part a

----CRT Subdomains----

1pxdesignconf.iiitd.edu.in : 192.168.1.27
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 : 192.168.1.240
adarsht.iiitd.edu.in : 192.168.1.7
amrorbit.tavlab.iiitd.edu.in : 192.168.3.74
antibioticsteward.tavlab.iiitd.edu.in : 192.168.1.52
antibioticsteward.tavlab.iiitd.edu.in
dataquality.tavlab.iiitd.edu.in
eda.tavlab.iiitd.edu.in
federatedhealthplatform.tavlab.iiitd.edu.in : 192.168.1.52
api.irb.iiitd.edu.in : 192.168.3.128
arms.iiitd.edu.in : 192.168.1.79
arms2.iiitd.edu.in : 192.168.1.7
armsdev.iiitd.edu.in : 192.168.2.61
ayushmanbharat.melange.iiitd.edu.in : 192.168.2.71
blr.opendata.iiitd.edu.in : 192.168.1.234
booking.fh.iiitd.edu.in : 192.168.1.240
booking.iiitd.edu.in : 192.168.1.7
byld.iiitd.edu.in : 192.168.3.70

byld5.iiitd.edu.in : 192.168.1.121
chikitsachakra.tavlab.iiitd.edu.in : 192.168.3.74
ciclop.raylab.iiitd.edu.in : 192.168.30.176
ciclop.raylab.iiitd.edu.in
digest.raylab.iiitd.edu.in : 192.168.30.176
cilab.iiitd.edu.in : 192.168.3.70
claps.iiitd.edu.in : 192.168.3.56
cloudlab.iiitd.edu.in : 192.168.3.54
collabamigo.iiitd.edu.in : 192.168.1.7
cosylab.iiitd.edu.in : 192.168.1.92
crohnaids.tavlab.iiitd.edu.in : 192.168.1.153
crohnaidsadmin.tavlab.iiitd.edu.in : 192.168.1.153
crohnaidsapi.tavlab.iiitd.edu.in : 192.168.1.153
dataquality.tavlab.iiitd.edu.in : 192.168.1.52
deepgraphh.ahujalab.iiitd.edu.in : 192.168.30.53
deepmoa.ahujalab.iiitd.edu.in : 192.168.1.7
digest.raylab.iiitd.edu.in : 192.168.30.176
ea.iiitd.edu.in : 198.49.23.145
easyscheduler.kracr.iiitd.edu.in : 192.168.1.255
easyscheduler.kracr.iiitd.edu.in
www.easyscheduler.kracr.iiitd.edu.in : 192.168.1.255
ecell.iiitd.edu.in : 192.168.1.27
ecgdetect.sbilab.iiitd.edu.in
merc.sbilab.iiitd.edu.in : 192.168.18.110
eda.tavlab.iiitd.edu.in : 192.168.3.144
ee.kobo.melange.iiitd.edu.in
kc.kobo.melange.iiitd.edu.in
kf.kobo.melange.iiitd.edu.in : 192.168.1.40
engageme.hmi.iiitd.edu.in : 192.168.30.207
esummit.iiitd.edu.in : 192.168.1.104
esya.iiitd.edu.in : 192.168.1.104
esya.iiitd.edu.in
www.esya.iiitd.edu.in : 192.168.1.104
events.iiitd.edu.in : 192.168.3.70
evidenceflow.tavlab.iiitd.edu.in : 192.168.1.211
evokg.ahujalab.iiitd.edu.in : 192.168.24.13
federatedhealthplatform.tavlab.iiitd.edu.in : 192.168.3.144
foobar.iiitd.edu.in : 192.168.1.116
greenpreneurs.iiitd.edu.in : 46.202.166.45
idp.iiitd.edu.in : 192.168.1.31
iiitd.edu.in
one-ird.iiitd.edu.in : 192.168.1.7
ims.ecelabs.iiitd.edu.in : 192.168.3.169
irb.iiitd.edu.in : 192.168.3.127

kracr.iiitd.edu.in : 192.168.1.166
libweb.iiitd.edu.in : 192.168.1.7
medicalleaveportal.iiitd.edu.in : 192.168.3.164
meet.iiitd.edu.in : 192.168.1.7
merc.sbilab.iiitd.edu.in : 192.168.18.110
metabokiller.ahujalab.iiitd.edu.in : 192.168.30.53
neurocare-liggen.iiitd.edu.in : 192.168.3.158
nodues.iiitd.edu.in : 192.168.3.198
odorify.ahujalab.iiitd.edu.in : 192.168.30.53
odyssey.iiitd.edu.in : 192.168.1.104
one-ird.iiitd.edu.in : 192.168.3.81
opendata.iiitd.edu.in : 192.168.1.234
opine.iiitd.edu.in : 192.168.1.120
orco.iiitd.edu.in : 192.168.3.70
perp.iiitd.edu.in : 192.168.1.7
phd-portal.iiitd.edu.in : 192.168.3.166
precog.iiitd.edu.in : 192.168.1.17
prid.iiitd.edu.in : 192.168.28.124
projecterp.iiitd.edu.in : 192.168.2.217
quickstart24.cqt.iiitd.edu.in : 192.168.1.7
raylab.iiitd.edu.in : 192.168.30.176
rims.iiitd.edu.in : 192.168.3.12
rms.iiitd.edu.in : 192.168.3.172
sapnansl.nrl.iiitd.edu.in : 192.168.29.160
smpportal.iiitd.edu.in : 192.168.3.168
taallocation.iiitd.edu.in : 192.168.3.170
tavlab.iiitd.edu.in : 192.168.3.74
techtree.iiitd.edu.in : 192.168.1.77
tedx.iiitd.edu.in : 192.168.1.104
transcend.senguptalab.iiitd.edu.in : 192.168.17.155
visiontoli.iiitd.edu.in : 192.168.1.7
weave.iiitd.edu.in : 153
webs.iiitd.edu.in : 192.168.22.132
wellbeing.iiitd.edu.in : 192.168.3.137
wiser.tavlab.iiitd.edu.in : 192.168.1.211
www.ea.iiitd.edu.in : 198.185.159.144

----DNSDumpster----

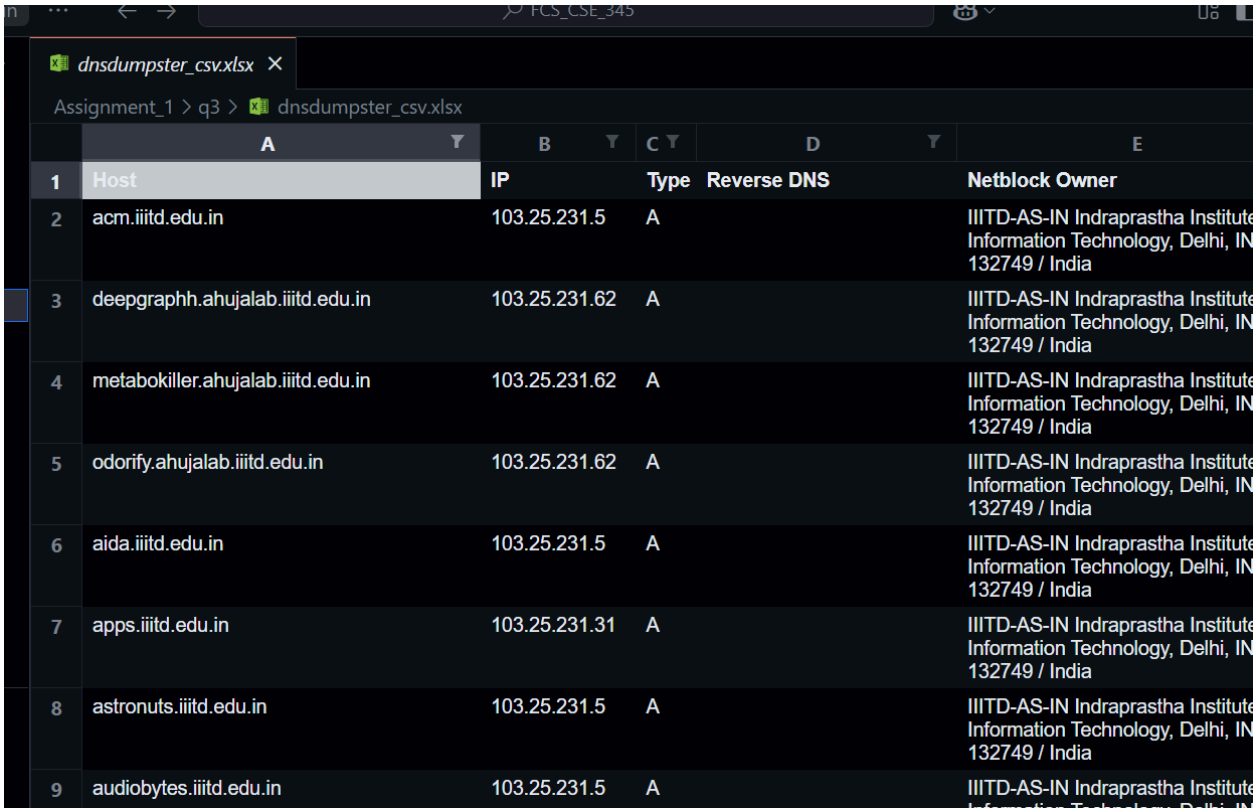
acm.iiitd.edu.in : 192.168.1.27
deepgraphh.ahujalab.iiitd.edu.in : 192.168.30.53
metabokiller.ahujalab.iiitd.edu.in : 192.168.30.53
odorify.ahujalab.iiitd.edu.in : 192.168.30.53
aida.iiitd.edu.in : 192.168.1.27

apps.iiitd.edu.in : 192.168.1.71
astronuts.iiitd.edu.in : 192.168.1.27
audiobytes.iiitd.edu.in : 192.168.1.27
byld.iiitd.edu.in : 192.168.3.70
byld5.iiitd.edu.in : 192.168.1.121
cc.iiitd.edu.in : 192.168.1.27
cellatlassearch.iiitd.edu.in : 192.168.2.104
cloudlab.iiitd.edu.in : 192.168.3.54
convergence.iiitd.edu.in : 192.168.1.27
cosylab.iiitd.edu.in : 192.168.1.92
quickstart24.cqt.iiitd.edu.in : 192.168.1.7
crypto.iiitd.edu.in : 192.168.1.27
cyborg.iiitd.edu.in : 192.168.1.27
d4rkc0de.iiitd.edu.in : 192.168.1.27
dsc.iiitd.edu.in : 192.168.1.27
ecelabs.iiitd.edu.in : 192.168.1.27
ent.iiitd.edu.in : 192.168.1.27
erp.iiitd.edu.in : 192.168.2.22
esya.iiitd.edu.in : 192.168.1.104
fh.iiitd.edu.in : 192.168.1.240
achieve.fh.iiitd.edu.in : 192.168.1.240
auth.fh.iiitd.edu.in : 192.168.1.240
booking.fh.iiitd.edu.in : 192.168.1.240
crams.fh.iiitd.edu.in : 192.168.1.240
fms.fh.iiitd.edu.in : 192.168.1.240
hostel.fh.iiitd.edu.in : 192.168.1.240
nodues.fh.iiitd.edu.in : 192.168.1.240
share.fh.iiitd.edu.in : 192.168.1.240
wellbeing.fh.iiitd.edu.in : 192.168.1.240
findmystuff.iiitd.edu.in : 192.168.1.133
foobar.iiitd.edu.in : 192.168.1.116
gamecraft.iiitd.edu.in : 192.168.1.27
graphics.iiitd.edu.in : 192.168.1.27
idp.iiitd.edu.in : 192.168.1.31
indocrypt2016.iiitd.edu.in : 192.168.1.27
induction.iiitd.edu.in : 192.168.1.27
innovatedelhi.iiitd.edu.in : 192.168.1.27
it.iiitd.edu.in : 192.168.3.70
jobport.iiitd.edu.in : 192.168.1.119
kracr.iiitd.edu.in : 192.168.1.166
easyscheduler.kracr.iiitd.edu.in : 192.168.1.255
library.iiitd.edu.in : 192.168.3.83
madtoes.iiitd.edu.in : 192.168.1.27
ayushmanbharat.melange.iiitd.edu.in : 192.168.2.71

ee.kobo.melange.iiitd.edu.in : 192.168.1.40
ns2.iiitd.edu.in : 192.168.1.7
ns1.iiitd.edu.in : 192.168.1.11

part b


```
[
    {
    "issuer_ca_id": 295814,
    "issuer_name": "C=US, O=Let's Encrypt, CN=R10",
    "common_name": "esya.iiitd.edu.in",
    "name_value": "esya.iiitd.edu.in",
    "id": 16839485502,
    "entry_timestamp": "2025-02-20T13:36:48.387",
    "not_before": "2025-02-20T12:38:18",
    "not_after": "2025-05-21T12:38:17",
    "serial_number": "03920b11e87bfaa6b7eee448d3087b5f38a6",
    "result_count": 2
    }
```

dnsdumpster_csv.xlsx

Assignment_1 > q3 > dnsdumpster_csv.xlsx

	A	B	C	D	E
1	Host	IP	Type	Reverse DNS	Netblock Owner
2	acm.iiitd.edu.in	103.25.231.5	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
3	deepgraphh.ahujalab.iiitd.edu.in	103.25.231.62	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
4	metabokiller.ahujalab.iiitd.edu.in	103.25.231.62	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
5	odorify.ahujalab.iiitd.edu.in	103.25.231.62	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
6	aida.iiitd.edu.in	103.25.231.5	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
7	apps.iiitd.edu.in	103.25.231.31	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
8	astronuts.iiitd.edu.in	103.25.231.5	A		IIITD-AS-IN Indraprastha Institute Information Technology, Delhi, IN 132749 / India
9	audiobytes.iiitd.edu.in	103.25.231.5	A		IIITD-AS-IN Indraprastha Institute

first the json and csv files were downloaded from crt.sh and dnsdumpster to get all the subdomain names.

Then **nslookup** command was used to find the private IPs by iterating over all the subdomains using the below function

```python
class NSLookupResolver(IPResolverStrategy):
    """IP Resolver using nslookup."""
    def get_ip_address(self, subdomain: str) -> str:
        try:
            result = subprocess.run(["nslookup", subdomain], capture_output=True, text=True)
            output = result.stdout

            lines = output.split("\n")
            addresses = []

            for line in lines:
                if "Address" in line and not line.startswith("Server"):
                    addresses.append(line.split(":")[-1].strip())

            if len(addresses) > 1:
                return addresses[1]
            elif addresses:
                return addresses[0]
            else:
                return "No IP address found"

        except Exception as e:
            return f"Error: {str(e)}"
```

```python
class SubdomainResolver:
    """Handles subdomain extraction and IP resolution."""
    def __init__(self, ip_resolver: IPResolverStrategy):
        self.ip_resolver = ip_resolver

    def extract_common_names(self, json_file: str):
        """Extracts common subdomain names from a JSON file."""
        with open(json_file, "r") as file:
            data = json.load(file)

        common_names = {entry["name_value"] for entry in data if not entry["name_value"].startswith
        return sorted(common_names)

    def resolve_subdomains(self, subdomains):
        """Resolves IP addresses for a list of subdomains."""
        for subdomain in subdomains:
            print(f"{subdomain} : {self.ip_resolver.get_ip_address(subdomain)}")

    def process_json_subdomains(self, json_file: str):
        """Processes subdomains from a JSON file and resolves IPs."""
        subdomains = self.extract_common_names(json_file)
        self.resolve_subdomains(subdomains)

    def process_excel_subdomains(self, excel_file: str):
        """Processes subdomains from an Excel file and resolves IPs."""
        df = pd.read_excel(excel_file)
        self.resolve_subdomains(df["Host"])
```

part c

-> attacker will be aware of the network topology
-> knowing the exact domain name will increase phishing attacks by creating fake pages
-> they will try to find the most vulnerable site to attack as now they know what services are hosted there
-> ip spoofing as now they know the internal IP;s they might try to target service that just accepts those internal IPs by spoofing them
-> its not necessary that all the services are well guarded, so it may try to attack the ones with weak authentication by using default passwords or SQL injection.