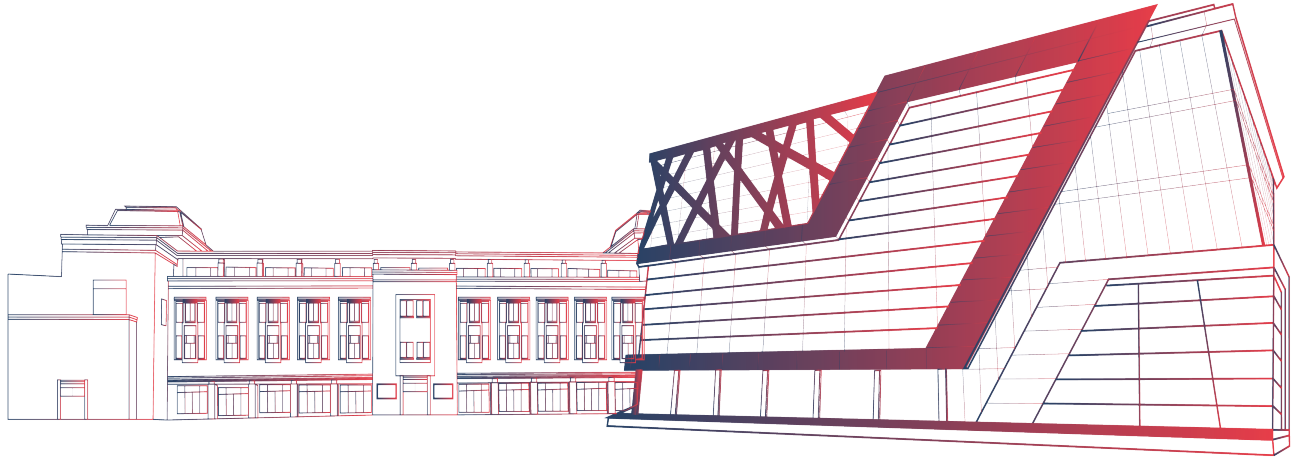
THE NORTHCAP UNIVERSITY

Information Gathering Tools (cont.)



30 YEARS OF EXCELLENCE

NAAC Accredited

Case Study

JW Marriott site was hacked where information of credit cards were leaked (search)

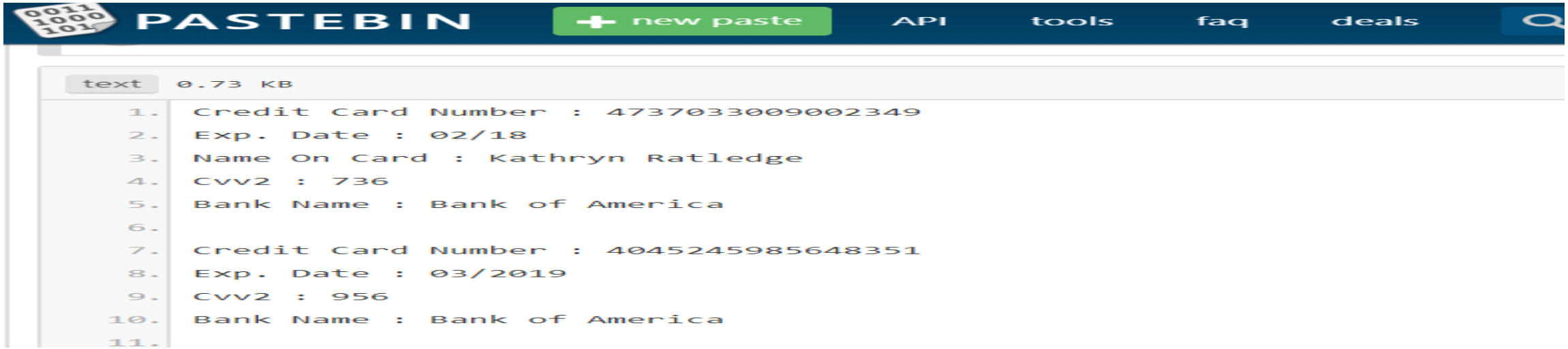
Marriott hotels hacked, credit card details and data of 500 million guests stolen: All you need to know

Hackers have stolen data of nearly 500 million guests who stayed at Marriott group hotels. This data includes in some cases credit card details, addresses and passport scans that people submitted to Marriott.

https://www.indiatoday.in/technology/features/story/marriott-hotels-hacked-credit-card-details-and-data-of-500-million-guests-stolen-all-you-need-to-know-1400263-2018-12-01

Pastebin.com
https://pastebin.com/

- It leaked out Credit card info with CVV.
- If you say OTP is required, internationally OTP's are not required.
- To break OTP is also not big task
- https://pastebin.com/fcte4qNL
- A **pastebin** is a Web **application** that allows users to upload and share text online. The most common use is for sharing source code or configuration information. There are thousands of pastebins online, often geared towards particular groups or focuses. Once text has been uploaded to a **pastebin**, other users can edit.
- It seems to be frequently **used** as a public repository of stolen information, such as network configuration details and authentication records.



Why is Pastebin blocked?

Pastebin was **blocked** because the BTK, Turkey's Information and Communication Technologies Authority was hacked by famous hacker community Anonymous and information obtained from the agency was dumped to **Pastebin**.

Case Study

- LPG gas
- Indane 7 million aadhaar cards breached (search)
- It gave details of 7 million people passbook 1st page
- https://www.indiatoday.in/technology/news/story/aadhaar-leaks-again-indane-gas-website-app-leak-data-of-6-7-million-subscribers-1459499-2019-02-19

Aadhaar leaks again: Indane Gas website, app leak data of 6.7 million subscribers

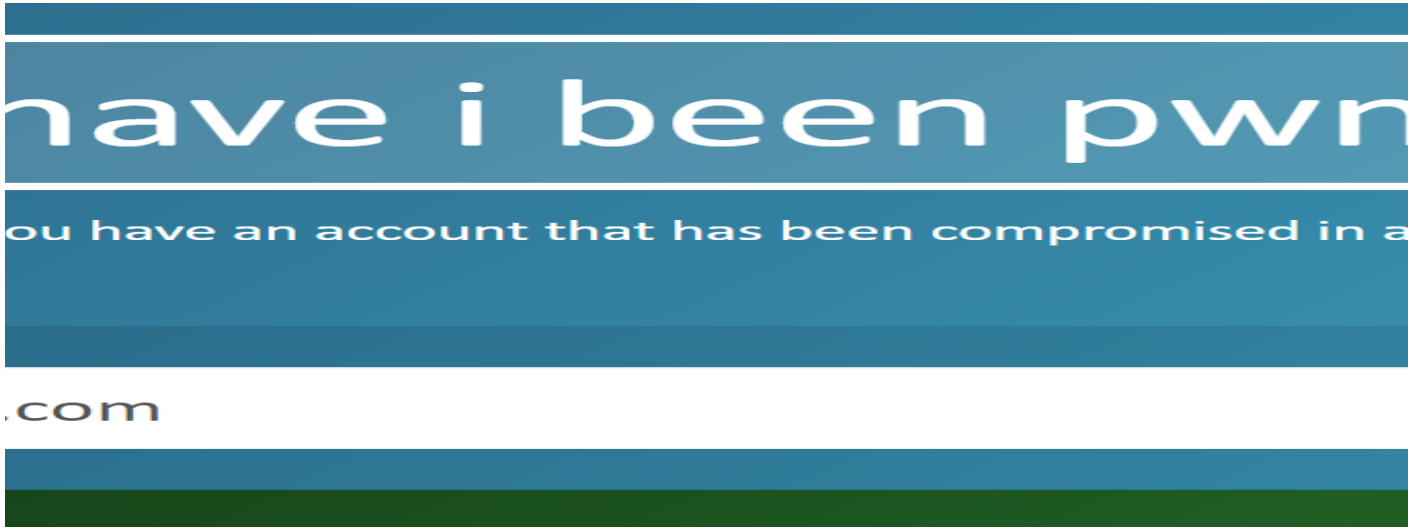
Security Researcher Elliot Anderson has discovered a huge leak of Aadhaar numbers from Indane's website as well as app. The leak has put Aadhaar number of 6.7 million people at stake.

Tool 10,11,12

Haveibeenpwned.com

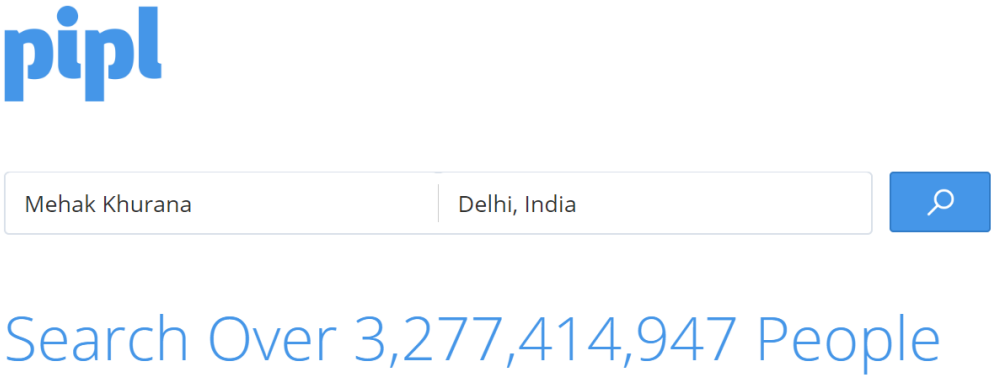
Have I Been Pwned?- is a website that allows Internet users to check whether their personal data has been compromised by data breaches.

- **Personal data has been compromised** by data breaches.
- **Collects and analyzes hundreds of database** dumps of billions of leaked accounts.
- Allows users to **search for their own information** by entering their username or email address.
- Users can also sign up to be notified if their email address appears in future dumps.

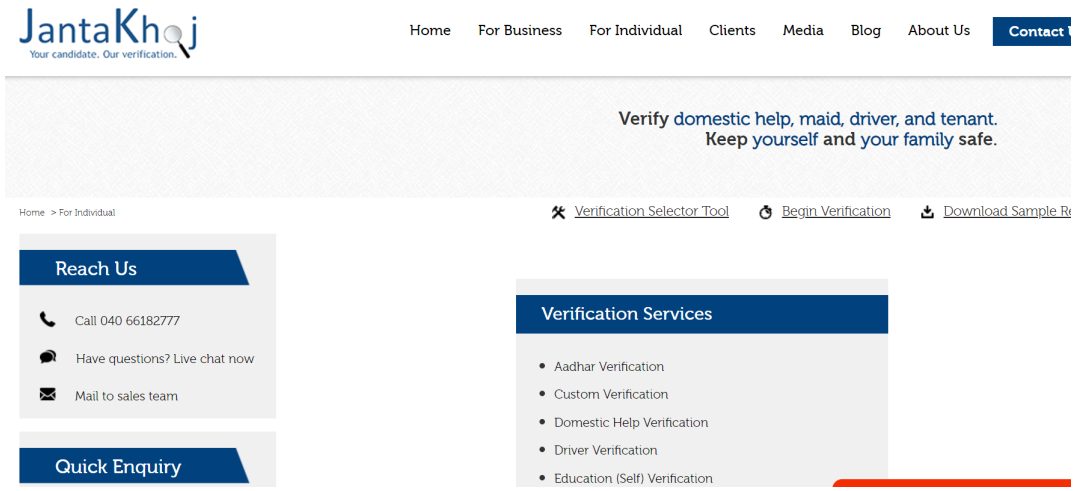


Pipl.com

- It asks for name and location of the person,
- it will the details of the people having the same name in that location
- https://pipl.com/



Jantakhoj.com



- **Democratize** the background verification process and bring it within easy reach of every individual.

- **Promote** greater transparency in society
- It gives details related to
  - verification,
  - police record,
  - photo,
  - location etc.
- Used for investigation purpose (tehquikat)

How many websites we need to search to find the information?

Solution:

- **OSINT Framework-** Open source Intelligence tracking
- It is **BIBLE** for cyber cell (**GRANTH)**
- All the information is available on it

OISNT Framework

Tons of public resources contains plenty of information spreaded across the internet.

That's why the **OSINT Framework plays** such an important role

Collection of OSINT tools to ease data collection.

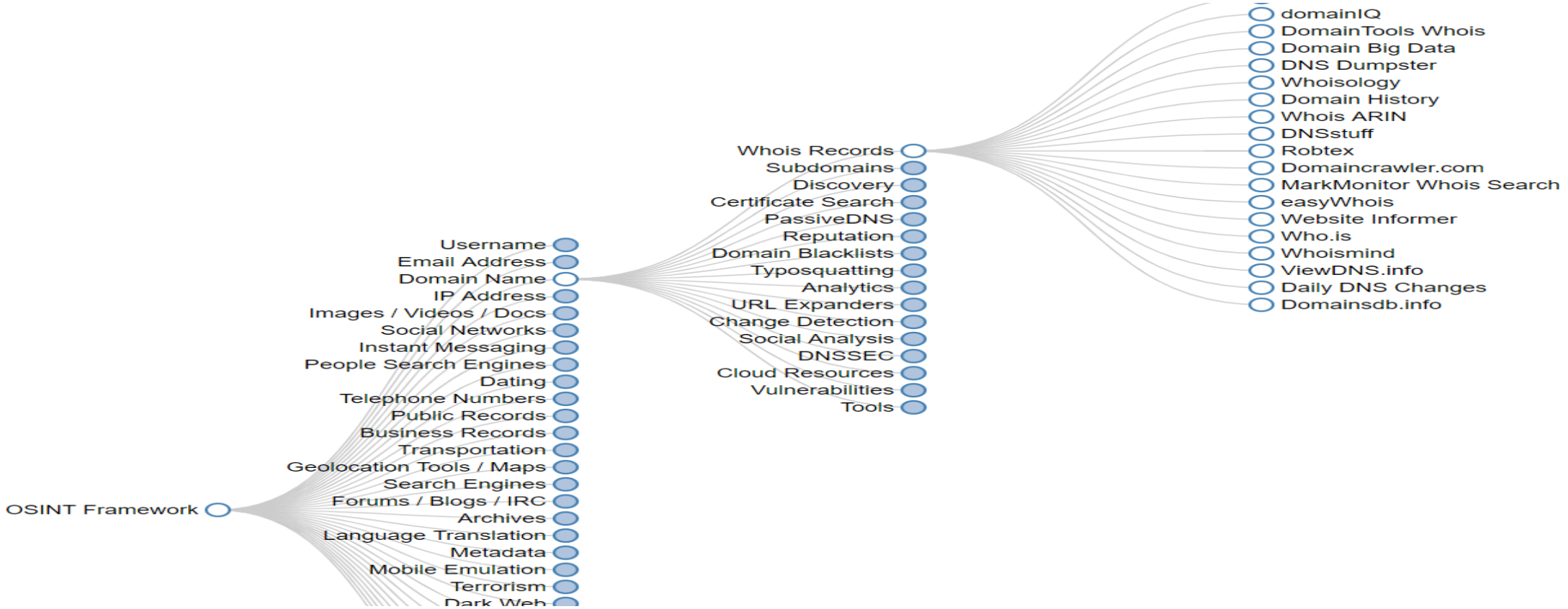
Used for

- **Digital footprinting,**
- **OSINT research,**
- **intelligence gathering, and**
- **reconnaissance.**

It provides a simple **web-based interface**

OSINT Framework

- Its shows tree like structure
- https://osintframework.com/



Kali Linux Tool 13

Maltego Tool- Patvera

THE NORTHCAP UNIVERSITY

Open Source Intelligence or forensic tool

US Based Tool

Used in online investigations for finding relationships between pieces of information from various sources of the Internet.

Patvera company (Patvera.com)

THE NORTHCAP UNIVERSITY

DEMO

30 YEARS OF EXCELLENCE

NAAC Accredited

Kali Linux Tool 14

Harvester

Tool	**Gathering Emails** that belongs to specific company/organisation	E.g. Lets Hack website bbc.com to get emails of employees
• Harvester • It is pre-installed in Kali Linux		• bulk emails can be used to send malicious link • advantageous for hacking purpose

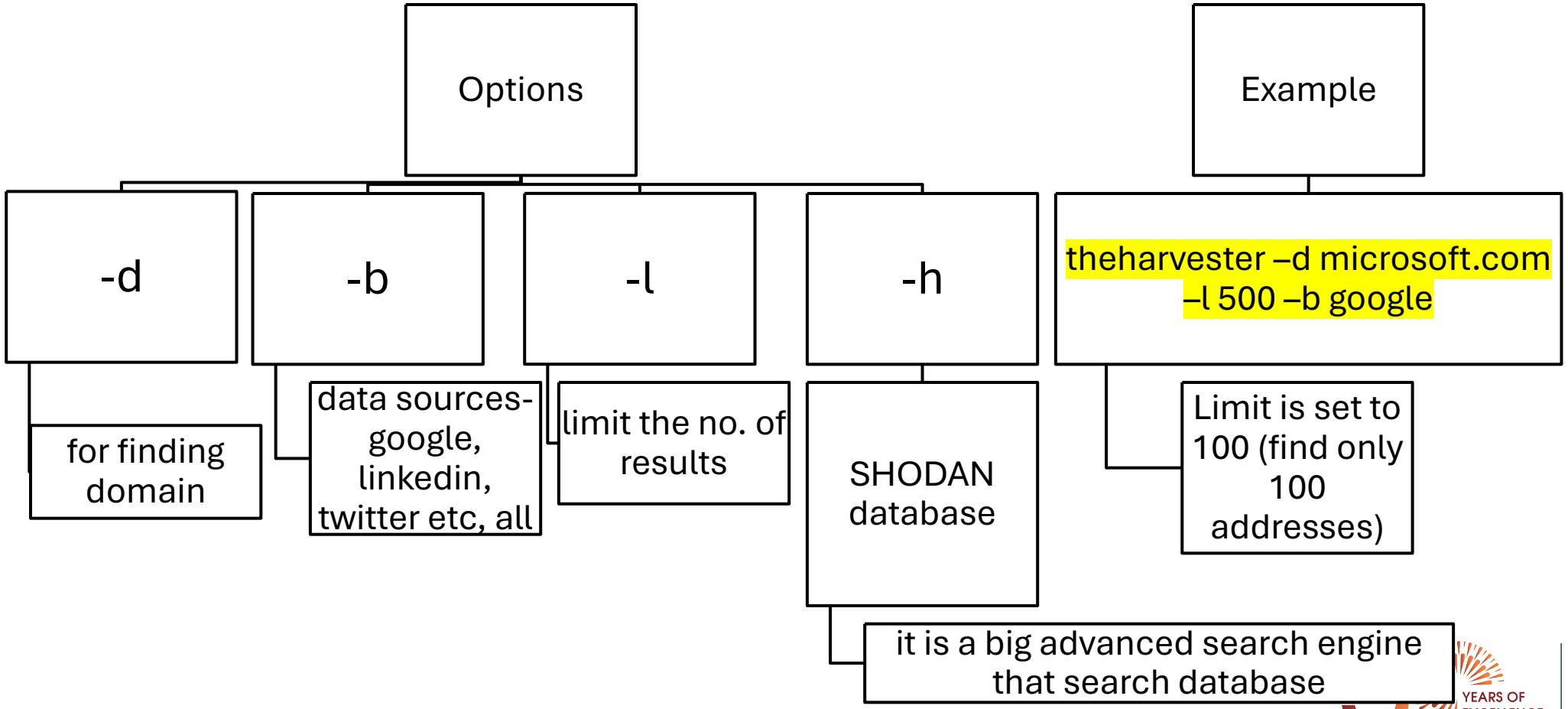
Harvester-Demo

Command :

Theharvester

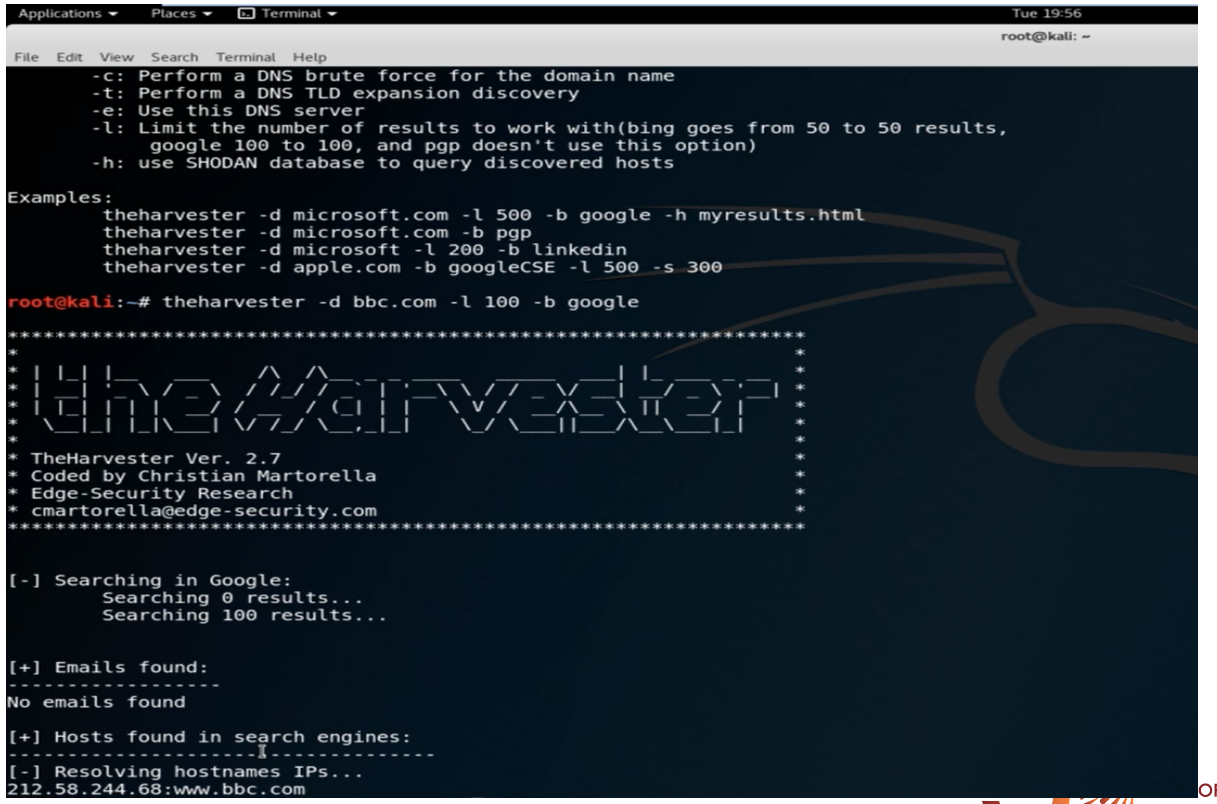
->gives many option

Harvester


Options
-d
for finding domain
-b
data sources- google, linkedin, twitter etc, all
-l
limit the no. of results
-h
SHODAN database
it is a big advanced search engine that search database
Example
theharvester –d microsoft.com –l 500 –b google
Limit is set to 100 (find only 100 addresses)

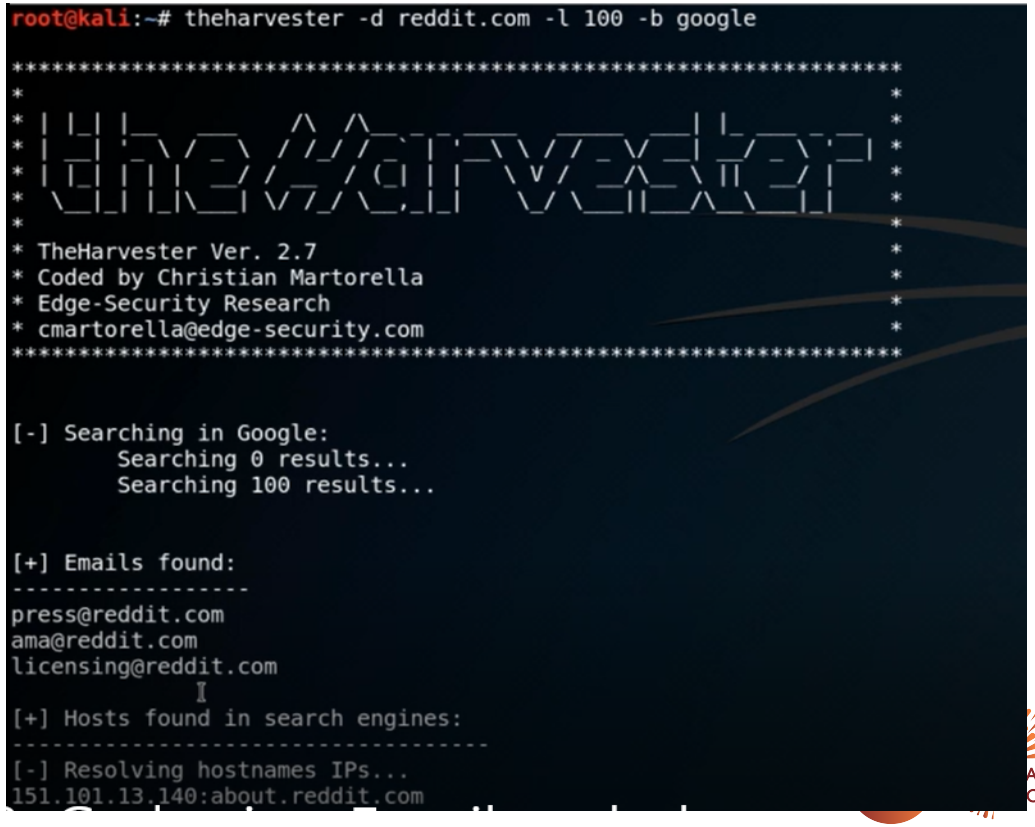
Harvester

- theharvester –d bbc.com –l 500 –b google
  - It is not showing emails



Harvester

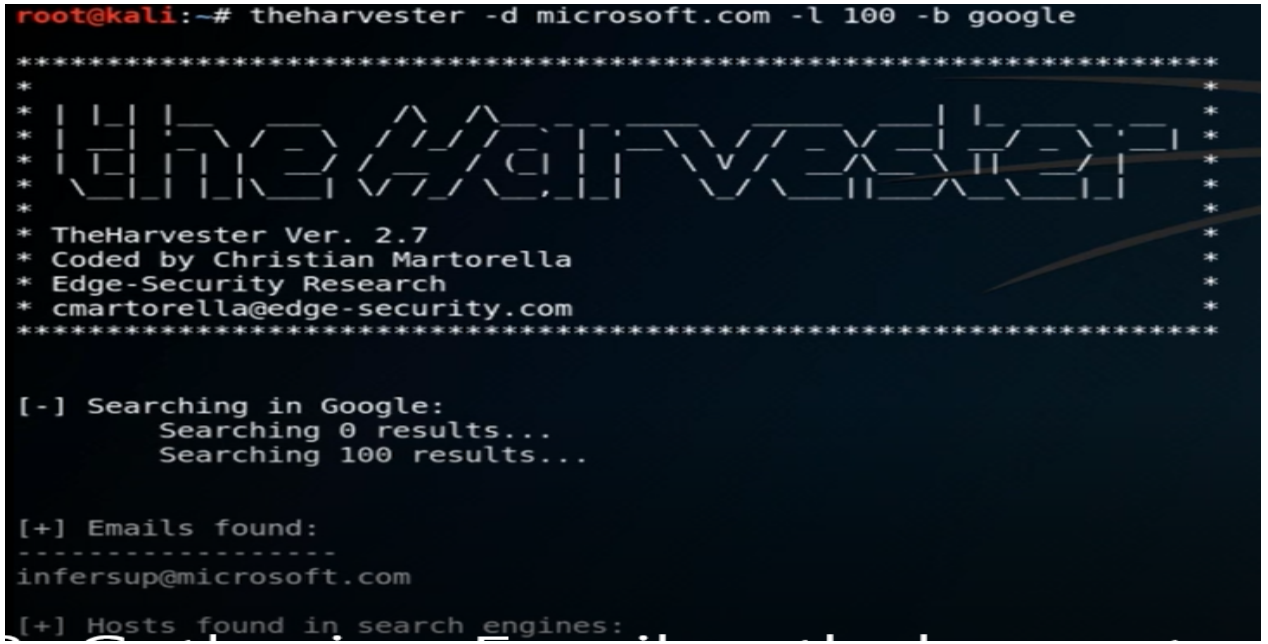
- theharvester –d Reddit.com –l 500 –b google
  - It shows emails
  - Shows hosts



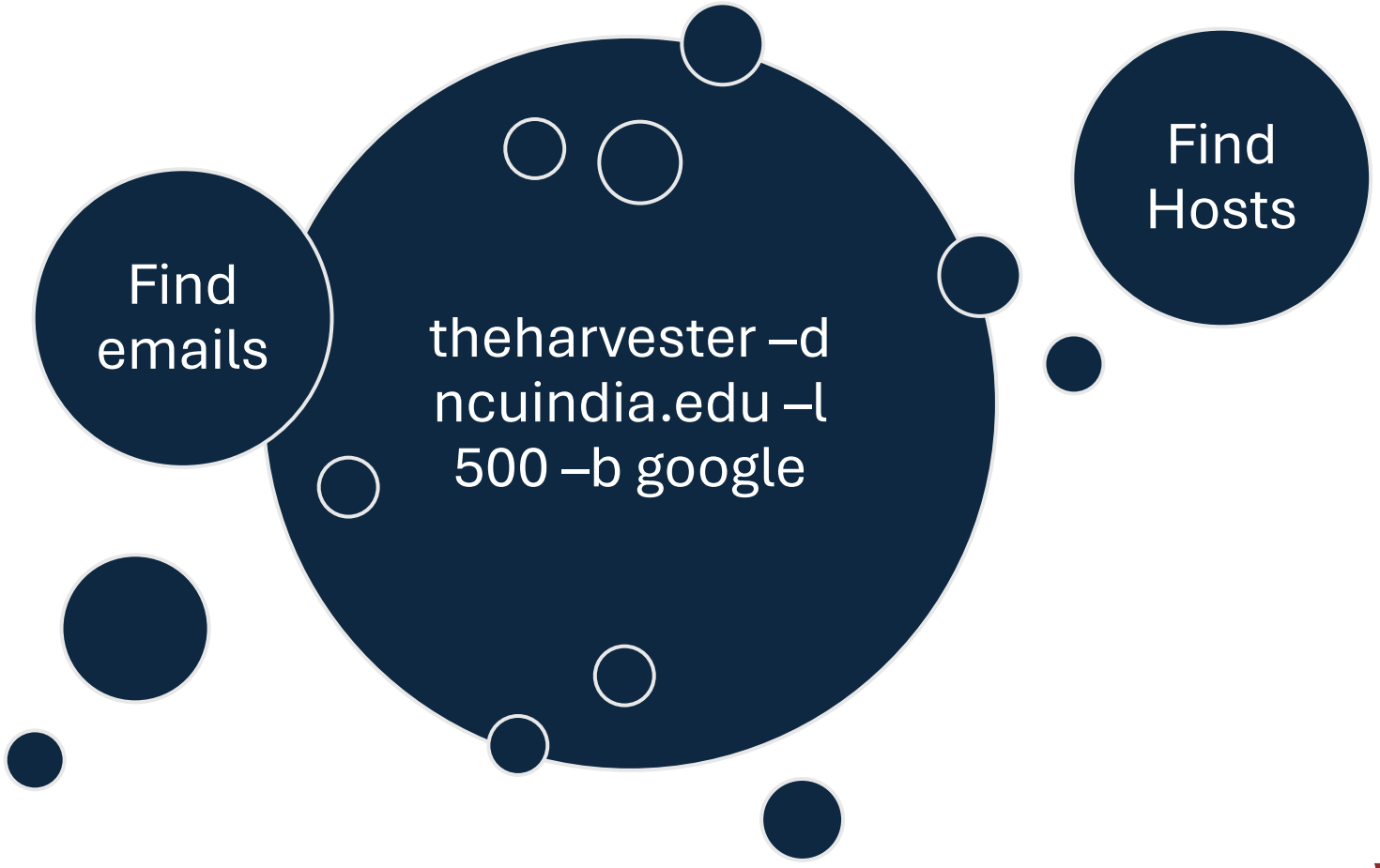
Harvester

So we can try with some other website

- theharvester –d microsoft.com –l 500 –b google
  - It shows one email id
  - We have also get hosts/subdomains with different IP addresses, which will be helpful



Harvester- Task



Tool 15

DNS Enumeration: NSLOOKUP

Nslookup is a network administration tool for querying the Domain Name System (DNS) to obtain

- **Domain name or**
- **IP address mapping or**
- **any other specific DNS record.**

Nslookup can operate on both “Interactive mode” and “Non-Interactive mode”.

- Interactive mode -allows the user to query the **DNS-Server about various host, and domains**.
- Non-Interactive mode -allows the user to query the **information for a host or domain.**

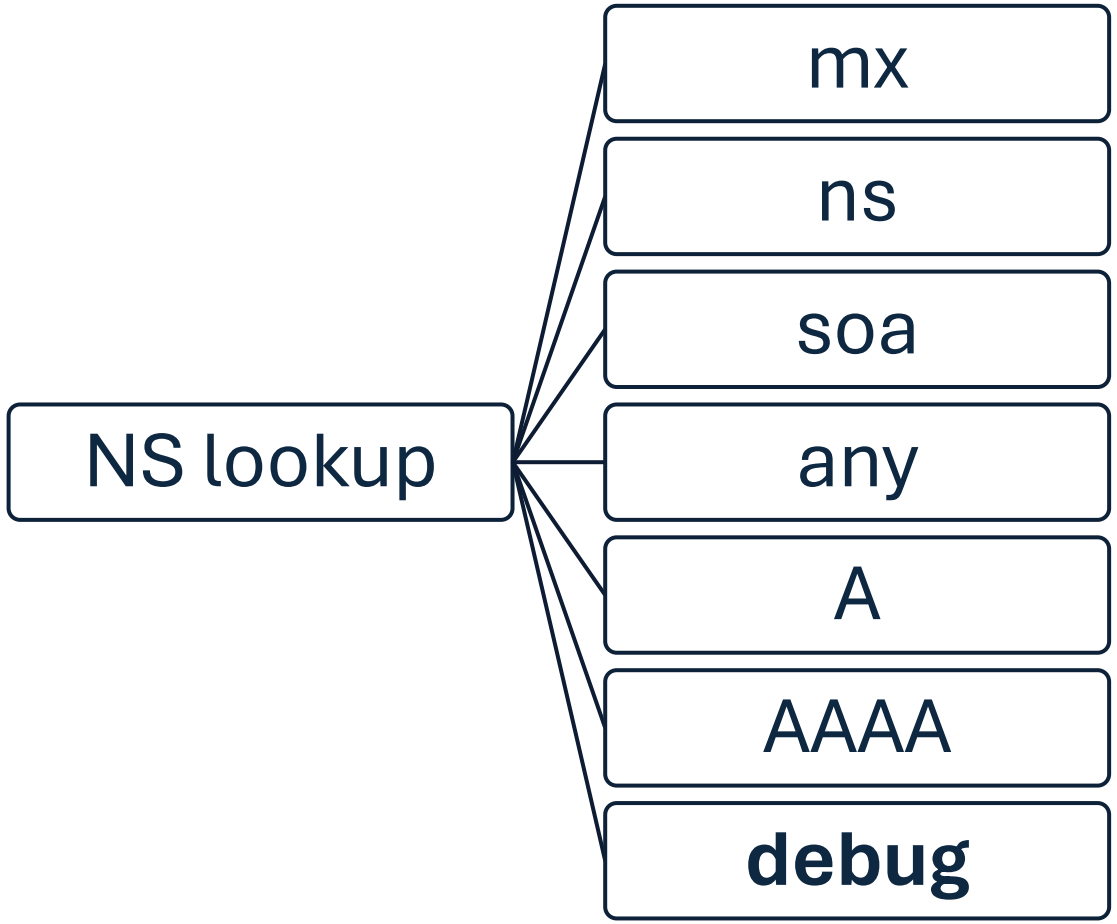
DNS Enumeration: NSLOOKUP

THE NORTHCAP UNIVERSITY

>nslookup microsoft.com

- Server: 8.8.8.8
  - **8.8.8.8** is the address of our system's DNS.
  - It is server our system is configured to translate domain into IP
- Address: 8.8.8.8#53
  - "**#53**" is the standard port number domain name servers use to accept queries.
- Non-authoritative answer:
  - Returned two entries, **134.170.185.46** and **134.170.188.221**.
    - Name: microsoft.com
    - Address: 134.170.185.46
    - Name: microsoft.com
    - Address: 134.170.188.221
      - **Microsoft.com** uses a round robin setup to distribute server load.

NSLookup commands



E.g. Different usage of nslookup

1. **Query the MX Record using -query=mx:** MX (Mail Exchange) record maps a domain name to a list of mail exchange servers for that domain.

The MX record tells that all the mails sent to “@redhat.com” should be routed to the Mail server in that domain.

Example: nslookup -query=mx redhat.com

```
Non-authoritative answer:

redhat.com      mail exchanger = 10 mx2.redhat.com.

redhat.com      mail exchanger = 5 mx1.redhat.com.
```

- mail exchanger address is prefixed with a number (**10**) and (5).
  - the lower numbers representing a higher priority.

E.g. Different usage of nslookup

- **Query the NS Record using -query=ns:** NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain. It will output the name serves which are associated with the given domain.
  - Example: nslookup -type=ns redhat.com

```
Non-authoritative answer:
redhat.com      nameserver = ns4.redhat.com.
redhat.com      nameserver = ns2.redhat.com.
redhat.com      nameserver = ns1.redhat.com.
redhat.com      nameserver = ns3.redhat.com.
```

- **Query the SOA Record using -query=soa:** SOA record (state of authority), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc...

```
origin = ns1.redhat.com
mail addr = noc.redhat.com
serial = 2012071601
refresh = 300
retry = 180
expire = 604800
minimum = 14400
```

Kali Linux Tool 16

Domain information groper (Dig)

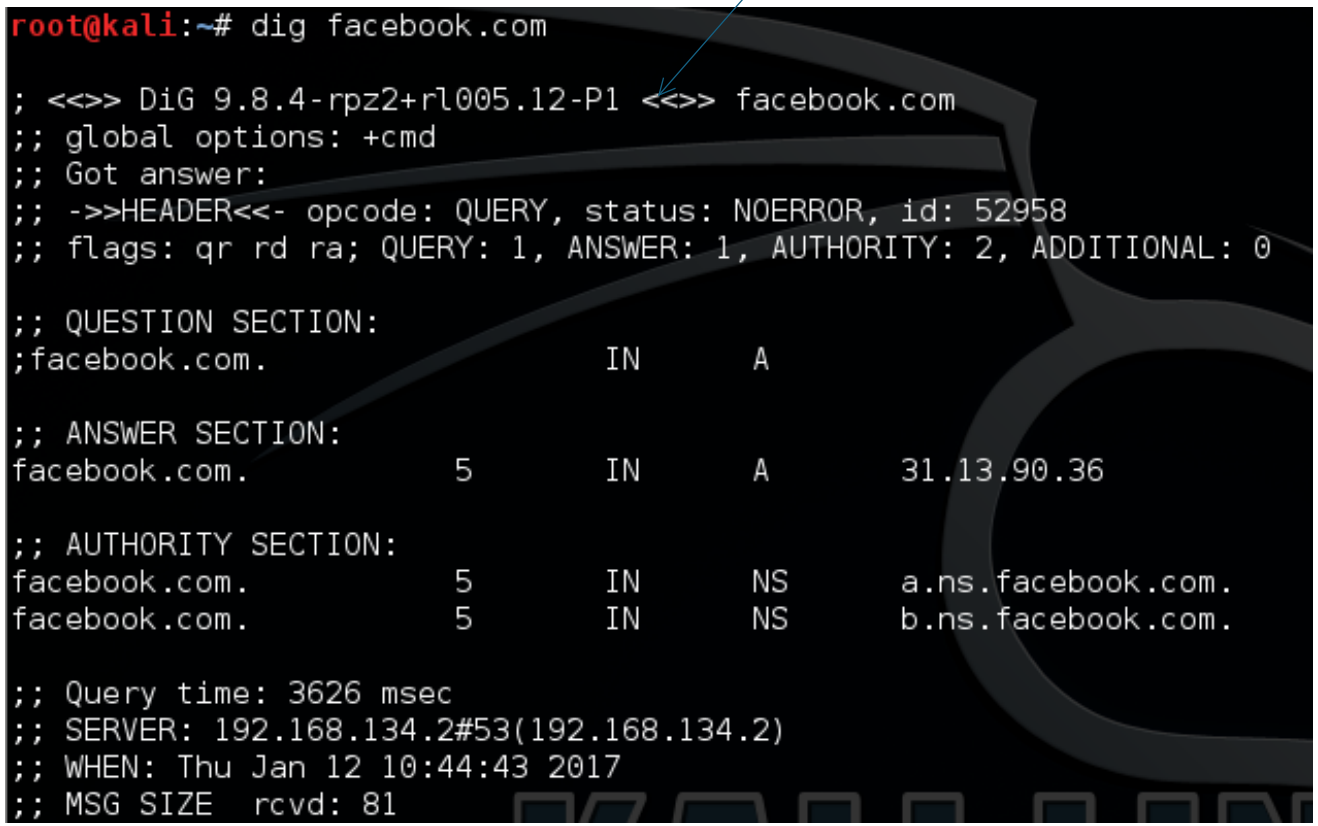
THE NORTHCAP UNIVERSITY

- **dig** is a network administration command-line tool for querying Domain Name System (DNS) servers.
- Is useful for network troubleshooting and for educational purposes.
- Similar options as of NSLookup-MX, NS, SOA, AAAA, A
- Inbuilt tool of Kali Linux
- E.g. dig NS google.com
  - search went from ns2->ns1->ns4->ns3, that means name server 2 have more preference over

Dig

Open innmong Section

Dig google.com NS ---- Find all name server
Dig google.com MX---- Find all mail server
Dig google.com A ---- Resolve domain name to IP addresses
Dig google.com AAAA– give IPV6 address



Tool 17,18

Netstat

THE NORTHCAP UNIVERSITY

Netstat command	Displays	Used for
• displays very detailed information about **how your computer is communicating with other computers or network devices.**	• **Active TCP connections** • **TCP state** • **Routing table** • **Interfaces information**. • **Local** IP address (your computer) • **Foreign IP address** (the other computer or network device) • Respective **port numbers**,	• **finding problems in the network** and • Determine the **amount of traffic on the network** as a performance measurement.

netstat command

netstat is a useful tool for checking network configuration and activity. It is a command line network utility that display TCP connections, routing table and interfaces information. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

#netstat –nr: Displays the Kernel's Routing Table

```
root@kali:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@kali:~#
```

The fourth column displays the following flags that describe the route:

- **G: The route uses a gateway.**
- **U: The interface to be used is up.**
- **H: Only a single host can be reached through the route.**
- **D: This route is dynamically created.**
- **M: This route is set if the table entry was modified by an ICMP redirect message.**

- **The MSS (Maximum Segment Size):** the size of the largest datagram the kernel will construct for transmission via this route.
- **The Window:** the maximum amount of data the system will accept in a single burst from a remote host.
- irtt : "initial round trip time."

#**netstat –i:** displays kernel's interface table

```
root@kali:~# netstat -i
Kernel Interface table
Iface   MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0   2879220      0      0 0       6481063      0      0      0 B
MRU
lo        65536 0      8960      0      0 0          8960      0      0      0 L
RU
```

- The MTU and Met fields: show the current MTU and metric values for that interface.
- The RX and TX columns: show how many packets have been received or transmitted error-free (RX-OK/TX-OK) or damaged (RX-ERR/TX-ERR); how many were dropped (RX-DRP/TX-DRP); and how many were lost because of an overrun (RX-OVR/TX-OVR).
- For More options check

  http://www.thegeekstuff.com/2010/03/netstat-command-examples/

#**netstat –ta:** displays list of all servers that are currently running on your system.

```
root@kali:~# netstat -ta
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      1 192.168.0.15:34629      sa-in-f109.1e100.ne:456 SYN_SENT
tcp        0      1 192.168.0.15:34635      sa-in-f109.1e100.ne:456 SYN_SENT
tcp        0      1 192.168.0.15:55840      sa-in-f108.1e100.:ssmtp SYN_SENT
tcp        0      1 192.168.0.15:55848      sa-in-f108.1e100.:ssmtp SYN_SENT
tcp        0      1 192.168.0.15:34637      sa-in-f109.1e100.ne:456 SYN_SENT
tcp        0      1 192.168.0.15:55845      sa-in-f108.1e100.:ssmtp SYN_SENT
tcp        0      1 192.168.0.15:34640      sa-in-f109.1e100.ne:456 SYN_SENT
tcp        0      1 192.168.0.15:34632      sa-in-f109.1e100.ne:456 SYN_SENT
```

- The options –t, –u, –w, and –x show active TCP, UDP, RAW, or Unix socket connections.
- –a flag in addition, sockets that are waiting for a connection (i.e., listening) are displayed as well.

Trace route

Trace route is a computer network diagnostic tool for

- Displaying the route (path) and
- measuring transit delays of packets across an Internet Protocol (IP) network.

Route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path);

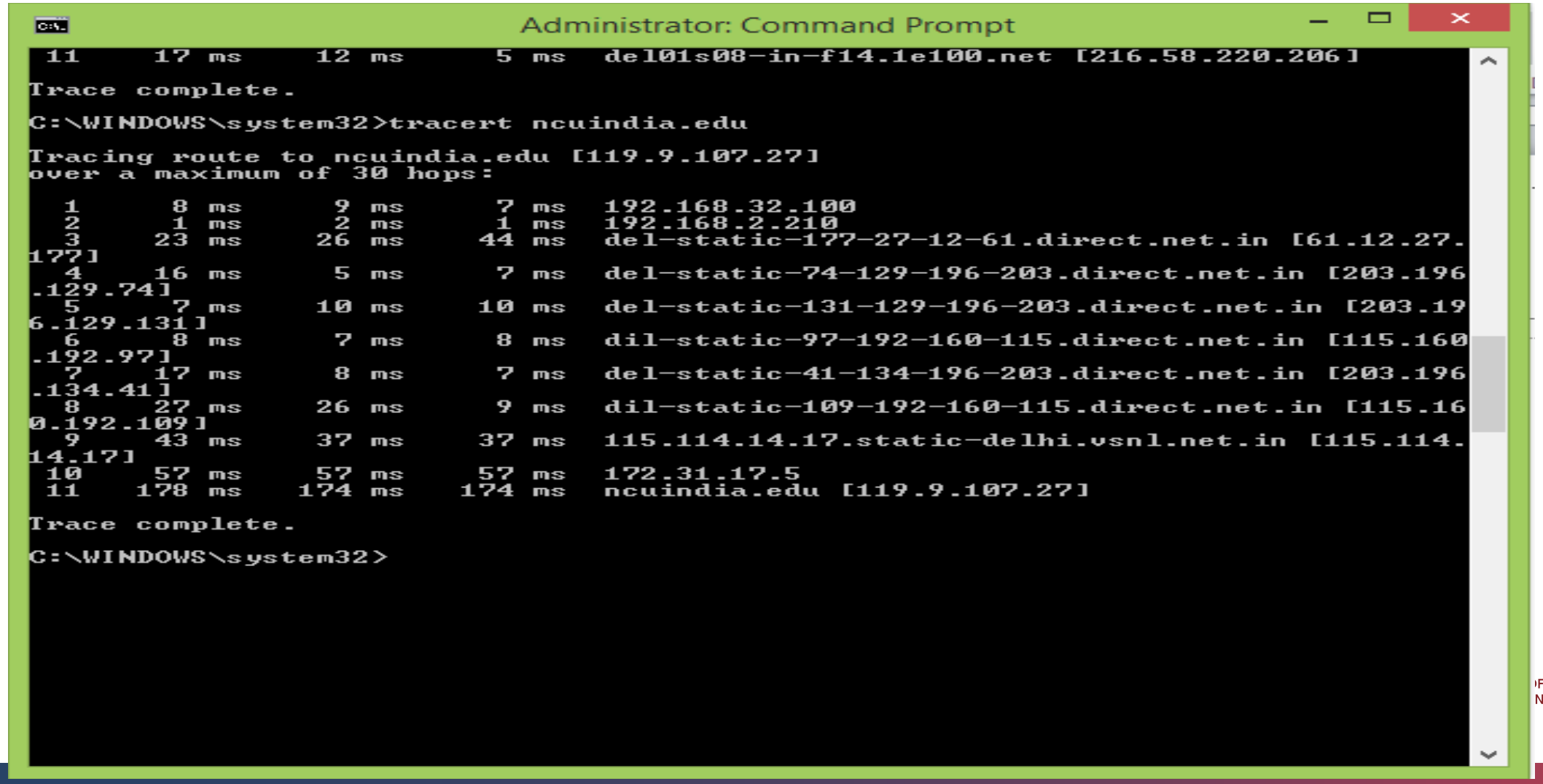
Sum of the mean times in each hop is a measure of the total time spent to establish the connection.

Trace route proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated.

Trace route Vs. Ping

- Ping only computes the final round-trip times from the destination point.

Trace Route- tracert



DRILL

THE NORTHCAP UNIVERSITY

Select

- Select one Website

Use

- Use the above tools to find all the relevant information of selected website

Prepare

- Prepare a report

30 YEARS OF EXCELLENCE

NAAC Accredited