Writeup by: **Danilo Nascimento | 1nv1ct4**
https://github.com/ndanilo8/PositiveHackCamp2024

Description:

Domain of our organization is `cyber-ed.ru`. Your goal is to find as many subdomains associated with it as possible.

Some subdomains in the `DNS` server `TXT record` contain various parameters.

One subdomain (its name is logically related to the task) will have a `TXT record` with a flag in the format: `FLAG=flag_value`, where `flag_value` is 32 alphanumerical symbols.

You have to submit flag in format `flag{flag_value}` (copy all alphanumerical symbols from DNS record and paste them inside curly braces).

Attacking

Method 1

First look at https://crt.sh/?q=cyber-ed.ru for passive scan of subdomains of the target
And to export we can do:

```
curl -s https://crt.sh/\?q\=cyber-ed.ru\&output\=json | jq .
```

As well as checking with `amass`

```
amass enum -d cyber-ed.ru
```

- as well as `subfinder`

```
subfinder -d cyber-ed.ru
```

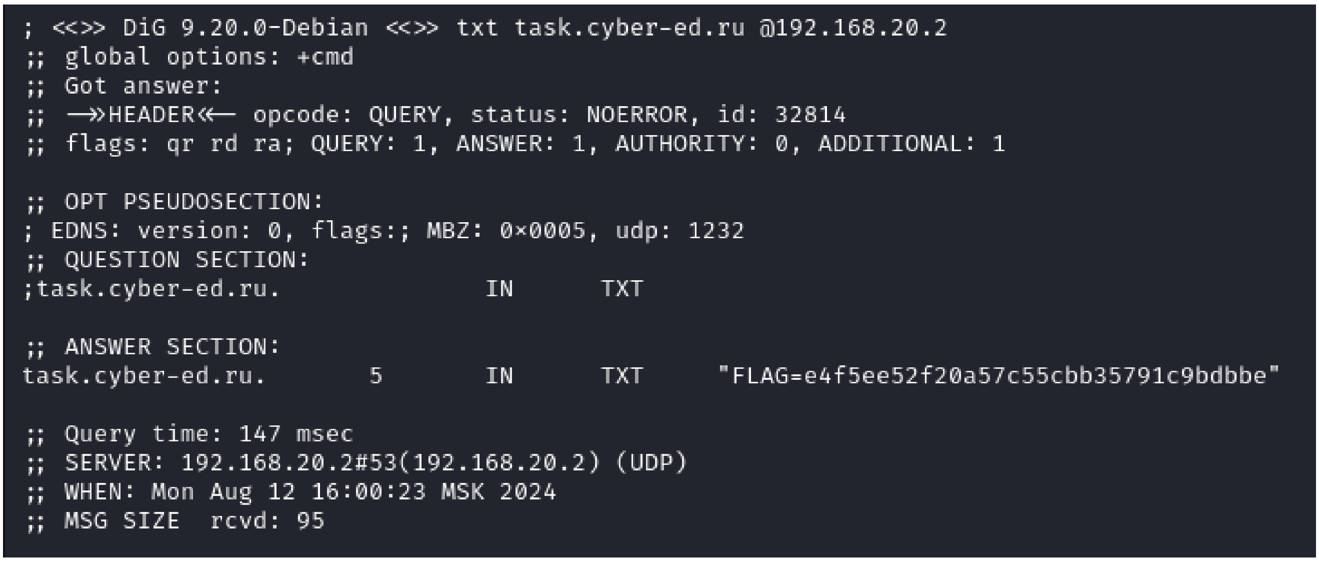
then combining everything into a list by using a `sort -u` for only unique options, we get the following list and we copy it to a file `subdomains.txt`

```
bitpasrep.cyber-ed.ru
bitwarden.cyber-ed.ru
```

```
blue.cyber-ed.ru
briefs.cyber-ed.ru
bugbounty-intensive.cyber-ed.ru
ceeperpas.cyber-ed.ru
connect.cyber-ed.ru
cyberclass.cyber-ed.ru
cyber-ed.ru
event.cyber-ed.ru
gitlab.cyber-ed.ru
infctf.cyber-ed.ru
infra.cyber-ed.ru
labs.cyber-ed.ru
labs.dev.cyber-ed.ru
learn.cyber-ed.ru
lms.cyber-ed.ru
lmstest.cyber-ed.ru
matterm.cyber-ed.ru
modlms.cyber-ed.ru
monitoring.cyber-ed.ru
newlms.cyber-ed.ru
old.cyber-ed.ru
one-task.cyber-ed.ru
one-task-of-the-month.cyber-ed.ru
qr-admin.cyber-ed.ru
qr-api.cyber-ed.ru
qr-front.cyber-ed.ru
sec-infra.cyber-ed.ru
step.cyber-ed.ru
task.cyber-ed.ru
test.cyber-ed.ru
wiki.cyber-ed.ru
www.cyber-ed.ru
```

- for the flag:

```
for sub in $(cat subdomains.txt);do dig txt $sub.cyber-ed.ru | tee -a
dig_TXT.txt;done
```



```
; <<>> DiG 9.20.0-Debian <<>> txt task.cyber-ed.ru @192.168.20.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32814
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;task.cyber-ed.ru.              IN      TXT

;; ANSWER SECTION:
task.cyber-ed.ru.       5       IN      TXT     "FLAG=e4f5ee52f20a57c55cbb35791c9bdbbe"

;; Query time: 147 msec
;; SERVER: 192.168.20.2#53(192.168.20.2) (UDP)
;; WHEN: Mon Aug 12 16:00:23 MSK 2024
;; MSG SIZE  rcvd: 95
```

Method 2

A script I made that automates the process from method 1

```
#!/bin/bash

# Ensure the script is executed with two arguments
if [ "$#" -ne 2 ]; then
    echo "Usage: $0 <domain> <record_type>"
    exit 1
fi

# Assign arguments to variables
DOMAIN=$1
RECORD_TYPE=$2

# Fetch subdomains from various sources and store them in an array
subdomains=()

# crt.sh
crt_subdomains=$(curl -s "https://crt.sh/?q=${DOMAIN}&output=json" | jq -r
'.[].name_value' | sed 's/\*\.//g' | sort -u)
subdomains+=($crt_subdomains)

# Amass
amass_subdomains=$(amass enum -d $DOMAIN)
subdomains+=($amass_subdomains)

# Subfinder
subfinder_subdomains=$(subfinder -d $DOMAIN)
subdomains+=($subfinder_subdomains)

# Remove duplicate subdomains with sort
```

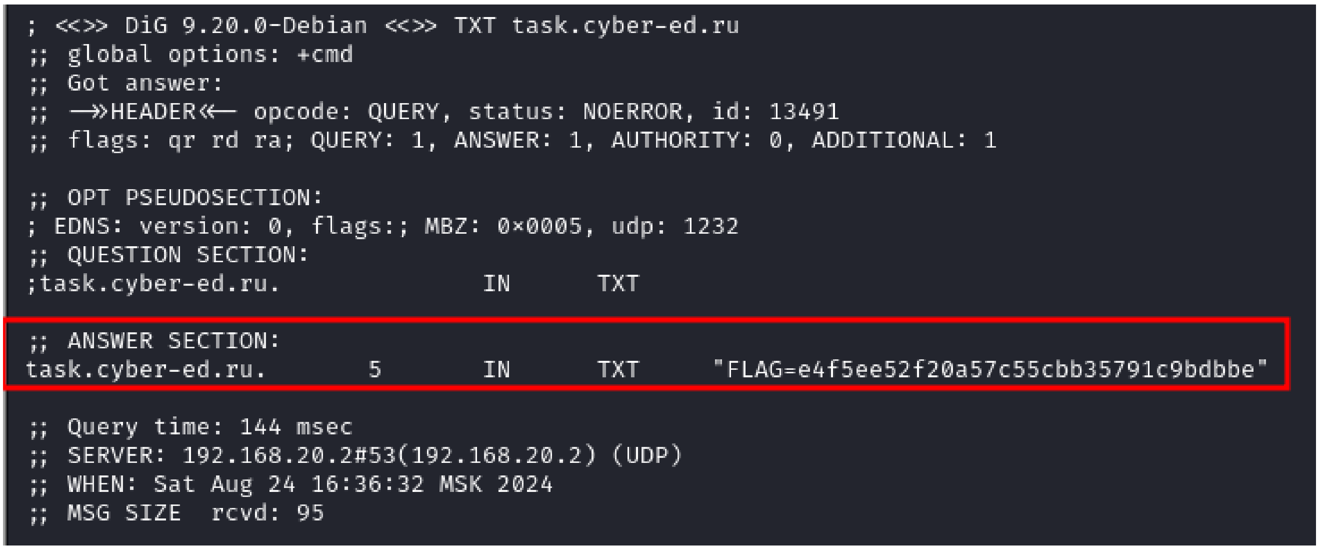
```
subdomains=($(echo "${subdomains[@]}" | tr ' ' '\n' | sort -u))

# Cut the subdomain part and perform DNS queries
# actually no need to cut the subdomains from the domain. this was because I wanted to extract the subdomain names to a list
for sub in "${subdomains[@]}"; do
    sub_cut=$(echo "$sub" | cut -d'.' -f1)
    dig $RECORD_TYPE $sub_cut.$DOMAIN | tee -a dig_results.txt
done
```

and you would run it as:

```
chmod +x searchSubdomains.sh
./searchSubdomains.sh cyber-ed.ru TXT
```

and we have:



```
; <<>> DiG 9.20.0-Debian <<>> TXT task.cyber-ed.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13491
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
;; QUESTION SECTION:
;task.cyber-ed.ru.             IN      TXT

;; ANSWER SECTION:
task.cyber-ed.ru.      5       IN      TXT     "FLAG=e4f5ee52f20a57c55cbb35791c9bdbbe"

;; Query time: 144 msec
;; SERVER: 192.168.20.2#53(192.168.20.2) (UDP)
;; WHEN: Sat Aug 24 16:36:32 MSK 2024
;; MSG SIZE  rcvd: 95
```