## PRET, reventando impresoras al vuelo

Publicado por Alejandro Taibo on jueves, 2 de febrero de 2017 Etiquetas: <u>hardware</u>, <u>herramientas</u>, <u>Internet de las cosas</u>, <u>python</u>



Todos nosotros alguna vez hemos manipulado alguna impresora, ya sea para hacer copias, imprimir documentos, escanear... También, muchos tenemos una en casa de las que desde hace unos años se comenzaron a desarrollar sin la necesidad de ser conectadas físicamente a nuestro ordenador. Poco después, se introdujo en ellas la funcionalidad de la conexión vía WiFi con la que podemos imprimir documentos inalambricamente, con la única condición de que tanto la impresora como el ordenador desde el que queremos enviar el documento, estén conectados a la misma red.

Con estos avances a algunas personas (*trolls*) se les encendió la bombilla y, utilizando el sentido común, pensaron que estando en la misma red que una impresora, podrían imprimir cualquier documento sin el permiso del propietario para, como no, trollear y reírse un rato.

Con el paso del tiempo, para evitar lo mencionado anteriormente, se han ido implementando algunas medidas de seguridad en algunos dispositivos, como por ejemplo contraseñas que se usan para vincular dispositivos para que solo ellos puedan realizar acciones sobre dicha impresora.

Pero como todos los que leemos este blog sabemos, la seguridad es algo "ilusorio".

Y sí, esta vez le ha tocado la china a las impresoras. Hace una semana, unos estudiantes de la universidad de *Ruhr University Bochum* presentaron su tesis en la cual, desarrollaron una herramienta que han liberado hace pocos días en Github, hablo de <u>PRET</u>, una herramienta desarrollada para probar las seguridad de las impresoras.

Esta herramienta se puede conectar a la impresora vía USB o vía WiFi y se encarga de explotar el lenguaje con el que fue desarrollada la impresora objetivo. Actualmente ataca a los lenguajes <a href="PostScript">PostScript</a>, PJL y PCL, los cuales se encuentran en la mayoría de impresoras láser.

Esta herramienta nos permitirá hacer cosas como: capturar documentos, modificarlos, acceder a la memoria de la impresora o incluso dañar la impresora físicamente. Esta tool ha sido programada en Python, que será un requisito imprescindible para su uso e instalación, más concretamente, deberemos

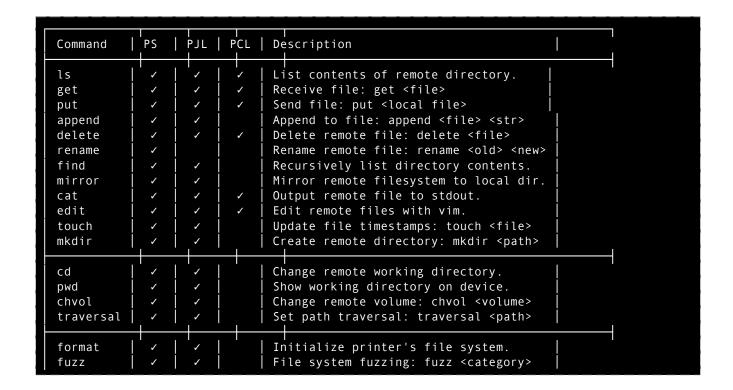
tener instalado el interprete Python2.

Cómo instalar esta herramienta:

- 1. Deberemos descargar la herramienta de Github: <a href="https://github.com/RUB-NDS/PRET">https://github.com/RUB-NDS/PRET</a>.
- 2. En la terminal ejecutaremos: pip install colorama pysnmp.
- 3. Posteriormente ejecutamos: pip install win\_unicode\_console.
- 4. Y por último: apt-get install imagemagick ghostscript.
- 5. Para ejecutarlo únicamente tendremos que escribir ./pret.py y nos mostrará los siguientes parámetros.

```
pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}
positional arguments:
                        printer device or hostname
  target
  {ps,pjl,pcl}
                        printing language to abuse
optional arguments:
  -h, --help
                        show this help message and exit
  -s, --safe
                        verify if language is supported
  -q, --quiet
                        suppress warnings and chit-chat
  -d, --debug
                        enter debug mode (show traffic)
  -i file, --load file load and run commands from file
  -o file, --log file
                       log raw data sent to the target
```

Los creadores de esta herramienta también nos muestran los comandos que podremos ejecutar en base al lenguaje de la impresora que estemos atacando. Serían los siguientes:



Y con ésto, una vez más queda demostrada la inseguridad de los IoT...

Por último comentaros también que esta herramienta ha sido creada para un proposito educativo, no ha sido diseñado para crear ningún tipo de daño... qué os veo!