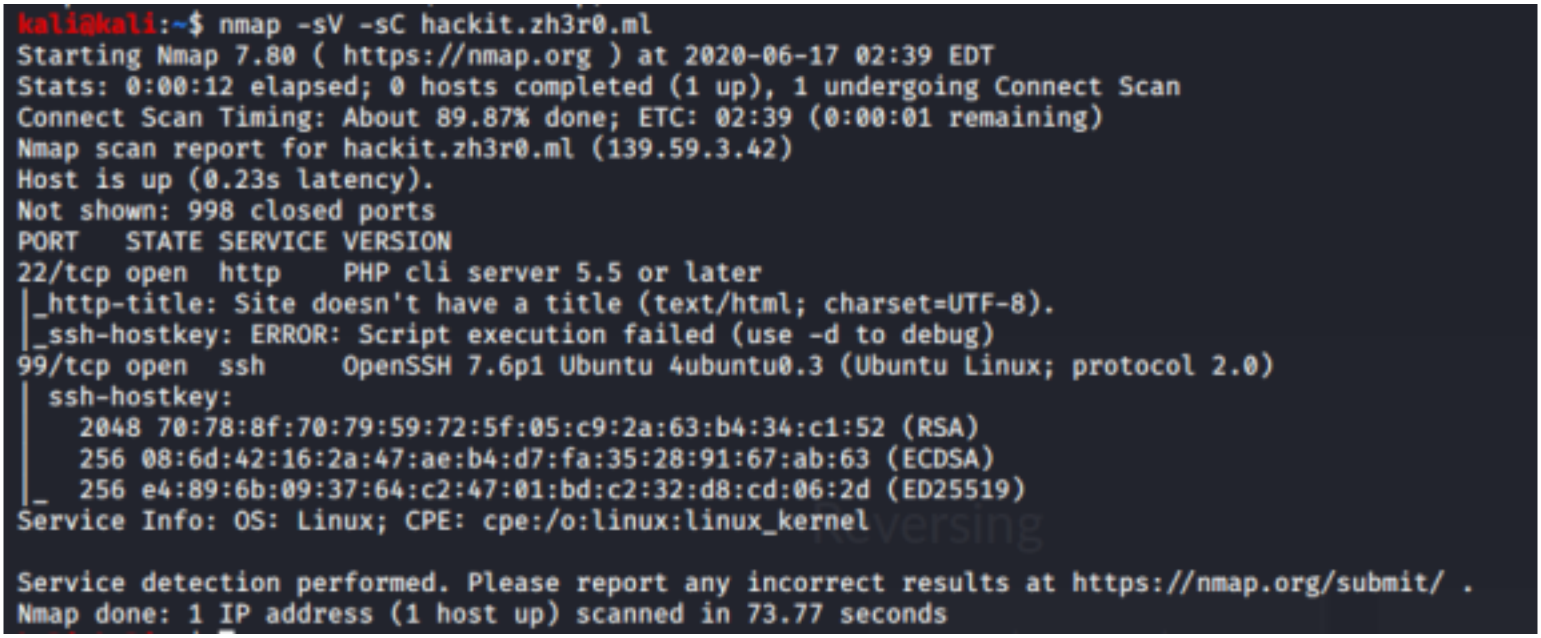
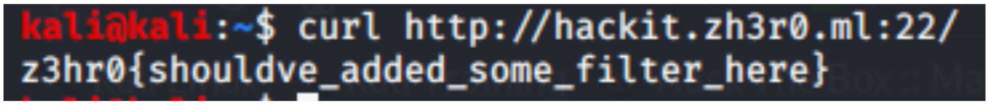
Flag 5



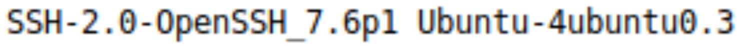
```
kali@kali:~$ nmap -sV -sC hackit.zh3r0.ml
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-17 02:39 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 89.87% done; ETC: 02:39 (0:00:01 remaining)
Nmap scan report for hackit.zh3r0.ml (139.59.3.42)
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  http    PHP cli server 5.5 or later
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
99/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 70:78:8f:70:79:59:72:5f:05:c9:2a:63:b4:34:c1:52 (RSA)
|   256 08:6d:42:16:2a:47:ae:b4:d7:fa:35:28:91:67:ab:63 (ECDSA)
|_  256 e4:89:6b:09:37:64:c2:47:01:bd:c2:32:d8:cd:06:2d (ED25519)
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 73.77 seconds
```



```
kali@kali:~$ curl http://hackit.zh3r0.ml:22/
z3hr0{shouldve_added_some_filter_here}
```

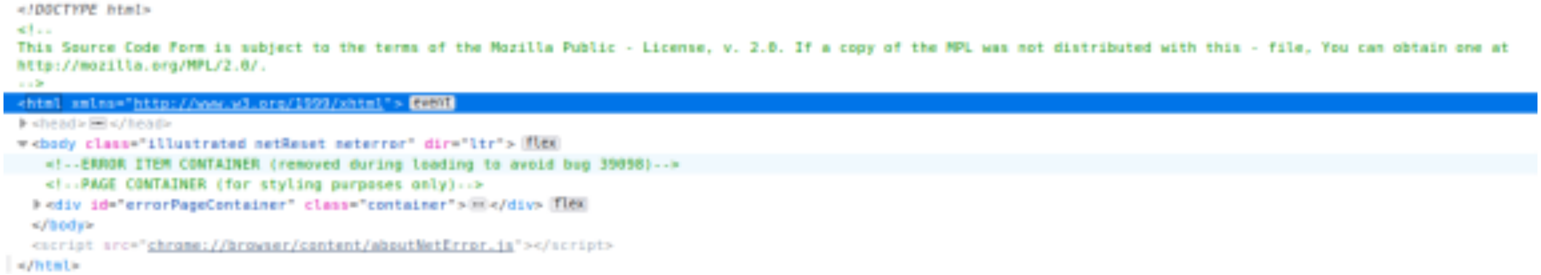
Flag 1

request to port 99 and we see



```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

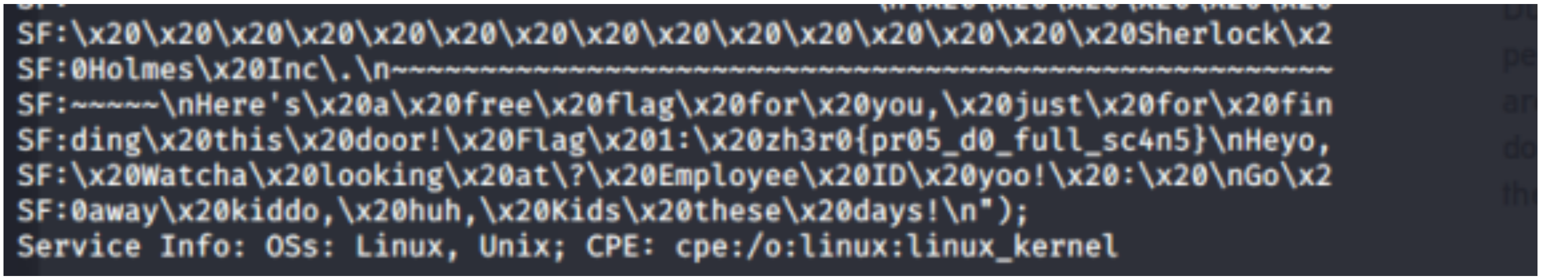
modified source and see connection reset +



```
<!DOCTYPE html>
<!--
This Source Code Form is subject to the terms of the Mozilla Public - License, v. 2.0. If a copy of the MPL was not distributed with this - file, You can obtain one at
http://mozilla.org/MPL/2.0/.
-->
<html xmlns="http://www.w3.org/1999/xhtml"> event
 ▸ <head> ⋯ </head>
 ▾ <body class="illustrated netReset neterror" dir="ltr"> flex
    <!--ERROR ITEM CONTAINER (removed during loading to avoid bug 39098)-->
    <!--PAGE CONTAINER (for styling purposes only)-->
  ▸ <div id="errorPageContainer" class="container"> ⋯ </div> flex
  </body>
  <script src="chrome://browser/content/aboutNetError.js"></script>
</html>
```

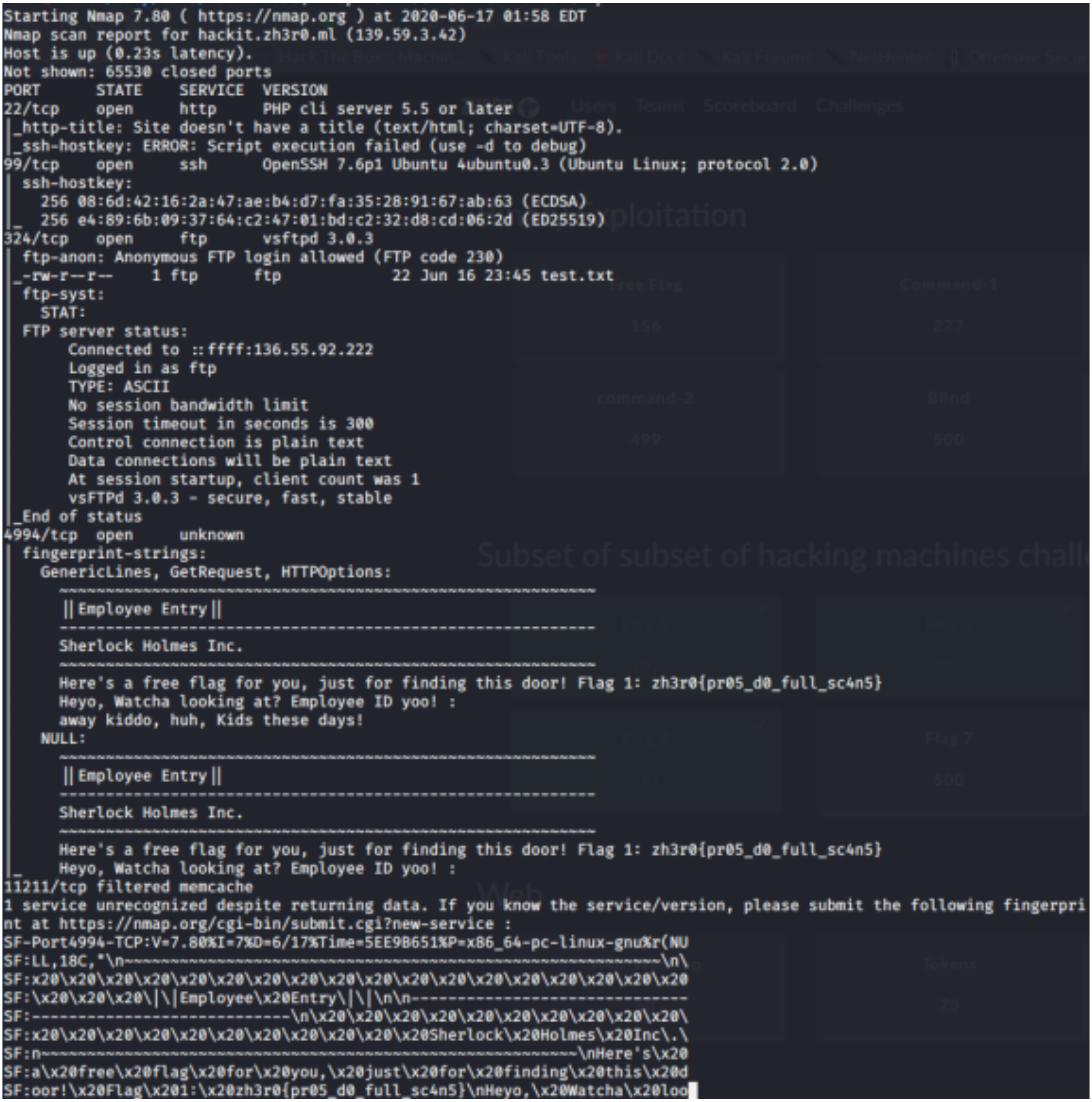
so I enumerate more

lol wtf is this flag for. probably 1? ye
zh3r0{pr05_d0_full_sc4n5}



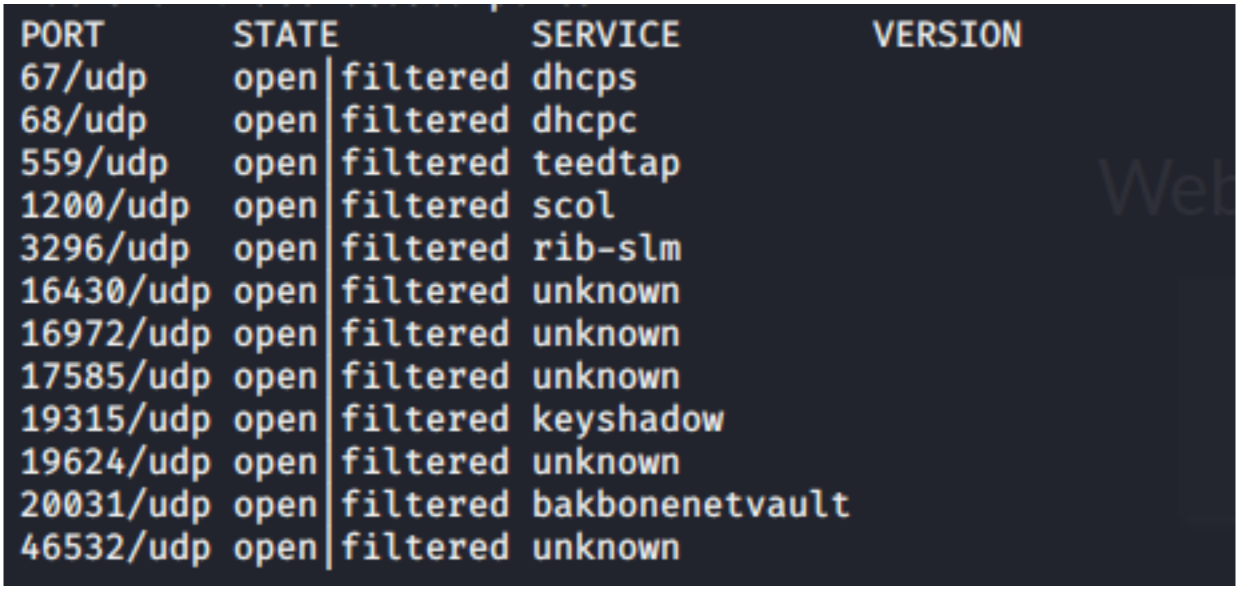
```
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Sherlock\x2
SF:0Holmes\x20Inc\.\n~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SF:~~~~~\nHere's\x20a\x20free\x20flag\x20for\x20you,\x20just\x20for\x20fin
SF:ding\x20this\x20door!\x20Flag\x201:\x20zh3r0{pr05_d0_full_sc4n5}\nHeyo,
SF:\x20Watcha\x20looking\x20at\?\x20Employee\x20ID\x20yoo!\x20:\x20\nGo\x2
SF:0away\x20kiddo,\x20huh,\x20Kids\x20these\x20days!\n");
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel
```

FULL SCAN OUTPUT



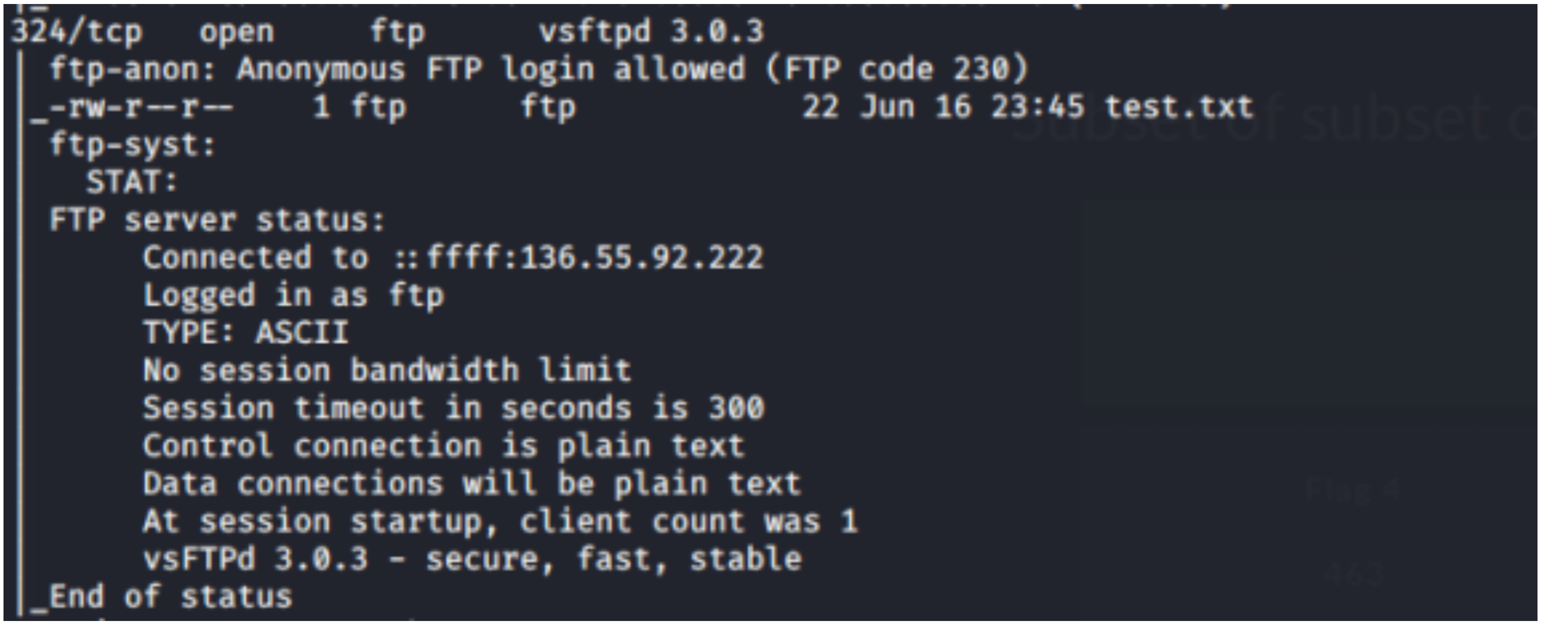
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-17 01:58 EDT
Nmap scan report for hackit.zh3r0.ml (139.59.3.42)
Host is up (0.23s latency).
Not shown: 65530 closed ports
PORT      STATE    SERVICE  VERSION
22/tcp    open     http     PHP cli server 5.5 or later
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
99/tcp    open     ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 08:6d:42:16:2a:47:ae:b4:d7:fa:35:28:91:67:ab:63 (ECDSA)
|_  256 e4:89:6b:09:37:64:c2:47:01:bd:c2:32:d8:cd:06:2d (ED25519)
324/tcp   open     ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:136.55.92.222
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
4994/tcp  open     unknown
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|      ||Employee Entry||
|     ----------------------------------------------------------
|     Sherlock Holmes Inc.
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     Here's a free flag for you, just for finding this door! Flag 1: zh3r0{pr05_d0_full_sc4n5}
|     Heyo, Watcha looking at? Employee ID yoo! :
|     away kiddo, huh, Kids these days!
|   NULL:
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|      ||Employee Entry||
|     ----------------------------------------------------------
|     Sherlock Holmes Inc.
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     Here's a free flag for you, just for finding this door! Flag 1: zh3r0{pr05_d0_full_sc4n5}
|_    Heyo, Watcha looking at? Employee ID yoo! :
11211/tcp filtered memcache
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpri
nt at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4994-TCP:V=7.80%I=7%D=6/17%Time=5EE9B651%P=x86_64-pc-linux-gnu%r(NU
SF:LL,18C,"\n~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\|\|Employee\x20Entry\|\|\n\n-----------------------------
SF:---------------------------\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Sherlock\x20Holmes\x20Inc\.\
SF:n~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~\nHere's\x20
SF:a\x20free\x20flag\x20for\x20you,\x20just\x20for\x20finding\x20this\x20d
SF:oor!\x20Flag\x201:\x20zh3r0{pr05_d0_full_sc4n5}\nHeyo,\x20Watcha\x20loo
```

UDP SCAN OUTPUT



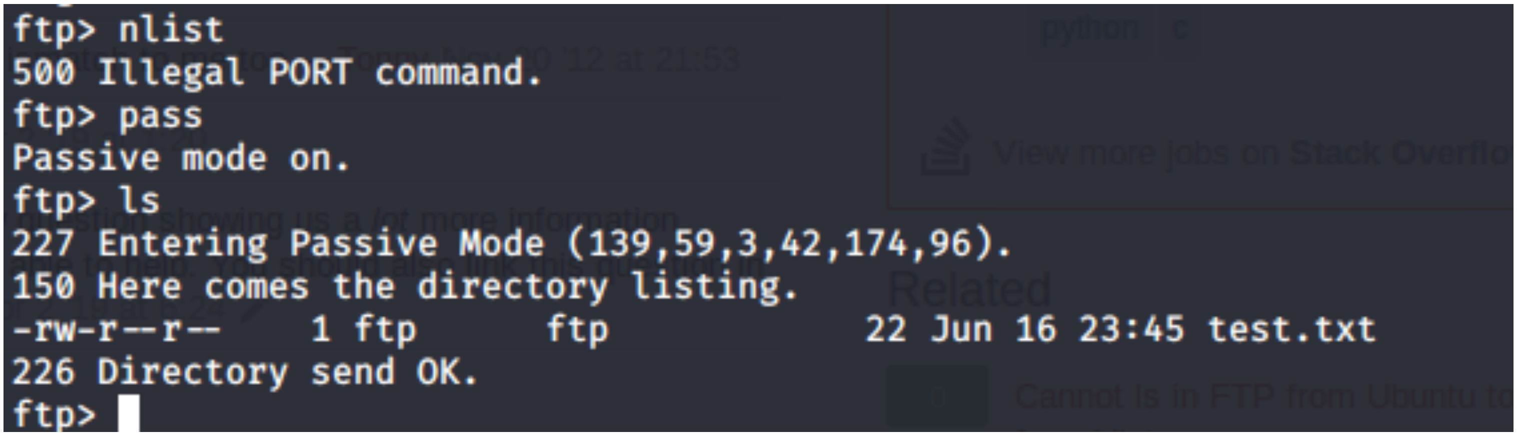
```
PORT      STATE         SERVICE         VERSION
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
559/udp   open|filtered teedtap
1200/udp  open|filtered scol
3296/udp  open|filtered rib-slm
16430/udp open|filtered unknown
16972/udp open|filtered unknown
17585/udp open|filtered unknown
19315/udp open|filtered keyshadow
19624/udp open|filtered unknown
20031/udp open|filtered bakbonenetvault
46532/udp open|filtered unknown
```

ftp port open w/anon login



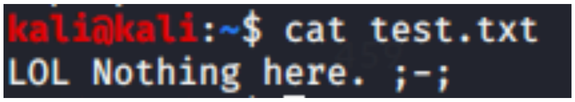
```
324/tcp   open     ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:136.55.92.222
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

commands not working so google search shows to use passive mode



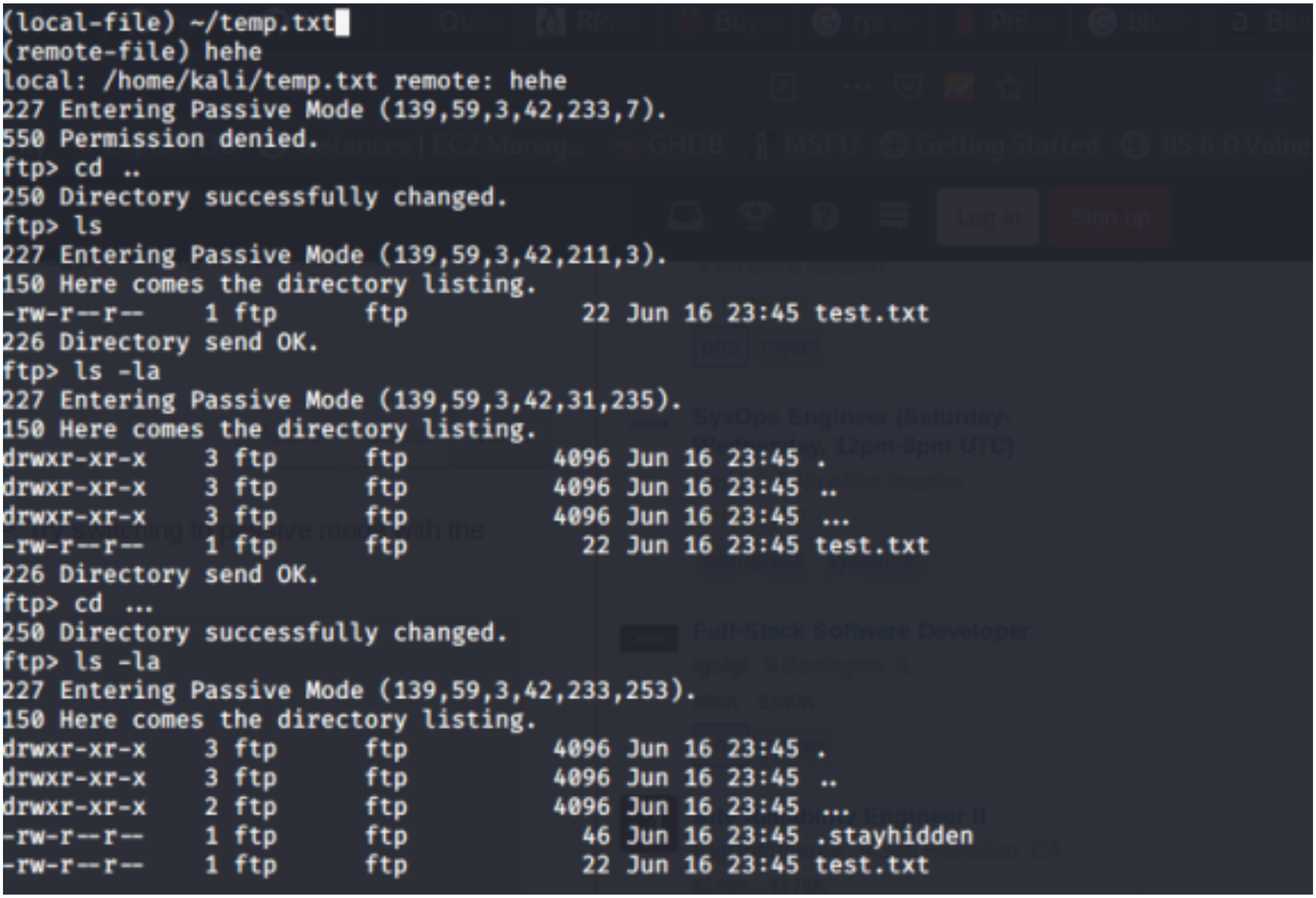
```
ftp> nlist
500 Illegal PORT command.
ftp> pass
Passive mode on.
ftp> ls
227 Entering Passive Mode (139,59,3,42,174,96).
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
226 Directory send OK.
ftp> 
```

fml

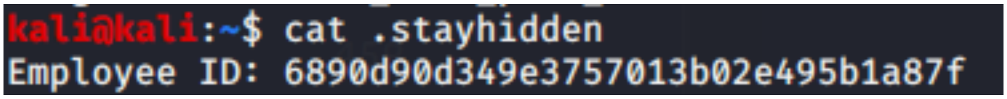


```
kali@kali:~$ cat test.txt
LOL Nothing here. ;-;
```

put command fails

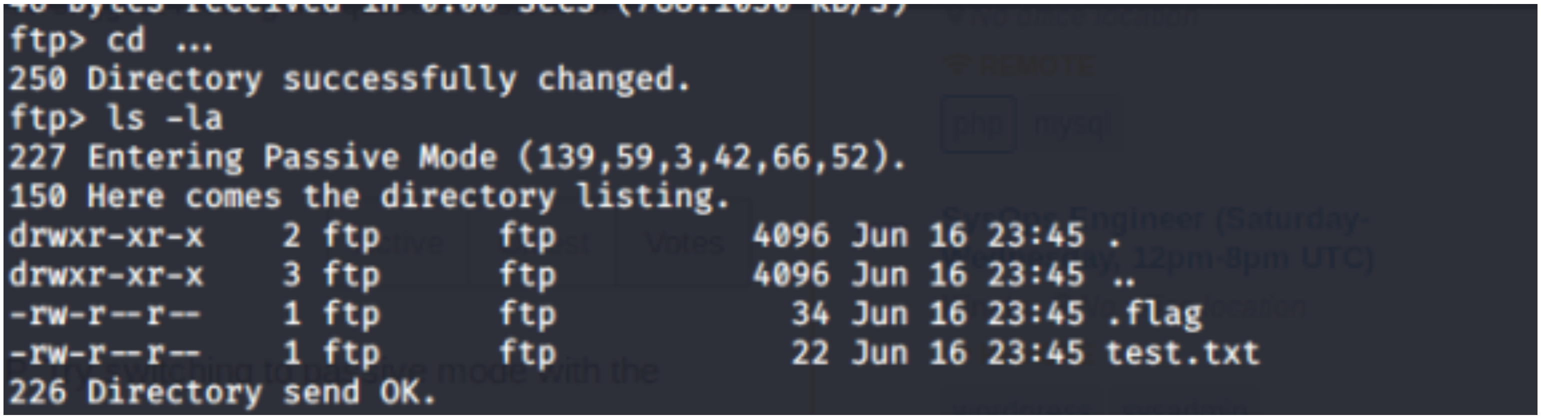


```
(local-file) ~/temp.txt
(remote-file) hehe
local: /home/kali/temp.txt remote: hehe
227 Entering Passive Mode (139,59,3,42,233,7).
550 Permission denied.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (139,59,3,42,211,3).
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
226 Directory send OK.
ftp> ls -la
227 Entering Passive Mode (139,59,3,42,31,235).
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 ..
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 ...
-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
227 Entering Passive Mode (139,59,3,42,233,253).
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 ..
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 23:45 ...
-rw-r--r--    1 ftp      ftp            46 Jun 16 23:45 .stayhidden
-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
```



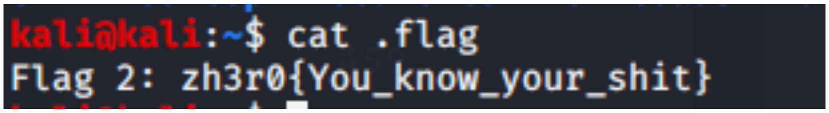
```
kali@kali:~$ cat .stayhidden
Employee ID: 6890d90d349e3757013b02e495b1a87f
```

I just tried this again in case...



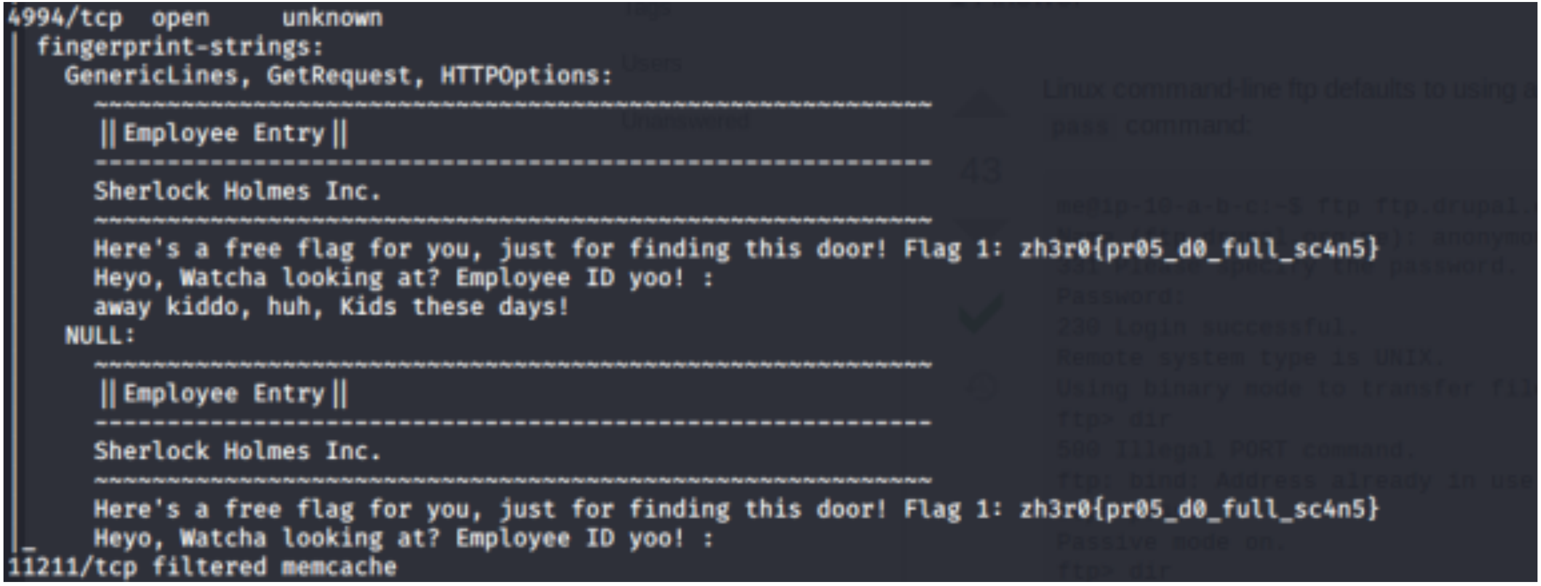
```
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
227 Entering Passive Mode (139,59,3,42,66,52).
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 23:45 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 23:45 ..
-rw-r--r--    1 ftp      ftp            34 Jun 16 23:45 .flag
-rw-r--r--    1 ftp      ftp            22 Jun 16 23:45 test.txt
226 Directory send OK.
```

we have a .flag?



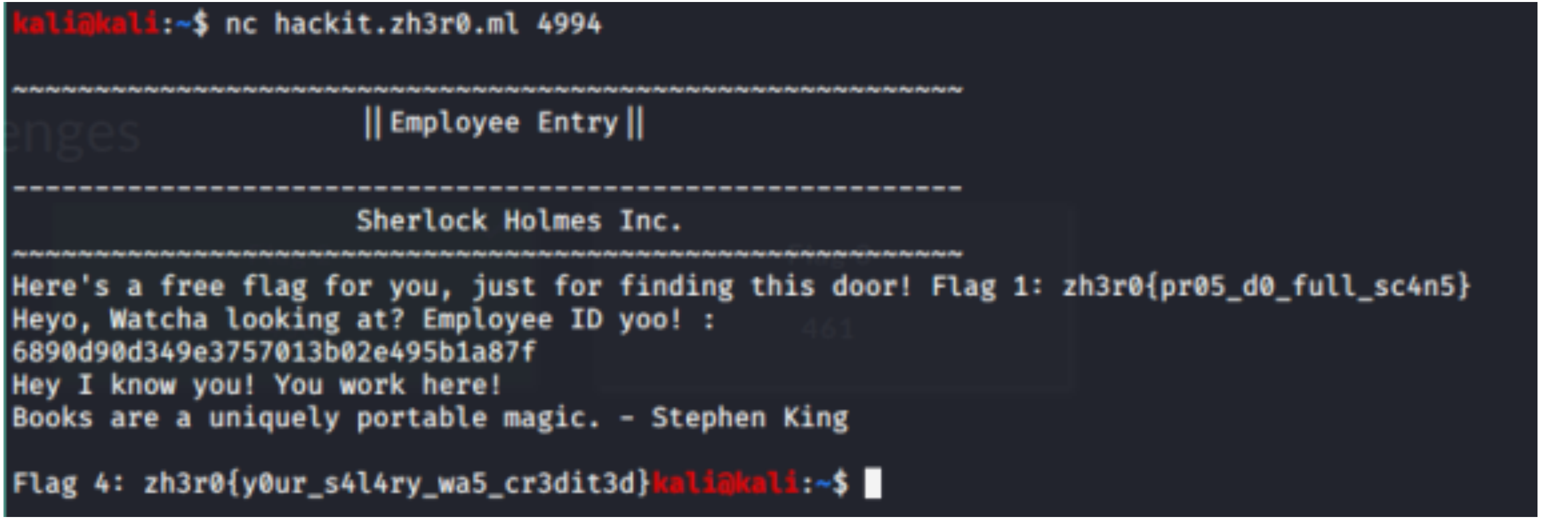
```
kali@kali:~$ cat .flag
Flag 2: zh3r0{You_know_your_shit}
```

port 4994 has this



```
4994/tcp  open     unknown
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     ||Employee Entry||
|     --------------------------------------------------------------
|     Sherlock Holmes Inc.
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     Here's a free flag for you, just for finding this door! Flag 1: zh3r0{pr05_d0_full_sc4n5}
|     Heyo, Watcha looking at? Employee ID yoo! :
|     away kiddo, huh, Kids these days!
|   NULL:
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     ||Employee Entry||
|     --------------------------------------------------------------
|     Sherlock Holmes Inc.
|     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
|     Here's a free flag for you, just for finding this door! Flag 1: zh3r0{pr05_d0_full_sc4n5}
|_    Heyo, Watcha looking at? Employee ID yoo! :
11211/tcp filtered memcache
```

flag 4



```
kali@kali:~$ nc hackit.zh3r0.ml 4994

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                        ||Employee Entry||

--------------------------------------------------------------
                        Sherlock Holmes Inc.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Here's a free flag for you, just for finding this door! Flag 1: zh3r0{pr05_d0_full_sc4n5}
Heyo, Watcha looking at? Employee ID yoo! :
6890d90d349e3757013b02e495b1a87f
Hey I know you! You work here!
Books are a uniquely portable magic. - Stephen King

Flag 4: zh3r0{y0ur_s4l4ry_wa5_cr3dit3d}kali@kali:~$ 
```

Flag 3 and 7 missing,... two more services open so we probably need to get something from memcache (possibly creds) and login to the ssh server with them. who knows... idk why port 22 shows up as php and 99 is ssh. who are these goons??