Wrocław 01.10.2022

# CYBERSECURITY

## LAB 10

### 1. Introduction

Information gathering is the first phase in the penetration testing process. In this phase, we try to collect as much information as we can about the target, for example, information about the Domain Name System (DNS) hostnames, IP addresses, technologies and configuration used, username's organization, documents, application code, password reset information, contact information, and so on. During information gathering, every piece of information gathered is considered important. Information gathering can be categorized in two ways based on the method used: active information gathering and passive information gathering.

In the active information gathering method, we collect information by introducing network traffic to the target network. While, in the passive information gathering method, we gather information about a target network by utilizing a third-party's services, such as the Google search engine. After we have gathered information about our target network from third-party sources, such as search engines, the next step would be to discover our
target machines.

The purpose of this process is as follows:

A. To find out which machine in the target network is available. If the target machine is not available, we won't continue the penetration testing process on that machine and move to the next machine.

B. To find the underlying operating system used by the target machine.
Collecting the previously mentioned information will help us during the vulnerabilities mapping process.
We can utilize the tools provided in Kali Linux for the target discovery process. Most of these tools are available in the Information Gathering menu, with the following submenus:

A. Identify Live Hosts

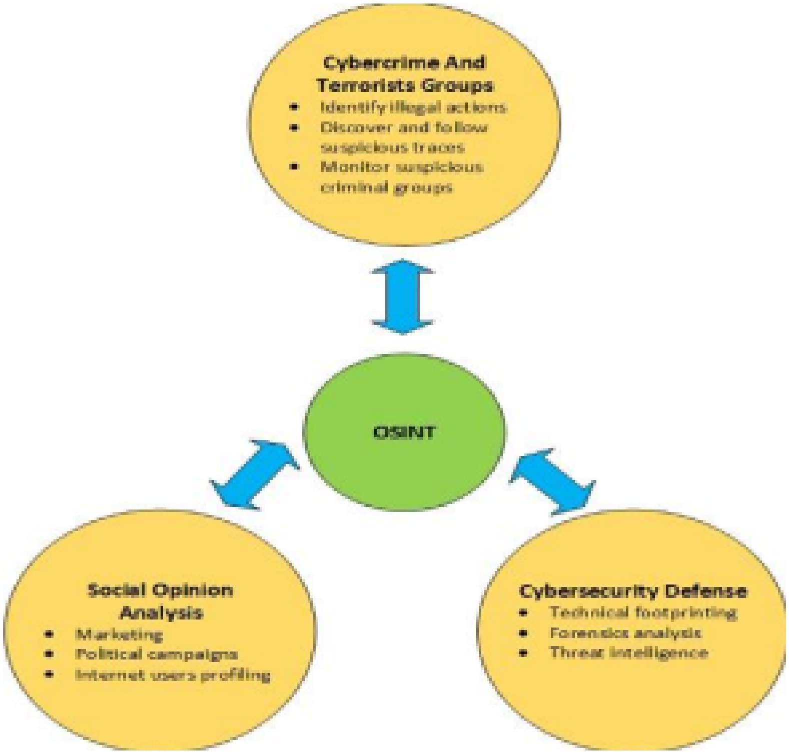
B. OS Fingerprinting

OSINT (Open Source Intelligence) is intelligence derived from public information--tailored intelligence which is based on information which can be obtained legally and ethically from public sources. On the Internet, there are several public resources that can be used to collect information regarding a target domain. The benefit of using these resources is that your network traffic is not sent to the target domain directly, so our activities are not recorded in the target domain logfiles.

In terms of cybersecurity, OSINT is mainly used to optimize attacks against specific users and to carry out social engineering attacks. A typical scenario is to use information about people related to the target of the attack: date of birth, work, school to crack passwords. "Humans are incapable of securely storing high-quality cryptographic keys..." [1] and despite many password security policies, quite simple keys are still used, often linked to a person, so using knowledge about the attacker significantly simplifies the process of breaking passwords.

[1] C Kaufman, R Perlman, M Speciner, 'Network Security–Private Communication in a Public World', Prentice Hall 1995

Many different entities today use OSINT for their purposes, not always legal.



[2] *Figure 1* *Actors interested in OSINT*

## 2. Required virtual machines

- Kali
- Metasploitable 2 or 3

## 3. Prerequisites

Get familiar with the following elements:

- whois
- dns
- fierce
- host
- Dmitry
- Traceroute
- p0f
- hping3/arping/fping/npin
- nbtscan

## 4. Problems and questions

I. What is the technical idea behind OS fingerprinting?

[2] https://cybersecurity-magazine.com/an-introduction-to-open-source-intelligence-osint/

> OS fingerprinting is a technique used to identify the operating system and version of a remote host by analyzing its network communication patterns and characteristics.

II. Why OS fingerprinting can be important for security?

> OS fingerprinting can be important for security as it allows identifying vulnerabilities specific to the operating system and version, and helps in configuring firewalls and intrusion detection systems.

III. What is the difference between passive and active OS fingerprinting?

> Passive OS fingerprinting involves collecting information about a target without introducing network traffic, while active OS fingerprinting involves sending network traffic to the target to collect information.

IV. Is it possible to protect your systems from OS fingerprinting?

> It is possible to protect your systems from OS fingerprinting by disabling unnecessary network services and using techniques such as IP spoofing and packet fragmentation to conceal the true operating system.

V. Is it possible to fool an intruder and to show him that your host is not alive?

> It is possible to fool an intruder by using techniques such as operating system emulation and honeypots.

VI. What is DNS zone transfer and what is a risk related to this mechanism?

> DNS zone transfer is a mechanism used to replicate the DNS database from a primary DNS server to a secondary DNS server. A risk related to this mechanism is that it can reveal sensitive information such as IP addresses and hostnames.

VII. Is it legal to use OSINT methods to get sensitive information?

>It is legal to use OSINT methods to gather information as long as it is obtained from publicly available sources and not obtained through illegal means.

VIII. What is the biggest threat in the context of security and OSINT methods?

> The biggest threat in the context of security and OSINT methods is the potential for sensitive information to be obtained and used for malicious purposes

IX. How to protect your sensitive data from OSINT search?

> To protect sensitive data from OSINT search, one can use techniques such as data encryption, access controls, and regular monitoring of public information sources.

## 5. Tasks

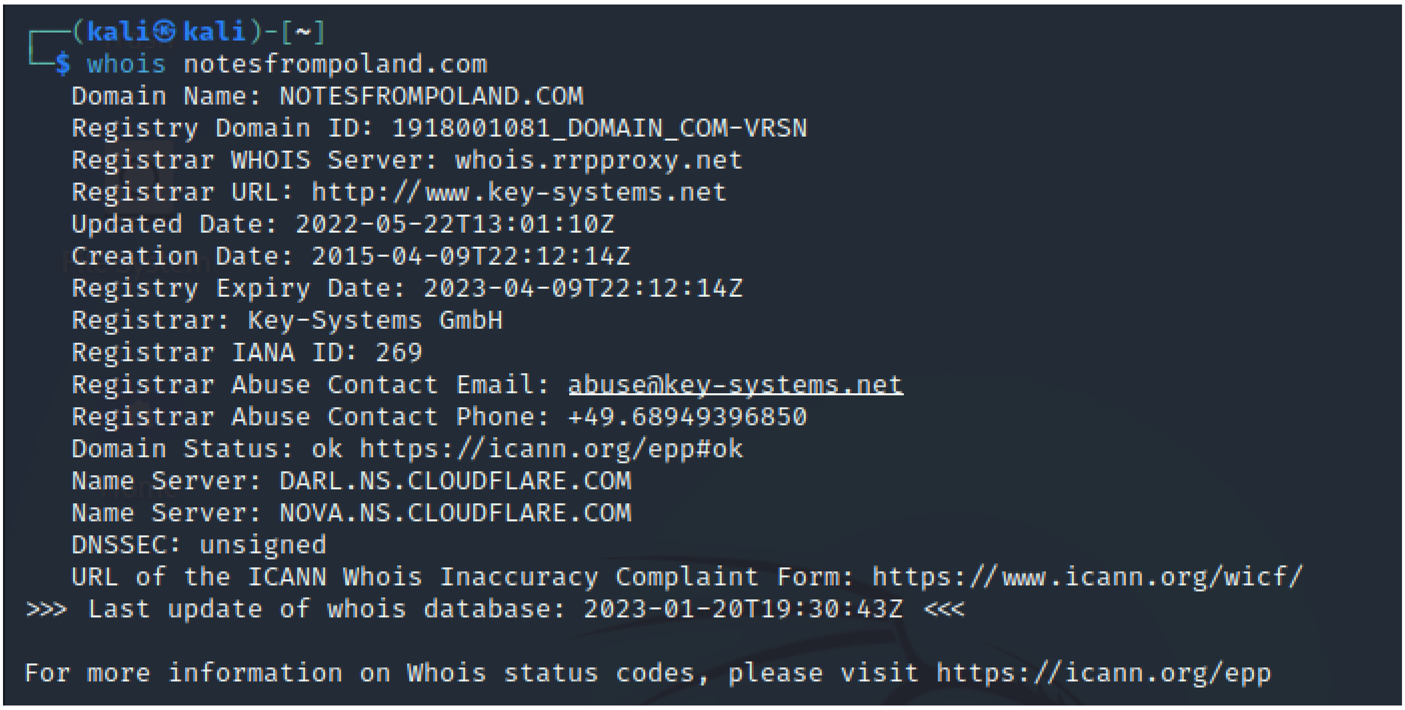
I. Select one well know domain (e.g. www.pwr.edu.pl)

Try to gather some more specific information about the domain and its owner: e.g. who have registered the domain and when, till when it is valid, is it using cloudflare or other DDOS protection,

> for this task i will be using - https://notesfrompoland.com/

II. Query the whois database about that domain

***whois example.com***

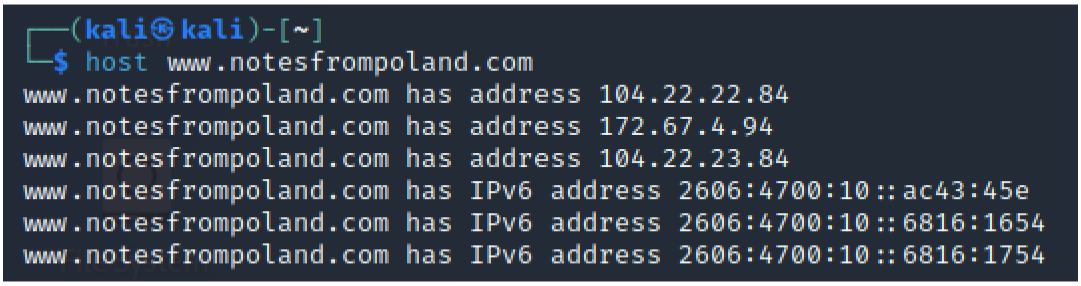


```
┌──(kali㉿kali)-[~]
└─$ whois notesfrompoland.com
   Domain Name: NOTESFROMPOLAND.COM
   Registry Domain ID: 1918001081_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.rrpproxy.net
   Registrar URL: http://www.key-systems.net
   Updated Date: 2022-05-22T13:01:10Z
   Creation Date: 2015-04-09T22:12:14Z
   Registry Expiry Date: 2023-04-09T22:12:14Z
   Registrar: Key-Systems GmbH
   Registrar IANA ID: 269
   Registrar Abuse Contact Email: abuse@key-systems.net
   Registrar Abuse Contact Phone: +49.68949396850
   Domain Status: ok https://icann.org/epp#ok
   Name Server: DARL.NS.CLOUDFLARE.COM
   Name Server: NOVA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-01-20T19:30:43Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

III. collect information about the DNS servers and the corresponding records of a target domain:

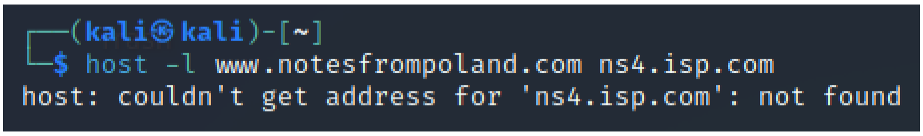
a. Use the host command line tool to lookup the IP address of a host from a DNS server

***host www.example.com***



```
┌──(kali㉿kali)-[~]
└─$ host www.notesfrompoland.com
www.notesfrompoland.com has address 104.22.22.84
www.notesfrompoland.com has address 172.67.4.94
www.notesfrompoland.com has address 104.22.23.84
www.notesfrompoland.com has IPv6 address 2606:4700:10::ac43:45e
www.notesfrompoland.com has IPv6 address 2606:4700:10::6816:1654
www.notesfrompoland.com has IPv6 address 2606:4700:10::6816:1754
```

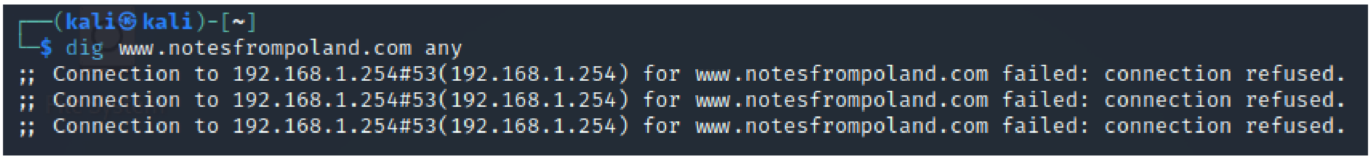
***host -l example.com ns4.isp.com  tart***



```
┌──(kali㉿kali)-[~]
└─$ host -l www.notesfrompoland.com ns4.isp.com
host: couldn't get address for 'ns4.isp.com': not found
```

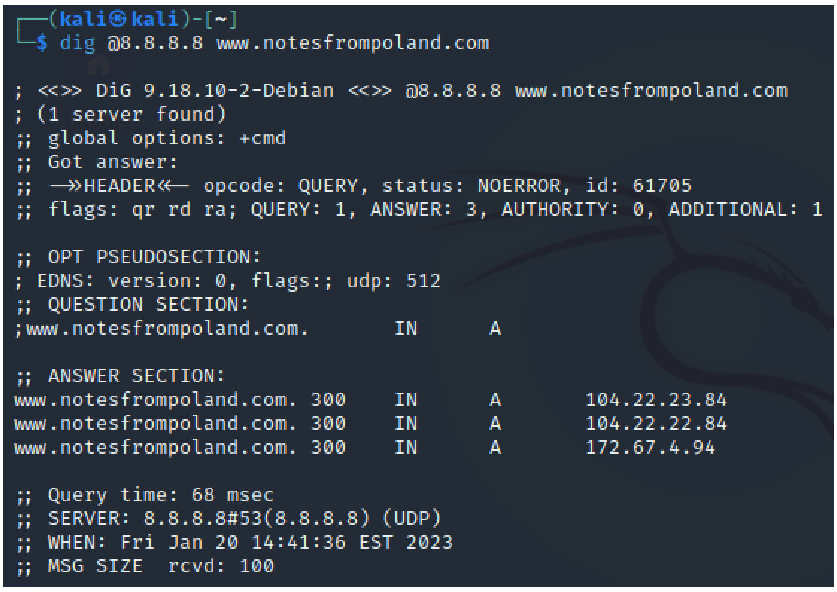
b. Use the dig command to do DNS interrogation

***dig example.com any***



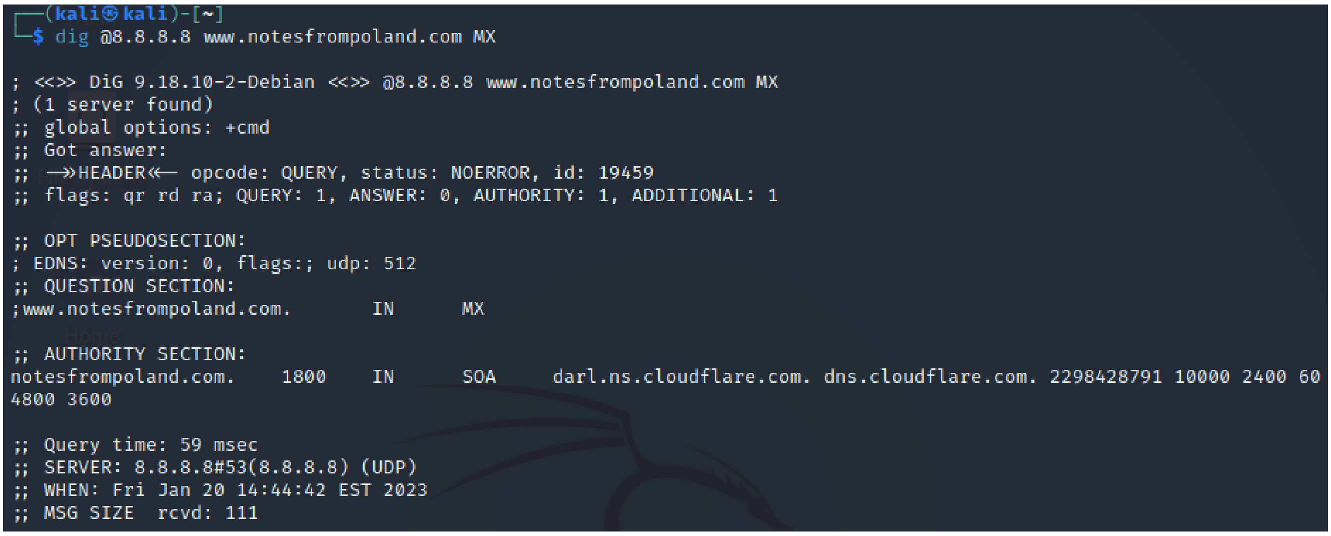
```
┌──(kali㉿kali)-[~]
└─$ dig www.notesfrompoland.com any
;; Connection to 192.168.1.254#53(192.168.1.254) for www.notesfrompoland.com failed: connection refused.
;; Connection to 192.168.1.254#53(192.168.1.254) for www.notesfrompoland.com failed: connection refused.
;; Connection to 192.168.1.254#53(192.168.1.254) for www.notesfrompoland.com failed: connection refused.
```

***dig @8.8.8.8 example.com***



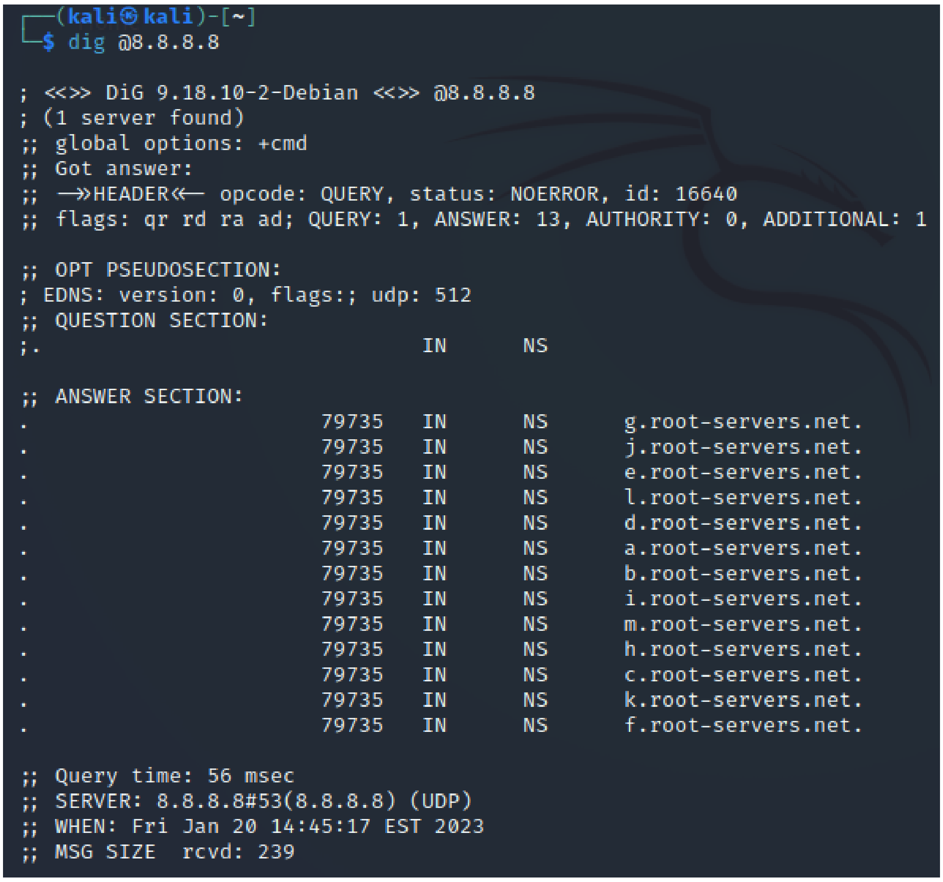
```
┌──(kali㉿kali)-[~]
└─$ dig @8.8.8.8 www.notesfrompoland.com

; <<>> DiG 9.18.10-2-Debian <<>> @8.8.8.8 www.notesfrompoland.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61705
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.notesfrompoland.com. 300    IN      A       104.22.23.84
www.notesfrompoland.com. 300    IN      A       104.22.22.84
www.notesfrompoland.com. 300    IN      A       172.67.4.94

;; Query time: 68 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Jan 20 14:41:36 EST 2023
;; MSG SIZE  rcvd: 100
```

***dig @8.8.8.8 example.com MX***



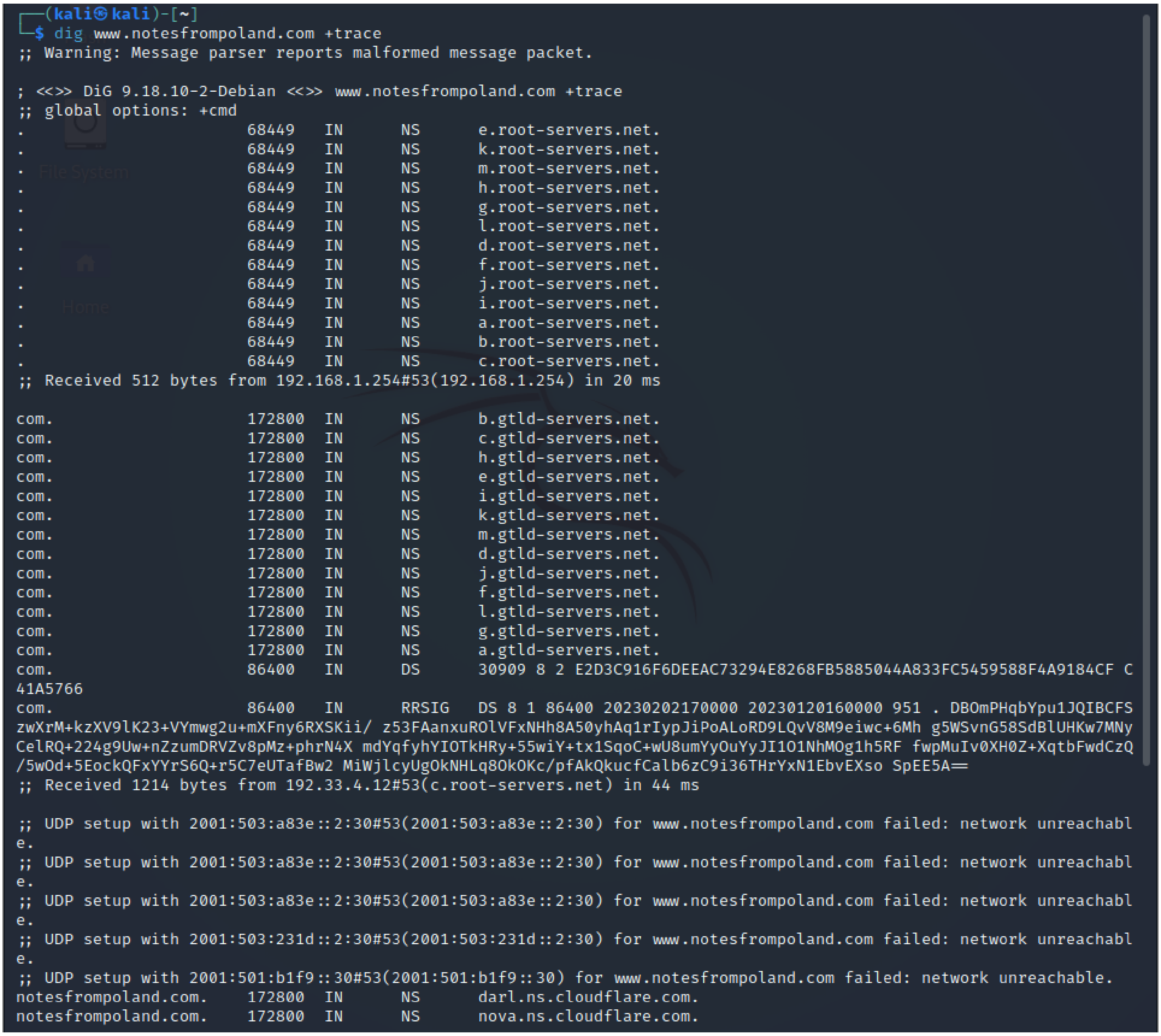
```
┌──(kali㉿kali)-[~]
└─$ dig @8.8.8.8 www.notesfrompoland.com MX

; <<>> DiG 9.18.10-2-Debian <<>> @8.8.8.8 www.notesfrompoland.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19459
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.notesfrompoland.com.       IN      MX

;; AUTHORITY SECTION:
notesfrompoland.com.    1800    IN      SOA     darl.ns.cloudflare.com. dns.cloudflare.com. 2298428791 10000 2400 60
4800 3600

;; Query time: 59 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Jan 20 14:44:42 EST 2023
;; MSG SIZE  rcvd: 111
```

*dig -x 8.8.8.8*



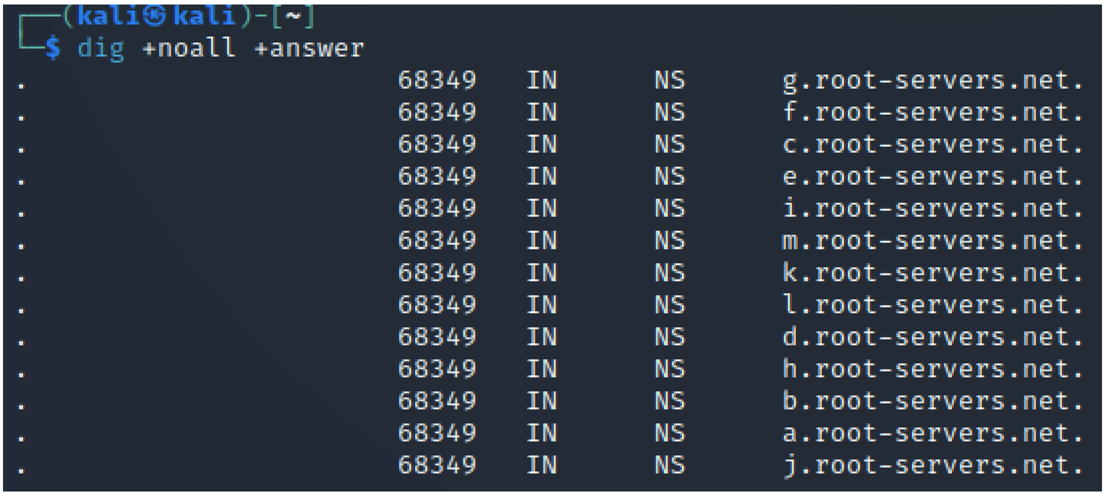
```
┌──(kali㉿kali)-[~]
└─$ dig @8.8.8.8

; <<>> DiG 9.18.10-2-Debian <<>> @8.8.8.8
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16640
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       79735   IN      NS      g.root-servers.net.
.                       79735   IN      NS      j.root-servers.net.
.                       79735   IN      NS      e.root-servers.net.
.                       79735   IN      NS      l.root-servers.net.
.                       79735   IN      NS      d.root-servers.net.
.                       79735   IN      NS      a.root-servers.net.
.                       79735   IN      NS      b.root-servers.net.
.                       79735   IN      NS      i.root-servers.net.
.                       79735   IN      NS      m.root-servers.net.
.                       79735   IN      NS      h.root-servers.net.
.                       79735   IN      NS      c.root-servers.net.
.                       79735   IN      NS      k.root-servers.net.
.                       79735   IN      NS      f.root-servers.net.

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Jan 20 14:45:17 EST 2023
;; MSG SIZE  rcvd: 239
```

*dig example.com +trace*



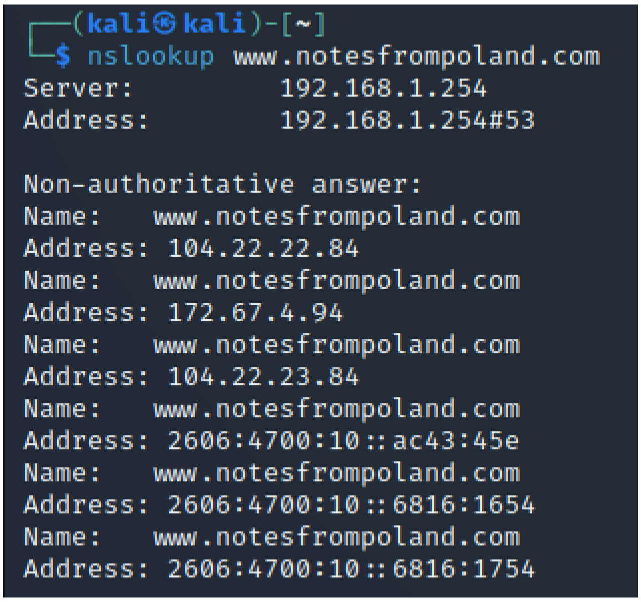
```
┌──(kali㉿kali)-[~]
└─$ dig www.notesfrompoland.com +trace
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.18.10-2-Debian <<>> www.notesfrompoland.com +trace
;; global options: +cmd
.                       68449   IN      NS      e.root-servers.net.
.                       68449   IN      NS      k.root-servers.net.
.                       68449   IN      NS      m.root-servers.net.
.                       68449   IN      NS      h.root-servers.net.
.                       68449   IN      NS      g.root-servers.net.
.                       68449   IN      NS      l.root-servers.net.
.                       68449   IN      NS      d.root-servers.net.
.                       68449   IN      NS      f.root-servers.net.
.                       68449   IN      NS      j.root-servers.net.
.                       68449   IN      NS      i.root-servers.net.
.                       68449   IN      NS      a.root-servers.net.
.                       68449   IN      NS      b.root-servers.net.
.                       68449   IN      NS      c.root-servers.net.
;; Received 512 bytes from 192.168.1.254#53(192.168.1.254) in 20 ms

com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C
41A5766
com.                    86400   IN      RRSIG   DS 8 1 86400 20230202170000 20230120160000 951 . DBOmPHqbYpu1JQIBCFS
zwXrM+kzXV9lK23+VYmwg2u+mXFny6RXSKii/ z53FAanxuROlVFxNHh8A50yhAq1rIypJiPoALoRD9LQvV8M9eiwc+6Mh g5WSvnG58SdBlUHKw7MNy
CelRQ+224g9Uw+nZzumDRVZv8pMz+phrN4X mdYqfyhYIOTkHRy+55wiY+tx1SqoC+wU8umYyOuYyJI1O1NhMOg1h5RF fwpMuIv0XH0Z+XqtbFwdCzQ
/5wOd+5EockQFxYYrS6Q+r5C7eUTafBw2 MiWjlcyUgOkNHLq8OkOKc/pfAkQkucfCalb6zC9i36THrYxN1EbvEXso SpEE5A==
;; Received 1214 bytes from 192.33.4.12#53(c.root-servers.net) in 44 ms

;; UDP setup with 2001:503:a83e::2:30#53(2001:503:a83e::2:30) for www.notesfrompoland.com failed: network unreachabl
e.
;; UDP setup with 2001:503:a83e::2:30#53(2001:503:a83e::2:30) for www.notesfrompoland.com failed: network unreachabl
e.
;; UDP setup with 2001:503:a83e::2:30#53(2001:503:a83e::2:30) for www.notesfrompoland.com failed: network unreachabl
e.
;; UDP setup with 2001:503:231d::2:30#53(2001:503:231d::2:30) for www.notesfrompoland.com failed: network unreachabl
e.
;; UDP setup with 2001:501:b1f9::30#53(2001:501:b1f9::30) for www.notesfrompoland.com failed: network unreachable.
notesfrompoland.com.    172800  IN      NS      darl.ns.cloudflare.com.
notesfrompoland.com.    172800  IN      NS      nova.ns.cloudflare.com.
```

***dig +noall +answer***



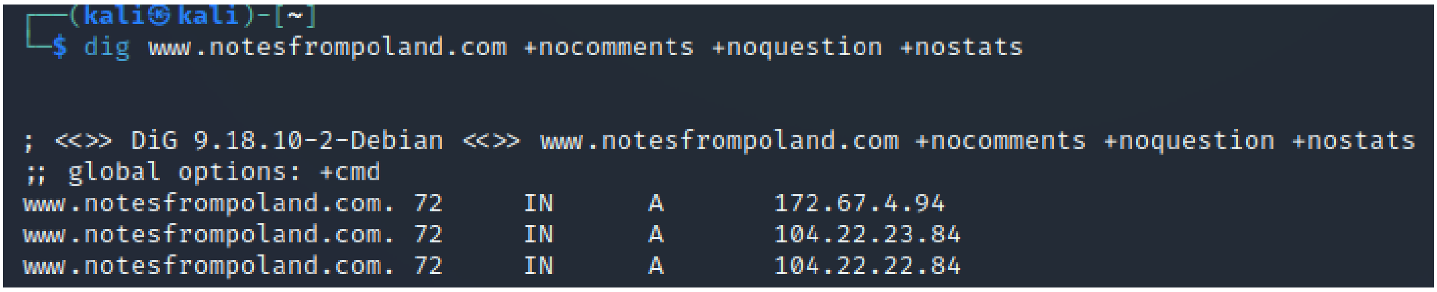
```
┌──(kali㉿kali)-[~]
└─$ dig +noall +answer
.                       68349   IN      NS      g.root-servers.net.
.                       68349   IN      NS      f.root-servers.net.
.                       68349   IN      NS      c.root-servers.net.
.                       68349   IN      NS      e.root-servers.net.
.                       68349   IN      NS      i.root-servers.net.
.                       68349   IN      NS      m.root-servers.net.
.                       68349   IN      NS      k.root-servers.net.
.                       68349   IN      NS      l.root-servers.net.
.                       68349   IN      NS      d.root-servers.net.
.                       68349   IN      NS      h.root-servers.net.
.                       68349   IN      NS      b.root-servers.net.
.                       68349   IN      NS      a.root-servers.net.
.                       68349   IN      NS      j.root-servers.net.
```

- Find the primary DNS for a given domain



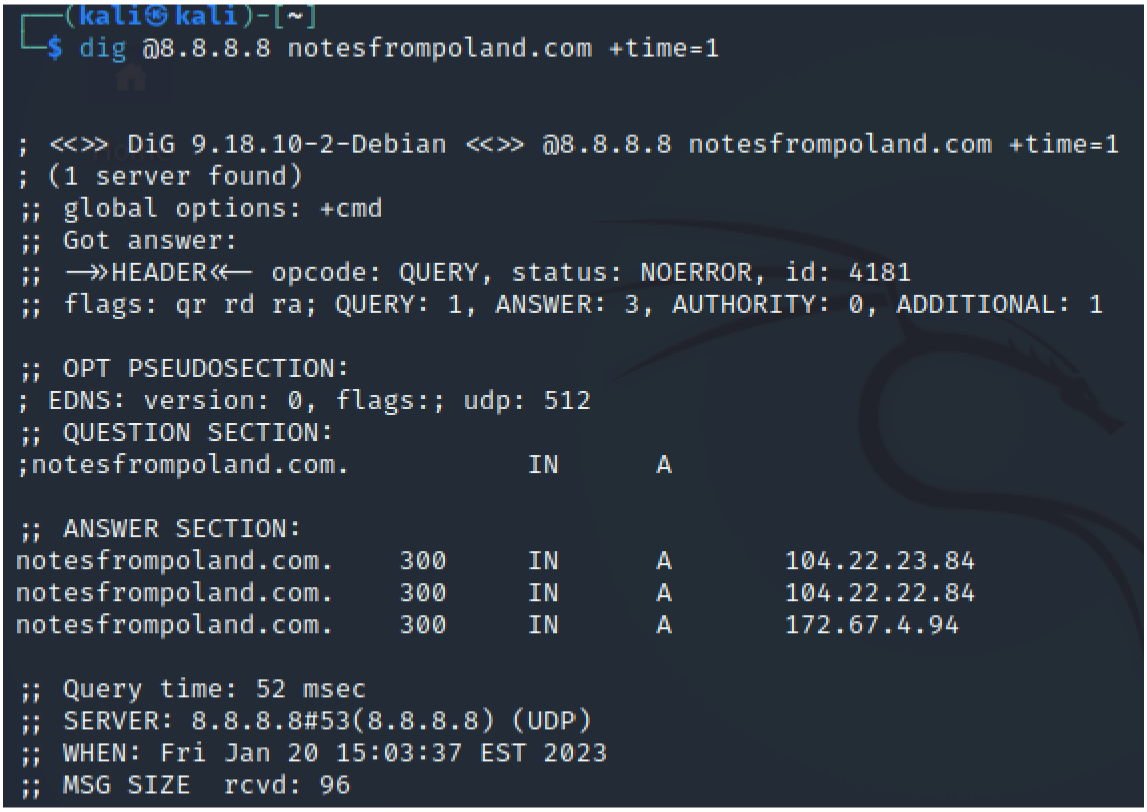
```
┌──(kali㉿kali)-[~]
└─$ nslookup www.notesfrompoland.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   www.notesfrompoland.com
Address: 104.22.22.84
Name:   www.notesfrompoland.com
Address: 172.67.4.94
Name:   www.notesfrompoland.com
Address: 104.22.23.84
Name:   www.notesfrompoland.com
Address: 2606:4700:10::ac43:45e
Name:   www.notesfrompoland.com
Address: 2606:4700:10::6816:1654
Name:   www.notesfrompoland.com
Address: 2606:4700:10::6816:1754
```

- Try to find out what is TTL and if the requested domain was cached by DNS.



```
┌──(kali㉿kali)-[~]
└─$ dig www.notesfrompoland.com +nocomments +noquestion +nostats


; <<>> DiG 9.18.10-2-Debian <<>> www.notesfrompoland.com +nocomments +noquestion +nostats
;; global options: +cmd
www.notesfrompoland.com. 72     IN      A       172.67.4.94
www.notesfrompoland.com. 72     IN      A       104.22.23.84
www.notesfrompoland.com. 72     IN      A       104.22.22.84
```

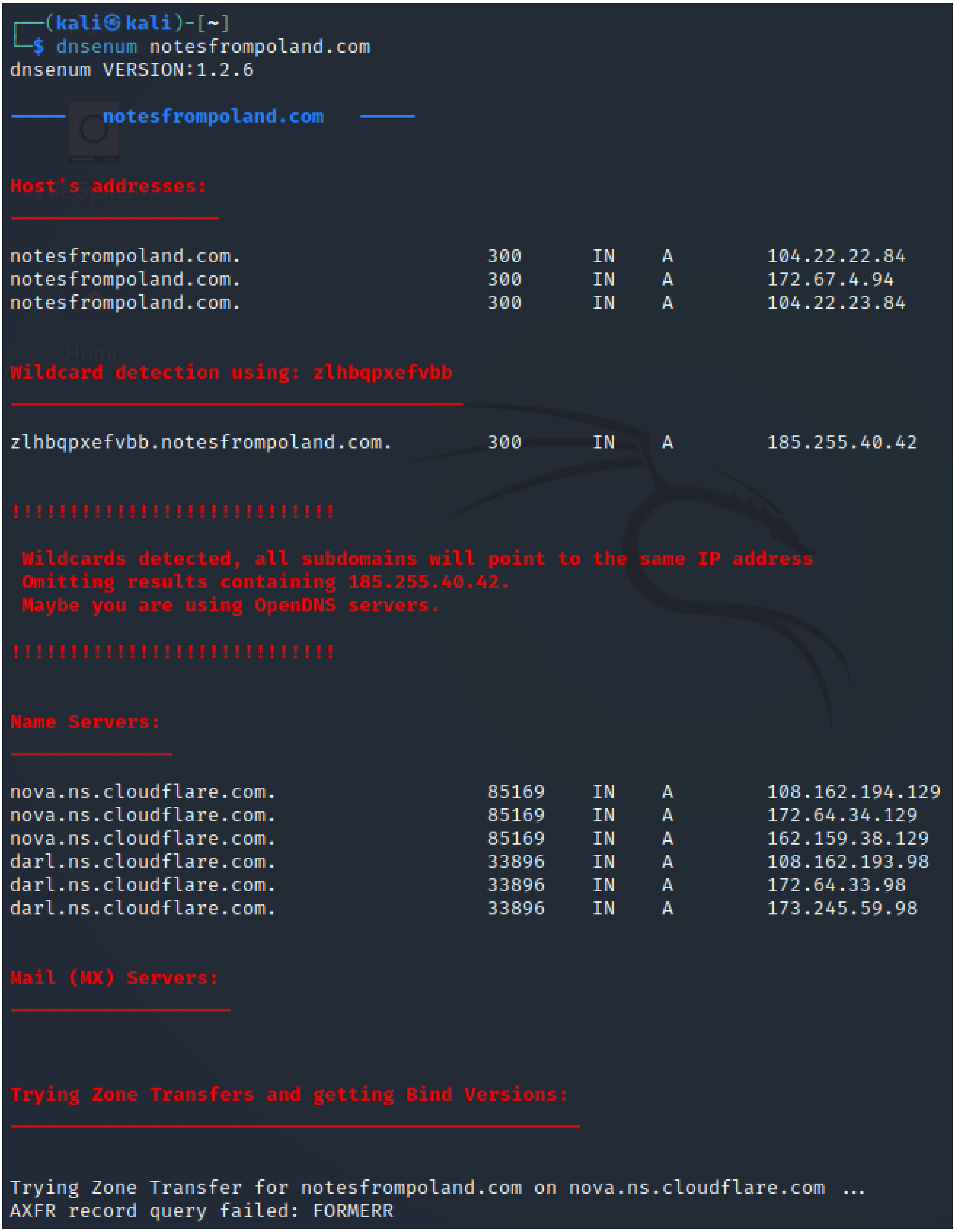
- Find out how long ago the given domain was requested at some DNSs (e.g. 1.1.1.1, 8.8.8.8, local DNS,…)



```
┌──(kali㉿kali)-[~]
└─$ dig @8.8.8.8 notesfrompoland.com +time=1


; <<>> DiG 9.18.10-2-Debian <<>> @8.8.8.8 notesfrompoland.com +time=1
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4181
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
notesfrompoland.com.    300     IN      A       104.22.23.84
notesfrompoland.com.    300     IN      A       104.22.22.84
notesfrompoland.com.    300     IN      A       172.67.4.94

;; Query time: 52 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Jan 20 15:03:37 EST 2023
;; MSG SIZE  rcvd: 96
```

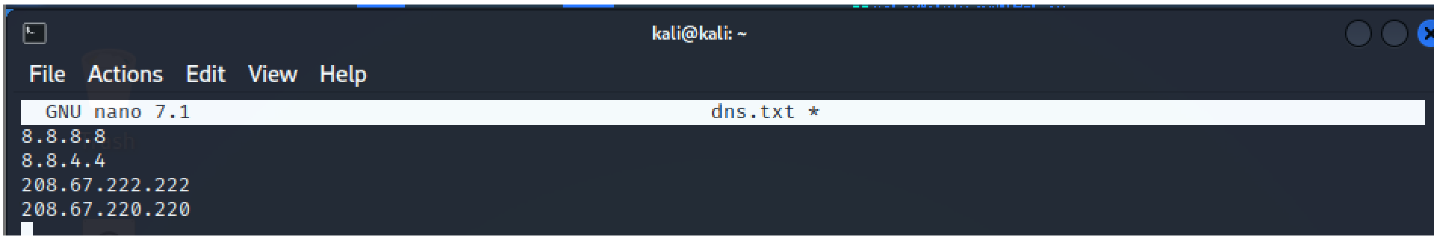
IV. Utilize dnsenum

***dnsenum example.com***

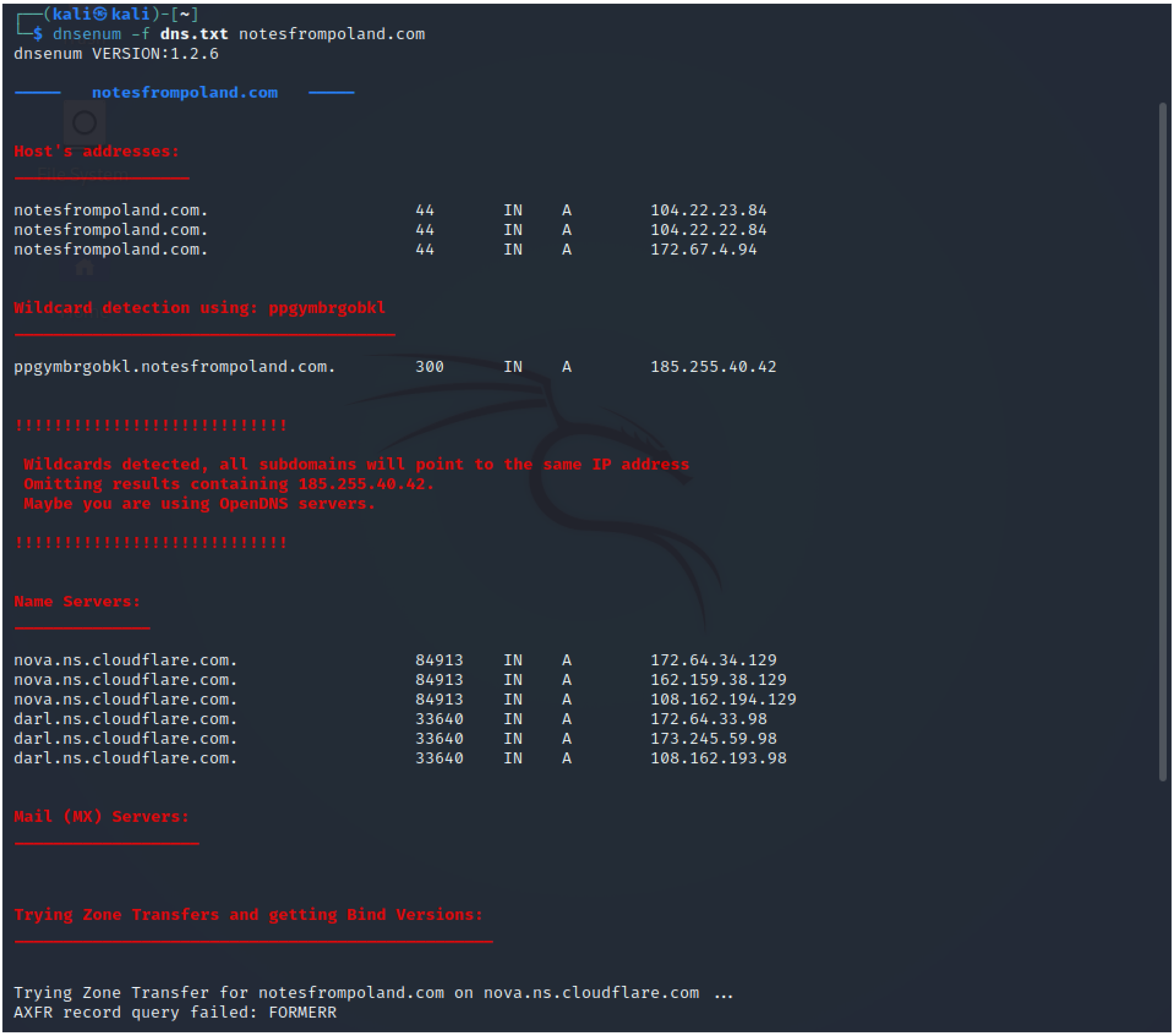


```
┌──(kali㉿kali)-[~]
└─$ dnsenum notesfrompoland.com
dnsenum VERSION:1.2.6

-----   notesfrompoland.com   -----


Host's addresses:
__________________

notesfrompoland.com.                     300      IN    A        104.22.22.84
notesfrompoland.com.                     300      IN    A        172.67.4.94
notesfrompoland.com.                     300      IN    A        104.22.23.84


Wildcard detection using: zlhbqpxefvbb
_______________________________________

zlhbqpxefvbb.notesfrompoland.com.        300      IN    A        185.255.40.42


!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 185.255.40.42.
 Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Name Servers:
______________

nova.ns.cloudflare.com.                  85169    IN    A        108.162.194.129
nova.ns.cloudflare.com.                  85169    IN    A        172.64.34.129
nova.ns.cloudflare.com.                  85169    IN    A        162.159.38.129
darl.ns.cloudflare.com.                  33896    IN    A        108.162.193.98
darl.ns.cloudflare.com.                  33896    IN    A        172.64.33.98
darl.ns.cloudflare.com.                  33896    IN    A        173.245.59.98


Mail (MX) Servers:
___________________



Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for notesfrompoland.com on nova.ns.cloudflare.com ...
AXFR record query failed: FORMERR
```

***dnsenum -f dns.txt example.com***

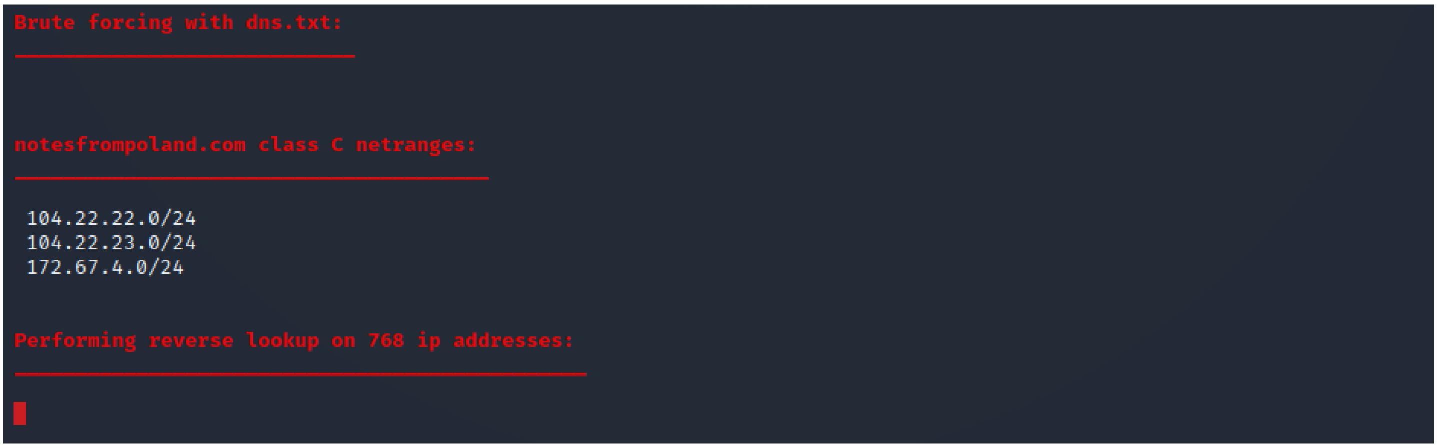


```
  GNU nano 7.1                                    dns.txt *
8.8.8.8
8.8.4.4
208.67.222.222
208.67.220.220
```



```
┌──(kali㉿kali)-[~]
└─$ dnsenum -f dns.txt notesfrompoland.com
dnsenum VERSION:1.2.6

─────   notesfrompoland.com   ─────


Host's addresses:
__________________

notesfrompoland.com.                     44       IN    A        104.22.23.84
notesfrompoland.com.                     44       IN    A        104.22.22.84
notesfrompoland.com.                     44       IN    A        172.67.4.94


Wildcard detection using: ppgymbrgobkl
_______________________________________

ppgymbrgobkl.notesfrompoland.com.        300      IN    A        185.255.40.42


!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 185.255.40.42.
 Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Name Servers:
______________

nova.ns.cloudflare.com.                  84913    IN    A        172.64.34.129
nova.ns.cloudflare.com.                  84913    IN    A        162.159.38.129
nova.ns.cloudflare.com.                  84913    IN    A        108.162.194.129
darl.ns.cloudflare.com.                  33640    IN    A        172.64.33.98
darl.ns.cloudflare.com.                  33640    IN    A        173.245.59.98
darl.ns.cloudflare.com.                  33640    IN    A        108.162.193.98


Mail (MX) Servers:
___________________



Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for notesfrompoland.com on nova.ns.cloudflare.com ...
AXFR record query failed: FORMERR
```

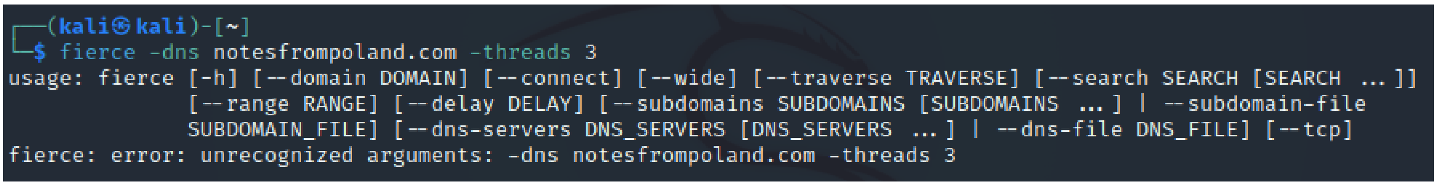
***>> After waiting a while it still remains the same <<***



```
Brute forcing with dns.txt:
_____________________________


notesfrompoland.com class C netranges:
_______________________________________

 104.22.22.0/24
 104.22.23.0/24
 172.67.4.0/24

Performing reverse lookup on 768 ip addresses:
_______________________________________________

█
```

V. Find all of the IP addresses and hostnames of a target

***fierce -dns example.com -threads 3***

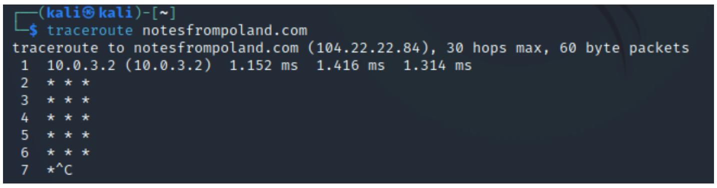


```
┌──(kali㉿kali)-[~]
└─$ fierce -dns notesfrompoland.com -threads 3
usage: fierce [-h] [--domain DOMAIN] [--connect] [--wide] [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]]
              [--range RANGE] [--delay DELAY] [--subdomains SUBDOMAINS [SUBDOMAINS ...] | --subdomain-file
              SUBDOMAIN_FILE] [--dns-servers DNS_SERVERS [DNS_SERVERS ...] | --dns-file DNS_FILE] [--tcp]
fierce: error: unrecognized arguments: -dns notesfrompoland.com -threads 3
```

***It is returning as an error!***

VI. Get network routing information.
a. Using tcptraceroute

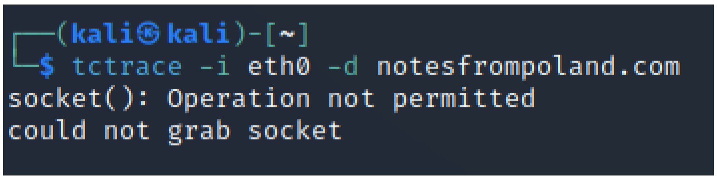
***traceroute www.example.com***



```
┌──(kali㉿kali)-[~]
└─$ traceroute notesfrompoland.com
traceroute to notesfrompoland.com (104.22.22.84), 30 hops max, 60 byte packets
 1  10.0.3.2 (10.0.3.2)  1.152 ms  1.416 ms  1.314 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *^C
```

b. Using tctrace

***tctrace -i<network_interface> -d<targethost>***



```
┌──(kali㉿kali)-[~]
└─$ tctrace -i eth0 -d notesfrompoland.com
socket(): Operation not permitted
could not grab socket
```

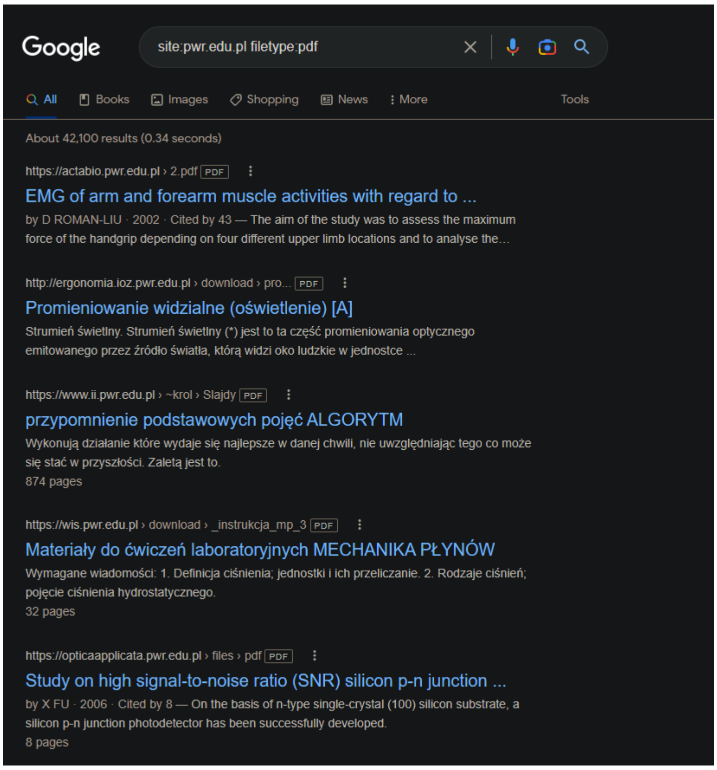
VII. Summarize your findings, compare tools and obtained results. What type of information do they provide? How malicious user can benefit from this type of information? Which tool is the most versatile?

> In this discussion, various command-line tools were presented

for gathering information about a target domain, such as, "dig", "whois", "dnsenum" and "fierce". Out of these, i was determined that "dig" was the most useful tool, as it provides extensive information about DNS servers, IP address and TTL value.

VIII. Try to find some Vulnerable Files or sensible information using google hacking  method (e.g. in domain pwr.*.edu.pl or in some other domain):

a. Search for documents files (.doc, .docx, .txt, .xls, pdf,….)



site:pwr.edu.pl filetype:pdf

About 42,100 results (0.34 seconds)

https://actabio.pwr.edu.pl › 2.pdf PDF
EMG of arm and forearm muscle activities with regard to ...
by D ROMAN-LIU · 2002 · Cited by 43 — The aim of the study was to assess the maximum force of the handgrip depending on four different upper limb locations and to analyse the...

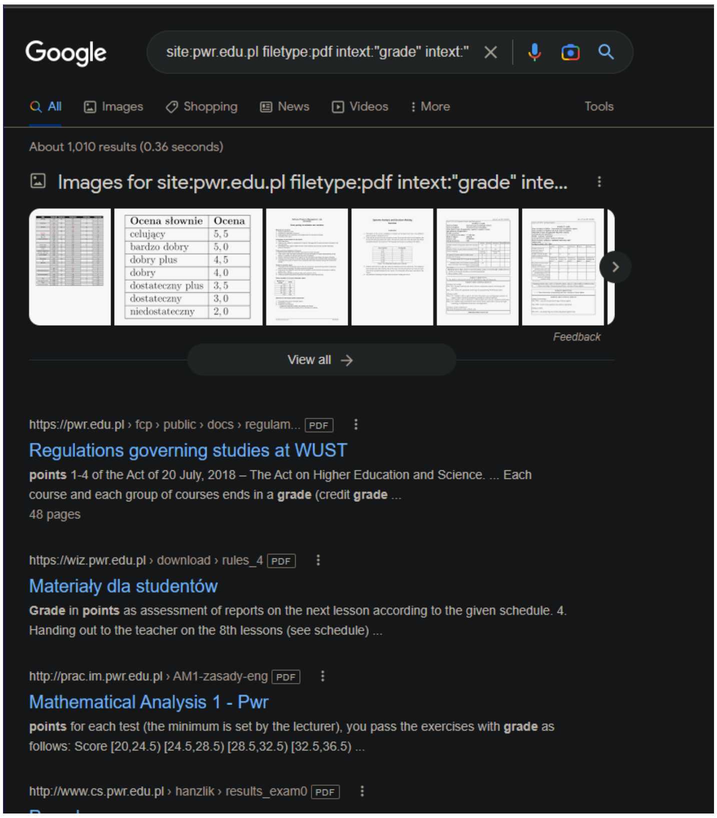
http://ergonomia.ioz.pwr.edu.pl › download › pro... PDF
Promieniowanie widzialne (oświetlenie) [A]
Strumień świetlny. Strumień świetlny (*) jest to ta część promieniowania optycznego emitowanego przez źródło światła, którą widzi oko ludzkie w jednostce ...

https://www.ii.pwr.edu.pl › ~krol › Slajdy PDF
przypomnienie podstawowych pojęć ALGORYTM
Wykonują działanie które wydaje się najlepsze w danej chwili, nie uwzględniając tego co może się stać w przyszłości. Zaletą jest to.
874 pages

https://wis.pwr.edu.pl › download › _instrukcja_mp_3 PDF
Materiały do ćwiczeń laboratoryjnych MECHANIKA PŁYNÓW
Wymagane wiadomości: 1. Definicja ciśnienia; jednostki i ich przeliczanie. 2. Rodzaje ciśnień; pojęcie ciśnienia hydrostatycznego.
32 pages

https://opticaapplicata.pwr.edu.pl › files › pdf PDF
Study on high signal-to-noise ratio (SNR) silicon p-n junction ...
by X FU · 2006 · Cited by 8 — On the basis of n-type single-crystal (100) silicon substrate, a silicon p-n junction photodetector has been successfully developed.
8 pages

b. Search for documents with some specific content (e.g. grade, password,  points, addresses, …)



About 1,010 results (0.36 seconds)

Images for site:pwr.edu.pl filetype:pdf intext:"grade" inte...

| Ocena słownie | Ocena |
|---|---|
| celujący | 5, 5 |
| bardzo dobry | 5, 0 |
| dobry plus | 4, 5 |
| dobry | 4, 0 |
| dostateczny plus | 3, 5 |
| dostateczny | 3, 0 |
| niedostateczny | 2, 0 |

https://pwr.edu.pl › fcp › public › docs › regulam... PDF

Regulations governing studies at WUST

**points** 1-4 of the Act of 20 July, 2018 – The Act on Higher Education and Science. ... Each course and each group of courses ends in a **grade** (credit **grade** ...

48 pages

https://wiz.pwr.edu.pl › download › rules_4 PDF

Materiały dla studentów

**Grade** in **points** as assessment of reports on the next lesson according to the given schedule. 4. Handing out to the teacher on the 8th lessons (see schedule) ...

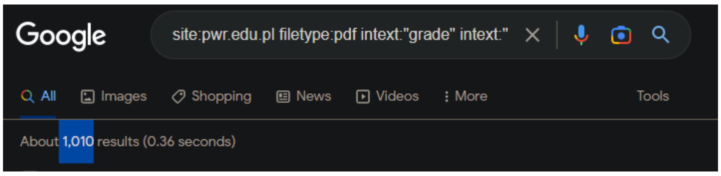
http://prac.im.pwr.edu.pl › AM1-zasady-eng PDF

Mathematical Analysis 1 - Pwr

**points** for each test (the minimum is set by the lecturer), you pass the exercises with **grade** as follows: Score [20,24.5) [24.5,28.5) [28.5,32.5) [32.5,36.5) ...

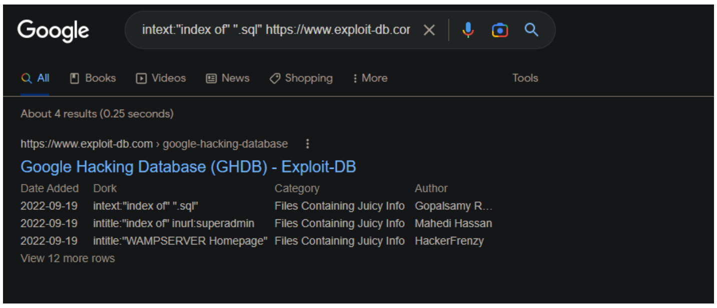
http://www.cs.pwr.edu.pl › hanzlik › results_exam0 PDF

c. Create statistics of findings (number of files, number of IP addresses, number of users, …)



About 1,010 results (0.36 seconds)

d. Find some interesting data using selected dorks from https://www.exploit-db.com/google-hacking-database/



About 4 results (0.25 seconds)

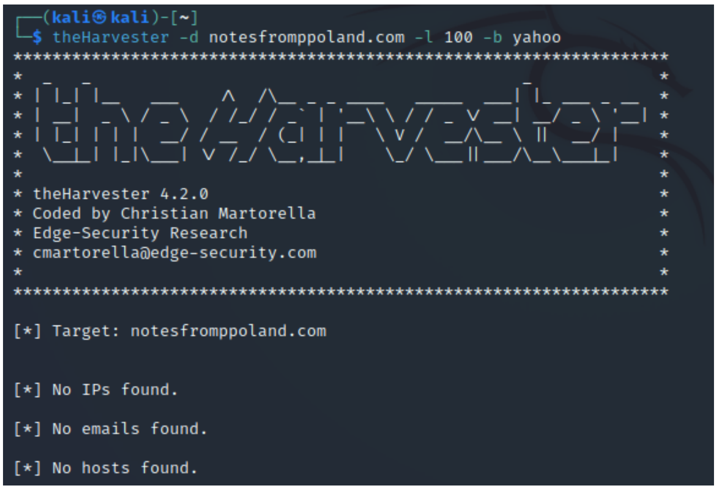
https://www.exploit-db.com › google-hacking-database

Google Hacking Database (GHDB) - Exploit-DB

| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2022-09-19 | intext:"index of" ".sql" | Files Containing Juicy Info | Gopalsamy R... |
| 2022-09-19 | intitle:"index of" inurl:superadmin | Files Containing Juicy Info | Mahedi Hassan |
| 2022-09-19 | intitle:"WAMPSERVER Homepage" | Files Containing Juicy Info | HackerFrenzy |

View 12 more rows

IX. Use theharvester to collect e-mail accounts, username, and hostname/subdomains: ***theharvester -d example.com -l 100 -b linkedin***
for a given domain name try to search data using different data sources (e.g. baidu,  bing, yahoo or use all)

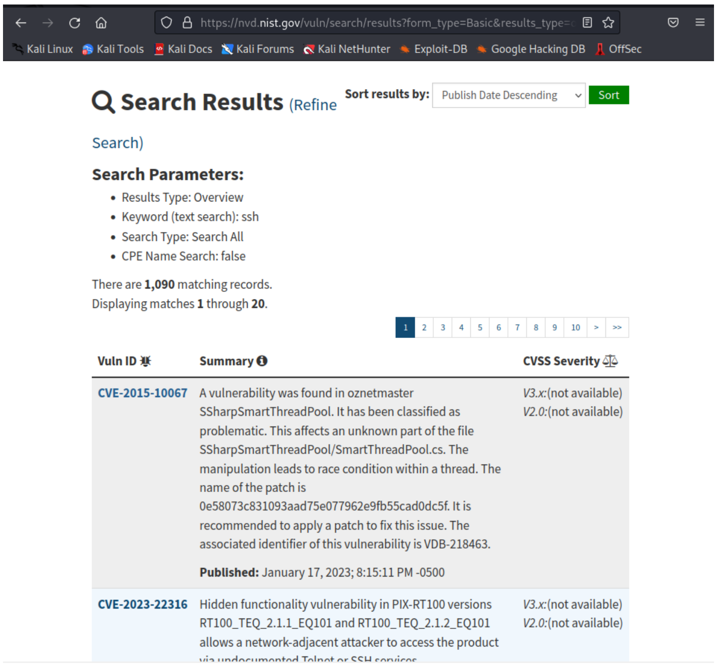


```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d notesfromppoland.com -l 100 -b yahoo
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: notesfromppoland.com


[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

X. Using https://nvd.nist.gov/vuln/search search for some vulnerabilities in some  type of the service (***ssh, ftp, ssl, apache, qnap, western digital*** …) and in next  query related to some device (e.g. ***wireless router, asus wireless router, tp-link***).  Find some specific problem related to this service (device) – it is described as CVE  – year – number.

>

ssh



## Search Results (Refine Search)

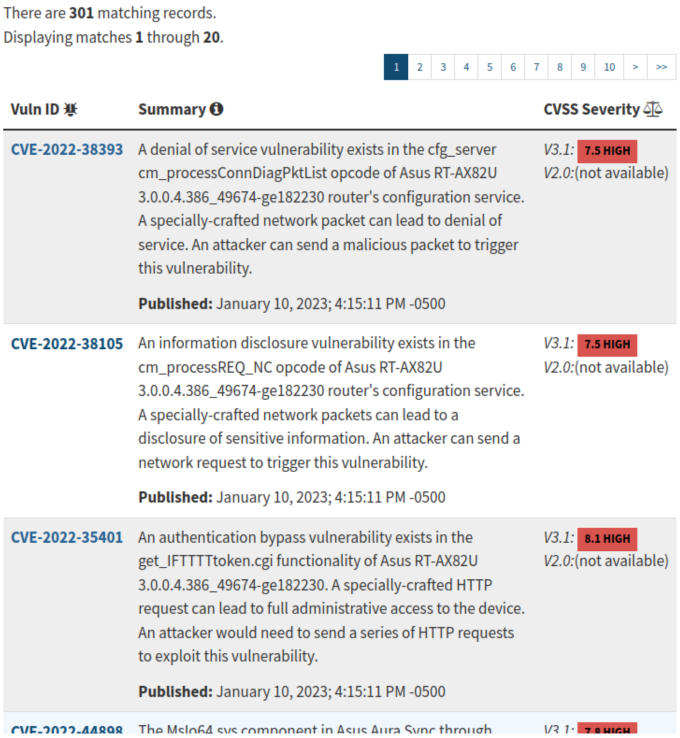
### Search Parameters:

- Results Type: Overview
- Keyword (text search): ssh
- Search Type: Search All
- CPE Name Search: false

There are **1,090** matching records.
Displaying matches **1** through **20**.

| Vuln ID | Summary | CVSS Severity |
|---|---|---|
| CVE-2015-10067 | A vulnerability was found in oznetmaster SSharpSmartThreadPool. It has been classified as problematic. This affects an unknown part of the file SSharpSmartThreadPool/SmartThreadPool.cs. The manipulation leads to race condition within a thread. The name of the patch is 0e58073c831093aad75e077962e9fb55cad0dc5f. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218463.<br>**Published:** January 17, 2023; 8:15:11 PM -0500 | *V3.x:*(not available)<br>*V2.0:*(not available) |
| CVE-2023-22316 | Hidden functionality vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker to access the product via undocumented Telnet or SSH services | *V3.x:*(not available)<br>*V2.0:*(not available) |

# Asus - routers



There are **301** matching records.
Displaying matches **1** through **20**.

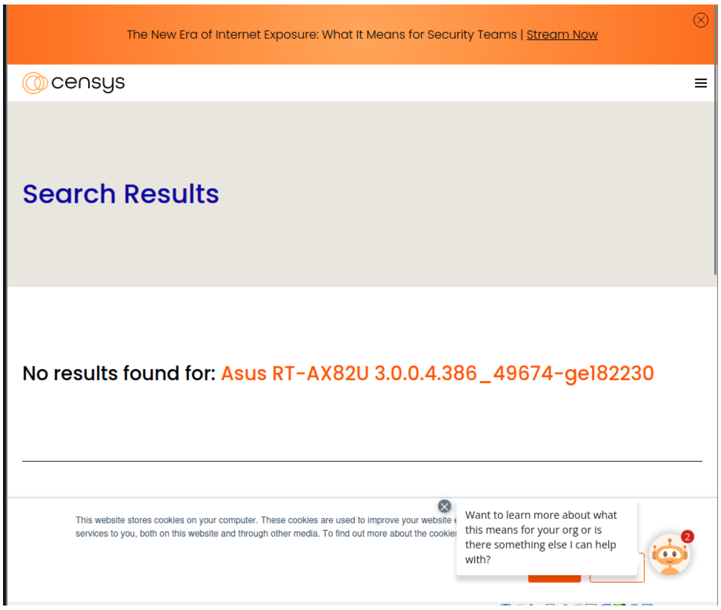
| Vuln ID | Summary | CVSS Severity |
|---|---|---|
| CVE-2022-38393 | A denial of service vulnerability exists in the cfg_server cm_processConnDiagPktList opcode of Asus RT-AX82U 3.0.0.4.386_49674-ge182230 router's configuration service. A specially-crafted network packet can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.<br>**Published:** January 10, 2023; 4:15:11 PM -0500 | *V3.1:* 7.5 HIGH<br>*V2.0:*(not available) |
| CVE-2022-38105 | An information disclosure vulnerability exists in the cm_processREQ_NC opcode of Asus RT-AX82U 3.0.0.4.386_49674-ge182230 router's configuration service. A specially-crafted network packets can lead to a disclosure of sensitive information. An attacker can send a network request to trigger this vulnerability.<br>**Published:** January 10, 2023; 4:15:11 PM -0500 | *V3.1:* 7.5 HIGH<br>*V2.0:*(not available) |
| CVE-2022-35401 | An authentication bypass vulnerability exists in the get_IFTTTtoken.cgi functionality of Asus RT-AX82U 3.0.0.4.386_49674-ge182230. A specially-crafted HTTP request can lead to full administrative access to the device. An attacker would need to send a series of HTTP requests to exploit this vulnerability.<br>**Published:** January 10, 2023; 4:15:11 PM -0500 | *V3.1:* 8.1 HIGH<br>*V2.0:*(not available) |
| CVE-2022-44898 | The MsIo64.sys component in Asus Aura Sync through | *V3.1:* 7.8 HIGH |

Description of the latest thread(problem),
Asus RT-AX82U 3.0.0.4.386_49674-ge182230
https://nvd.nist.gov/vuln/detail/CVE-2022-38393

Find critical vulnerabilities. Describe the vulnerability. Find the link to the webpage with exploit or/and detailed description of the vulnerability.

XI. Using results from the previous point (e.g. openssh 7.7 is vulnerable) search for the systems with this vulnerability (from point X) using

a. https://censys.io



The New Era of Internet Exposure: What It Means for Security Teams | Stream Now

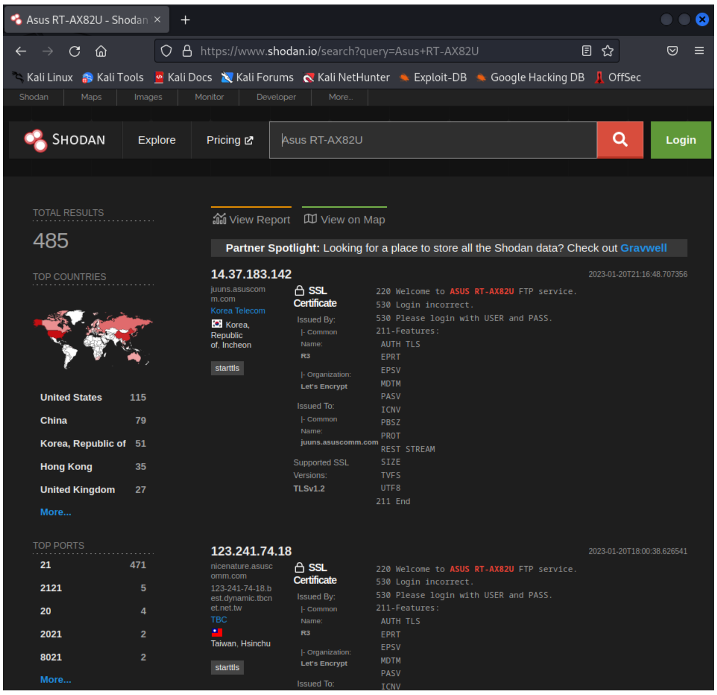
Search Results

No results found for: Asus RT-AX82U 3.0.0.4.386_49674-ge182230

This website stores cookies on your computer. These cookies are used to improve your website e
services to you, both on this website and through other media. To find out more about the cookies

Want to learn more about what this means for your org or is there something else I can help with?

b. https://www.shodan.io



TOTAL RESULTS

485

TOP COUNTRIES

| | |
|---|---|
| United States | 115 |
| China | 79 |
| Korea, Republic of | 51 |
| Hong Kong | 35 |
| United Kingdom | 27 |
| More... | |

TOP PORTS

| | |
|---|---|
| 21 | 471 |
| 2121 | 5 |
| 20 | 4 |
| 2021 | 2 |
| 8021 | 2 |
| More... | |

**Partner Spotlight:** Looking for a place to store all the Shodan data? Check out Gravwell

**14.37.183.142** 2023-01-20T21:16:48.707356

juuns.asuscomm.com
Korea Telecom
Korea, Republic of, Incheon
starttls

SSL Certificate
Issued By:
|- Common Name: R3
|- Organization: Let's Encrypt
Issued To:
|- Common Name: juuns.asuscomm.com
Supported SSL Versions: TLSv1.2

```
220 Welcome to ASUS RT-AX82U FTP service.
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
 AUTH TLS
 EPRT
 EPSV
 MDTM
 PASV
 ICNV
 PBSZ
 PROT
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End
```

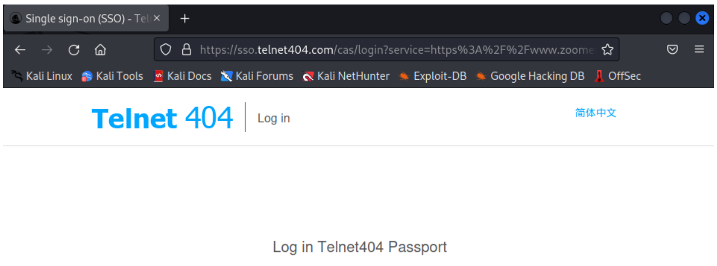
**123.241.74.18** 2023-01-20T18:00:38.626541

nicenature.asuscomm.com
123-241-74-18.best.dynamic.tbcnet.net.tw
TBC
Taiwan, Hsinchu
starttls

SSL Certificate
Issued By:
|- Common Name: R3
|- Organization: Let's Encrypt
Issued To:

```
220 Welcome to ASUS RT-AX82U FTP service.
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
 AUTH TLS
 EPRT
 EPSV
 MDTM
 PASV
 ICNV
```

c. https://zoomeye.org



Log in Telnet404 Passport

Write how many vulnerable systems have been found. Which countries are the 'top most' vulnerable?

>> censys & zoomeye had an error,

Where shodan found vulnerable results!