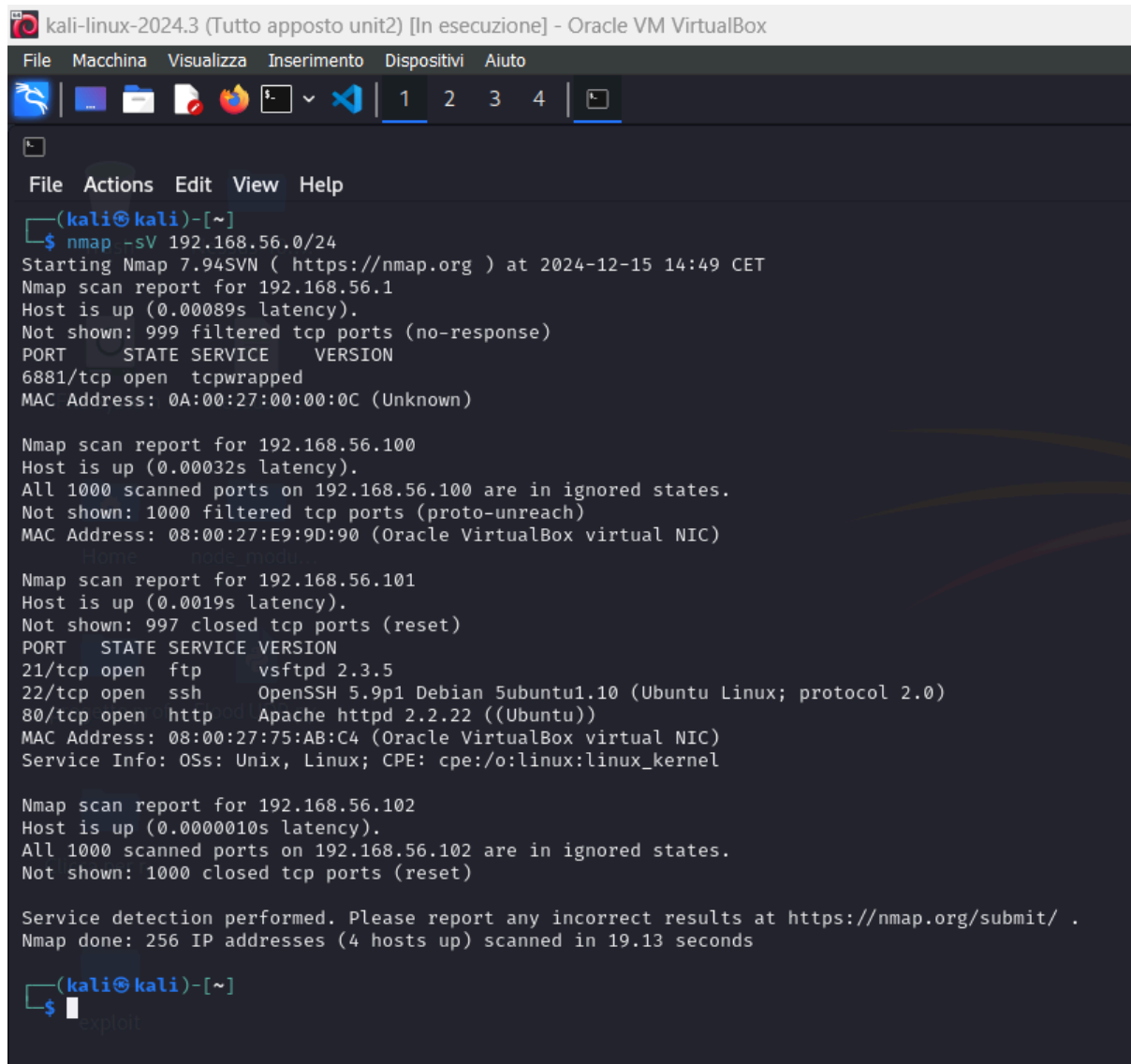


Per prima cosa ho eseguito uno scan nmap col parametro -sV su tutto il range di ip interessato quindi 192.168.56.0/24



```
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)

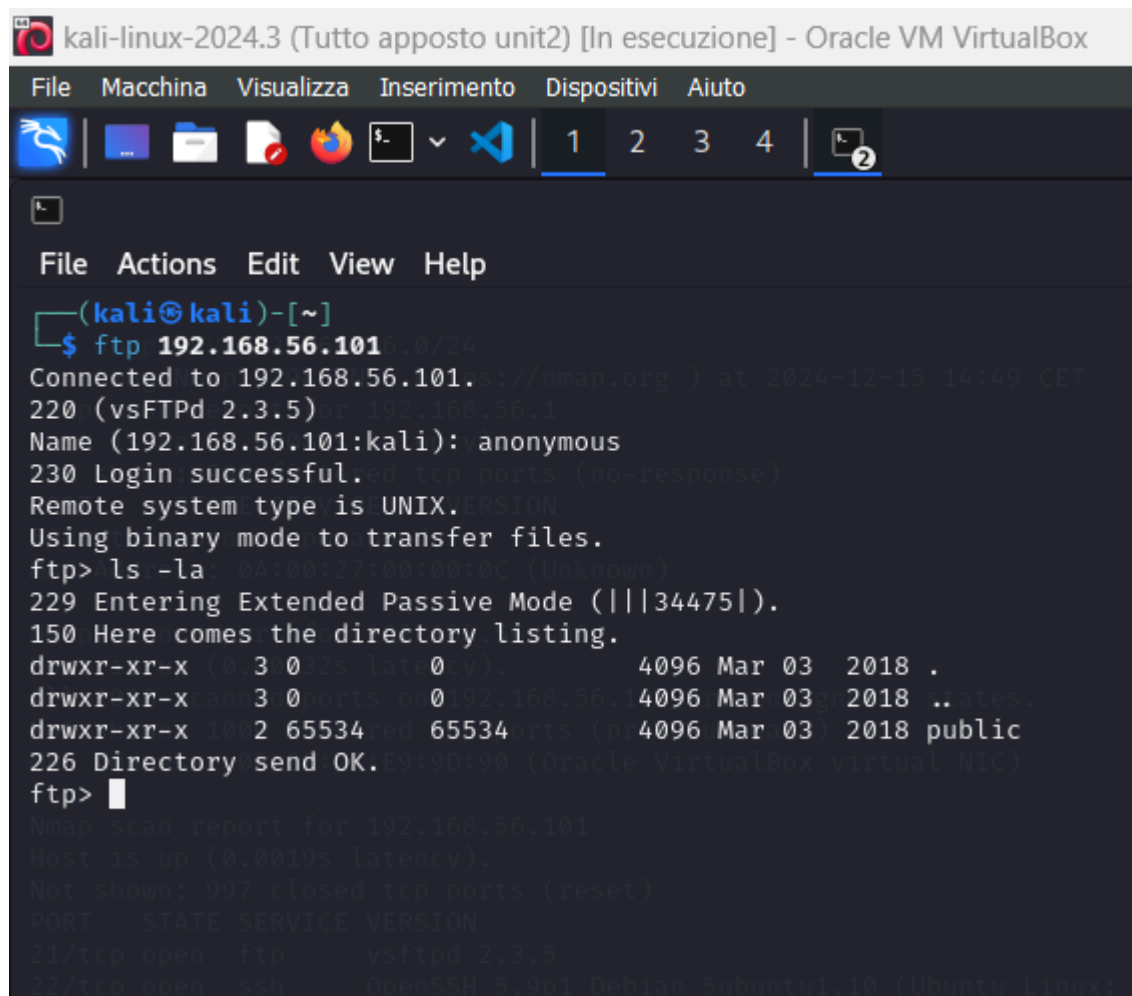
Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.5
22/tcp    open  ssh          OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         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)-[~]
$
```

Sgamati i servizi aperti ho scelto di esplorarli tutti son partito dal primo ftp



```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4 2
File Actions Edit View Help
(kali@kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101. (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 65534 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 un ls -la ho visto il contenuto e c'era una cartella pubblica, ci sono entrato dentro ed ho rifatto un ls trovando un file di testo, che ho deciso di provare a scaricare con un GET che ha avuto successo!

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
File  Actions  Edit  View  Help

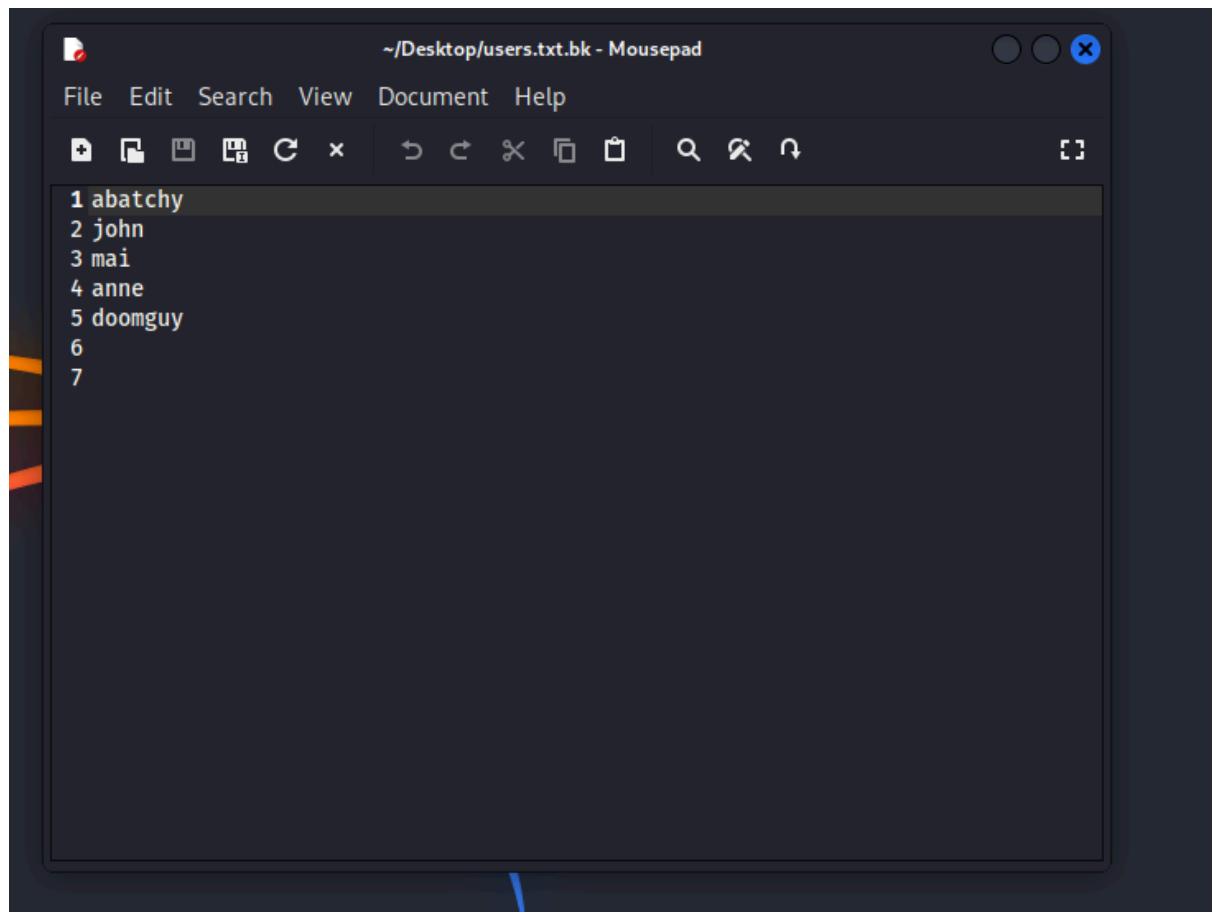
(kali@kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101. (vsftpd.org) at 2024-12-15 14:49 CET
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> 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)

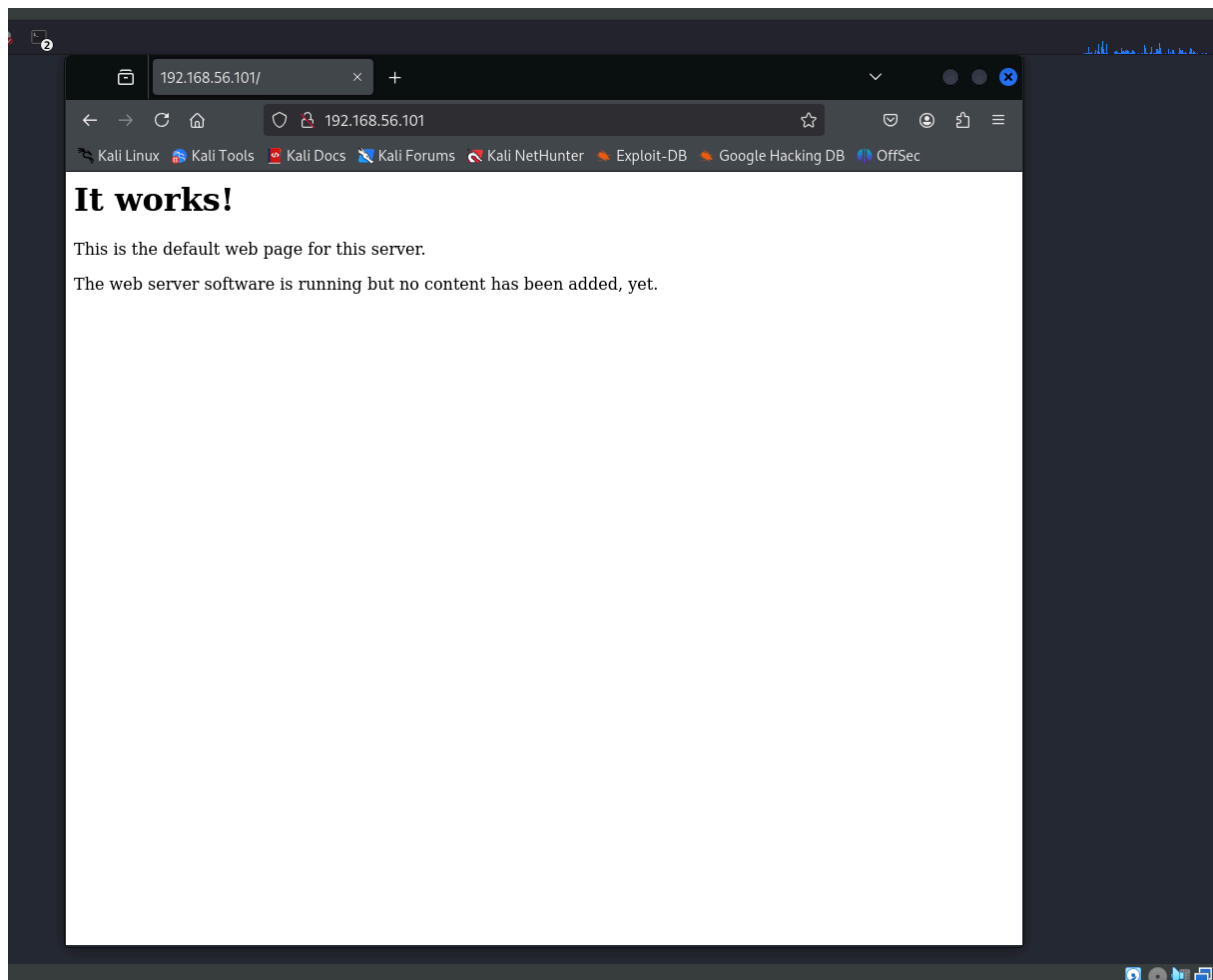
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 19.13 seconds

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

ho aperto il file e mi sono ritrovato degli username da tenermi buoni.



Dopo ho deciso di visitare il servizio http, semplicemente ho inserito l'ip bersaglio nel browser



Sono andato avanti facendo una scansione web con nikto che mi ha tirato fuori dei risultati da esplorare

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

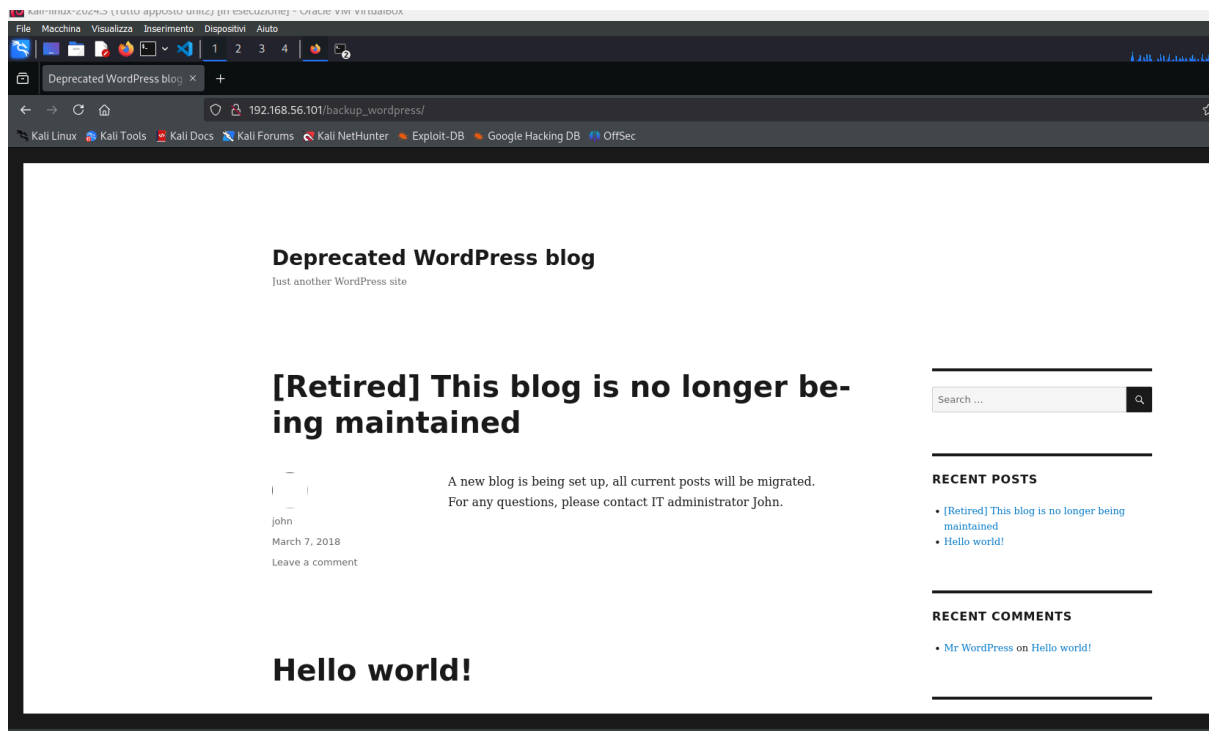
+ Target IP: 192.168.56.101
+ Target Hostname: 192.168.56.101
+ Target Port: 80
+ Start Time: 2024-12-15 15:23:43 (GMT1)

+ Server: 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)~$
```

Ha catturato la mia attenzione /backup wordpress



dopodichè ho testato tutti gli username sulla pagina di login del wordpress finchè non ho beccato quello corretto

