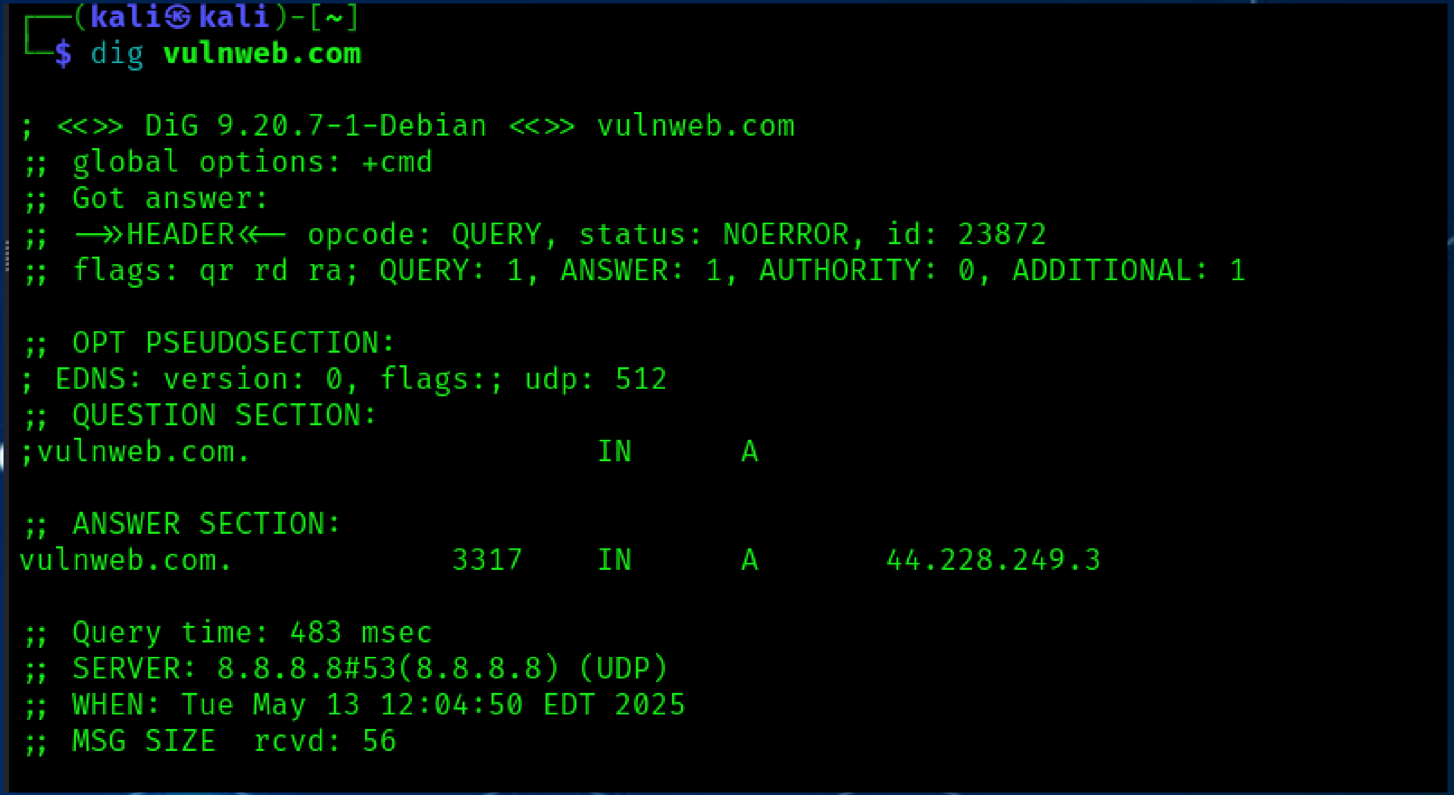
```
┌──(kali㉿kali)-[~]
└─$ nslookup vulnweb.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   vulnweb.com
Address: 44.228.249.3


┌──(kali㉿kali)-[~]
└─$ nslookup -type=NS vulnweb.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
vulnweb.com     nameserver = ns3.eurodns.com.
vulnweb.com     nameserver = ns1.eurodns.com.
vulnweb.com     nameserver = ns2.eurodns.com.
vulnweb.com     nameserver = ns4.eurodns.com.

Authoritative answers can be found from:
```

Dig(domain information groper)

- ✓ **Command:**

```
dig vulnweb.com
```

- ✓ **Output:**



```
┌──(kali㉿kali)-[~]
└─$ dig vulnweb.com

; <<>> DiG 9.20.7-1-Debian <<>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23872
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;vulnweb.com.                   IN      A

;; ANSWER SECTION:
vulnweb.com.            3317    IN      A       44.228.249.3

;; Query time: 483 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Tue May 13 12:04:50 EDT 2025
;; MSG SIZE  rcvd: 56
```

Google Dorking

- ✓ **Definition:** Using advanced Google search operators to find sensitive information.
- ✓ **Examples:**
  - ➢ **Find all indexed pages**
    `site:vulnweb.com`
  - ➢ **Find login pages**
    `site:vulnweb.com inurl:login`
  - ➢ **Find admin panels**
    `site:vulnweb.com inurl:admin`
  - ➢ **Find config files**
    `site:vulnweb.com ext:xml OR ext:conf`
  - ➢ **Search for password in logs**
    `site:vulnweb.com intext:password filetype:log`

Google Dorking

- ✓ **Examples:**
  - ➢ **Find backup files**
    site:vulnweb.com ext:bak OR ext:old OR ext:backup
  - ➢ **Search for SQL error messages**
    site:vulnweb.com intext:"You have an error in your SQL syntax"
  - ➢ **Find public documents**
    site:vulnweb.com filetype:pdf OR filetype:docx
  - ➢ **Find confidential info**
    site:vulnweb.com intext:"confidential" OR intext:"private"
  - ➢ **Check for SQL injection points**
    site:vulnweb.com inurl:"id=" intext:"sql"

- ✓ **Goal:** Discover exposed files, directories, and data.

The Deep Web

✓ **Definition:**

The deep web refers to parts of the internet that are not indexed by search engines, such as private databases, email accounts, and password-protected pages

✓ **Difference:**

❖ Surface Web: Accessible via Google.
❖ Deep Web: Behind logins, forms, databases.
❖ Dark Web : All .onion domain included

Recon-ng Framework

- ✓ **Description:**

  Recon-ng is a full-featured web reconnaissance framework written in Python. It's like Metasploit but for recon. It automates information gathering using modules..

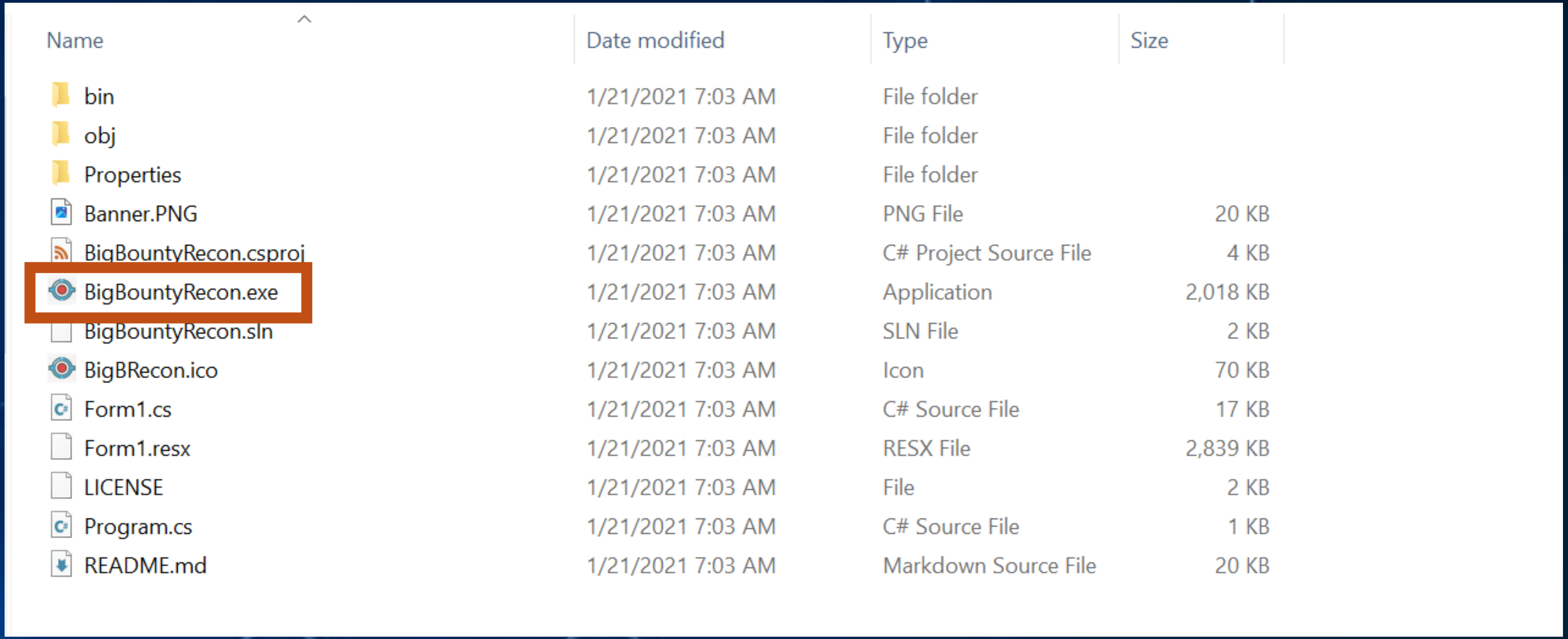
- ✓ **Features**:
  - ❖ Modular design (like Metasploit)
  - ❖ API support (e.g., for WHOIS, IPInfo)
  - ❖ Integration with external tools

- ✓ **Use:** Automate info gathering.

BigBounty Recon Practice in windows

- ✓ **Download Link:** **https://drive.google.com/drive/folders/12mTyI_RY5UB_jGxhU9ORI7N0YabrsWIQ?usp=sharing**

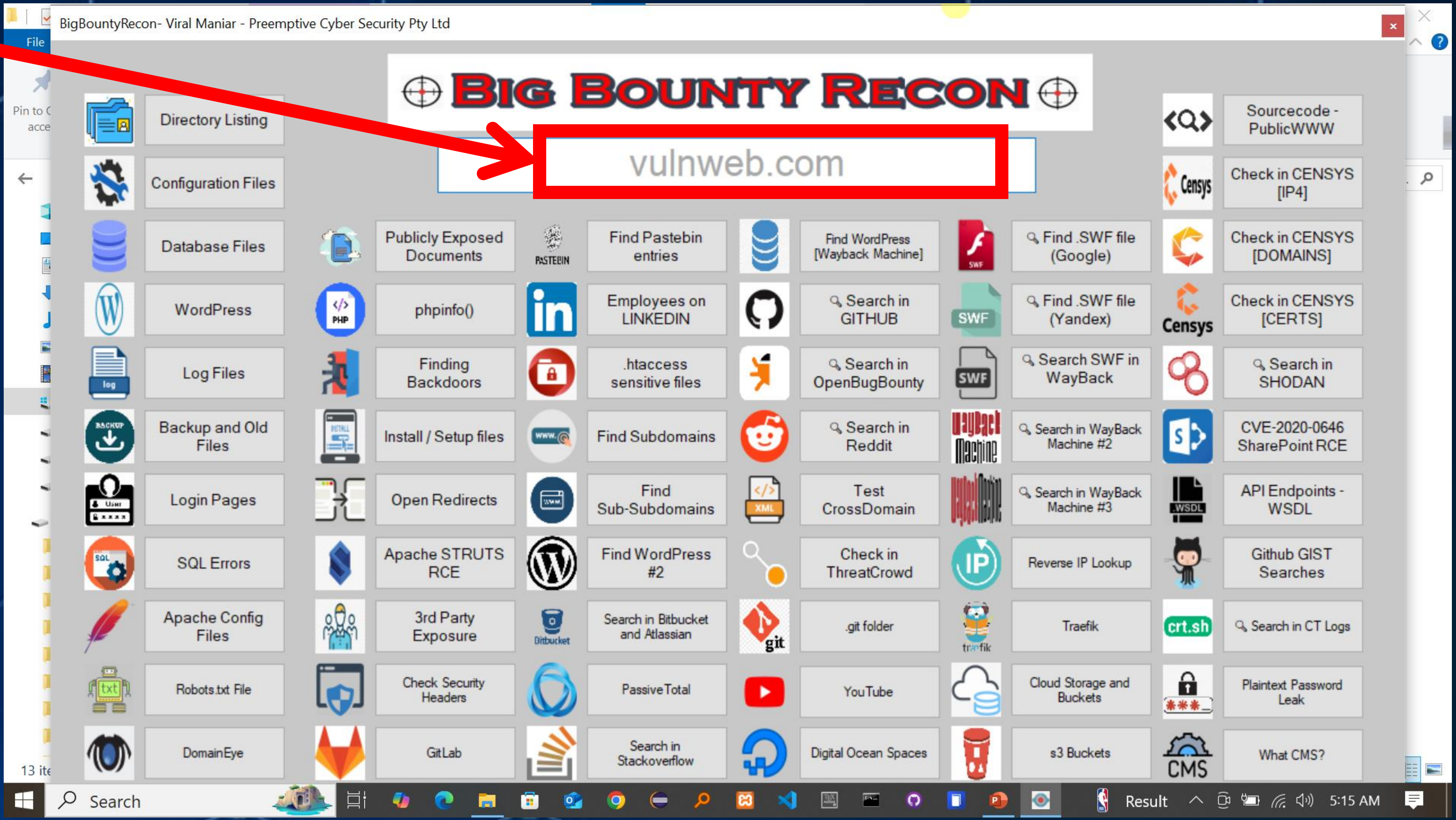
1st step:



Name	Date modified	Type	Size
bin	1/21/2021 7:03 AM	File folder	
obj	1/21/2021 7:03 AM	File folder	
Properties	1/21/2021 7:03 AM	File folder	
Banner.PNG	1/21/2021 7:03 AM	PNG File	20 KB
BigBountyRecon.csproj	1/21/2021 7:03 AM	C# Project Source File	4 KB
BigBountyRecon.exe	1/21/2021 7:03 AM	Application	2,018 KB
BigBountyRecon.sln	1/21/2021 7:03 AM	SLN File	2 KB
BigBRecon.ico	1/21/2021 7:03 AM	Icon	70 KB
Form1.cs	1/21/2021 7:03 AM	C# Source File	17 KB
Form1.resx	1/21/2021 7:03 AM	RESX File	2,839 KB
LICENSE	1/21/2021 7:03 AM	File	2 KB
Program.cs	1/21/2021 7:03 AM	C# Source File	1 KB
README.md	1/21/2021 7:03 AM	Markdown Source File	20 KB

BigBounty Recon Practice in windows

2nd step:



vulnweb.com

Maltego Tool

- ✓ **Description:** Open-source intelligence (OSINT) tool for graphical link analysis.
- ✓ **Features**:
  - ❖ Visual map of relationships
  - ❖ Entities: Domains, IPs, People, Emails, etc.
  - ❖ Transform-based querying
- ✓ **Use:** Analyze social networks, domains, organizations.

Summary & Best Practices

➢ Summary:

- Recon is the first step in ethical hacking.
- Passive recon is stealthy; active can trigger defenses.
- Use WHOIS, nslookup, dig, Google Dorks, and tools like Recon-ng & Maltego.

➢ Best Practices:

- Always follow legal/ethical guidelines.
- Combine tools for a complete picture.
- Document findings for later use.

Answer these questions

- ✓ ________ types of Reconnaissance perform in Cybersecurity.
- ✓ What is the Full Form of dig?
- ✓ Scanning open port is _______ Reconnaissance?
- ✓ Difference between deep web and Surface web.

PRESENTATION FINISHED
ANY QUESTIONS?
makeameme.org

The End

Thank You

Presented by:

Shajalal
Cybersecurity & Ethical Hacking Enthusiast
BSc in Engineering, University of Chittagong

Contact :01850989488
shajalal.cse.cu@gmail.com
https://www.linkedin.com/in/shajal-cse-cu/