🔎 The Reconnaissance Workflow: From Subdomains to Open Doors

This practical takes the foundational OSINT concepts you learned earlier and combines them into a cohesive, hands-on workflow. You've simulated the first crucial steps an ethical hacker or security professional would take to map out a target's digital footprint and find potential entry points.

Step 1: Subdomain Enumeration

What it is:

Subdomain enumeration is the process of finding all the "other" websites or services that belong to a single main domain. Think of the main domain, like `instagram.com`, as a large house. The subdomains, like `blog.instagram.com` or `dev.instagram.com`, are the different rooms or smaller buildings on the property.

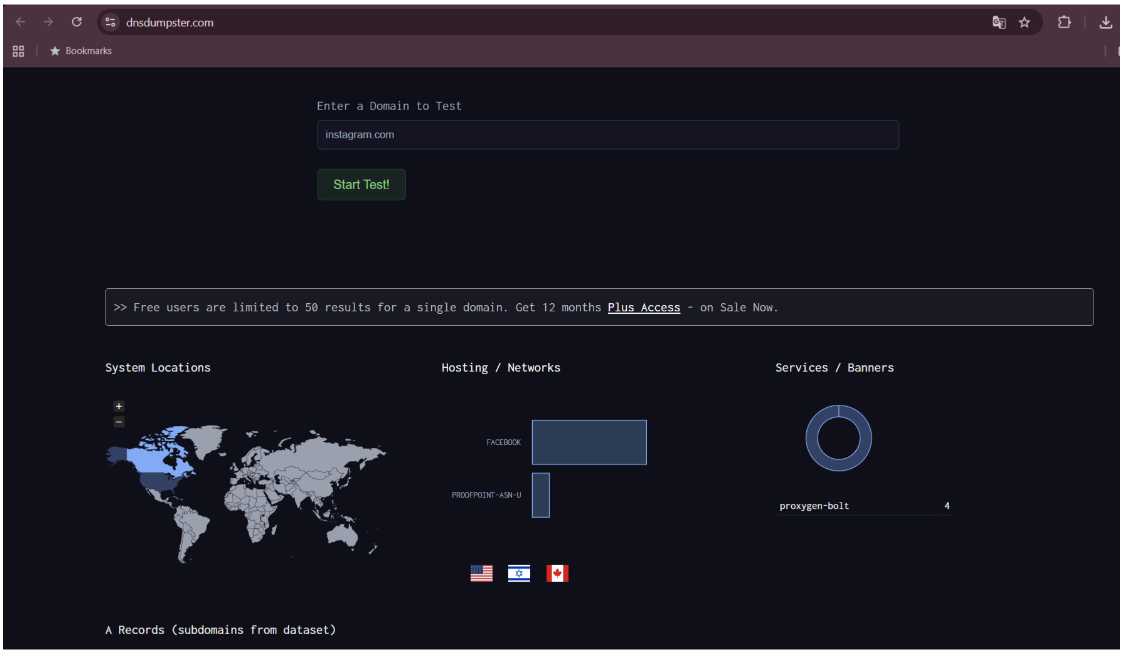
Why we do it:

An organization's main website is usually very well-defended. However, they might forget about a subdomain they set up years ago, or a testing server that's still publicly accessible. These "forgotten doors" are often less secure and can be a prime target for attackers. By finding them, you've expanded your potential attack surface.

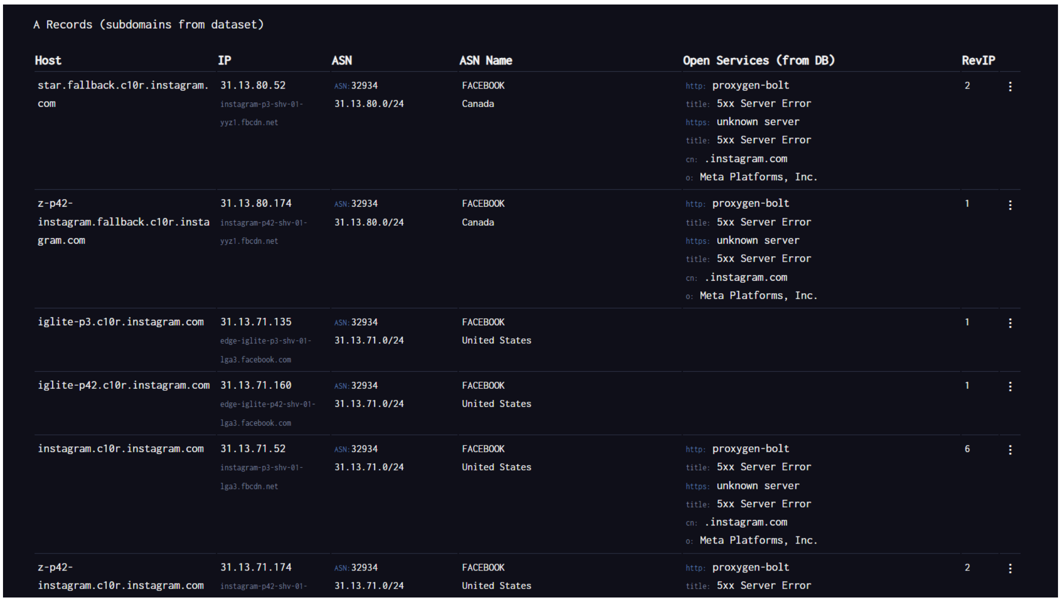
Tools & Techniques:

You used **Amass**, a powerful tool for this task. It works by gathering information from various public sources (like Certificate Transparency logs and DNS records) to build a comprehensive list of subdomains.

> **Tip:** You're not attacking anything here. You're just asking public databases, "Hey, what subdomains do you know about for this main domain?" This is a **passive** and safe way to gather information.



>> Free users are limited to 50 results for a single domain. Get 12 months Plus Access - on Sale Now.



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
star.fallback.c10r.instagram.com	31.13.80.52 instagram-p3-shv-01-yyz1.fbcdn.net	ASN:32934 31.13.80.0/24	FACEBOOK Canada	http: proxygen-bolt title: 5xx Server Error https: unknown server title: 5xx Server Error cn: .instagram.com o: Meta Platforms, Inc.	2
z-p42-instagram.fallback.c10r.instagram.com	31.13.80.174 instagram-p42-shv-01-yyz1.fbcdn.net	ASN:32934 31.13.80.0/24	FACEBOOK Canada	http: proxygen-bolt title: 5xx Server Error https: unknown server title: 5xx Server Error cn: .instagram.com o: Meta Platforms, Inc.	1
iglite-p3.c10r.instagram.com	31.13.71.135 edge-iglite-p3-shv-01-lga3.facebook.com	ASN:32934 31.13.71.0/24	FACEBOOK United States		1
iglite-p42.c10r.instagram.com	31.13.71.160 edge-iglite-p42-shv-01-lga3.facebook.com	ASN:32934 31.13.71.0/24	FACEBOOK United States		1
instagram.c10r.instagram.com	31.13.71.52 instagram-p3-shv-01-lga3.fbcdn.net	ASN:32934 31.13.71.0/24	FACEBOOK United States	http: proxygen-bolt title: 5xx Server Error https: unknown server title: 5xx Server Error cn: .instagram.com o: Meta Platforms, Inc.	6
z-p42-instagram.c10r.instagram.com	31.13.71.174 instagram-p42-shv-01-	ASN:32934 31.13.71.0/24	FACEBOOK United States	http: proxygen-bolt title: 5xx Server Error	2

Step 2: Verify Live Hosts

What it is:

Once you have a list of subdomains, not all of them will be active or "live." Some might be old or no longer in use. This step is about filtering out the inactive ones and only keeping the ones that actually exist and have a corresponding IP address. You are confirming that the "doors" you found are actually attached to a building.

Why we do it:

This is a crucial efficiency step. There's no point in spending time and resources scanning a target that doesn't exist. By only focusing on live hosts, you make your next steps faster and more effective.

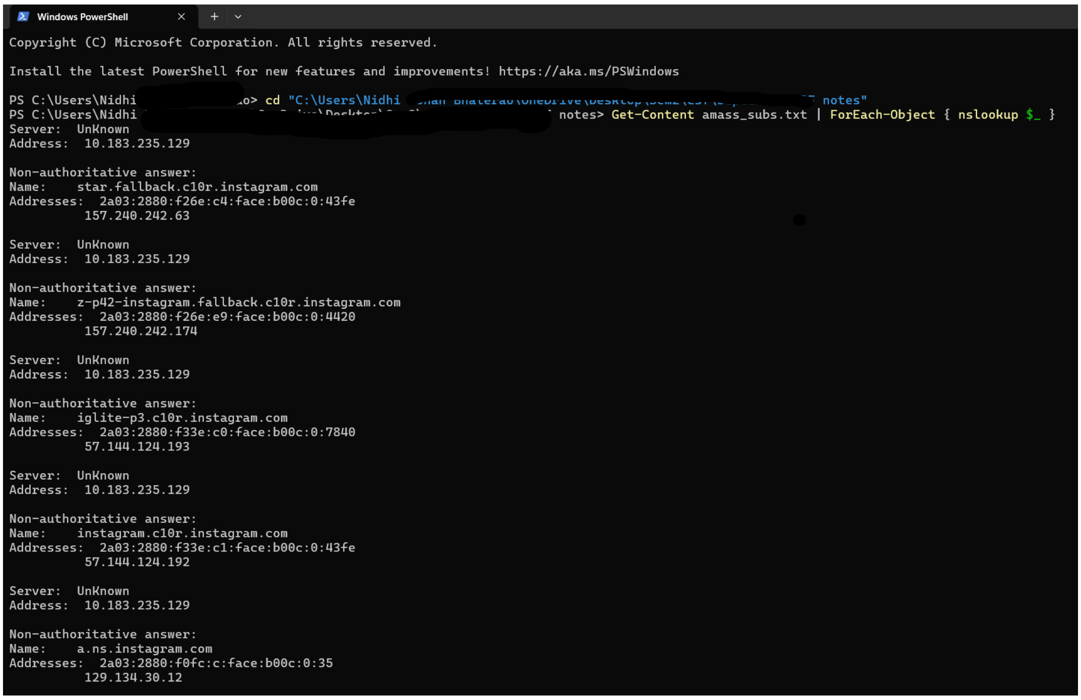
Tools & Techniques:

You used **`nslookup`** in a simple script to verify each subdomain.

- `nslookup` is a command-line tool that looks up an IP address for a given domain name.
- The `ForEach-Object` loop in PowerShell automated this process, running the command for every single subdomain you found in the previous step.

Diagram:

```
 List of Subdomains
 (amass_subs.txt)
+-----------------+
star.fallback.c10r.instagram.com
z-p42-instagram.fallback.c10r.instagram.com
iglite-p3.c10r.instagram.com
instagram.c10r.instagram.com
a.ns.instagram.com   |
+-----------------+
      |
      | nslookup
      v
  Verifying...
+-----------------+
| a.example.com ->[redacted](Live) |
| b.example.com -> No IP (Inactive) |
| c.example.com ->[redacted](Live) |
| d.example.com ->[redacted] (Live) |
+-----------------+
      |
      | Filter
      v
  List of Live IPs
 (live_ips.txt)
+-----------------+
157.240.242.[redacted]
157.240.242[redacted]
57.144.124.[redacted]
57.144.[redacted]
129.134.[redacted]
+-----------------+
```



```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Nidhi [redacted]o> cd "C:\Users\Nidhi [redacted] notes"
PS C:\Users\Nidhi [redacted] notes> Get-Content amass_subs.txt | ForEach-Object { nslookup $_ }
Server:  UnKnown
Address:  10.183.235.129

Non-authoritative answer:
Name:    star.fallback.c10r.instagram.com
Addresses:  2a03:2880:f26e:c4:face:b00c:0:43fe
          157.240.242.63

Server:  UnKnown
Address:  10.183.235.129

Non-authoritative answer:
Name:    z-p42-instagram.fallback.c10r.instagram.com
Addresses:  2a03:2880:f26e:e9:face:b00c:0:4420
          157.240.242.174

Server:  UnKnown
Address:  10.183.235.129

Non-authoritative answer:
Name:    iglite-p3.c10r.instagram.com
Addresses:  2a03:2880:f33e:c0:face:b00c:0:7840
          57.144.124.193

Server:  UnKnown
Address:  10.183.235.129

Non-authoritative answer:
Name:    instagram.c10r.instagram.com
Addresses:  2a03:2880:f33e:c1:face:b00c:0:43fe
          57.144.124.192

Server:  UnKnown
Address:  10.183.235.129

Non-authoritative answer:
Name:    a.ns.instagram.com
Addresses:  2a03:2880:f0fc:c:face:b00c:0:35
          129.134.30.12
```

Step 3: Port Scanning

What it is:

A **port scan** is like knocking on every single door and window of the buildings you just identified. Every IP address has thousands of "ports" (65,535, to be exact) that act as communication endpoints for different services. A port scan checks which of these ports are "open" and listening for connections.

Why we do it:

An open port means a service is running on that port. By identifying open ports, you know what services are exposed to the internet. For example:

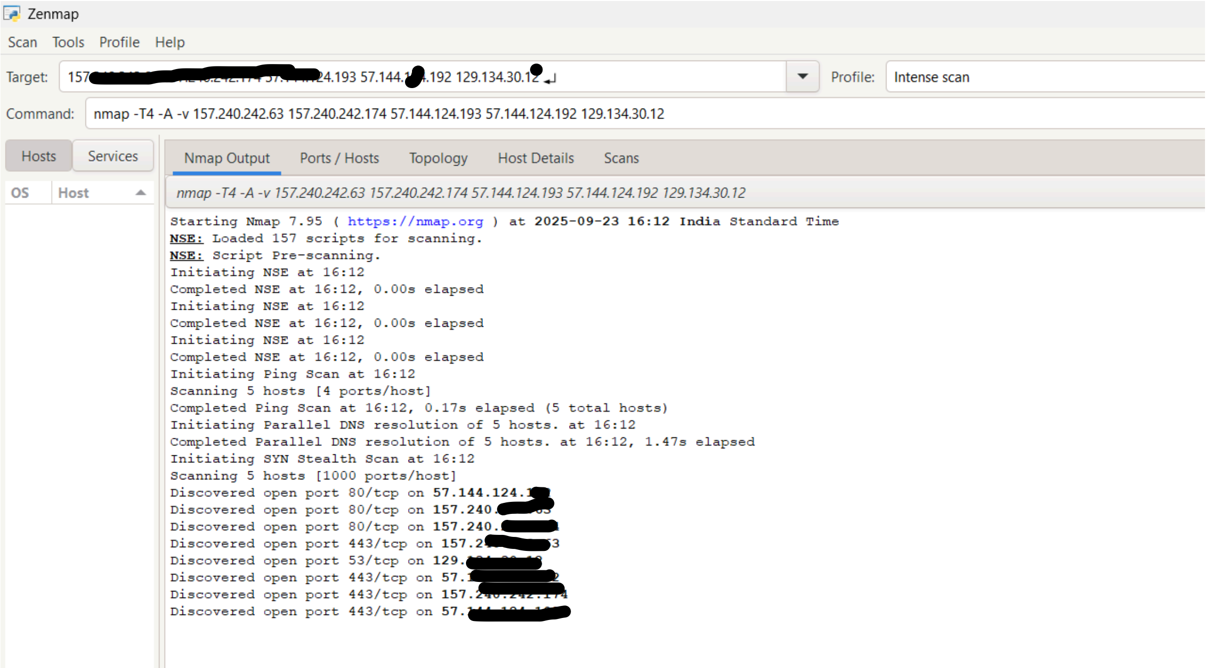
- **Port 80/tcp:** A web server (HTTP) is running here.
- **Port 443/tcp:** A secure web server (HTTPS) is running here.
- **Port 22/tcp:** A secure shell (SSH) service is running here, often used for remote access.

Finding an unusual open port (like an administrative panel or a database) is a major finding that can be a target for exploitation.

Tools & Techniques:

You used **Zenmap**, which is the graphical user interface (GUI) for **Nmap**, a famous port scanning tool.

Important Note: Unlike passive reconnaissance, port scanning is considered **active reconnaissance**. You are sending packets directly to the target's servers, and they will see that you are scanning them. This is why you should **only perform this step on targets you have permission to test**.



Target: 157[redacted]24.193 57.144.[redacted].192 129.134.30.12[redacted]

Profile: Intense scan

Command: nmap -T4 -A -v 157.240.242.63 157.240.242.174 57.144.124.193 57.144.124.192 129.134.30.12

```
nmap -T4 -A -v 157.240.242.63 157.240.242.174 57.144.124.193 57.144.124.192 129.134.30.12

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 16:12 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating Ping Scan at 16:12
Scanning 5 hosts [4 ports/host]
Completed Ping Scan at 16:12, 0.17s elapsed (5 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 16:12
Completed Parallel DNS resolution of 5 hosts. at 16:12, 1.47s elapsed
Initiating SYN Stealth Scan at 16:12
Scanning 5 hosts [1000 ports/host]
Discovered open port 80/tcp on 57.144.124.1[redacted]
Discovered open port 80/tcp on 157.240.[redacted]
Discovered open port 80/tcp on 157.240.[redacted]
Discovered open port 443/tcp on 157.2[redacted]3
Discovered open port 53/tcp on 129.[redacted]
Discovered open port 443/tcp on 57.1[redacted]2
Discovered open port 443/tcp on 157.[redacted]
Discovered open port 443/tcp on 57.[redacted]
```

Step 4: Public Info Check (Optional but Recommended)

What it is:

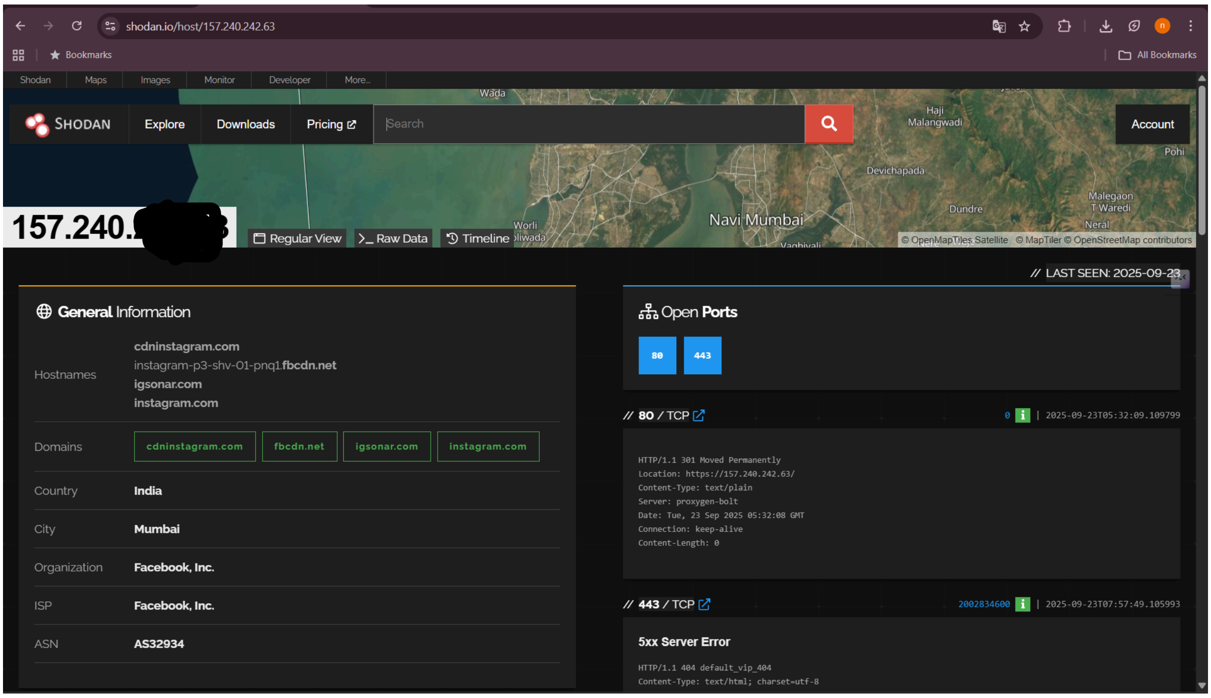
After actively scanning, you perform a check with a public database like **Shodan**. Shodan is like a search engine for internet-connected devices. It has already scanned the entire internet and collected information on what ports and services are open for every IP address.

Why we do it:

This step helps you verify your findings from the port scan. It's a quick way to confirm what you've found and see if the information is already publicly available to anyone who uses Shodan. It can also provide more details, such as the version number of the software running on a specific port.

Observation:

You observed that Shodan's results confirmed the open ports and services you found with Zenmap. This is a good sign that your Zenmap scan was successful and accurate. It also shows you what is visible to the rest of the world and potential attackers.



157.240.[redacted]

// LAST SEEN: 2025-09-23

General Information

Hostnames	cdninstagram.com instagram-p3-shv-01-pnq1.**fbcdn.net** igsonar.com instagram.com
Domains	cdninstagram.com fbcdn.net igsonar.com instagram.com
Country	India
City	Mumbai
Organization	Facebook, Inc.
ISP	Facebook, Inc.
ASN	AS32934

Open Ports

80 443

// **80** / TCP 0 | 2025-09-23T05:32:09.109799

```
HTTP/1.1 301 Moved Permanently
Location: https://157.240.242.63/
Content-Type: text/plain
Server: proxygen-bolt
Date: Tue, 23 Sep 2025 05:32:08 GMT
Connection: keep-alive
Content-Length: 0
```

// **443** / TCP 2002834600 | 2025-09-23T07:57:49.105993

5xx Server Error

```
HTTP/1.1 404 default_vip_404
Content-Type: text/html; charset=utf-8
```