

# FCS REPORT

Yashasvi Chaurasia  
2020159


## Question 3

- a) I first used the crt. sh and dnsdumpster tools to get the subdomain names and then used those names to fetch the private ip's using nslookup on my machine terminal

Using crt.sh:

crt.sh

Identity Search

 Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'iiitd.edu.in'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">7746158468</a>	2022-10-12	2022-10-12	2023-01-10	weave.iiitd.edu.in	weave.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7733568567</a>	2022-10-12	2022-10-12	2023-01-10	weave.iiitd.edu.in	weave.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7745062670</a>	2022-10-12	2022-10-12	2023-01-10	adarsh.iiitd.edu.in	adarsh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7731948630</a>	2022-10-12	2022-10-12	2023-01-10	adarsh.iiitd.edu.in	adarsh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7723384990</a>	2022-10-08	2022-10-08	2023-01-06	webs.iiitd.edu.in	webs.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7710577156</a>	2022-10-08	2022-10-08	2023-01-06	webs.iiitd.edu.in	webs.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7676113177</a>	2022-10-01	2022-10-01	2022-12-30	blr.opendata.iiitd.edu.in	blr.opendata.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7658188062</a>	2022-10-01	2022-10-01	2022-12-30	blr.opendata.iiitd.edu.in	blr.opendata.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7663572419</a>	2022-09-30	2022-09-30	2022-12-29	fh.iiitd.edu.in	achieve.fh.iiitd.edu.in auth.fh.iiitd.edu.in booking.fh.iiitd.edu.in crams.fh.iiitd.edu.in fh.iiitd.edu.in fms.fh.iiitd.edu.in hostel.fh.iiitd.edu.in nodues.fh.iiitd.edu.in share.fh.iiitd.edu.in wellbeing.fh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7650029643</a>	2022-09-30	2022-09-30	2022-12-29	fh.iiitd.edu.in	achieve.fh.iiitd.edu.in auth.fh.iiitd.edu.in booking.fh.iiitd.edu.in crams.fh.iiitd.edu.in fh.iiitd.edu.in fms.fh.iiitd.edu.in hostel.fh.iiitd.edu.in nodues.fh.iiitd.edu.in share.fh.iiitd.edu.in wellbeing.fh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7655991293</a>	2022-09-29	2022-09-29	2022-12-28	federatedhealthplatform.tavlab.iiitd.edu.in	federatedhealthplatform.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7643435116</a>	2022-09-29	2022-09-29	2022-12-28	federatedhealthplatform.tavlab.iiitd.edu.in	federatedhealthplatform.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7647046149</a>	2022-09-28	2022-09-28	2022-12-27	odorify.ahujalab.iiitd.edu.in	odorify.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7635851553</a>	2022-09-28	2022-09-28	2022-12-27	odorify.ahujalab.iiitd.edu.in	odorify.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7643245052</a>	2022-09-27	2022-09-27	2022-12-26	evidenceflow.tavlab.iiitd.edu.in	evidenceflow.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7632383091</a>	2022-09-27	2022-09-27	2022-12-26	evidenceflow.tavlab.iiitd.edu.in	evidenceflow.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7639147880</a>	2022-09-27	2022-09-27	2022-12-26	kracr.iiitd.edu.in	kracr.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7628552853</a>	2022-09-27	2022-09-27	2022-12-26	kracr.iiitd.edu.in	kracr.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7626927022</a>	2022-09-25	2022-09-25	2022-12-24	antibioticsteward.tavlab.iiitd.edu.in	antibioticsteward.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7617955958</a>	2022-09-25	2022-09-25	2022-12-24	antibioticsteward.tavlab.iiitd.edu.in	antibioticsteward.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7625194367</a>	2022-09-25	2022-09-25	2022-12-24	visiontoli.iiitd.edu.in	visiontoli.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
	<a href="#">7616000045</a>	2022-09-25	2022-09-25	2022-12-24	visiontoli.iiitd.edu.in	visiontoli.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3

Top 5 results:

webs.iiitd.edu.in [192.168.16.122]  
fh.iiitd.edu.in [192.168.1.240]  
visiontoli.iiitd.edu.in [192.168.2.11]  
Eda.tavlab.iiitd.edu.in[192.168.1.52]

```
> webs.iiitd.edu.in
Server:      192.168.1.8
Address:     192.168.1.8#53

Name:  webs.iiitd.edu.in
Address: 192.168.16.122
> fh.iiitd.edu.in
Server:      192.168.1.8
Address:     192.168.1.8#53

Name:  fh.iiitd.edu.in
Address: 192.168.1.240
> visiontoli.iiitd.edu.in
Server:      192.168.1.8
Address:     192.168.1.8#53

Name:  visiontoli.iiitd.edu.in
Address: 192.168.2.11
> eda.tavlab.iiitd.edu.in
Server:      192.168.1.8
Address:     192.168.1.8#53

Name:  eda.tavlab.iiitd.edu.in
Address: 192.168.1.52
> ea.iiitd.edu.in
Server:      192.168.1.8
Address:     192.168.1.8#53

ea.iiitd.edu.in canonical name = ext-cust.squarespace.com.
Name:  ext-cust.squarespace.com
Address: 198.185.159.145
Name:  ext-cust.squarespace.com
Address: 198.49.23.144
Name:  ext-cust.squarespace.com
Address: 198.185.159.144
Name:  ext-cust.squarespace.com
Address: 198.49.23.145
> 
```

# Using dnsdumpster:

5

ctrl.sh | iitd.edu.in

DNSDumpster.com - dns recon and research, find and lookup dns records

🏠

🛡️

🎓

🟢

dns recon & research, find & lookup dns records

ipxampldomain.com

Search ▶

Showing results for iitd.edu.in

DNS Servers

MX Records

TXT Records

Host (A) Records

Domain Map

Hosting (IP block owners)

GeoIP of Host Locations

96

80

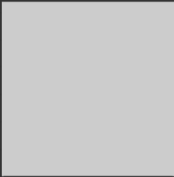
64

48


32

16

0



NKN-CORE-NW NKN Core Network



<div>iidcn2022.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div> <div>HTTP TECH: Apache/2.2.15</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	<div>🏠</div> <div>🛡️</div> <div>🎓</div> <div>🟢</div>
<div>lcs2.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div> <div>HTTP TECH: Apache/2.2.15</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	
<div>ns2.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div></div> <div></div> <div></div>	103.25.231.10	NKN-CORE-NW NKN Core Network India	
<div>bda2014.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div> <div>HTTP TECH: Apache/2.2.15</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	
<div>ask2014.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div> <div>HTTP TECH: Apache/2.2.15</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	
<div>byld5.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: nginx/1.14.0 (Ubuntu)</div> <div>HTTP TECH: Ubuntu nginx,1.14.0</div>	103.25.231.35	NKN-CORE-NW NKN Core Network India	
<div>indocrypt2016.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div> <div>HTTP TECH: Apache/2.2.15</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	
<div>aida.iitd.edu.in</div> <div>🏠 🛡️ 🎓 🟢</div> <div>HTTP: Apache/2.2.15 (Oracle)</div> <div>SSH: SSH-2.0-OpenSSH_5.3</div>	103.25.231.5	NKN-CORE-NW NKN Core Network India	

Top 5 results :

```
Ask2014.iiitd.edu.in [192.168.1.27]  
byld5.iiitd.edu.in [192.168.1.121]  
lcs2.iiitd.edu.in [192.168.1.27]  
finnexia.iiitd.edu.in [192.168.1.27]  
wiser.tavlab.iiitd.edu.in [192.168.1.211]
```

```
> ask2014.iiitd.edu.in  
Server:      192.168.1.8  
Address:     192.168.1.8#53  
  
Name:  ask2014.iiitd.edu.in  
Address: 192.168.1.27  
> byld5.iiitd.edu.in  
Server:      192.168.1.8  
Address:     192.168.1.8#53  
  
Name:  byld5.iiitd.edu.in  
Address: 192.168.1.121  
> lcs2.iiitd.edu.in  
Server:      192.168.1.8  
Address:     192.168.1.8#53  
  
Name:  lcs2.iiitd.edu.in  
Address: 192.168.1.27  
> finnexia.iiitd.edu.in  
Server:      192.168.1.8  
Address:     192.168.1.8#53  
  
Name:  finnexia.iiitd.edu.in  
Address: 192.168.1.27  
> wiser.tavlab.iiitd.edu.in  
Server:      192.168.1.8  
Address:     192.168.1.8#53  
  
Name:  wiser.tavlab.iiitd.edu.in  
Address: 192.168.1.211  
> 
```

b)

Methodology:

I used dnsdumpster to search for subdomains with iitd.edu.in and then downloaded the xlsx sheet from the website.

Once the sheet is downloaded I generated a python script and used the sockets library in python to lookup the private IP of the server using the server domain name from the xlsx sheet. Later I wrote the output of the private IPs in the file called subdomains.txt, which contains the domain name along with the private IP of the server.

The automated script is written in python, and it creates a list of dictionaries of the xlsx sheet.

I then use the list and iterate through the list to find subdomains in the dictionary .

After looking up the subdomain I simply find the private IP using the hostname of the server and write it in a file and hence automating the manual process of finding the private IP addresses for the server.

c)

The private IP if leaked to the public can cause harm as the corrupted or people with malicious intent inside the local network of the institute can know the exact IP address of the server and hence they can cause “Ddos Attacks” or MITM attacks and they can even blacklist these server IP from accessing other useful resources inside the campus network.

People outside the campus network will have to get into the local network to cause any harm to the webserver and launch server-IP-specific attacks.

An attacker from outside the campus cannot access the server from the server’s private IP and hence he cannot deal much damage to the server unless he reaches inside the local network.

Once inside the local network along with the server, the attacker can pretend to be the server and deliver malicious content to the outside world as the attacker uses the server IP to fake its own IP.