

# Information Gathering — Project Report

**Name:** Janhavi Mestry

**Intern Id:** ITID4679

**Environment / Tools:** Kali Linux (VM) — whois, nslookup/host/dig, whatweb, nmap, dirb, theHarvester / Google dorking, host, ping.

**Target (examples used):** Local VM **192.168.68.128** (authorized lab: bWAPP, DVWA, Bricks) and public example **instagram.com** (passive checks only).

## 1. Objective

Gather as much publicly available information about the given targets using only passive or allowed active methods. Do not perform exploitation. Produce a clear report with screenshots and recommended next steps.

## 2. Scope & Rules

- Only passive and non-intrusive active checks (whois, DNS, ping, nmap service discovery, dirb directory discovery).
- No exploitation or unauthorized access.
- Testing performed only on authorized local VM (**192.168.68.128**). Public domain checks were passive.

## 3. Basic Information

**Target domain/IP:** **instagram.com** (public example) / **192.168.68.128** (lab VM)

**WHOIS:** Captured registrar and registrant data for public example (Instagram LLC, Menlo Park, CA).

**Hosting & Location (example):** Resolved IPs geolocated to United States (sample shown in screenshots).

```
Site24x7
(kali@kali)-[~]
$ whois instagram.com
Domain Name: INSTAGRAM.COM
Registry Domain ID: 121748357_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2025-06-25T19:12:42Z
Creation Date: 2004-06-04T13:37:18Z
Registry Expiry Date: 2034-06-04T13:37:18Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.INSTAGRAM.COM
Name Server: B.NS.INSTAGRAM.COM
Name Server: C.NS.INSTAGRAM.COM
Name Server: D.NS.INSTAGRAM.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-28T19:08:18Z <<<
```

```
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Updated Date: 2025-06-25T19:12:42Z
Creation Date: 2004-06-04T13:37:18Z
Registrar Registration Expiration Date: 2034-06-04T13:37:18Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Instagram LLC
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Instagram LLC
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
```

S.No	Domain Name	IP Address
1	instagram.com.	31.13.70.174

Country Code	Country Name	Region	City
US	UNITED STATES	CALIFORNIA	LOS ANGELES

## 4. DNS Information

**Commands used:** `nslookup instagram.com / host instagram.com / dig instagram.com any`

**Findings:**

- A records and name servers found (e.g., `a.ns.instagram.com`, `b.ns.instagram.com`).
- No zone transfer allowed (no AXFR) on public nameservers (no unauthorized transfers attempted).

```
(kali㉿kali)-[~]
$ host instagram.com
instagram.com has address 157.240.16.174
instagram.com has IPv6 address 2a03:2880:f22f:e5:face:b00c:0:4420
instagram.com mail is handled by 10 mxa-00082601.gslb.pphosted.com.
instagram.com mail is handled by 10 mxb-00082601.gslb.pphosted.com.
instagram.com has HTTP service bindings 1 . alpn="h2,h3"
instagram.com has HTTP service bindings 2 z-p42-instagram.fallback.c10r.facebook.com. alpn="h2,h3"
```

```
(kali㉿kali)-[~]
$ nslookup instagram.com
Server:      192.168.68.2
Address:     192.168.68.2#53

Non-authoritative answer:
Name:   instagram.com
Address: 157.240.16.174
Name:   instagram.com
Address: 2a03:2880:f22f:e5:face:b00c:0:4420
```

## 5. Technology Fingerprinting

Tools used: **whatweb**

**Findings (example):** whatweb showed web server headers and security headers such as HSTS, X-Frame-Options — indicates proper hardening on the public site.

```
(kali@kali)~$ whatweb instagram.com
http://instagram.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[proxygen-bolt], IP[157.240.16.174], RedirectLocation[https://instagram.com/]
https://instagram.com/ [301 Moved Permanently] Country[UNITED STATES][US], IP[157.240.16.174], RedirectLocation[https://www.instagram.com/], Strict-Transport-Security[max-age=31536000; preload; includeSubDomains], UncommonHeaders[x-stack,x-fb-debug,alt-svc,x-fb-connection-quality]
https://www.instagram.com/ [200 OK] Cookies[csrftoken], Country[UNITED STATES][US], Django, HTML5, IP[157.240.16.174], Open-Graph-Protocol[124024574287414], Script[application/json], Strict-Transport-Security[max-age=31536000; preload; includeSubDomains], Title[Instagram], UncommonHeaders[accept-ch-lifetime,accept-ch,reporting-endpoints,report-to,content-security-policy-report-only,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,origin-trial,cross-origin-opener-policy,x-content-type-options,origin-agent-cluster,x-stack,x-fb-debug,alt-svc,x-fb-connection-quality], X-Frame-Options[DENY], X-XSS-Protection[0]
```

## 6. Directory & File Discovery

Tools used: **dirb**, wordlist **/usr/share/wordlists/dirb/common.txt**

Command example:

```
dirb http://192.168.68.128
/usr/share/wordlists/dirb/common.txt
```

**Findings:** Discovered many directories such as **/assets/**, **/cgi-bin/**, **/phpmyadmin/**, **/wordpress/**, **/images/**, **/index.html**. These may expose admin panels or sensitive files.

```
GENERATED WORDS: 4612

— Scanning URL: http://192.168.68.128/ —
+ http://192.168.68.128/.bash_history (CODE:200|SIZE:302)
=> DIRECTORY: http://192.168.68.128/assets/
=> DIRECTORY: http://192.168.68.128/cgi-bin/
+ http://192.168.68.128/cgi-bin/ (CODE:200|SIZE:1070)
+ http://192.168.68.128/crossdomain (CODE:200|SIZE:200)
+ http://192.168.68.128/crossdomain.xml (CODE:200|SIZE:200)
=> DIRECTORY: http://192.168.68.128/evil/
+ http://192.168.68.128/favicon.ico (CODE:200|SIZE:3638)
=> DIRECTORY: http://192.168.68.128/gallery2/
=> DIRECTORY: http://192.168.68.128/icon/
=> DIRECTORY: http://192.168.68.128/images/
+ http://192.168.68.128/index (CODE:200|SIZE:1227)
+ http://192.168.68.128/index.html (CODE:200|SIZE:28067)
=> DIRECTORY: http://192.168.68.128/javascript/
=> DIRECTORY: http://192.168.68.128/joomla/
=> DIRECTORY: http://192.168.68.128/phpBB2/
=> DIRECTORY: http://192.168.68.128/phpmyadmin/
+ http://192.168.68.128/server-status (CODE:403|SIZE:215)
=> DIRECTORY: http://192.168.68.128/test/
=> DIRECTORY: http://192.168.68.128/wordpress/
```

## 7. Open Ports & Services

**Tools used:** `nmap`, `nmap -sV` (service/version detection), selected NSE scripts for information only.

**Commands used:**

```
nmap 192.168.68.128
```

```
nmap -sV 192.168.68.128
```

**Findings (sample):**

- Open ports found on VM: **22** (SSH), **80** (HTTP), **443** (HTTPS), **139/445** (SMB), **8080/8081** (alternate web services).
- Services: Apache HTTPD, OpenSSH, Tomcat/Coyote, Jetty, Samba.
- NSE script flagged informational issue (CVE-2011-3192) — treat as a pointer to check versions and patch.

```
(kali㉿kali)-[~]
$ nmap 192.168.68.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 15:39 EDT
Nmap scan report for 192.168.68.128
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
143/tcp    open  imap
443/tcp    open  https
445/tcp    open  microsoft-ds
5001/tcp   open  complex-link
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap
MAC Address: 00:0C:29:E0:F3:32 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

```

(kali㉿kali)-[~]
$ nmap -sV 192.168.68.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 15:42 EDT
Nmap scan report for 192.168.68.128
Host is up (0.0030s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-P
xy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ... )
3309/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp    open  imap         Courier Imapd (released 2008)
443/tcp    open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-P
xy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ... )
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp   open  java-object  Java Object Serialization
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp   open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following
nt at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=10/28%Time=69011C9A%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4,"\xac\xed\x0\x05");
MAC Address: 00:0C:29:E0:F3:32 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds

```

```

Nmap scan report for 192.168.68.128
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-internal-ip-disclosure:
|_ Internal IP Leaked: 127.0.1.1
| http-vuln-cve2011-3192:
| VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| IDs: CVE:CVE-2011-3192 BID:49303
| Page 1 The Apache web server is vulnerable to a denial of service attack when numerous
| overlapping byte ranges are requested.
| Disclosure date: 2011-08-19
| References:
| https://www.tenable.com/plugins/nessus/55976
| https://seclists.org/fulldisclosure/2011/Aug/175
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| https://www.exploit-db.com/exploits/48303

```

## 8. Email Harvesting & Google Dorking

**Tools / methods:** Google dorks, simple searches, theHarvester (optional).

**Example Google dork used:** `site:lists.etf.bg.ac.rs "rc-admin"`

**Findings:** Public mailing list pages and contact emails (e.g., `rc-admin@lists.etf.rs`) were found on example domains. This shows how public data can be harvested.

Mailing lists service

List of lists

Home

Help

email address :

password :

Login

First login ?

Lost password ?

Subscribers: 5

Owners

vladimir

Contact owners

Subscribe

Unsubscribe

Info

Archive

Post

RSS

Shared documents

rc-admin@lists.etf.rs

RC-Admin

RC-Admin mail list

Google

@etf.bg.ac.rs" -site:etf.bg.ac.rs|

×

🔊

📷

🔍

⚙️

AI Mode

All

Images

Shopping

News

Videos

Short videos

More ▾

Tools ▾

W

Wikipedia

https://en.wikipedia.org › wiki › University\_of\_Belgrad...

University of Belgrade School of Electrical Engineering

Urban. Website, etf.bg.ac.rs. The first university level lecture in the field of electrical engineering in Serbia was held in 1894. Professor Stevan Marković ...

Univerzitet u Beogradu

http://arhiva.rect.bg.ac.rs › members › faculties › SEE

School of Electrical Engineering - Универзитет у Београду

Phone number 1: +381 11 3218 321 ; Phone number 2: +381 11 3218 323 ; Fax: +381 11 3248 681 ; Website: www.etf.bg.ac.rs ; E-mail: dekanat@etf.bg.ac.rs.

dih-hero.eu

https://dih-hero.eu › service › etf-laboratories

ETF laboratories - Digital Innovation Hubs - DIH Hero

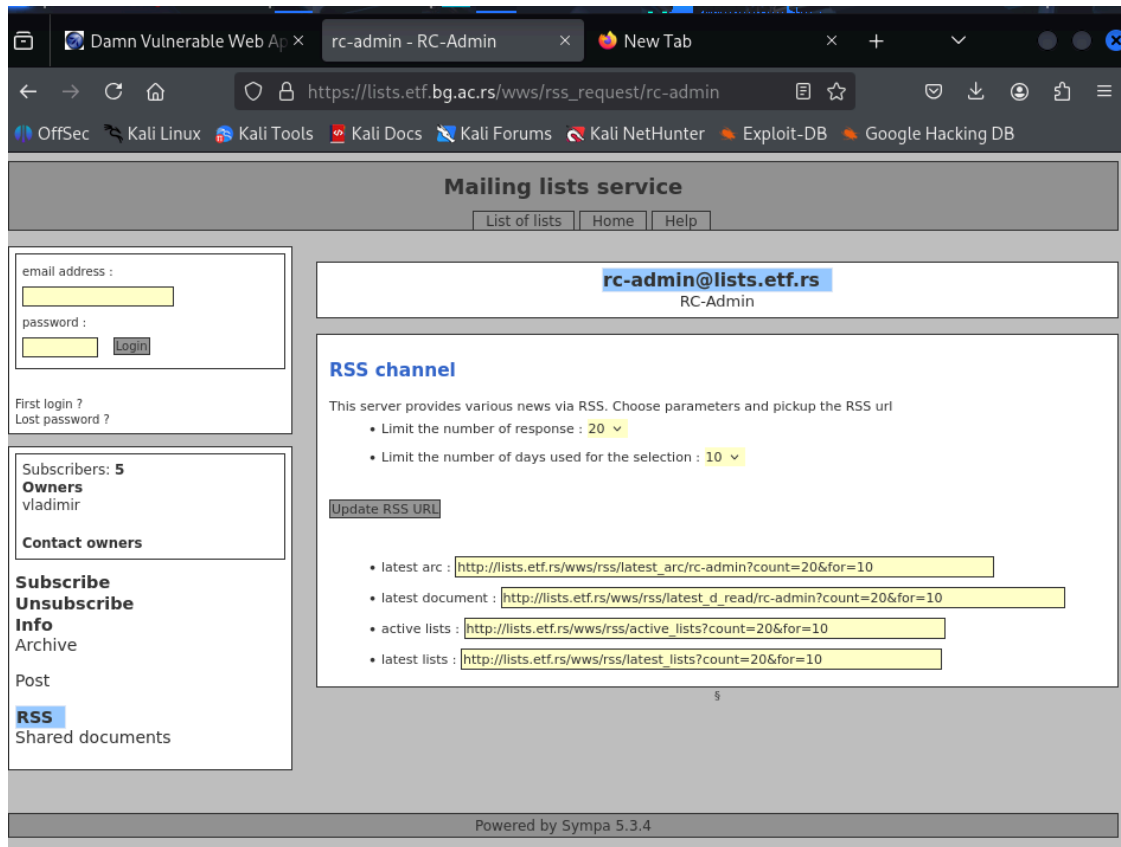
This is a service of. University of Belgrade - School of Electrical Engineering (ETF). https://www.etf.bg.ac.rs/; Research and Technology Organisation (RTO) ...

Instagram · etfbgd

4.4K+ followers

ETF Beograd (@etfbgd)

Zvanična stranica Elektrotehničkog fakulteta u Beogradu. www.etf.bg.ac.rs and 1 more ... etf.bg.ac.rs/ Пријемни испит из математике одржаће се у петак, 3 ...



## Conclusion

This information-gathering task collected domain, DNS, service, directory and publicly available contact data using safe, non-exploitative methods. The local VM intentionally exposes services and admin pages for learning; in real systems these should be restricted and patched. Follow the recommendations above to reduce the attack surface.