Reconnaissance & Information Gathering – Mini Project

A study on passive Footprinting and OSINT techniques

Executive Summary

This mini-project focuses on the reconnaissance phase of ethical hacking and penetration testing. It explores passive information gathering (OSINT) techniques such as DNS analysis, Whois lookups, archive searches, subdomain enumeration, reverse IP lookups, and SSL certificate analysis. The goal is to understand how attackers collect information and how defenders can use the same insights to strengthen security.

Objectives

- Understand passive footprinting and reconnaissance.
- Explore OSINT techniques without active exploitation.
- Document findings in a structured manner.

Emphasize ethical considerations in cybersecurity practices.

Skills Developed: Digital footprint analysis, website reconnaissance, information gathering.

Methodology

DNS Information Gathering

Used nslookup to identify IP addresses and authoritative DNS servers for the target website.

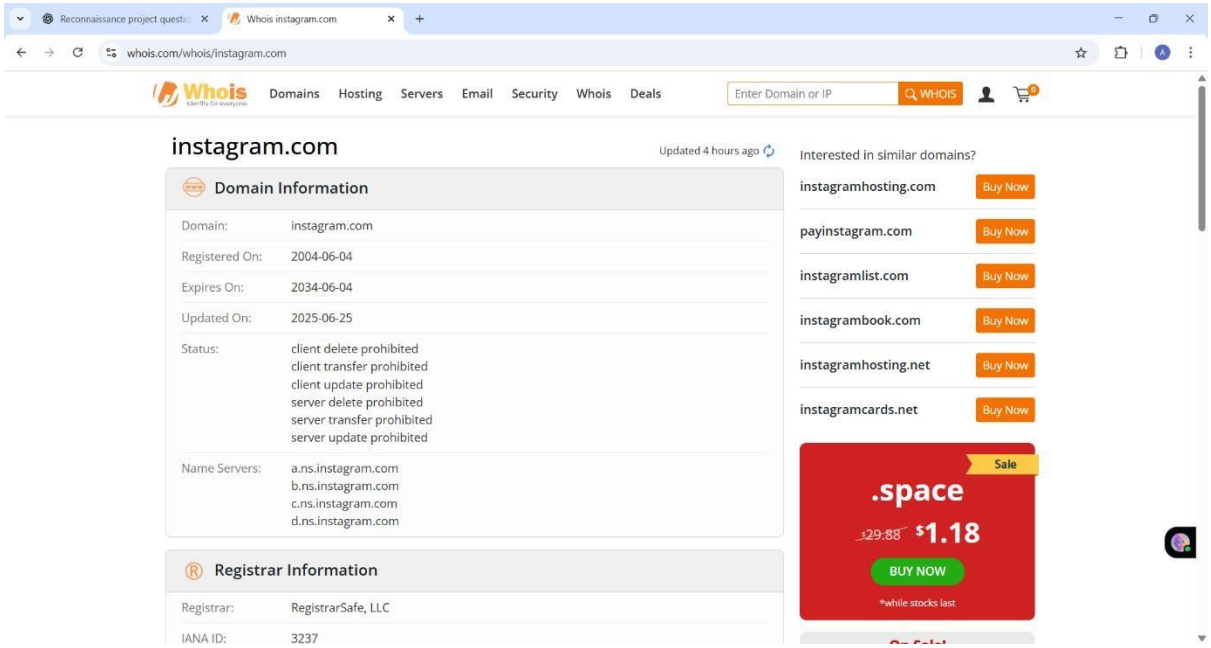
Side Note: This is like checking which post office is responsible for delivering mail to a house.

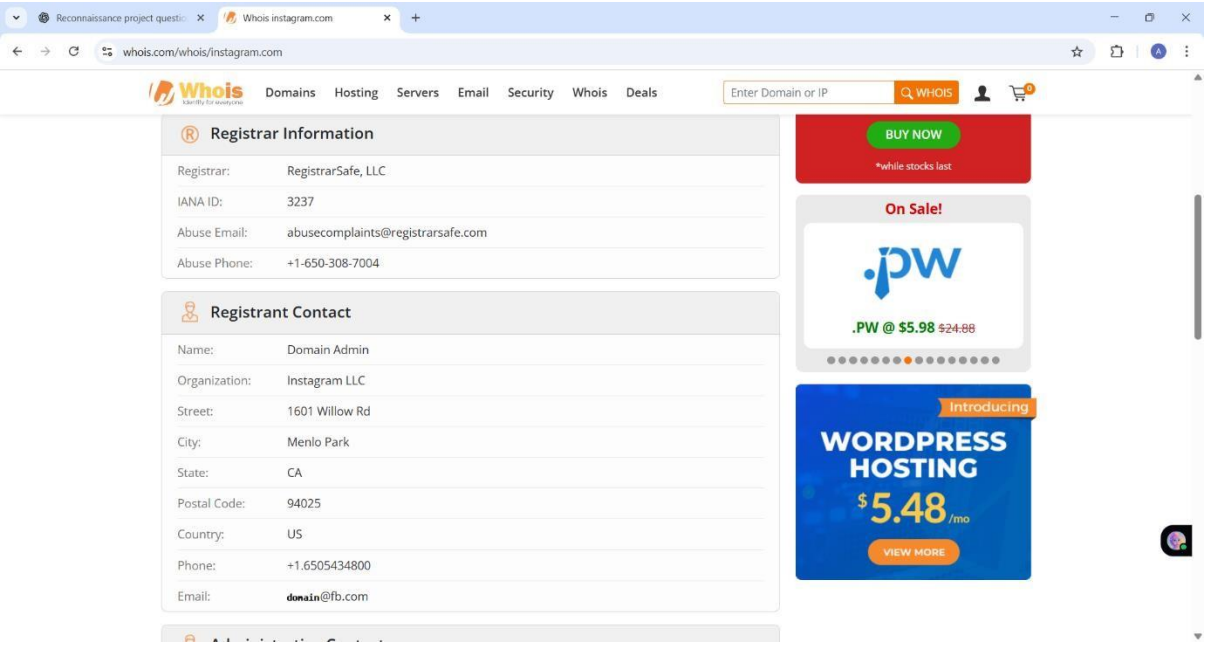
```
Windows PowerShell
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> nslookup instagram.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    instagram.com
Addresses:  2a03:2880:f368:22:face:b00c:0:4420
          57.144.142.34

PS C:\Users\User> nslookup -type=ns instagram.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
instagram.com   nameserver = c.ns.instagram.com
instagram.com   nameserver = b.ns.instagram.com
instagram.com   nameserver = a.ns.instagram.com
instagram.com   nameserver = d.ns.instagram.com

b.ns.instagram.com      AAAA IPv6 address = 2a03:2880:f0fd:c:face:b00c:0:35
b.ns.instagram.com      internet address = 129.134.31.12
a.ns.instagram.com      AAAA IPv6 address = 2a03:2880:f0fc:c:face:b00c:0:35
a.ns.instagram.com      internet address = 129.134.30.12
d.ns.instagram.com      AAAA IPv6 address = 2a03:2880:f1fd:c:face:b00c:0:35
d.ns.instagram.com      internet address = 185.89.219.12
c.ns.instagram.com      AAAA IPv6 address = 2a03:2880:f1fc:c:face:b00c:0:35
c.ns.instagram.com      internet address = 185.89.218.12
PS C:\Users\User>
```

Whois Lookup

Performed a Whois query to gather domain registration details such as owner, registrar, and registration date.

Side Note: Similar to checking property records to see who owns a building



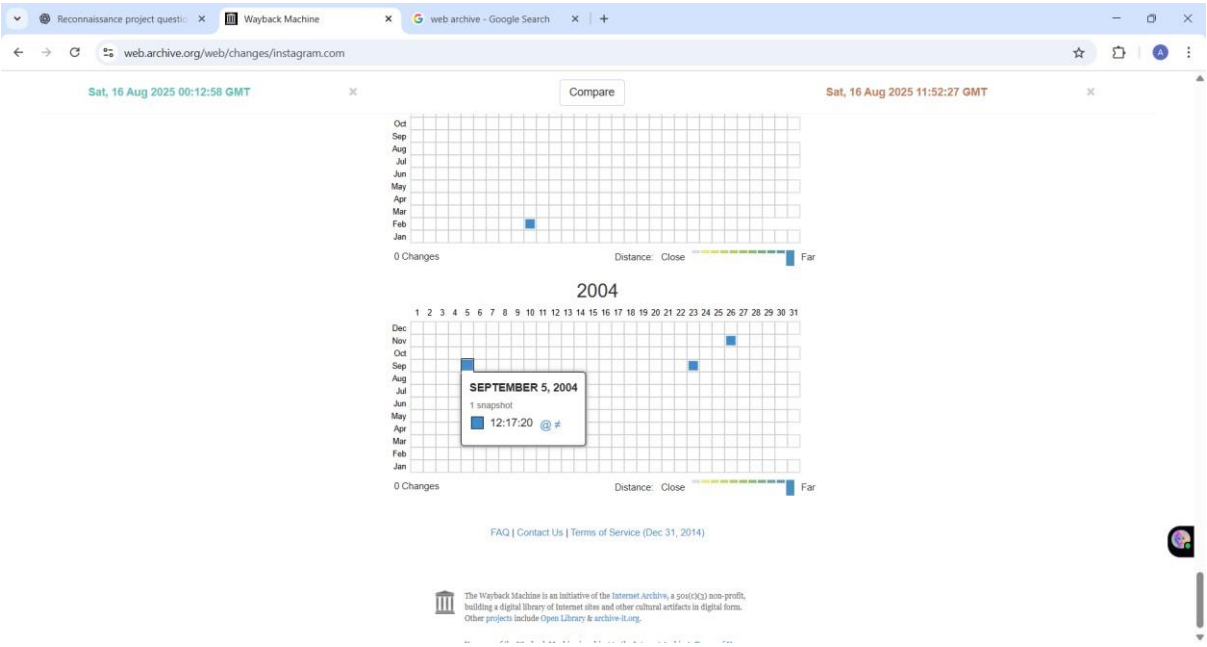


Web Archive Analysis

Viewed historical versions of the site using the Wayback Machine to identify past content and design changes.

Side Note: Like looking at old photographs of a shop to see what products they sold earlier.

1. WebArchive Search:



Step 3: Advanced Information Gathering:

Subdomain Enumeration

Discovered additional subdomains using crt.sh certificate transparency logs.

Side Note: Subdomains are like hidden rooms in a large building – sometimes they reveal extra services

```
Windows PowerShell
PS C:\Users\User>
PS C:\Users\User> Invoke-RestMethod 'https://api.ipify.org?format=json'

ip
--
157.40.163.82


PS C:\Users\User> $domain = 'instagram.com'
PS C:\Users\User> $url = "https://crt.sh/?q=%25.$domain&output=json"
PS C:\Users\User> try {
>>   $resp = Invoke-RestMethod -Uri $url -ErrorAction Stop
>>   $resp | Select-Object -ExpandProperty name_value | ForEach-Object { $_ -split "`n" } | Sort-Object -Unique | Out-Fi
le "$domain-crtsh-subdomains.txt" -Encoding utf8
>>   "Saved: $domain-crtsh-subdomains.txt. Lines: $((Get-Content $domain-crtsh-subdomains.txt).Count)"
>> } catch {
>>   "ERROR: $($_.Exception.Message)"
>>   # Save raw response for inspection
>>   try { (Invoke-WebRequest -Uri $url -UseBasicParsing).Content | Out-File "$domain-crtsh-raw.html" -Encoding utf8; "S
aved raw HTML to $domain-crtsh-raw.html" } catch {}
>> }
Saved: instagram.com-crtsh-subdomains.txt. Lines: 55
PS C:\Users\User> Get-Content instagram.com-crtsh-subdomains.txt | Select-Object -First 30
*.beta.instagram.com
*.cdninstagram.com
*.graph.instagram.com
*.i.instagram.com
*.instagram.com
*.intern.instagram.com
*.latest.instagram.com
```

```
PS C:\Users\User> Get-Content instagram.com-crtsh-subdomains.txt | Select-Object -First 30
*.beta.instagram.com
*.cdninstagram.com
*.graph.instagram.com
*.i.instagram.com
*.instagram.com
*.intern.instagram.com
*.latest.instagram.com
*.m.instagram.com
*.mail--instagram.com
*.maps.instagram.com
*.prod.instagram.com
*.secure.instagram.com
*.secure.latest.instagram.com
*.trunkstable.instagram.com
*.upload.instagram.com
*.www.instagram.com
api.instagram.com
autodiscover.instagram.com
beta.instagram.com
cdninstagram.com
copyright--instagram.com
cpanel.mail--instagram.com
cpanel.security--instagram.com
cpcalendars.security--instagram.com
cpcontacts.security--instagram.com
engineering.instagram.com
graph.instagram.com
graphql.instagram.com
i.instagram.com
```

Reverse IP Lookup

Checked which other domains were hosted on the same server IP using ipinfo.io.

Side Note: This is like seeing which other businesses share the same office building.

1. Reverse IP Lookup:

```
PS C:\Users\User> Invoke-RestMethod -Uri "https://ipinfo.io/$ip/json" | ConvertTo-Json -Depth 4
{
    "ip":  "157.240.0.35",
    "hostname":  "edge-star-mini-shv-02-fra3.facebook.com",
    "city":  "Frankfurt am Main",
    "region":  "Hesse",
    "country":  "DE",
    "loc":  "50.1112,8.6831",
    "org":  "AS32934 Facebook, Inc.",
    "postal":  "60311",
    "timezone":  "Europe/Berlin",
    "readme":  "https://ipinfo.io/missingauth"
}
PS C:\Users\User>
PS C:\Users\User> # Hackertarget reverse IP (simple text list)
PS C:\Users\User> Invoke-RestMethod -Uri "https://api.hackertarget.com/reverseiplookup/?q=$ip"
edge-star-mini-shv-02-fra3.facebook.com
ww1.kuaimiaovpn.com
passgenix.com
prod.prod.se.antivirus.bo.webproxy.idc.tencent.com
mayshu.my.id
irulztzy.shop
PS C:\Users\User> |
```

SSL Certificate Analysis

Examined SSL certificates to identify the certificate authority, expiration date, and related subdomains.

Side Note: A certificate is like a shop's license – it proves authenticity and sometimes lists branch locations.

2. SSL Certificate Analysis:

Subject (Issued To):

CN=targetwebsite.com → This is the domain the certificate is valid for.

Issuer (Certificate Authority):

DigiCert Inc – Encryption Everywhere DV TLS CA - G2

Certificate Chain:

Root: DigiCert Global Root G2

Intermediate: DigiCert Encryption Everywhere DV TLS CA - G2

Leaf: targetwebsite.com

Validity Period:

Start (NotBefore): Oct 16, 2024

End (NotAfter): Oct 16, 2025

Public Key Algorithm: RSA (2048-bit)

Signature Algorithm: RSA-SHA256

TLS Version Used: TLSv1.3 with cipher TLS_AES_128_GCM_SHA256

Verification: Verify return code: 0 (ok) → Certificate is valid and trusted.

.

Google Dorking

Applied advanced Google operators (dorks) to locate hidden or sensitive files such as PDFs.

***Side Note: Like using a library** catalog to find very specific hidden books.*

Reconnaissance project questio | About Us • Instagram

instagram.com/about/us/

Instagram

_aditya.yadav10

ABOUT

Company

Press

Jobs

LEGAL

Terms

Privacy

Platform

Libraries

About Us

Head of Instagram

Adam Mosseri (@mosseri) is the Head of Instagram where he oversees all functions of the business including engineering, product and operations. A designer at heart, Adam is known for balancing sharp design thinking with thoughtful product strategy to create experiences that bring people together and encourage authentic communication.

Adam has been at Facebook for more than ten years. He was design director for Facebook's mobile apps and then moved into product management where he led the News Feed product and engineering teams for many years. He was Head of News Feed prior to joining Instagram where he oversaw product before managing the entire organization.

Prior to Facebook, Adam worked at TokBox as the company's first designer. He began his career founding a design consultancy in 2003 with offices in New York and San Francisco that focused on graphic, interaction and exhibition design. Adam holds a BA from the Gallatin School of Interdisciplinary Study at NYU where he studied Information Design and Media.

Born and raised in New York, he now lives in San Francisco with his wife and two sons.

Founders

Kevin Systrom (Co-founder)

Kevin Systrom (@kevin) co-founded Instagram and served as CEO for 8 years before

instagram-press.com

Reconnaissance project questio | About Us • Instagram

instagram.com/about/us/

Instagram

_aditya.yadav10

Founders

Kevin Systrom (Co-founder)

Kevin Systrom (@kevin) co-founded Instagram and served as CEO for 8 years before leaving the company in September 2018 to pursue his next passion project. With Kevin's focus on simplicity and inspiring creativity through solving problems with thoughtful product design, Instagram became the home for innovation on visual storytelling launching dozens of products including Stories and IGTV.

Prior to founding Instagram, Kevin was part of the startup Odeo, which later became Twitter, and spent two years at Google working on products like Gmail and Google Reader. He graduated from Stanford University with a BS in Management Science & Engineering.

Mike Krieger (Co-founder)

Mike Krieger (@mikeyk) co-founded Instagram and served as Instagram's Head of Engineering for 8 years, before leaving the company in September 2018 to explore new projects. Mike focused on building a broad range of creative products to empower the community on Instagram to connect with their interests and passions. In addition, Mike grew the engineering organization to more than 400 employees in Instagram offices located in Menlo Park, New York and San Francisco.

A native of São Paulo, Brazil, Mike holds an MS in Symbolic Systems from Stanford University. Prior to founding Instagram, he worked at Meebo as a user experience designer and front-end engineer.

Tools & Resources Used

Tool / Resource	Purpose
nslookup	Fetch DNS records
Whois	Domain registration details
crt.sh	Subdomain discovery via certificate logs
archive.org	Historical snapshots of website
ipinfo.io	Reverse IP lookup
SSL Labs / Cert tools	SSL certificate analysis
Google Dorks	Advanced search queries
Social Media	Branding, employee info
Public pages	Email harvesting

Findings & Observations

The reconnaissance activities revealed key insights about the target environment. DNS and Whois lookups exposed IP infrastructure and registration details. Web archives highlighted historical shifts. Subdomain enumeration and SSL analysis uncovered hidden services. Social media and Google dorking provided additional open-source intelligence. These findings demonstrate how much can be learned passively, underlining the need for organizations to minimize their exposed information.