WEB APP RECONNAISSANCE AND MAPPING

NAME-RISHABH VATS

Web app attack methodology

1. RECONNAISSANCE: - We research the targets
2. MAPPING: - We understand what makes up the application and its surrounding
3. DISCOVERY: - We look for the vulnerabilities
4. EXPLOITATION: -We launch the attack

The attack process is cyclical. Means Once you exploit a vulnerability, you can further the exploitation by starting the process again from that point. Example if I am successful in launching a SQL injection then I won't stop there. I will try to find root(admin) access of the system or try to uncover more vulnerabilities.

What is Reconnaissance

- Reconnaissance or Information gathering is the very first and most critical step of every penetration test. It does not matter if you have to assess the security of an entire network or a single web application, you need to know your targets in as much detail as possible.

- Gathering information about the target is the initial phase of any penetration test. At this stage, there is no unnecessary information everything you collect should be noted for future use. The wealth of information you collect will become useful in both understanding application logic and during the attack phase

Why Reconnaissance is important

- Unfortunately, like breakfast, many people skip reconnaissance without even realizing that it is vital. Many attackers skip this step, thinking it is a waste of time and blindly start launching attack. This can be successful, but it is inefficient and can tip off the target. By focusing our time on finding out as much as possible before launching attack. We can better focus and lower the risk of detection.
- With reconnaissance time reduced because we narrow the scope of testing and Good scoping can protect testers from being overwhelmed and running out of time.
- A good attacker, develops his or her strategy based on reconnaissance because it allows them to craft attack in an informed fashion, elevating our probability of success.

What is Mapping

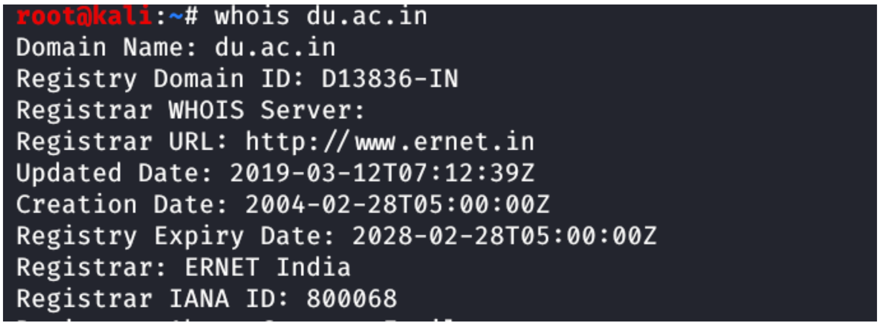
- In mapping, Tester understand what makes up the application and its surrounding. It involves understanding how application work and its underline infrastructure like services, OS, application framework and application enumeration etc.
- This step usually takes least amount of time. Mapping the application enables the tester to see all the pieces of application in one place and then it’s easy to target the least secure piece of application like an old service.

What sorts of information are we going after in recon and mapping

- Infrastructure (Web server, Database, operating system, services….)
- Application Logic
- IP, Domains and Subdomains
- Virtual hosts

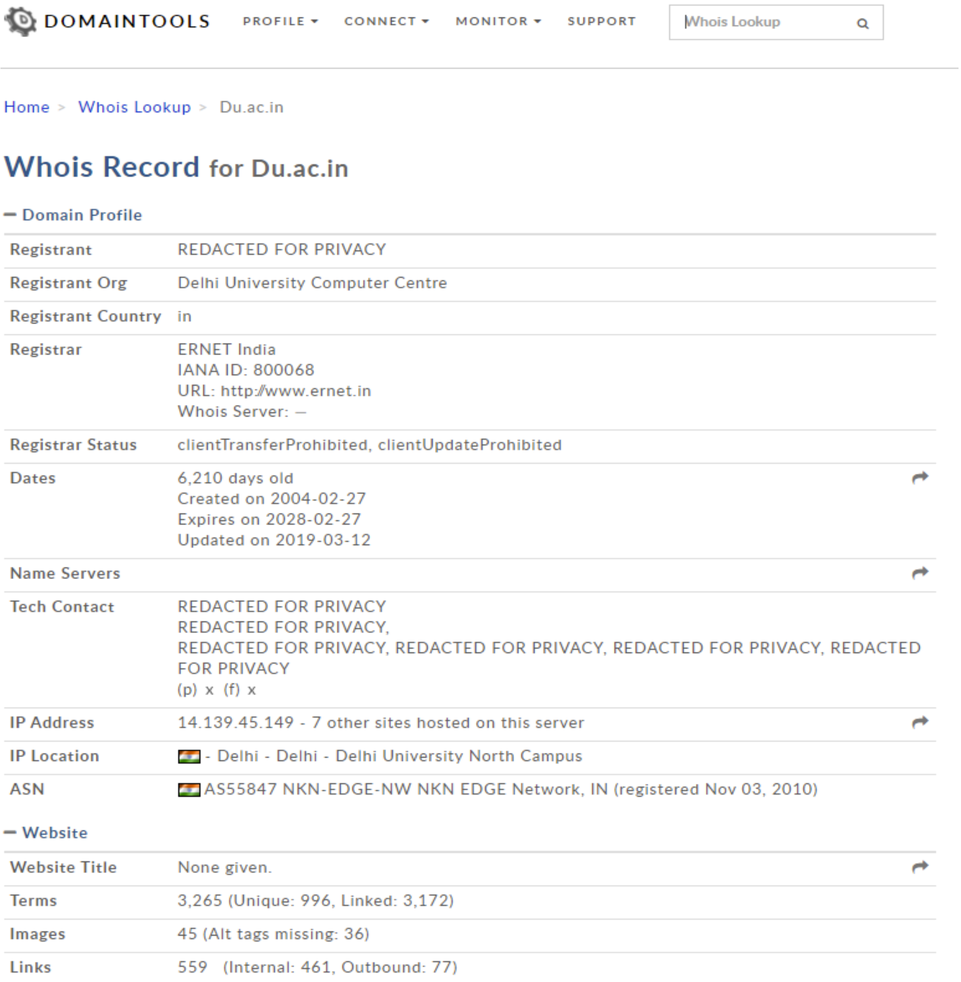
Tools use for recon and mapping

- WHOIS
  - WHOIS lookups were traditionally done using a command line interface, but a number of simplified web-based tools now exist for looking up domain ownership details from different databases.
  - Web-based WHOIS clients still rely on the WHOIS protocol to connect to a WHOIS server and do lookups and command line WHOIS clients are still widely used by system administrators. WHOIS normally runs on TCP port 43
  - Instead of using the command line tools, you can also rely on web-based tools such as: whois.domaintools.com. The *Whois* database contains public information, so you can freely check it
  - Information we can get from WHOIS tool: -administrative contact information, Technical contact information, Name server, IP address and location, Dates (Created, Expires, Updated) etc.
  - In linux go to terminal and type “whois du.ac.in(domain name)”



```
root@kali:~# whois du.ac.in
Domain Name: du.ac.in
Registry Domain ID: D13836-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-03-12T07:12:39Z
Creation Date: 2004-02-28T05:00:00Z
Registry Expiry Date: 2028-02-28T05:00:00Z
Registrar: ERNET India
Registrar IANA ID: 800068
```

- Go to “whois.domaintools.com” and search “du.ac.in” (domain name)



Whois Record for Du.ac.in

— Domain Profile

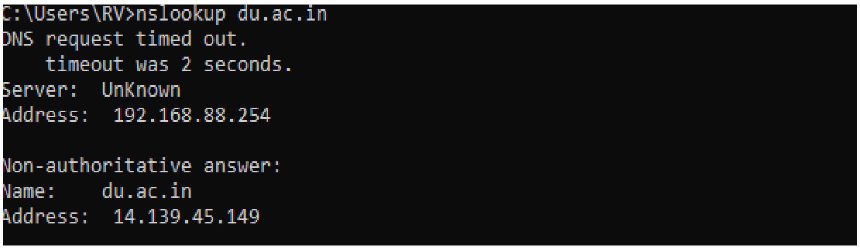
Registrant	REDACTED FOR PRIVACY
Registrant Org	Delhi University Computer Centre
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: –
Registrar Status	clientTransferProhibited, clientUpdateProhibited
Dates	6,210 days old Created on 2004-02-27 Expires on 2028-02-27 Updated on 2019-03-12
Name Servers	
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	14.139.45.149 - 7 other sites hosted on this server
IP Location	- Delhi - Delhi - Delhi University North Campus
ASN	AS55847 NKN-EDGE-NW NKN EDGE Network, IN (registered Nov 03, 2010)

— Website

Website Title	None given.
Terms	3,265 (Unique: 996, Linked: 3,172)
Images	45 (Alt tags missing: 36)
Links	559 (Internal: 461, Outbound: 77)

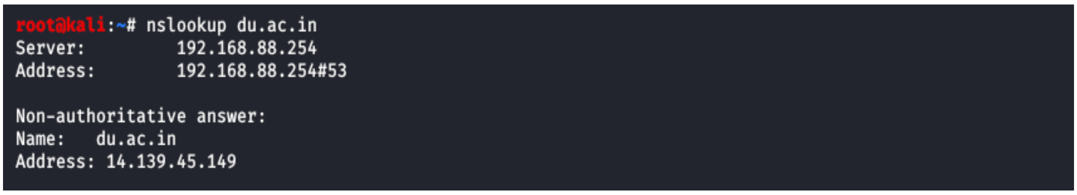
➨ NSLOOKUP

- Nslookup is another very handy tool that lets you translate hostnames to IP addresses and vice versa.
- Under *Windows*, click Start>Run>cmd . EX :- “nslookup du.ac.in(domain name)”.



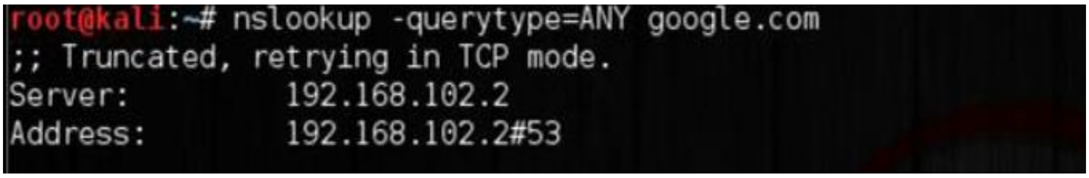
```
C:\Users\RV>nslookup du.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.88.254

Non-authoritative answer:
Name:    du.ac.in
Address:  14.139.45.149
```

- Under *linux* systems, open a console and type : “nslookup du.ac.in”

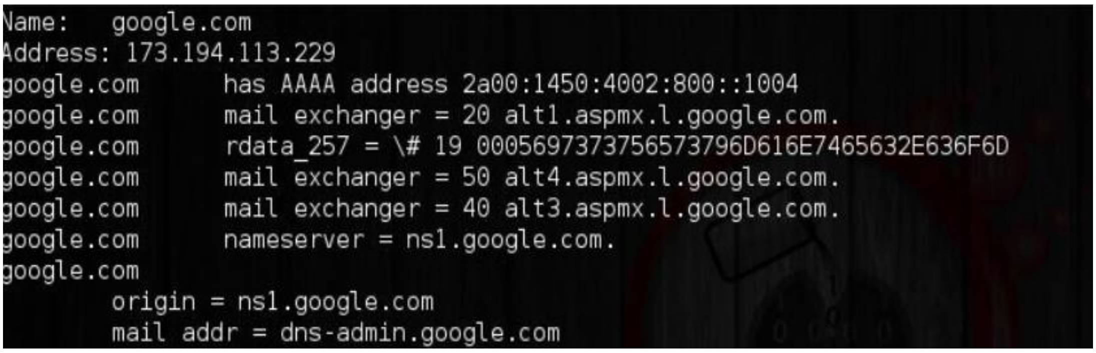


```
root@kali:~# nslookup du.ac.in
Server:         192.168.88.254
Address:        192.168.88.254#53

Non-authoritative answer:
Name:   du.ac.in
Address: 14.139.45.149
```

- With the help of NSLOOKUP we can also query the DNS server for the whole record. COMMAND: - “nslookup -querytype=ANY google.com (domain name)”



```
root@kali:~# nslookup -querytype=ANY google.com
;; Truncated, retrying in TCP mode.
Server:         192.168.102.2
Address:        192.168.102.2#53
```



```
Name:   google.com
Address: 173.194.113.229
google.com      has AAAA address 2a00:1450:4002:800::1004
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      rdata_257 = \# 19 0005697373756573796D616E7465632E636F6D
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      nameserver = ns1.google.com.
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
```

➨ NETCRAFT

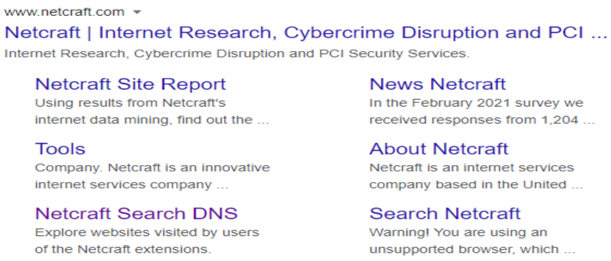
- Netcraft is a fast way to uncover the organization’s hosting scheme and ownership. we can go to www.netcraft.com to use this tool.
- We can find info like: -

  A. Hosting company and country

  B. IP address, IPv4 autonomous systems, ipv6 address

  C. DNS admin, top level domain Etc.

- Visit www.netcraft.com and doing a search on du.ac.in will reveal the hosting provider for du.ac.in as well as IP netblock etc.



www.netcraft.com ▾

Netcraft | Internet Research, Cybercrime Disruption and PCI ...

Internet Research, Cybercrime Disruption and PCI Security Services.

Netcraft Site Report
Using results from Netcraft's internet data mining, find out the ...

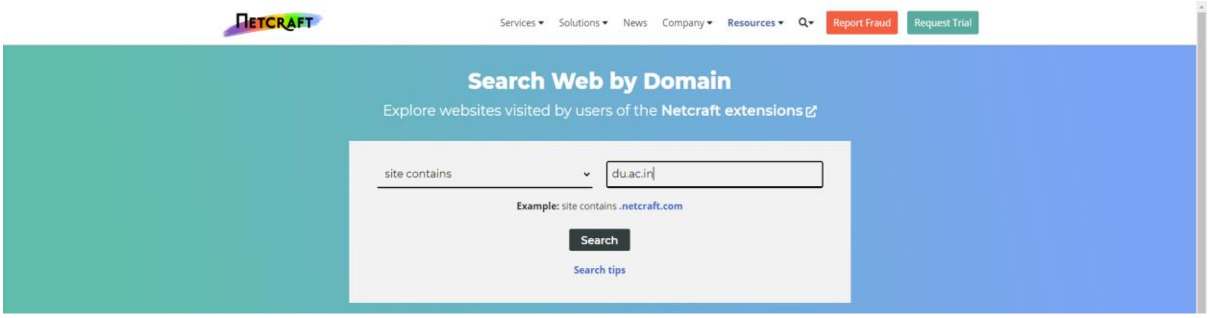
News Netcraft
In the February 2021 survey we received responses from 1,204 ...

Tools
Company. Netcraft is an innovative internet services company ...

About Netcraft
Netcraft is an internet services company based in the United ...

Netcraft Search DNS
Explore websites visited by users of the Netcraft extensions.

Search Netcraft
Warning! You are using an unsupported browser, which ...



Search Web by Domain

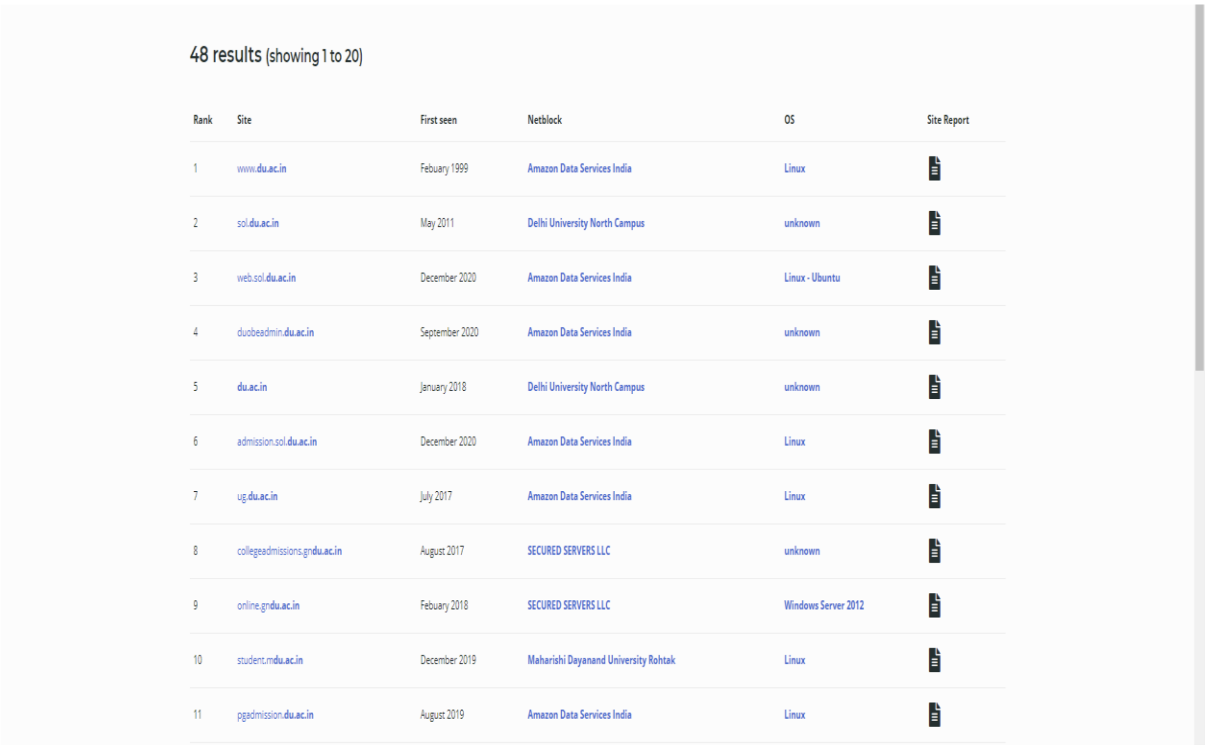
Explore websites visited by users of the Netcraft extensions

site contains ⌄ | du.ac.in

Example: site contains .netcraft.com

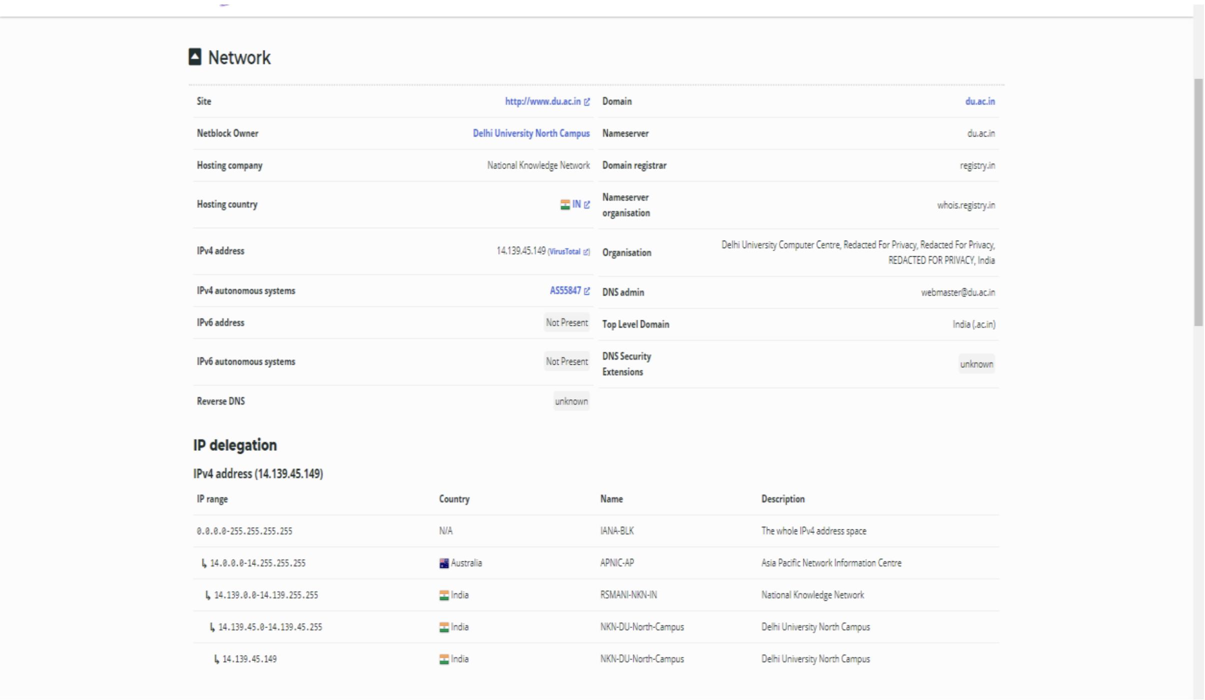
Search

Search tips



48 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
1	www.du.ac.in	Febuary 1999	Amazon Data Services India	Linux	🗎
2	sol.du.ac.in	May 2011	Delhi University North Campus	unknown	🗎
3	web.sol.du.ac.in	December 2020	Amazon Data Services India	Linux - Ubuntu	🗎
4	duobeadmin.du.ac.in	September 2020	Amazon Data Services India	unknown	🗎
5	du.ac.in	January 2018	Delhi University North Campus	unknown	🗎
6	admission.sol.du.ac.in	December 2020	Amazon Data Services India	Linux	🗎
7	ug.du.ac.in	July 2017	Amazon Data Services India	Linux	🗎
8	collegeadmissions.gndu.ac.in	August 2017	SECURED SERVERS LLC	unknown	🗎
9	online.gndu.ac.in	Febuary 2018	SECURED SERVERS LLC	Windows Server 2012	🗎
10	student.mdu.ac.in	December 2019	Maharishi Dayanand University Rohtak	Linux	🗎
11	pgadmission.du.ac.in	August 2019	Amazon Data Services India	Linux	🗎



Network

Site	http://www.du.ac.in	Domain	du.ac.in
Netblock Owner	Delhi University North Campus	Nameserver	du.ac.in
Hosting company	National Knowledge Network	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.registry.in
IPv4 address	14.139.45.149 (VirusTotal)	Organisation	Delhi University Computer Centre, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS55847	DNS admin	webmaster@du.ac.in
IPv6 address	Not Present	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	unknown		

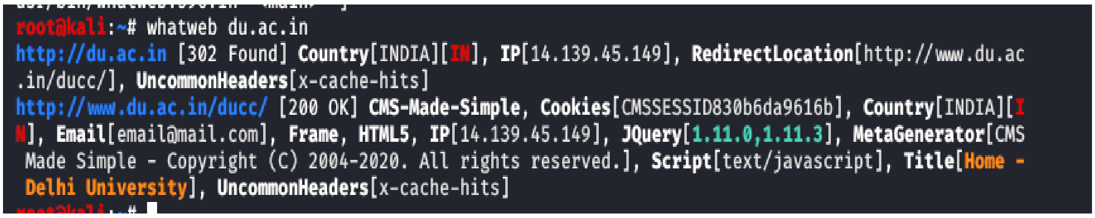
IP delegation

IPv4 address (14.139.45.149)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 14.0.0.0-14.255.255.255	Australia	APNIC-AP	Asia Pacific Network Information Centre
↳ 14.139.0.0-14.139.255.255	India	RSMANI-NKN-IN	National Knowledge Network
↳ 14.139.45.0-14.139.45.255	India	NKN-DU-North-Campus	Delhi University North Campus
↳ 14.139.45.149	India	NKN-DU-North-Campus	Delhi University North Campus

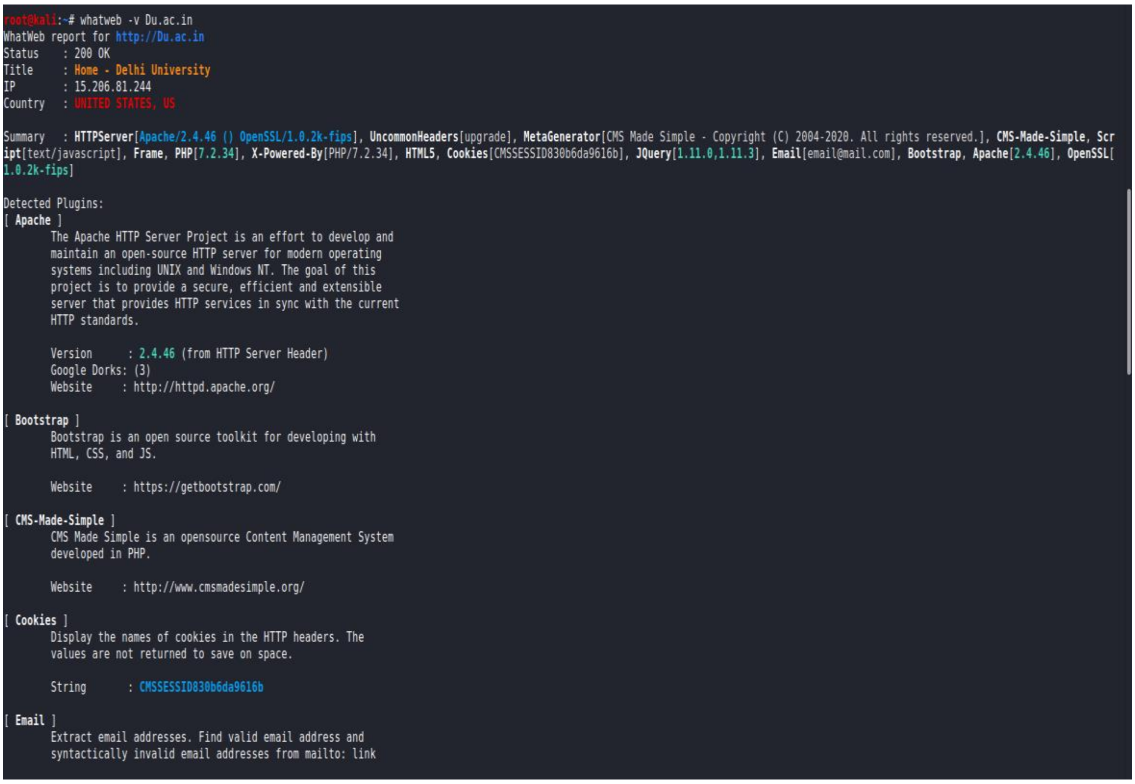
➨ WHATWEB

- It is a command line tool that can be used to recognize website technologies, Web server versions, blogging platforms, JavaScript libraries and much more.
- The tool is very easy to use. We just need to type the name of the tool followed by the address (IP or URL) of our target and hit enter
- It offers options that allow us to specify different user agents, HTTP basic authentication credentials, cookies, proxy and much more
- Pentesting distributions of Linux such as Kali already have it installed by default, so you can start using it by running the following command : whatweb



```
root@kali:~# whatweb du.ac.in
http://du.ac.in [302 Found] Country[INDIA][IN], IP[14.139.45.149], RedirectLocation[http://www.du.ac
.in/ducc/], UncommonHeaders[x-cache-hits]
http://www.du.ac.in/ducc/ [200 OK] CMS-Made-Simple, Cookies[CMSSESSID830b6da9616b], Country[INDIA][I
N], Email[email@mail.com], Frame, HTML5, IP[14.139.45.149], JQuery[1.11.0,1.11.3], MetaGenerator[CMS
 Made Simple - Copyright (C) 2004-2020. All rights reserved.], Script[text/javascript], Title[Home -
 Delhi University], UncommonHeaders[x-cache-hits]
root@kali:~#
```

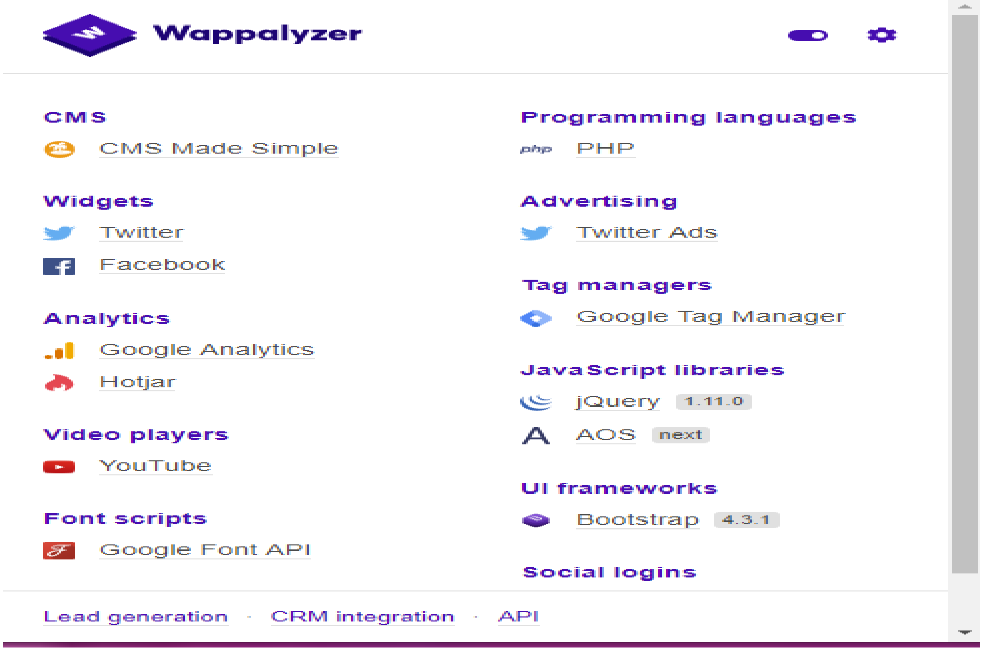
As you can see output is little messy. Use “-v” argument to get a readable output



```
root@kali:~# whatweb -v Du.ac.in
WhatWeb report for http://Du.ac.in
Status    : 200 OK
Title     : Home - Delhi University
IP        : 15.206.81.244
Country   : UNITED STATES, US

Summary   : HTTPServer[Apache/2.4.46 () OpenSSL/1.0.2k-fips], UncommonHeaders[upgrade], MetaGenerator[CMS Made Simple - Copyright (C) 2004-2020. All rights reserved.], CMS-Made-Simple, Scr
ipt[text/javascript], Frame, PHP[7.2.34], X-Powered-By[PHP/7.2.34], HTML5, Cookies[CMSSESSID830b6da9616b], JQuery[1.11.0,1.11.3], Email[email@mail.com], Bootstrap, Apache[2.4.46], OpenSSL[
1.0.2k-fips]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.46 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ CMS-Made-Simple ]
        CMS Made Simple is an opensource Content Management System
        developed in PHP.

        Website     : http://www.cmsmadesimple.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : CMSSESSID830b6da9616b

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
```

➨ WAPPALYZER

- It is a Web Browser plugin based tool that works both on *Firefox* and *Chrome*.
- Once you install the plugin from the previous link, you just have to navigate your target website: you will see some icons in your address bar. Each icon gives you information about the Web Server, such as the Operating System, The Web Server, JavaScript,frameworks and much more
- In order to inspect the information found, just click on an icon and a pop up will appear on your right, listing all the information gathered



Wappalyzer

CMS
CMS Made Simple

Widgets
Twitter
Facebook

Analytics
Google Analytics
Hotjar

Video players
YouTube

Font scripts
Google Font API

Programming languages
PHP

Advertising
Twitter Ads

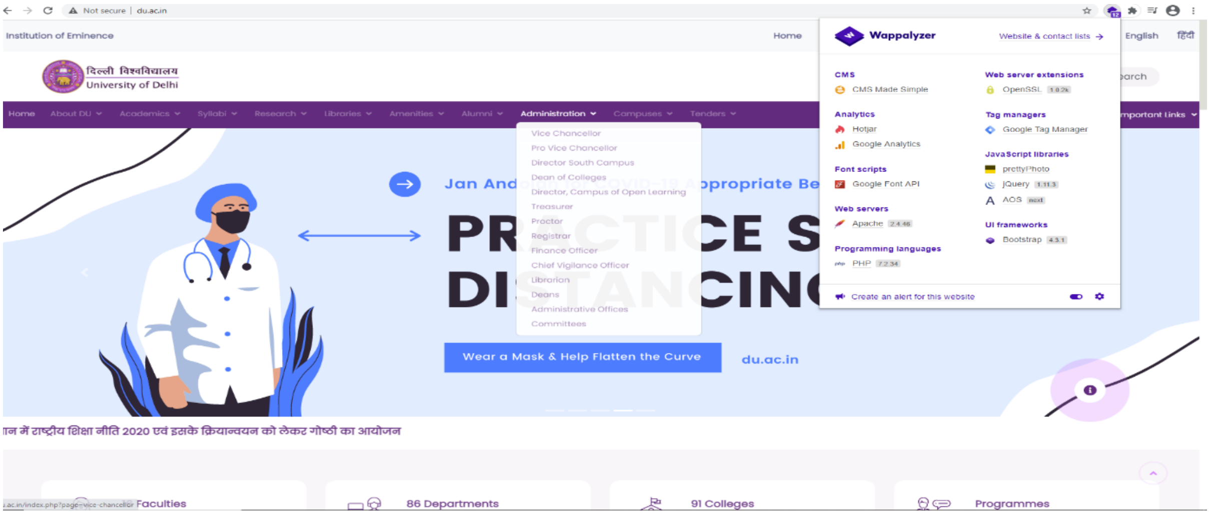
Tag managers
Google Tag Manager

JavaScript libraries
jQuery 1.11.0
AOS next

UI frameworks
Bootstrap 4.3.1

Social logins

Lead generation · CRM integration · API



Wappalyzer   Website & contact lists →

CMS
CMS Made Simple

Analytics
Hotjar
Google Analytics

Font scripts
Google Font API

Web servers
Apache 2.4.46

Programming languages
PHP 7.2.34

Web server extensions
OpenSSL 1.0.2k

Tag managers
Google Tag Manager

JavaScript libraries
prettyPhoto
jQuery 1.11.3
AOS next

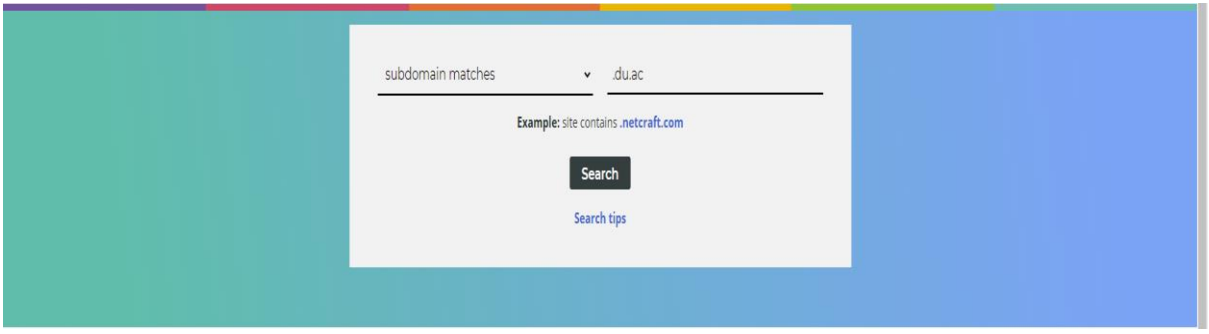
UI frameworks
Bootstrap 4.3.1

Create an alert for this website

➨ How to find Subdomain

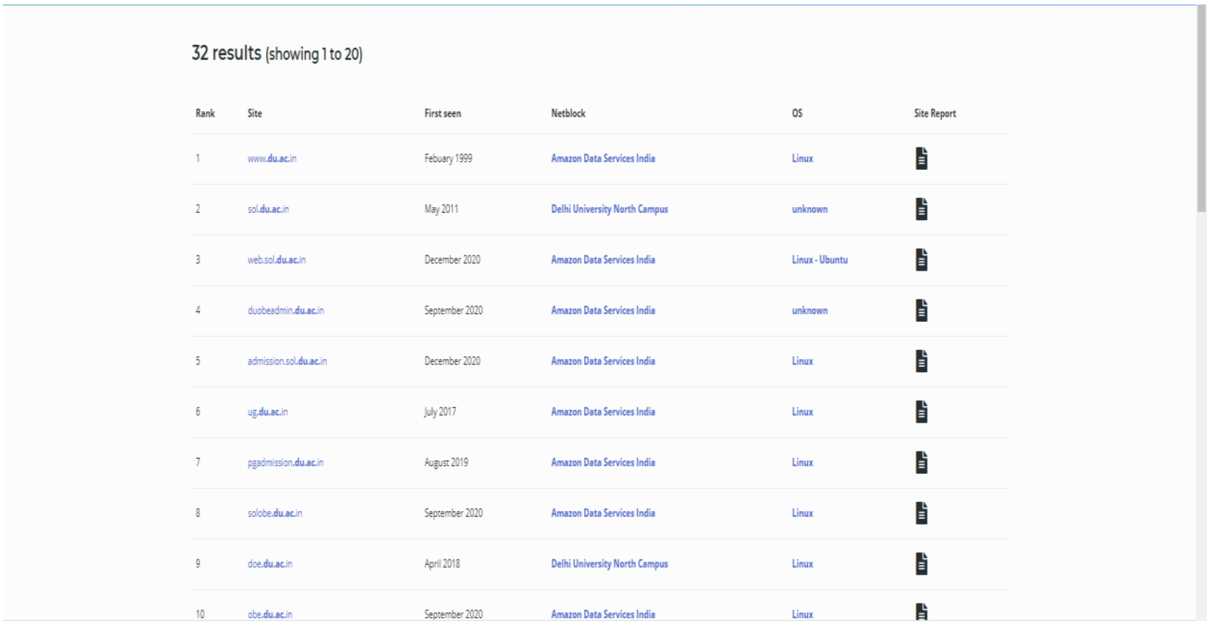
- The enumeration exercise starts by mapping all available subdomains within a domain name.
- This will widen our attack surface and sometimes reveal hidden management backend panels or intranet web applications that the network administrators intended to protect through the old disgraced method of security through obscurity.
- There are lots of ways to enumerate subdomains:
    - Netcraft
    - Google
    - Crawling / Brute force

- We have already used Netcraft to gather information from a specific domain but Netcraft can also be used to enumerate subdomains.In order to list all the subdomains of a specific target we just need to open the Netcraft search page, select "*subdomain matches*" from the dropdown menu and type in our string:



subdomain matches ˅ .du.ac

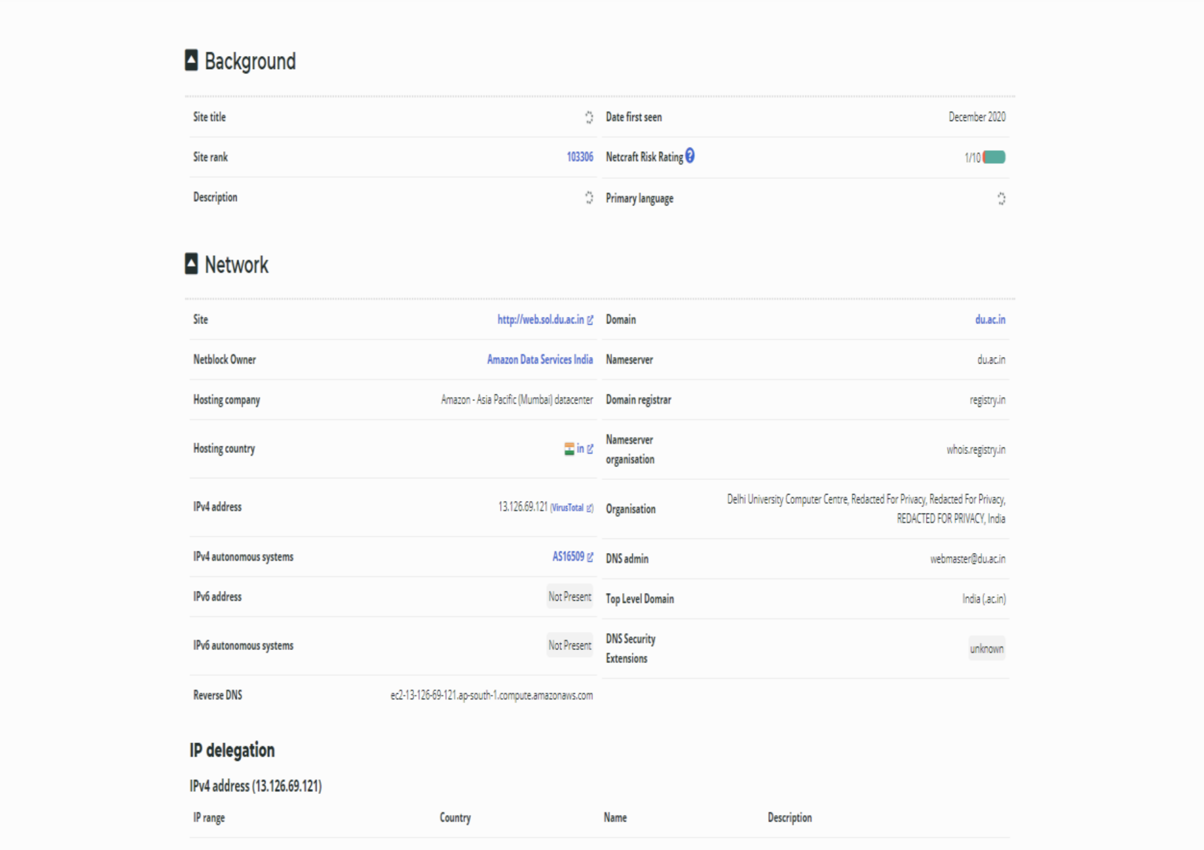
Example: site contains .netcraft.com



32 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
1	www.**du.ac.**in	Febuary 1999	Amazon Data Services India	Linux	📄
2	sol.**du.ac.**in	May 2011	Delhi University North Campus	unknown	📄
3	web.sol.**du.ac.**in	December 2020	Amazon Data Services India	Linux - Ubuntu	📄
4	duobeadmin.**du.ac.**in	September 2020	Amazon Data Services India	unknown	📄
5	admission.sol.**du.ac.**in	December 2020	Amazon Data Services India	Linux	📄
6	ug.**du.ac.**in	July 2017	Amazon Data Services India	Linux	📄
7	pgadmission.**du.ac.**in	August 2019	Amazon Data Services India	Linux	📄
8	solobe.**du.ac.**in	September 2020	Amazon Data Services India	Linux	📄
9	doe.**du.ac.**in	April 2018	Delhi University North Campus	Linux	📄
10	obe.**du.ac.**in	September 2020	Amazon Data Services India	Linux	📄

Click on Site report for more detail



Background

Site title		Date first seen	December 2020
Site rank	103306	Netcraft Risk Rating	1/10
Description		Primary language	

Network

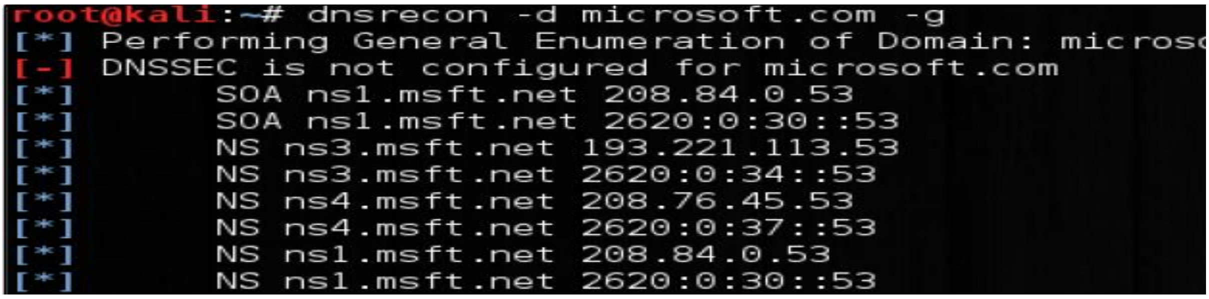
Site	http://web.sol.du.ac.in	Domain	du.ac.in
Netblock Owner	Amazon Data Services India	Nameserver	du.ac.in
Hosting company	Amazon - Asia Pacific (Mumbai) datacenter	Domain registrar	registry.in
Hosting country	in	Nameserver organisation	whois.registry.in
IPv4 address	13.126.69.121 (VirusTotal)	Organisation	Delhi University Computer Centre, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS16509	DNS admin	webmaster@du.ac.in
IPv6 address	Not Present	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ec2-13-126-69-121.ap-south-1.compute.amazonaws.com		

IP delegation

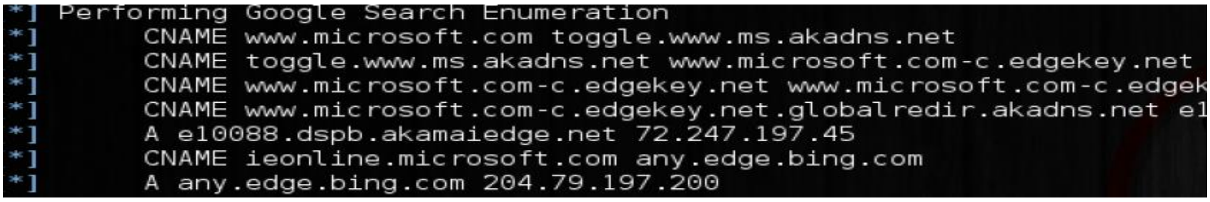
IPv4 address (13.126.69.121)

IP range	Country	Name	Description

- The second tool we can use is dnsrecon. If you are using Kali Linux, it is already installed on your machine and you can simply run it with the following command: dnsrecon -d microsoft.com –g. –d argument is for domain and –g is for “perform Google enumeration with standard enumeration”.



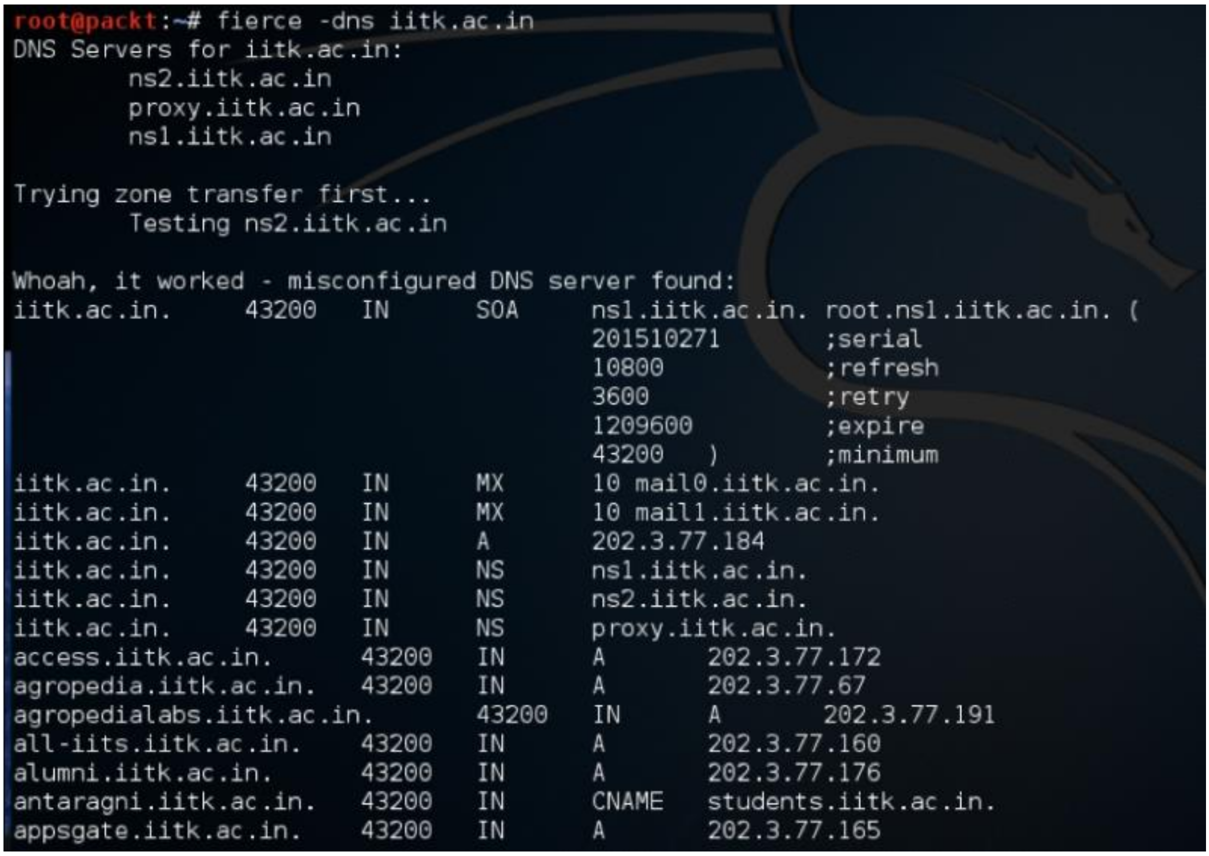
```
root@kali:~# dnsrecon -d microsoft.com -g
[*] Performing General Enumeration of Domain: micros
[-] DNSSEC is not configured for microsoft.com
[*]      SOA ns1.msft.net 208.84.0.53
[*]      SOA ns1.msft.net 2620:0:30::53
[*]      NS ns3.msft.net 193.221.113.53
[*]      NS ns3.msft.net 2620:0:34::53
[*]      NS ns4.msft.net 208.76.45.53
[*]      NS ns4.msft.net 2620:0:37::53
[*]      NS ns1.msft.net 208.84.0.53
[*]      NS ns1.msft.net 2620:0:30::53
```



```
*] Performing Google Search Enumeration
*]      CNAME www.microsoft.com toggle.www.ms.akadns.net
*]      CNAME toggle.www.ms.akadns.net www.microsoft.com-c.edgekey.net
*]      CNAME www.microsoft.com-c.edgekey.net www.microsoft.com-c.edgek
*]      CNAME www.microsoft.com-c.edgekey.net.globalredir.akadns.net el
*]      A e10088.dspb.akamaiedge.net 72.247.197.45
*]      CNAME ieonline.microsoft.com any.edge.bing.com
*]      A any.edge.bing.com 204.79.197.200
```

- How to find virtual host

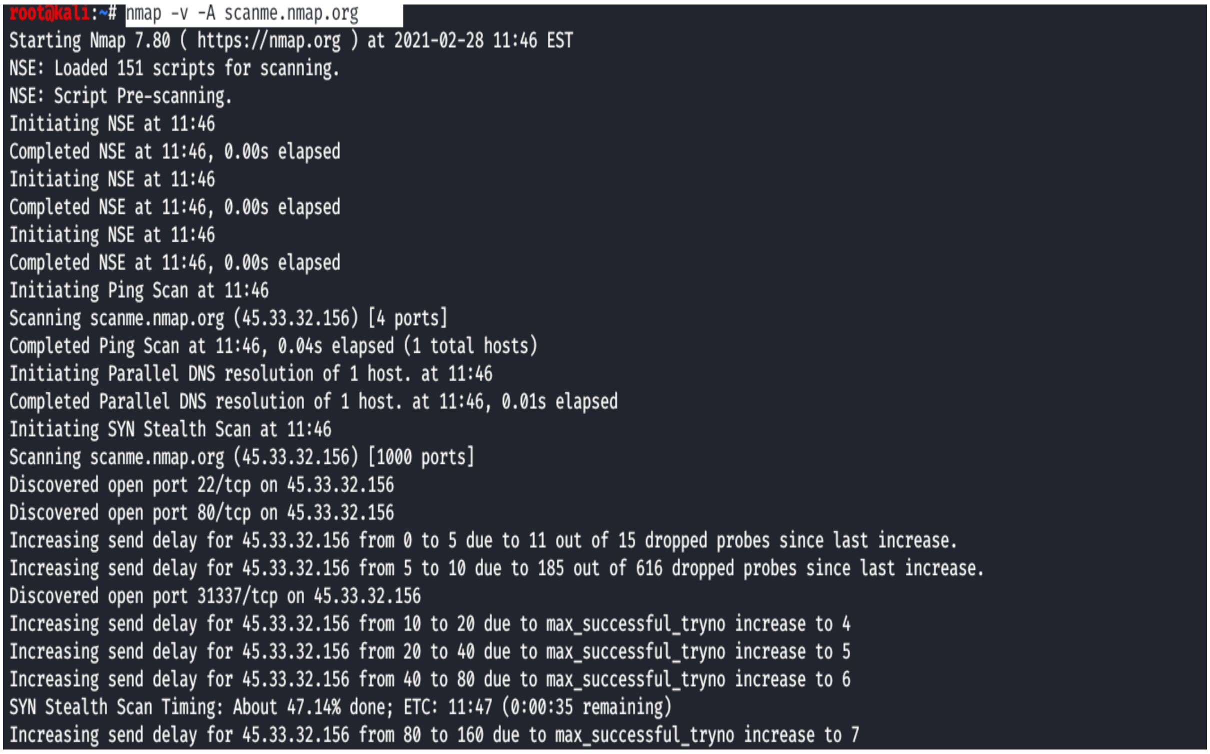
  - A virtual host is simply a website that shares an IP address with one or more other virtual hosts. These hosts are domains and subdomains. This is very common in a shared hosting environment where a multitude of websites share the same server/IP address
  - We can use tool name fierce for finding if website is hosted on a shared server or own server. Command : fierce –dns iitk.ac.in. As you can see in screenshot this website is hosted on a shared server.



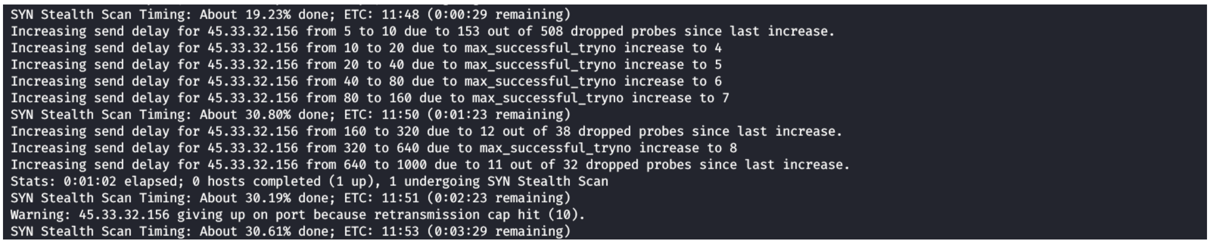
```
root@packt:~# fierce -dns iitk.ac.in
DNS Servers for iitk.ac.in:
        ns2.iitk.ac.in
        proxy.iitk.ac.in
        ns1.iitk.ac.in

Trying zone transfer first...
        Testing ns2.iitk.ac.in

Whoah, it worked - misconfigured DNS server found:
iitk.ac.in.     43200   IN      SOA     ns1.iitk.ac.in. root.ns1.iitk.ac.in. (
                                        201510271       ;serial
                                        10800           ;refresh
                                        3600            ;retry
                                        1209600         ;expire
                                        43200   )       ;minimum
iitk.ac.in.     43200   IN      MX      10 mail0.iitk.ac.in.
iitk.ac.in.     43200   IN      MX      10 mail1.iitk.ac.in.
iitk.ac.in.     43200   IN      A       202.3.77.184
iitk.ac.in.     43200   IN      NS      ns1.iitk.ac.in.
iitk.ac.in.     43200   IN      NS      ns2.iitk.ac.in.
iitk.ac.in.     43200   IN      NS      proxy.iitk.ac.in.
access.iitk.ac.in.      43200   IN      A       202.3.77.172
agropedia.iitk.ac.in.   43200   IN      A       202.3.77.67
agropedialabs.iitk.ac.in.       43200   IN      A       202.3.77.191
all-iits.iitk.ac.in.    43200   IN      A       202.3.77.160
alumni.iitk.ac.in.      43200   IN      A       202.3.77.176
antaragni.iitk.ac.in.   43200   IN      CNAME   students.iitk.ac.in.
appsgate.iitk.ac.in.    43200   IN      A       202.3.77.165
```

- NMAP

  - Nmap is the most popular port scanner tool. It is mostly used to enumerate open ports on a system
  - It can also verify operating system and running services on that port with high degree of accuracy. It is preinstalled in kali linux just type : nmap -v -A scanme.nmap.org



```
root@kali:~# nmap -v -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-28 11:46 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Initiating Ping Scan at 11:46
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 11:46, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:46
Completed Parallel DNS resolution of 1 host. at 11:46, 0.01s elapsed
Initiating SYN Stealth Scan at 11:46
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 185 out of 616 dropped probes since last increase.
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 47.14% done; ETC: 11:47 (0:00:35 remaining)
Increasing send delay for 45.33.32.156 from 80 to 160 due to max_successful_tryno increase to 7
```



```
SYN Stealth Scan Timing: About 19.23% done; ETC: 11:48 (0:00:29 remaining)
Increasing send delay for 45.33.32.156 from 5 to 10 due to 153 out of 508 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 6
Increasing send delay for 45.33.32.156 from 80 to 160 due to max_successful_tryno increase to 7
SYN Stealth Scan Timing: About 30.80% done; ETC: 11:50 (0:01:23 remaining)
Increasing send delay for 45.33.32.156 from 160 to 320 due to 12 out of 38 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 320 to 640 due to max_successful_tryno increase to 8
Increasing send delay for 45.33.32.156 from 640 to 1000 due to 11 out of 32 dropped probes since last increase.
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.19% done; ETC: 11:51 (0:02:23 remaining)
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 30.61% done; ETC: 11:53 (0:03:29 remaining)
```