PLOUZENNEC Eliaz

TP : Port 80, wordpress, wpscan

02/02/24

Contenu

Introduction :

Nous avons une adresse ip d'une machine : **192.168.0.31**

Objectif :

Récupérer un login et un mot de passe

Etape 1 : scan des port vulnerables

```
┌──(root㉿plouzennec)-[~]
└─# nmap -A -sV --script vuln 192.168.0.31
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-02 11:17 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

On tape cette commande pour trouver les ports ouvert sur la machine.

```
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.41:
|       PACKETSTORM:176334      7.5     https://vulners.com/packetstorm/PACKETSTORM:176334      *EXPLOIT*
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       OSV:BIT-APACHE-2023-25690       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2023-25690
|       OSV:BIT-APACHE-2022-31813       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2022-31813
|       OSV:BIT-APACHE-2022-23943       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2022-23943
|       OSV:BIT-APACHE-2022-22720       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2022-22720
|       OSV:BIT-APACHE-2021-44790       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2021-44790
|       OSV:BIT-APACHE-2021-42013       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2021-42013
|       OSV:BIT-APACHE-2021-41773       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2021-41773
|       OSV:BIT-APACHE-2021-39275       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2021-39275
|       OSV:BIT-APACHE-2021-26691       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2021-26691
|       OSV:BIT-APACHE-2020-11984       7.5     https://vulners.com/osv/OSV:BIT-APACHE-2020-11984
|       MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-       7.5     https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-  *
EXPLOIT*
|       MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-       7.5     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-  *
EXPLOIT*
|       F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5    7.5     https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5  *EXPLOIT*
|       EDB-ID:51193    7.5     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       EDB-ID:50512    7.5     https://vulners.com/exploitdb/EDB-ID:50512      *EXPLOIT*
|       EDB-ID:50406    7.5     https://vulners.com/exploitdb/EDB-ID:50406      *EXPLOIT*
|       E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6    7.5     https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6  *EXPLOIT*
|       CVE-2023-25690  7.5     https://vulners.com/cve/CVE-2023-25690
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
```

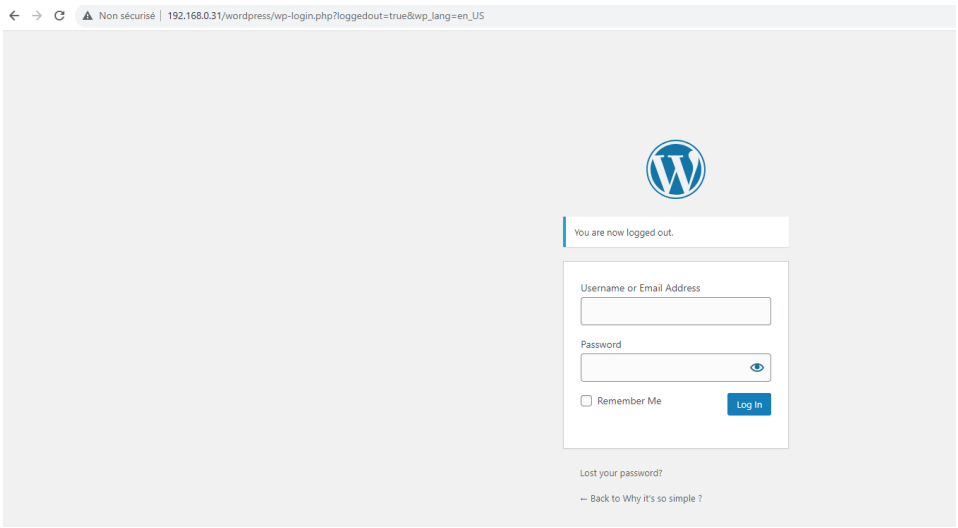
Ici le port 80 donc il y a un site web.

Un site apparait à cette adresse ip.

On peut donc chercher ce qui fait apparaitre ce site.

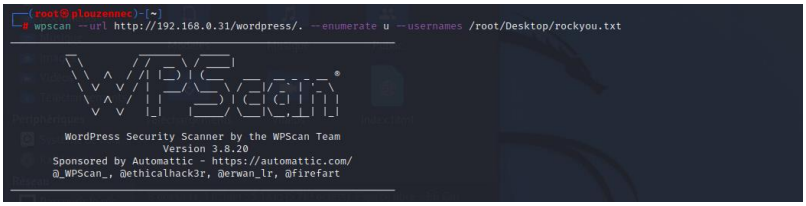
```
┌──(root㉿plouzennec)-[~]
└─# dirb http://192.168.0.31/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Feb  2 11:24:46 2024
URL_BASE: http://192.168.0.31/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.31/ ----
+ http://192.168.0.31/index.html (CODE:200|SIZE:495)
+ http://192.168.0.31/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.0.31/wordpress/

---- Entering directory: http://192.168.0.31/wordpress/ ----
+ http://192.168.0.31/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.0.31/wordpress/wp-admin/
==> DIRECTORY: http://192.168.0.31/wordpress/wp-content/
==> DIRECTORY: http://192.168.0.31/wordpress/wp-includes/
+ http://192.168.0.31/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

On peut chercher la page pour se connecter au wordpress, ici /wordpress/wp-admin

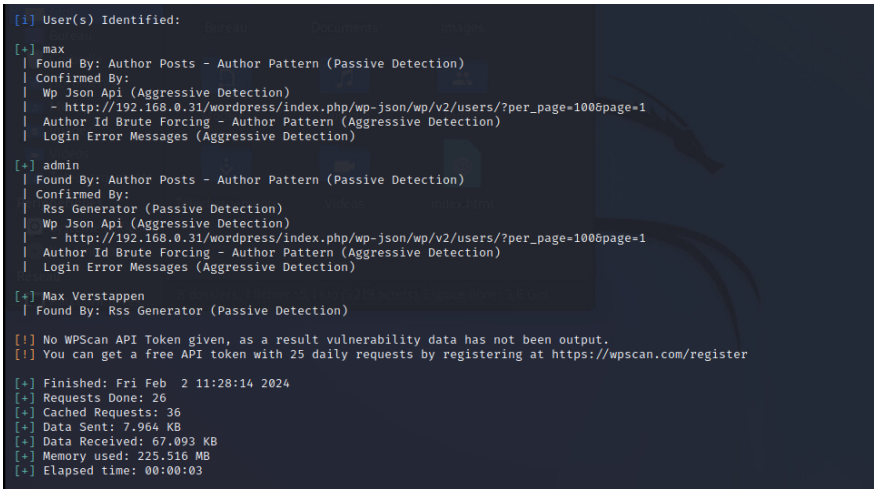


On tombe là-dessus

Etapte 2 : wpscan des user



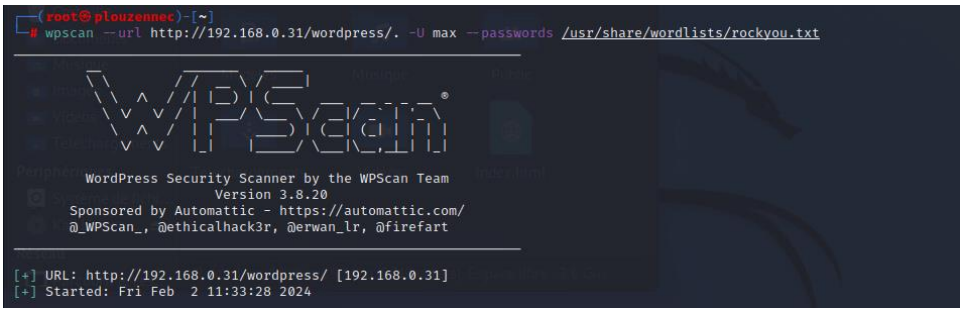
On cherche ainsi à trouver les user avec cette commande



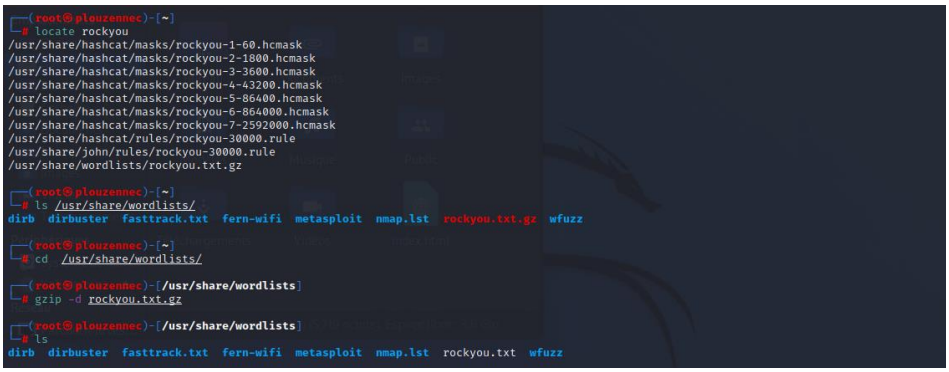
On trouve ici les utilisateurs max, max verstappen, et admin.

Etape 3 : wpscan du mot de passe

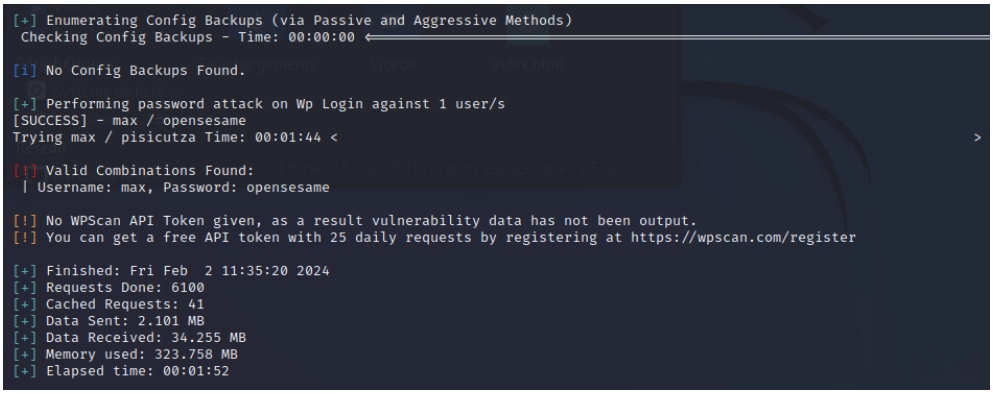
Avec maintenant pour objectif de trouver un mdp d'un utilisateur connu, ici max.



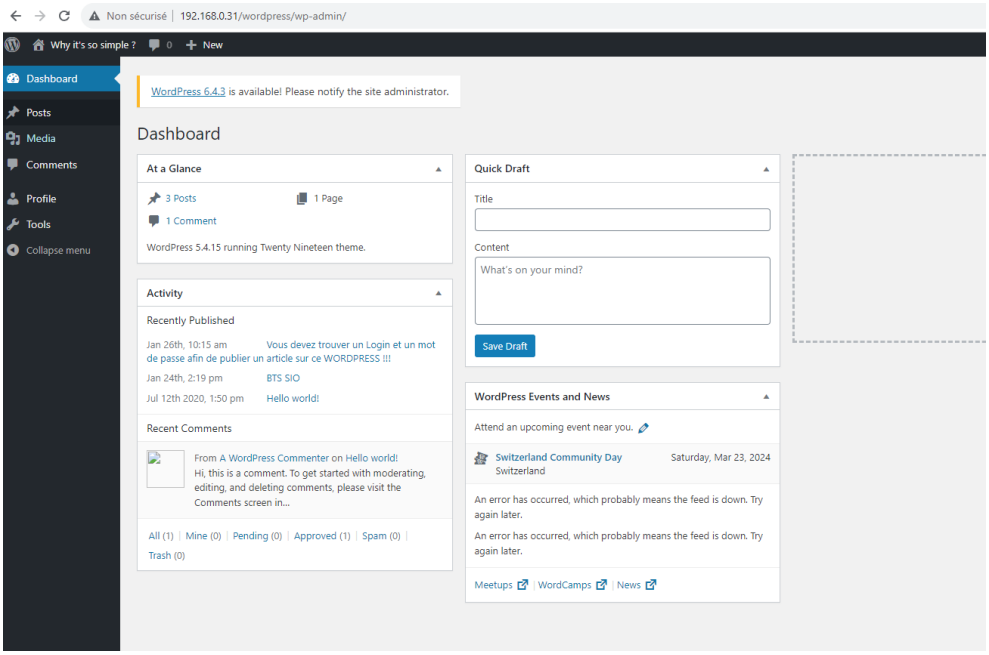
On rentre cette commande pour trouver le mdp avec une wordlist.



Cette commande à été utilisée en la trouvant et la dezipant, rockyou.txt.



Ainsi on trouve le mdp, ici opensesame



On a donc acces au site avec max et openesame.