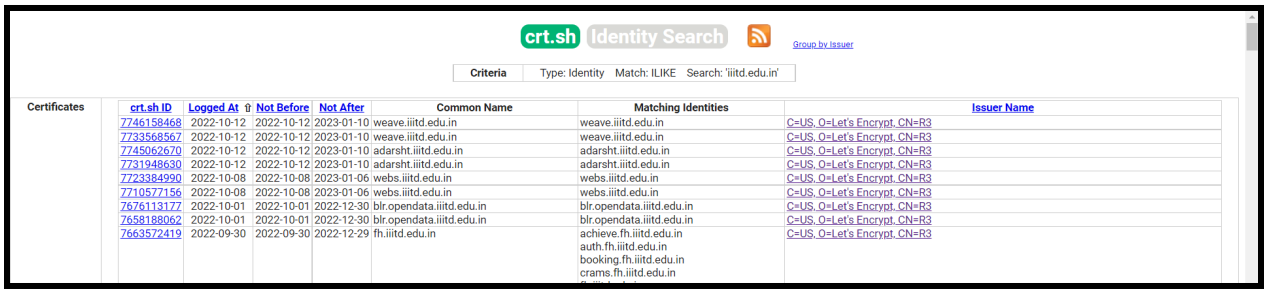
Fundamentals of Computer Security
(CSE 345/CSE 545)
Assignment 1
Question 3

Nakul Thureja
2020528

Part A

Finding IP Addresses of subdomains present on [crt.sh](crt.sh) using host command in wsl.

```
nakul@NakulThureja:~$ host nodues.fh.iiitd.edu.in
nodues.fh.iiitd.edu.in has address 192.168.1.240
nakul@NakulThureja:~$ host hostel.fh.iiitd.edu.in
hostel.fh.iiitd.edu.in has address 192.168.1.240
nakul@NakulThureja:~$ host achieve.fh.iiitd.edu.in
achieve.fh.iiitd.edu.in has address 192.168.1.240
nakul@NakulThureja:~$ host weave.iiitd.edu.in
weave.iiitd.edu.in is an alias for weave-lab-iiitd.github.io.
weave-lab-iiitd.github.io has address 185.199.109.153
weave-lab-iiitd.github.io has address 185.199.111.153
weave-lab-iiitd.github.io has address 185.199.110.153
weave-lab-iiitd.github.io has address 185.199.108.153
weave-lab-iiitd.github.io has IPv6 address 2606:50c0:8000::153
weave-lab-iiitd.github.io has IPv6 address 2606:50c0:8003::153
weave-lab-iiitd.github.io has IPv6 address 2606:50c0:8001::153
weave-lab-iiitd.github.io has IPv6 address 2606:50c0:8002::153
nakul@NakulThureja:~$ host merc.sbilab.iiitd.edu.in
merc.sbilab.iiitd.edu.in has address 192.168.18.110
nakul@NakulThureja:~$
```



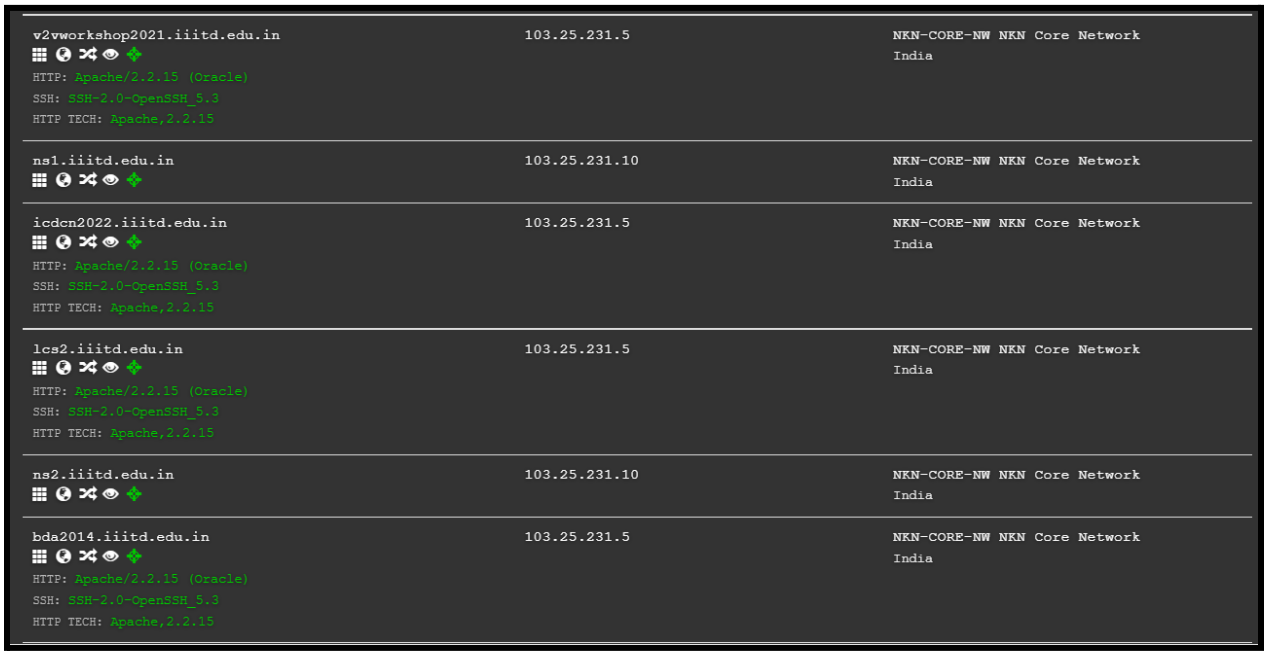
crt.sh Identity Search — Group by Issuer

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

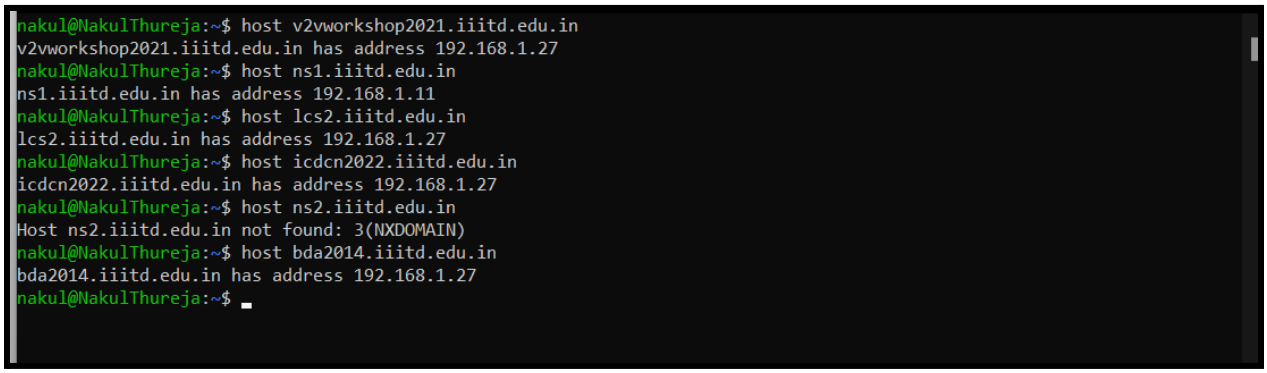
Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
7746158468	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
7733568567	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
7745062670	2022-10-12	2022-10-12	2023-01-10	adarsht.iiitd.edu.in	adarsht.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7731948630	2022-10-12	2022-10-12	2023-01-10	adarsht.iiitd.edu.in	adarsht.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7723384990	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
7710577156	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
7676113177	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
7658188062	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
7663572419	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	C=US, O=Let's Encrypt, CN=R3

Finding IP Addresses of subdomains present on dnsdumpster.com using host command in wsl.



v2vworkshop2021.iiitd.edu.in HTTP: Apache/2.2.15 (Oracle) SSH: SSH-2.0-OpenSSH_5.3 HTTP TECH: Apache,2.2.15	103.25.231.5	NKN-CORE-NW NKN Core Network India
ns1.iiitd.edu.in	103.25.231.10	NKN-CORE-NW NKN Core Network India
icdcn2022.iiitd.edu.in HTTP: Apache/2.2.15 (Oracle) SSH: SSH-2.0-OpenSSH_5.3 HTTP TECH: Apache,2.2.15	103.25.231.5	NKN-CORE-NW NKN Core Network India
lcs2.iiitd.edu.in HTTP: Apache/2.2.15 (Oracle) SSH: SSH-2.0-OpenSSH_5.3 HTTP TECH: Apache,2.2.15	103.25.231.5	NKN-CORE-NW NKN Core Network India
ns2.iiitd.edu.in	103.25.231.10	NKN-CORE-NW NKN Core Network India
bda2014.iiitd.edu.in HTTP: Apache/2.2.15 (Oracle) SSH: SSH-2.0-OpenSSH_5.3 HTTP TECH: Apache,2.2.15	103.25.231.5	NKN-CORE-NW NKN Core Network India



```
nakul@NakulThureja:~$ host v2vworkshop2021.iiitd.edu.in
v2vworkshop2021.iiitd.edu.in has address 192.168.1.27
nakul@NakulThureja:~$ host ns1.iiitd.edu.in
ns1.iiitd.edu.in has address 192.168.1.11
nakul@NakulThureja:~$ host lcs2.iiitd.edu.in
lcs2.iiitd.edu.in has address 192.168.1.27
nakul@NakulThureja:~$ host icdcn2022.iiitd.edu.in
icdcn2022.iiitd.edu.in has address 192.168.1.27
nakul@NakulThureja:~$ host ns2.iiitd.edu.in
Host ns2.iiitd.edu.in not found: 3(NXDOMAIN)
nakul@NakulThureja:~$ host bda2014.iiitd.edu.in
bda2014.iiitd.edu.in has address 192.168.1.27
nakul@NakulThureja:~$
```

Subdomain : IP (Generated with Automation) -

federatedhealthplatform.tavlab.iiitd.edu.in : 192.168.1.52
www.ea.iiitd.edu.in : 198.185.159.144
quiz.autoscuolaburnout.it : 151.101.1.195
odorify.ahujalab.iiitd.edu.in : 192.168.30.53
esya.iiitd.edu.in : 192.168.1.104
weave.iiitd.edu.in : 185.199.108.153
crams.fh.iiitd.edu.in : 192.168.1.240
prid.iiitd.edu.in : 192.168.28.124
evidenceflow.tavlab.iiitd.edu.in : 192.168.1.211
opendata.iiitd.edu.in : 192.168.1.234
dataquality.tavlab.iiitd.edu.in : 192.168.1.52
events.iiitd.edu.in : 192.168.1.121
fh.iiitd.edu.in : 192.168.1.240
ecell.iiitd.edu.in : 192.168.1.27
booking.fh.iiitd.edu.in : 192.168.1.240
iiitd.edu.in : 192.168.1.7
ecgdetect.sbilab.iiitd.edu.in : 192.168.18.110
ciclop.raylab.iiitd.edu.in : 192.168.30.176
kc.kobo.melange.iiitd.edu.in : 192.168.1.40
cosylab.iiitd.edu.in : 192.168.1.92
digest.raylab.iiitd.edu.in : 192.168.30.176
foods.com.my : 151.101.1.195
byld.iiitd.edu.in : 192.168.1.133
byld5.iiitd.edu.in : 192.168.1.121
www.kritterscountrylane.com : 151.101.1.195
eda.tavlab.iiitd.edu.in : 192.168.1.52
hostel.fh.iiitd.edu.in : 192.168.1.240
ee.kobo.melange.iiitd.edu.in : 192.168.1.40
www.chaosfingershop.com : 151.101.1.195
visiontoli.iiitd.edu.in : 192.168.2.11
transcend.senguptalab.iiitd.edu.in : 192.168.17.155
antibioticsteward.tavlab.iiitd.edu.in : 192.168.1.52
ea.iiitd.edu.in : 198.185.159.145
links.jialonso.com : 151.101.65.195
precog.iiitd.edu.in : 192.168.1.17
wiser.tavlab.iiitd.edu.in : 192.168.1.211
nodues.fh.iiitd.edu.in : 192.168.1.240
tedx.iiitd.edu.in : 192.168.1.104
deepgraphh.ahujalab.iiitd.edu.in : 192.168.30.53

```
webs.iiitd.edu.in  :  192.168.16.122
www.ewaytax.in  :  34.98.99.30
collectskins.com  :  172.67.139.16
auth.fh.iiitd.edu.in  :  192.168.1.240
merc.sbilab.iiitd.edu.in  :  192.168.18.110
fms.fh.iiitd.edu.in  :  192.168.1.240
idp.iiitd.edu.in  :  192.168.1.31
kracr.iiitd.edu.in  :  192.168.1.166
easyscheduler.kracr.iiitd.edu.in  :  192.168.1.255
share.fh.iiitd.edu.in  :  192.168.1.240
kf.kobo.melange.iiitd.edu.in  :  192.168.1.40
blr.opendata.iiitd.edu.in  :  192.168.1.234
foobar.iiitd.edu.in  :  192.168.1.116
odyssey.iiitd.edu.in  :  192.168.1.104
wellbeing.fh.iiitd.edu.in  :  192.168.1.240
ayushmanbharat.melange.iiitd.edu.in  :  192.168.2.71
achieve.fh.iiitd.edu.in  :  192.168.1.240
metabokiller.ahujalab.iiitd.edu.in  :  192.168.30.53
```

Part B

I used the site crt.sh to find all the subdomains, then using the pandas libraries read_html() function I read all the possible subdomains in a list and then made a set of the these subdomains since many of them were repeating. To read the subdomains, I took the 5th and 6th columns of the table present on the webpage (https://crt.sh/?q=iiitd.edu.in).

```
File = open('2020528_q3.txt', 'w')
url = "https://crt.sh/?q=iiitd.edu.in"
page = pd.read_html(url)
table = page[2]
```

Finally, I iterated through the set and found the private IP addresses using the gethostbyname() function in the socket library, and write the output in the file 2020528_q3.txt.
Note: Since I was present in the IIITD intranet, this function returned private IP addresses, and when the same script is run outside the network, it will not give the same results.

```
for i in res:
    try:
        print(i," : ", socket.gethostbyname(i),file = File)
    except:
        pass
```

Part C:

Having a list of private IP addresses inherently does not help the hacker as they might not be present in the internal network of IIITD.
If an attacker from outside the network tries to ping these IPs they will not be able to as these IP addresses do not exist publicly.

But having the list of all subdomains gives enough information to the attacker to find vulnerabilities in any subdomain to bypass the firewall and get access to the internal network. Some variations of these attacks is known as subdomain enumeration. Here the attacker finds as many subdomains as they can using the tools discussed in Part A and find hidden or forgotten subdomains with vulnerabilities exploit.

Once an attacker is inside the network they can perform various kinds of attacks such as IP spoofing. They can also try to get root access to the server and wreck the server. Other attacks may constitute getting the personal information stored on the servers and monitoring organizations' activities on the internet.