

25-10-2016



Manual de instalación.

Escáner de vulnerabilidades en DRUPAL.
(DruSpawn)

PBSC 10^a generación.

- Fernando Castañeda G.

Manual de instalación.

INDICE.

1. Requerimientos técnicos.....	2
2. Proceso de instalación.....	2
3. Estructura de la instalación.	4
4. Desinstalación.....	5
5. Modificaciones.....	5

1. Requerimientos técnicos.

Las pruebas se han realizado en su totalidad sobre Ubuntu 14.04, 16.04 y Debian 8.6, sin embargo, se extiende dentro de las características de la herramienta la capacidad de trabajar con cualquier distribución de GNU/Linux. Los entornos en los cuales se han llevado a cabo las pruebas con resultados óptimos cuentan con las siguientes características.

- Distribución GNU/Linux a 32 o 64 bits.
- 512GB de RAM mínimos.
- 4 MB disponibles de espacio en disco para archivos de instalación.
- Interprete de Python 2.7 instalado en el sistema operativo.
- Instalación de sh en el sistema operativo.
- Instalación de sudo en el sistema operativo, con permisos para ejecutar scripts para el usuario que realice la instalación.
- Instalación de GIT en el equipo.
- Instalación de tor en el caso de distribuciones como Arch Linux, o Suse, de lo contrario no es necesaria una instalación previa.

2. Proceso de instalación.

El proceso de instalación es realmente sencillo si se cubren todos los requerimientos técnicos mencionados en el punto anterior.

La dirección del repositorio en el cual se encuentra el proyecto es el siguiente.

<https://github.com/f99942/DruSpawn>

Esta dirección incluye un manual de instalación express en la misma página del repositorio, así como uno de uso de manera más directa, esto con el fin de descargar y comenzar a utilizar en seguida, en caso de que no se deseen leer los manuales.

Ya sea que se clone el repositorio o que se copie de algún otro lugar, dentro del directorio, se encuentra el archivo install.sh.

```
common docs DruSpawn.py README.md reportes user.sh
config druspawn install.sh remove.sh script
```

Dicho archivo debe ejecutarse para comenzar con la instalación. Durante el proceso de instalación de la herramienta se llevará a cabo una actualización de los repositorios, y a través del gestor de paquetes de la distribución se instalarán las dependencias, mismas que se listan a continuación.

- python-pip
- tor

- sqlite3

Una vez instalados estos, el mismo script de instalación ejecutara pip para instalar las dependencias de Python.

- requests
- requesocks
- requests[socks]
- ansicolors
- untangle
- BeautifulSoup
- bs4

La instalación se realiza como se muestra a continuación.

```
~/DruSpawn (master=) $ sudo ./install.sh
```

El proceso de instalación debe transcurrir como se muestra a continuación.

```
Fetchd 877 kB in 9s (93.8 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pip is already the newest version.
sqlite3 is already the newest version.
tor is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 95 not upgraded.
Requirement already satisfied (use --upgrade to upgrade): requests in /usr/lib/python2.7/dist-packages
Cleaning up...
Requirement already satisfied (use --upgrade to upgrade): requesocks in /usr/local/lib/python2.7/dist-packages
Requirement already satisfied (use --upgrade to upgrade): certifi>=0.0.7 in /usr/local/lib/python2.7/dist-packages (from requesocks)
Requirement already satisfied (use --upgrade to upgrade): chardet>=1.0.0 in /usr/lib/python2.7/dist-packages (from requesocks)
Cleaning up...
Requirement already satisfied (use --upgrade to upgrade): requests[socks] in /usr/lib/python2.7/dist-packages
Installing extra requirements: 'socks'
Cleaning up...
```

Ya que la herramienta trabaja con una base de datos obtenida a partir de las páginas de seguridad de Drupal, la generación de esta base de datos debe darse al momento de la instalación, con el fin de tener dicha base de datos actualizada, en caso de que se desee utilizar una base de datos que viene con la aplicación, se debe interactuar con el script indicándole la opción deseada cuando se muestre el siguiente mensaje.

```
CREANDO DIRECTORIO PARA USUARIO...
Moviendo archivos necesarios a /opt/drushawn
¿Desea utilizar la base de datos que viene con el programa, o desea crear una propia? [ Ingrese S para crearla, cualquier otro caracter para utilizar la base de datos por defecto. ]
```

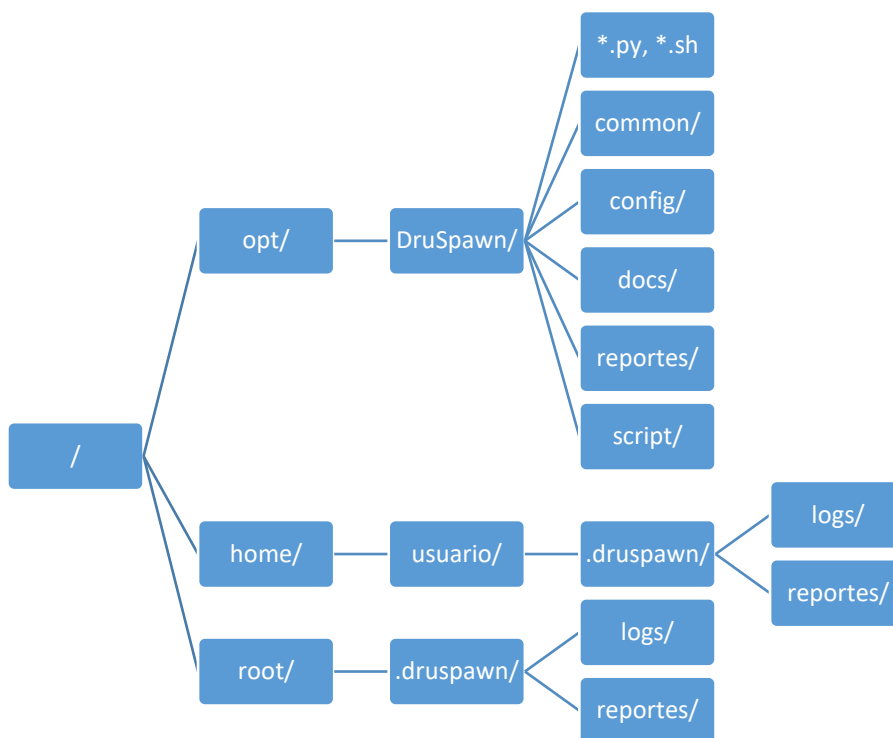
Si se selecciona la opción de crear la base de datos desde 0, la instalación demorara aproximadamente una hora, esto dependiendo del hardware y de la velocidad de la conexión a internet, se debe tener esto en consideración. Si la instalación finaliza de manera exitosa, bastará con escribir en línea de comandos druspawn, se mostrará este mensaje que comprueba que todo resulto exitoso.

```
fernando@fcg ~/DruSpawn (master *) $ druspawn
usage: DruSpawn.py [-h] -d [https://direccion del escaneo] [--full]
                  [-p [http://direccion del proxy]] [--pdf]
                  [-u [Archivo con user agent]] [-s [script.py]] [--script]
                  [--tor] [--verbose]
DruSpawn.py: error: argument -d is required
```

Ahora puede utilizar la herramienta sin problemas. Leer el manual de usuario para más información al respecto.

3. Estructura de la instalación.

Todos los archivos que constituyen a DruSpawn, están ubicados en opt/, estos están configurados para siempre encontrarse en ese punto. Mientras que para cada usuario, incluido el superusuario, se creara un directorio en donde se almacenaran los logs y los reportes generados a partir de la herramienta, se debe verificar que en efecto existan estos directorios, de lo contrario la herramienta podría fallar.



4. Desinstalación.

Dentro del directorio que contiene los archivos de la herramienta, se incluye uno con el nombre `remove.sh`, este script, desinstalara la aplicación del equipo, así como versiones anteriores de la aplicación.

```
fernando@fcg ~/DruSpawn (master *) $ ./remove.sh  
DruSpawn desinstalado de manera exitosa...
```

5. Modificaciones.

Usted es libre de realizar las modificaciones que desee a los scripts de instalación según sus necesidades, puede guiarse en el manual de programación de módulos que se encuentra en `docs/` para seguir el modelo empleado en la herramienta.