| Ex. No. 1 | Passive Reconnaissance-1: Whois Database, Google Dorking |
|---|---|
| Date of Exercise | 29/07/23 |

**Aim:**

The objective of this experiment is to:

- Gain information about targeted computers
- Gain information about targeted networks
- Generate reports for conducted reconnaissance.

**Lab Environment:**

To carry out the Experiment, you need:

- Penetration testing operating system [ Kali Linux / parrot ]
- Web browser with Internet access
- Administration privileges to run the tools.

**Overview of the Passive Reconnaissance:**

Passive reconnaissance is an attempt to gather information about targeted computers and networks without actually communicating with them. The term originated from the military, which does passive reconnaissance before embarking on an information-gathering mission. Instead of attacking right away, they first obtain the necessary information to direct their strategies. Passive reconnaissance is the first step hackers take before exploiting system or network vulnerabilities.

Passive reconnaissance is part of the pre-attack phase for hackers. Attackers first “get to know” their targets to ensure that they have all the relevant information to make their attacks successful. They can do so by gathering intelligence in two ways—passive or active reconnaissance.

In a pen-testing scenario, alongside uncovering vulnerabilities in the hardware and software systems and exploiting them, the most effective of all is penetrating the human mind to extract the desired information.

**Sublist3r:**

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

subbrute was integrated with Sublist3r to increase the possibility of finding more subdomains using bruteforce with an improved wordlist. The credit goes to TheRook who is the author of sub brute.

| **Form** | **Long Form** | **Description** |
|---|---|---|
| -d | --domain | Domain name to enumerate subdomains of |
| -b | --bruteforce | Enable the subbrute bruteforce module |
| -p | --portsScan | the found subdomains against specific tcp ports |
| -v | --verbose | Enable the verbose mode and display results in realtime |
| -t | --threads | Number of threads to use for subbrute bruteforce |

| | | |
|---|---|---|
| -e | --engines | Specify a comma-separated list of search engines |
| -o | --output | Save the results to text file |
| -h | --help | Show the help message and exit |

**Whois:**

WHOIS (pronounced as the phrase "who is") is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems, but it is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The current iteration of the WHOIS protocol was drafted by the Internet Society, and is documented in RFC 3912.

Whois is also the name of the command-line utility on most UNIX systems used to make WHOIS protocol queries. In addition, WHOIS has a sister protocol called Referral Whois (RWhois).

**Google Dorking:**

“Google dork” is an advanced Google search technique. “Google dorking” (aka “Google hacking”) is the activity of performing advanced searches on Google. You can combine different Google dorks to comb data otherwise inaccessible to ordinary users of Google search. On a browser, if too many Google searches are made in a short time, Google requires that unscramble garbled letters in an image called a captcha before it can be proceeded. Captcha completion can frustrate end users but Google servers must nip denial-of-service cyberattacks in the bud.

Examples:

- inurl:"view.shtml""Network Camera",
- "Camera LiveImage"
- inurl:"guestimage.html"

- intitle:"webcamXP 5’"
- "Not for Public Release" + "Confidential" ext:pdf | ext:doc | ext:xlsx
- site:.hk & inurl:wp-login

**Expected Input/Output:**

Case-1: Find publicly accessible cameras Case-2: Find information about a website

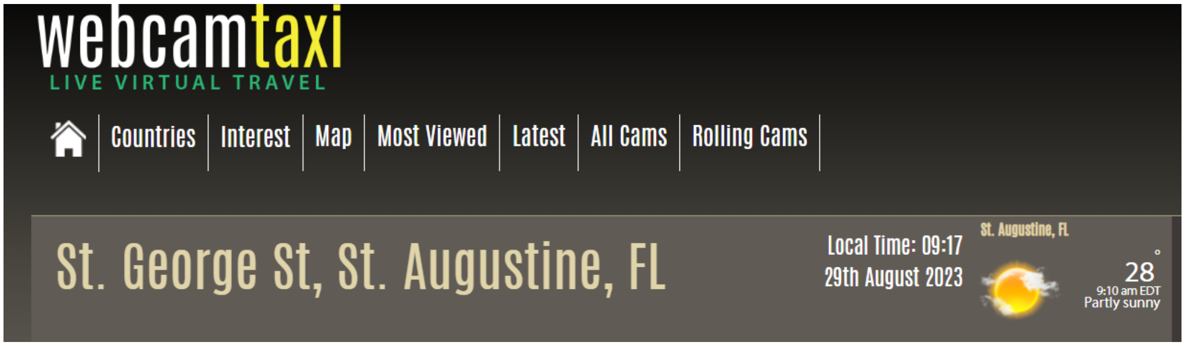
**Case1:** Steps

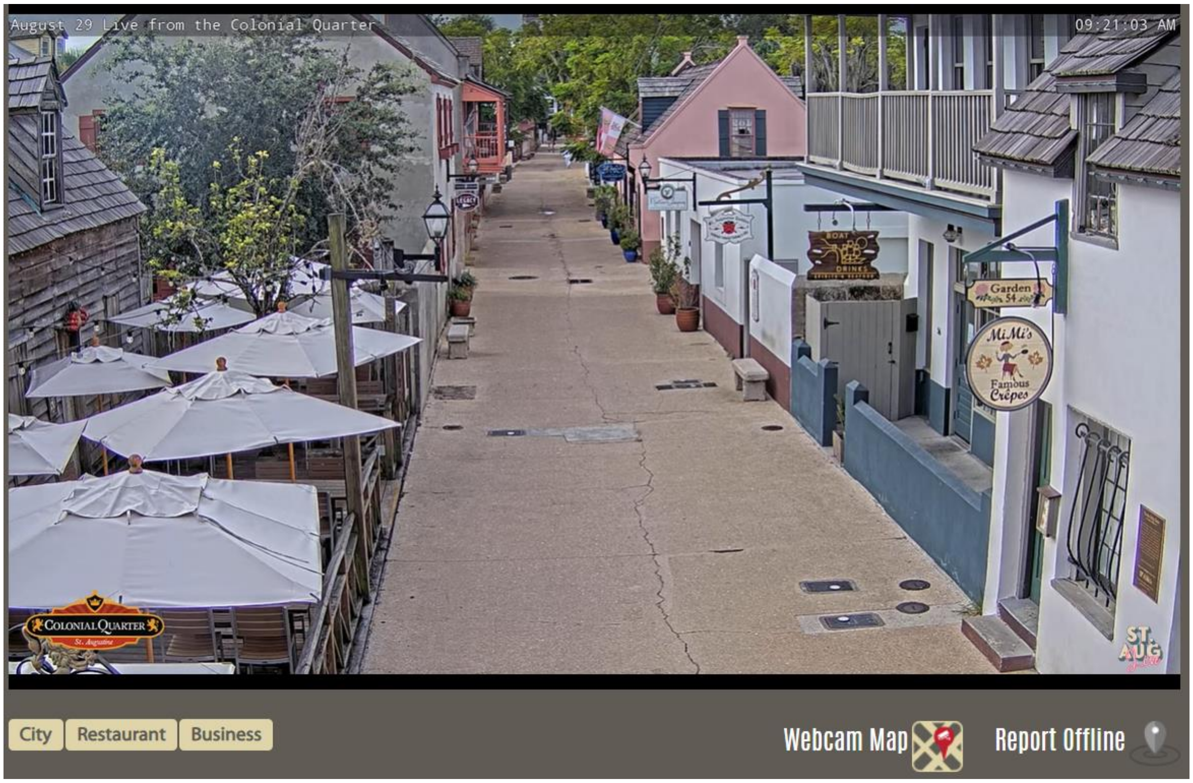
1: Go to www.google.com

2. website searched: intitle:” webcam uk"

3. It will display all the publicly accessible live camera’s in UK

**Output:**





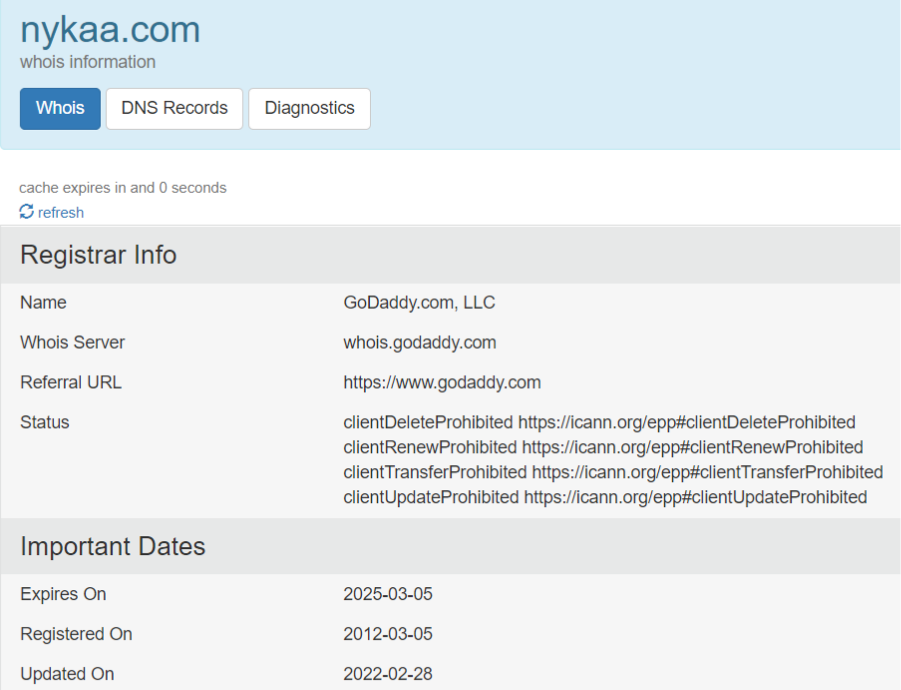
**Case 2:** Steps:

1. Go to www.google.com

2. Go to https://who.is/

3. Search for the domain name.

**Output:**



# nykaa.com

whois information

cache expires in and 0 seconds

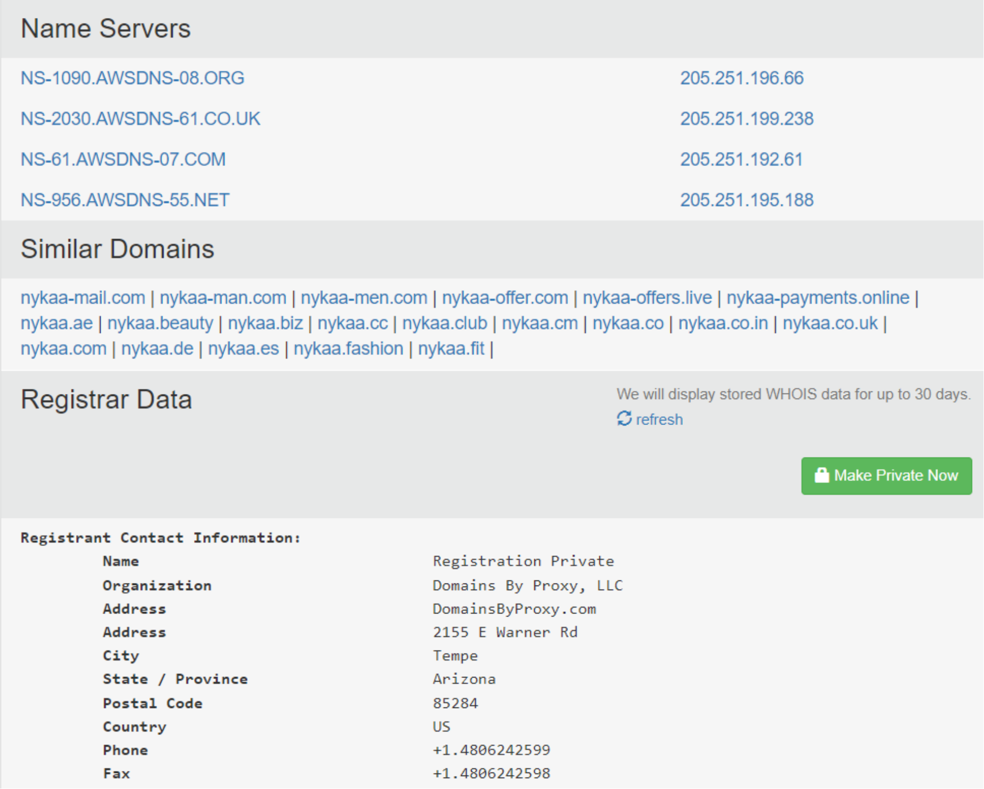
refresh

## Registrar Info

| | |
|---|---|
| Name | GoDaddy.com, LLC |
| Whois Server | whois.godaddy.com |
| Referral URL | https://www.godaddy.com |
| Status | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited<br>clientRenewProhibited https://icann.org/epp#clientRenewProhibited<br>clientTransferProhibited https://icann.org/epp#clientTransferProhibited<br>clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited |

## Important Dates

| | |
|---|---|
| Expires On | 2025-03-05 |
| Registered On | 2012-03-05 |
| Updated On | 2022-02-28 |



## Name Servers

| | |
|---|---|
| NS-1090.AWSDNS-08.ORG | 205.251.196.66 |
| NS-2030.AWSDNS-61.CO.UK | 205.251.199.238 |
| NS-61.AWSDNS-07.COM | 205.251.192.61 |
| NS-956.AWSDNS-55.NET | 205.251.195.188 |

## Similar Domains

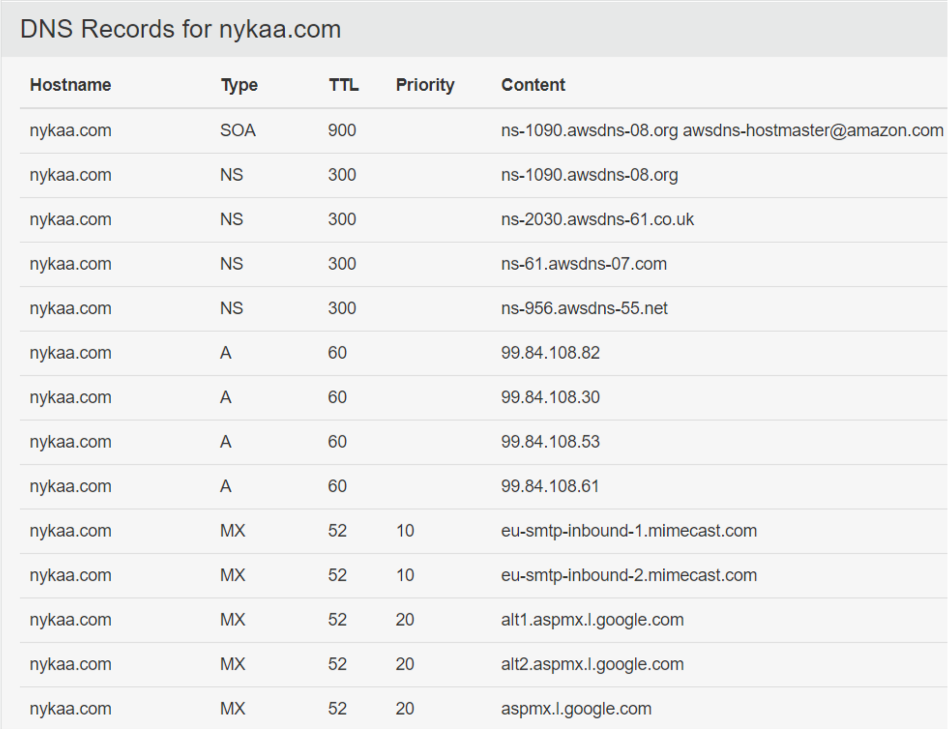
nykaa-mail.com | nykaa-man.com | nykaa-men.com | nykaa-offer.com | nykaa-offers.live | nykaa-payments.online | nykaa.ae | nykaa.beauty | nykaa.biz | nykaa.cc | nykaa.club | nykaa.cm | nykaa.co | nykaa.co.in | nykaa.co.uk | nykaa.com | nykaa.de | nykaa.es | nykaa.fashion | nykaa.fit |

## Registrar Data

We will display stored WHOIS data for up to 30 days.

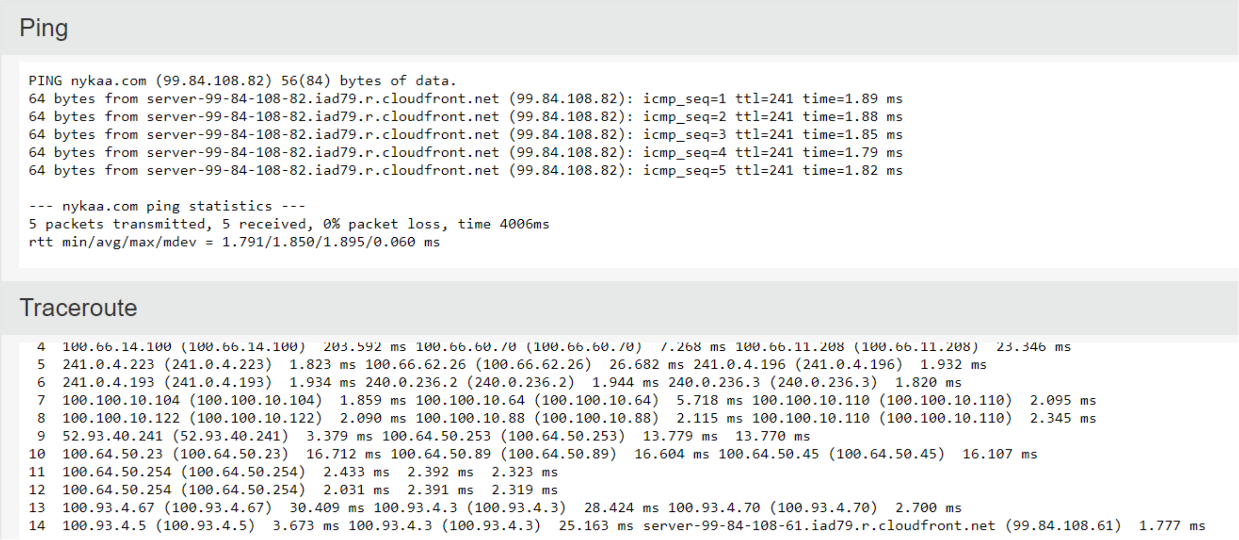
refresh

```
Registrant Contact Information:
         Name                                 Registration Private
         Organization                         Domains By Proxy, LLC
         Address                              DomainsByProxy.com
         Address                              2155 E Warner Rd
         City                                 Tempe
         State / Province                     Arizona
         Postal Code                          85284
         Country                              US
         Phone                                +1.4806242599
         Fax                                  +1.4806242598
```



DNS Records for nykaa.com

| Hostname | Type | TTL | Priority | Content |
|---|---|---|---|---|
| nykaa.com | SOA | 900 | | ns-1090.awsdns-08.org awsdns-hostmaster@amazon.com |
| nykaa.com | NS | 300 | | ns-1090.awsdns-08.org |
| nykaa.com | NS | 300 | | ns-2030.awsdns-61.co.uk |
| nykaa.com | NS | 300 | | ns-61.awsdns-07.com |
| nykaa.com | NS | 300 | | ns-956.awsdns-55.net |
| nykaa.com | A | 60 | | 99.84.108.82 |
| nykaa.com | A | 60 | | 99.84.108.30 |
| nykaa.com | A | 60 | | 99.84.108.53 |
| nykaa.com | A | 60 | | 99.84.108.61 |
| nykaa.com | MX | 52 | 10 | eu-smtp-inbound-1.mimecast.com |
| nykaa.com | MX | 52 | 10 | eu-smtp-inbound-2.mimecast.com |
| nykaa.com | MX | 52 | 20 | alt1.aspmx.l.google.com |
| nykaa.com | MX | 52 | 20 | alt2.aspmx.l.google.com |
| nykaa.com | MX | 52 | 20 | aspmx.l.google.com |



Ping

```
PING nykaa.com (99.84.108.82) 56(84) bytes of data.
64 bytes from server-99-84-108-82.iad79.r.cloudfront.net (99.84.108.82): icmp_seq=1 ttl=241 time=1.89 ms
64 bytes from server-99-84-108-82.iad79.r.cloudfront.net (99.84.108.82): icmp_seq=2 ttl=241 time=1.88 ms
64 bytes from server-99-84-108-82.iad79.r.cloudfront.net (99.84.108.82): icmp_seq=3 ttl=241 time=1.85 ms
64 bytes from server-99-84-108-82.iad79.r.cloudfront.net (99.84.108.82): icmp_seq=4 ttl=241 time=1.79 ms
64 bytes from server-99-84-108-82.iad79.r.cloudfront.net (99.84.108.82): icmp_seq=5 ttl=241 time=1.82 ms

--- nykaa.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.791/1.850/1.895/0.060 ms
```

Traceroute

```
 4  100.66.14.100 (100.66.14.100)  203.592 ms 100.66.60.70 (100.66.60.70)  7.268 ms 100.66.11.208 (100.66.11.208)  23.346 ms
 5  241.0.4.223 (241.0.4.223)  1.823 ms 100.66.62.26 (100.66.62.26)  26.682 ms 241.0.4.196 (241.0.4.196)  1.932 ms
 6  241.0.4.193 (241.0.4.193)  1.934 ms 240.0.236.2 (240.0.236.2)  1.944 ms 240.0.236.3 (240.0.236.3)  1.820 ms
 7  100.100.10.104 (100.100.10.104)  1.859 ms 100.100.10.64 (100.100.10.64)  5.718 ms 100.100.10.110 (100.100.10.110)  2.095 ms
 8  100.100.10.122 (100.100.10.122)  2.090 ms 100.100.10.88 (100.100.10.88)  2.115 ms 100.100.10.110 (100.100.10.110)  2.345 ms
 9  52.93.40.241 (52.93.40.241)  3.379 ms 100.64.50.253 (100.64.50.253)  13.779 ms  13.770 ms
10  100.64.50.23 (100.64.50.23)  16.712 ms 100.64.50.89 (100.64.50.89)  16.604 ms 100.64.50.45 (100.64.50.45)  16.107 ms
11  100.64.50.254 (100.64.50.254)  2.433 ms  2.392 ms  2.323 ms
12  100.64.50.254 (100.64.50.254)  2.031 ms  2.391 ms  2.319 ms
13  100.93.4.67 (100.93.4.67)  30.409 ms 100.93.4.3 (100.93.4.3)  28.424 ms 100.93.4.70 (100.93.4.70)  2.700 ms
14  100.93.4.5 (100.93.4.5)  3.673 ms 100.93.4.3 (100.93.4.3)  25.163 ms server-99-84-108-61.iad79.r.cloudfront.net (99.84.108.61)  1.777 ms
```

## Result:

Google dorking and whois database has been used for performing passive reconnaissance.