FCS assignment - 1.1

Q3.a

Crt.sh

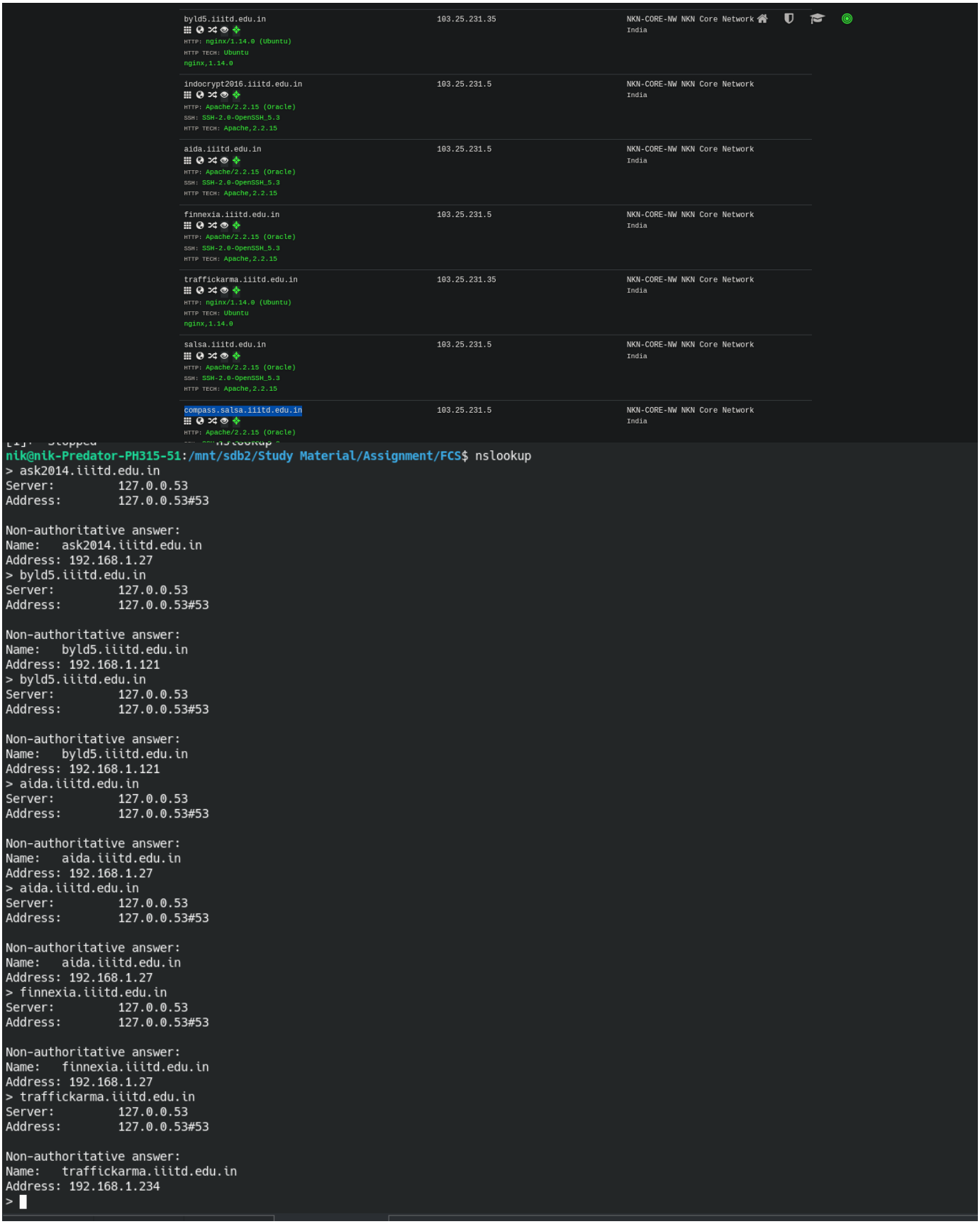
Criteria | Type: Identity Match: ILIKE Search: 'iiitd.edu.in'

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 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
7650029643	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
7655991293	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
7643435116	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
7647046149	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
7635851553	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
7643245052	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
7632383091	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
7639147880	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
7628552853	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
7626927022	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

```
nik@nik-Predator-PH315-51:/mnt/sdb2/Study Material/Assignment/FCS$ nslookup
> webs.iiitd.edu.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   webs.iiitd.edu.in
Address: 192.168.16.122
> blr.opendata.iiitd.edu.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   blr.opendata.iiitd.edu.in
Address: 192.168.1.234
> achieve.fh.iiitd.edu.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   achieve.fh.iiitd.edu.in
Address: 192.168.1.240
> odorify.ahujalab.iiitd.edu.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   odorify.ahujalab.iiitd.edu.in
Address: 192.168.30.53
> kracr.iiitd.edu.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   kracr.iiitd.edu.in
Address: 192.168.1.166
>
```

Dnsdumpster



Below is all the ip's from the script

```
'achieve.fh.iiitd.edu.in:192.168.1.240',
'dataquality.tavlab.iiitd.edu.in:192.168.1.52',
'ciclop.raylab.iiitd.edu.in:192.168.30.176',
'crams.fh.iiitd.edu.in:192.168.1.240',
```

```
'idp.iiitd.edu.in:192.168.1.31',
'odorify.ahujalab.iiitd.edu.in:192.168.30.53',
'transcend.senguptalab.iiitd.edu.in:192.168.17.155',
'merc.sbilab.iiitd.edu.in:192.168.18.110',
'fh.iiitd.edu.in:192.168.1.240',
'precog.iiitd.edu.in:192.168.1.17',
'tedx.iiitd.edu.in:192.168.1.104',
'auth.fh.iiitd.edu.in:192.168.1.240',
'prid.iiitd.edu.in:192.168.28.124',
'webs.iiitd.edu.in:192.168.16.122',
'wiser.tavlab.iiitd.edu.in:192.168.1.21',
'easyscheduler.kracr.iiitd.edu.in:192.168.1.255',
'ayushmanbharat.melange.iiitd.edu.in:192.168.2.71',
'ea.iiitd.edu.in:198.49.23.144',
'nodues.fh.iiitd.edu.in:192.168.1.240',
'foobar.iiitd.edu.in:192.168.1.116',
'eda.tavlab.iiitd.edu.in:192.168.1.52',
'antibioticsteward.tavlab.iiitd.edu.in:192.168.1.52',
'cosylab.iiitd.edu.in:192.168.1.92',
'visiontoli.iiitd.edu.in:192.168.2.11',
'odyssey.iiitd.edu.in:192.168.1.104',
'esya.iiitd.edu.in:192.168.1.104',
'events.iiitd.edu.in:192.168.1.121',
'wellbeing.fh.iiitd.edu.in:192.168.1.240',
'www.ea.iiitd.edu.in:198.49.23.144',
'ee.kobo.melange.iiitd.edu.in:192.168.1.40',
'byld.iiitd.edu.in:192.168.1.133',
'opendata.iiitd.edu.in:192.168.1.234',
'deepgraphh.ahujalab.iiitd.edu.in:192.168.30.53',
'digest.raylab.iiitd.edu.in:192.168.30.176',
'blr.opendata.iiitd.edu.in:192.168.1.234',
'iiitd.edu.in:192.168.1.7',
'booking.fh.iiitd.edu.in:192.168.1.240',
'metabokiller.ahujalab.iiitd.edu.in:192.168.30.53',
'ecell.iiitd.edu.in:192.168.1.27',
'ecgdetect.sbilab.iiitd.edu.in:192.168.18.110',
'kf.kobo.melange.iiitd.edu.in:192.168.1.40',
'fms.fh.iiitd.edu.in:192.168.1.240',
'byld5.iiitd.edu.in:192.168.1.121',
'kracr.iiitd.edu.in:192.168.1.166',
'weave.iiitd.edu.in:185.199.108.153',
'kc.kobo.melange.iiitd.edu.in:192.168.1.40',
'federatedhealthplatform.tavlab.iiitd.edu.in:192.168.1.52',
```

```
'hostel.fh.iiitd.edu.in:192.168.1.240',
'share.fh.iiitd.edu.in:192.168.1.240']
```

Q3.b

- As mentioned in python ipynb file , I am using pycrtsh library.
- It gets all the certificates information of the website.
- After that I am storing all the sub domain in the list
- Some sub domain contains mutiple url with `\n` delimiter , so splitting those string and appending in res_list
    - Also filtering some url which contain *.___.___ subdomain, because we cannot get resolve this type of domain
- using socket resolving domain name
- and then printing all the values in the console.

Q3.c

- Attacker can do ddos attack on the network using ip spoofing (using private ips) , to bypass firewall.
- any it will be very difficult to protect the from these attack because we cannot know the attacker ips
- Also attacker can do man in the middle attack by hijacking the connection using servers ip (subdomain ip).
- They can also hijack user session by saying , this is new website ip (arp spoofing in router). and redirect to their version of hosted website, such that they can steal user information
- Also attacker can try to attack nameserver domain (dns) that resolves all the ips using information about private ip's.