CN Industry Problem

TOPIC:
TCP PORT SCANNER WITH WEB SERVER FINGERPRINTING

TEAM:
UJWAL KV - PES1UG20CS475. ROLL NO-29
VARUN SATHEESH - PES1UG20CS489. ROLL NO-19
THUSHAR M - PES1UG20CS471. ROLL NO-9
VANSHIKA GOEL - PES1UG20CS484. ROLL NO-40

SECTION: H
DATE: 21-04-22

Code:

```
# Ujwal kv - pes1ug20cs475. Roll no-29
# Varun Satheesh - pes1ug20cs489. Roll no-19
# Thushar m - pes1ug20cs471. Roll no-9
# Vanshika goel - pes1ug20cs481. Roll no-40

import requests
import logging
from tabnanny import verbose
from telnetlib import IP
from urllib import response;
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
import sys
from scapy.all import *
import socket
#Fingerprinting Web Server
if len(sys.argv) != 4:
    print("usage: %s target startport endport   "%(sys.argv[0]))
    sys.exit(0)
target = str(sys.argv[1])
startport = int(sys.argv[2])
endport  = int(sys.argv[3])
print('Scanning'+target+' for open TCP ports \n')
url = socket.gethostbyname(target)

req = requests.get('https://'+target)
headers = ['Server', 'Date', 'Via', 'X-Powered-By', 'X-Country-
Code']
for header in headers:
```

```
    try:
        result = req.headers[header]
        print ('%s: %s' % (header, result))
    except Exception:
        print ('%s: Not found' %  header)

#Port Scanning
if startport == endport:
     endport +=1

for x in range(startport,endport):
    packet = IP(dst=url)/TCP(dport=x,flags='S')
    response = sr1(packet,timeout=1,verbose=0)
    if response and  response.haslayer(TCP) and


response.getlayer(TCP).flags==0x12:
        print('Port'+str(x)+'is OPEN!')
    else:
        print('Port'+str(x)+'is CLOSED!')

print("SCAN IS COMPLETE\n")
```

Validation of ports using NMAP

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-21 14:29 UTC
Initiating Ping Scan at 14:29
Scanning 142.250.195.238 [2 ports]
Completed Ping Scan at 14:29, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:29
Completed Parallel DNS resolution of 1 host. at 14:29, 0.40s elapsed
Initiating Connect Scan at 14:29
Scanning maa03s43-in-f14.1e100.net (142.250.195.238) [1000 ports]
Discovered open port 443/tcp on 142.250.195.238
Discovered open port 80/tcp on 142.250.195.238
Completed Connect Scan at 14:29, 4.87s elapsed (1000 total ports)
Nmap scan report for maa03s43-in-f14.1e100.net (142.250.195.238)
Host is up (0.014s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
139/tcp  closed netbios-ssn
443/tcp  open   https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
varun@varun:~$
```

Output

```
ujwal_nischal@Ujwal-Nischals-MacBook-Air CN INDUSTRY % python3 sup.py www.youtube.com  80 80
Scanningwww.youtube.com for open TCP ports

Server: ESF
Date: Thu, 21 Apr 2022 09:08:26 GMT
Via: Not found
X-Powered-By: Not found
X-Country-Code: Not found
Port80is OPEN!
SCAN IS COMPLETE

ujwal_nischal@Ujwal-Nischals-MacBook-Air CN INDUSTRY % python3 sup.py www.youtube.com  139 139
Scanningwww.youtube.com for open TCP ports

Server: ESF
Date: Thu, 21 Apr 2022 09:08:46 GMT
Via: Not found
X-Powered-By: Not found
X-Country-Code: Not found
Port139is CLOSED!
SCAN IS COMPLETE

ujwal_nischal@Ujwal-Nischals-MacBook-Air CN INDUSTRY % python3 sup.py www.youtube.com  443 443
Scanningwww.youtube.com for open TCP ports

Server: ESF
Date: Thu, 21 Apr 2022 09:08:58 GMT
Via: Not found
X-Powered-By: Not found
X-Country-Code: Not found
Port443is OPEN!
SCAN IS COMPLETE

ujwal_nischal@Ujwal-Nischals-MacBook-Air CN INDUSTRY % python3 sup.py www.youtube.com  443 446
Scanningwww.youtube.com for open TCP ports

Server: ESF
Date: Thu, 21 Apr 2022 09:09:06 GMT
Via: Not found
X-Powered-By: Not found
X-Country-Code: Not found
Port443is OPEN!
Port444is CLOSED!
Port445is CLOSED!
SCAN IS COMPLETE

ujwal_nischal@Ujwal-Nischals-MacBook-Air CN INDUSTRY % python3 sup.py www.youtube.com  3389 3389
Scanningwww.youtube.com for open TCP ports

Server: ESF
Date: Thu, 21 Apr 2022 09:09:23 GMT
Via: Not found
X-Powered-By: Not found
X-Country-Code: Not found
Port3389is CLOSED!
SCAN IS COMPLETE
```