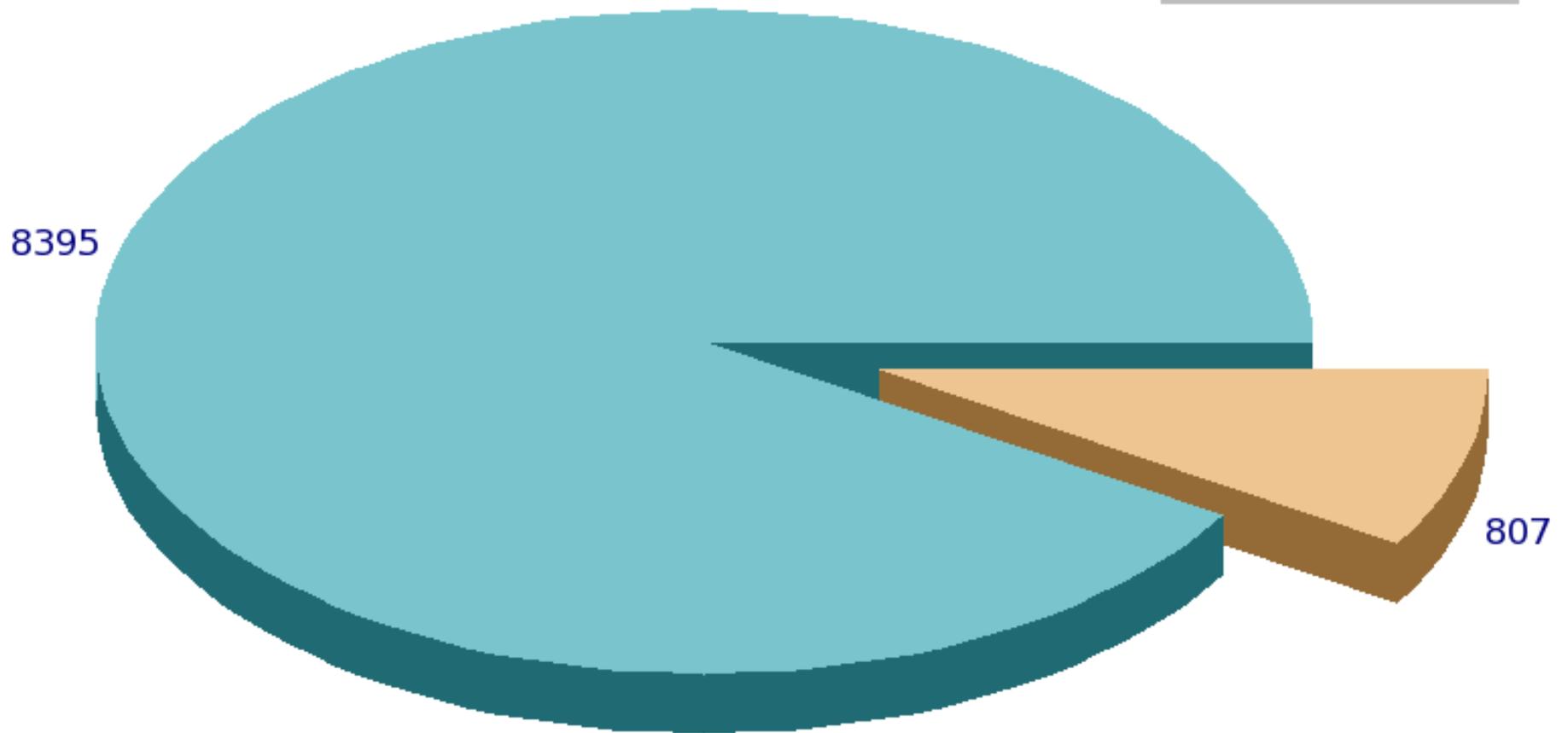
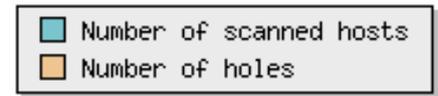


Pentest Debrief

Site Quarterly Pentest
 $\frac{1}{4}$ 07

Number of Devices Scanned vs. Number of Holes Found



Number of hosts with at least
one hole

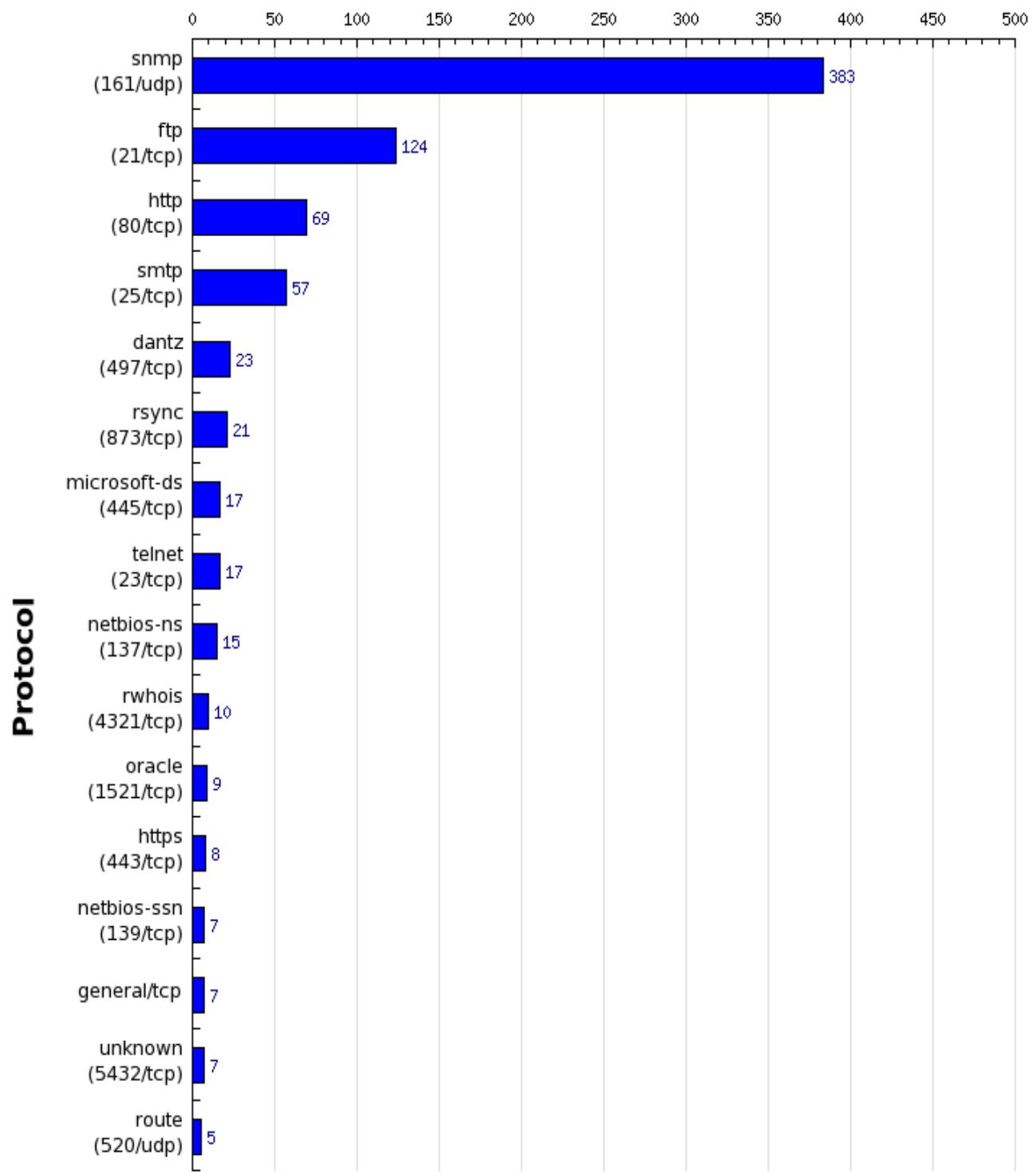
570

or

~ 7 %

of nodes scanned

Number of Holes



Total
Number
of
Holes
By
Protocol
(upper bound)

807 total holes

383	snmp
124	ftp
69	http
+17	telnet

~ 593 were ...

... printers

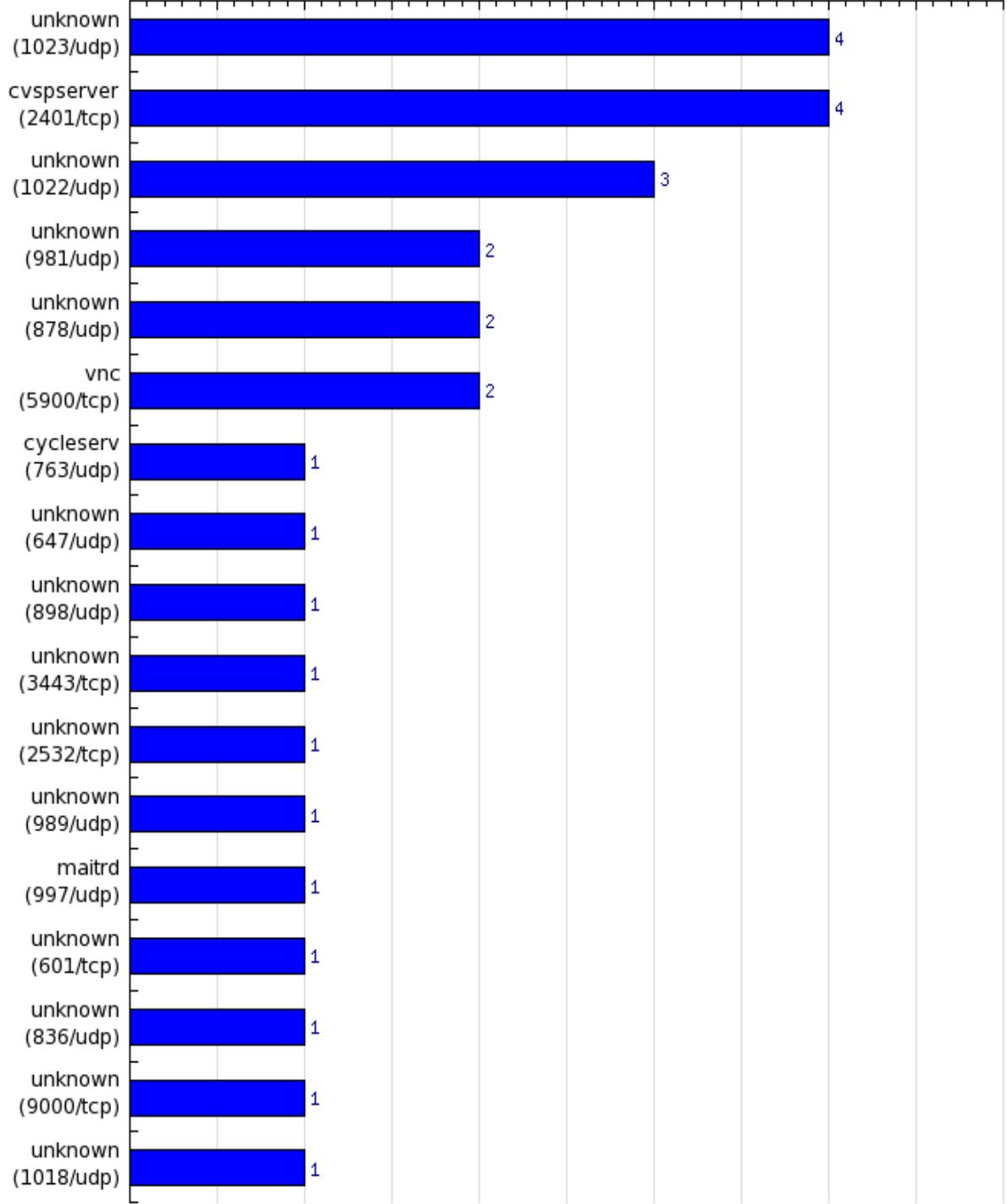
Or

~ 75 %

of the reported holes

Number of Holes

0.0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0



Protocol

Total
Number
of
Holes
By
Protocol
(lower bound)

Printer Debrief

Oh but it's just paper

This is just downright annoying

It's just paper until it's your print job that is being backlogged due to someone sending a constant stream of garbage to the printer



Is Your Printer Out to Get You?

Non-PC network devices pose a growing threat to your data security

By Ira Victor

Your company has invested heavily in IT security. All the protections IT has recommended have been purchased and put in place. You feel confident that the company's electronic data is secure. But is it? What about all those non-PC networked devices lying around? Are they safe?

Printers, scanners, video cameras, anti-spam and anti-spyware appliances, VoIP devices, and other network-aware devices represent a growing threat. Many newer models of these devices are equipped with

large hard drives (60GB or more), powerful Pentium processors, and versions of popular operating sys-

The Non-PC Threat

Many organizations have purchased powerful firewalls, in-line

SECURITY TECHNOLOGY & DESIGN

• March 2007

scanner's hard drive stores its output—output that may contain copies of medical records, account information or social security numbers.

the outside, many newer devices are more like PCs on the inside.

Run a quick search on hacker and security Web sites, blogging sites, or underground IRC chat boards, and

General Findings

- ~600 printers
- 62 unauthenticated access via web
- ~40 more with unauthenticated access via telnet
- Last 2 numbers above are just on the second day. It doesn't include the counts from the first day
- Every device had default SNMP community strings

What does bad look like?

Feature Authorization Settings

	Key		Any
	Admin	User	User
Administration			
Modify Configuration Web Pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Configuration Web Pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Home & Status Web Pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Initiate Multiple Printer Discovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Custom Web Pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

User ID and Password

User ID and Password

System Manager ID : (Max 7 digits)

System Password : (Max 7 digits)

Firm : (Max 7 digits)

	Key		Any
	Admin	User	User
Modify Configuration Web Pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Configuration Web Pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Home & Status Web Pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Initiate Multiple Printer Discovery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Write	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Custom Web Pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

```

331 Username OK, send identity (email :
Password:
230- Hewlett-Packard J3113A FTP Server
Directory:      Description:
-----
PORT1          Print to port 1 HP Color
To print a file, use the command: put
or 'cd' to a desired port and use: put
Ready to print to PORT1
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put a.txt
local: a.txt remote: a.txt
200 PORT command successful.
150 Opening data connection.
226- Ready
226 Transfer complete.
127 bytes sent in 0.011 seconds (11 Kb)
ftp>
    
```

What does good look like?



The server 131.225.84.33 at Administration requires a username and password.

Warning: This server is requesting that password be sent in an insecure manner without a secure connection).

User name:

Password:

Remember my password

OK

Feature Authorization	Key		Any User
	Admin	User	
Administration			
Modify Configuration Web Pages	✓	<input type="checkbox"/>	<input type="checkbox"/>
View Configuration Web Pages	✓	<input type="checkbox"/>	<input type="checkbox"/>
View Home & Status Web Pages	✓	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Writes (SET)	✓	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Reads (GET)	✓	<input type="checkbox"/>	<input type="checkbox"/>
Manage Custom Web Pages	✓	<input type="checkbox"/>	<input type="checkbox"/>
Delete Secure Jobs	✓	<input type="checkbox"/>	<input type="checkbox"/>
Manage Saved Jobs	✓	<input type="checkbox"/>	<input type="checkbox"/>
Manage Job Accounting	✓	<input type="checkbox"/>	<input type="checkbox"/>
Delete Font Files	✓	<input type="checkbox"/>	<input type="checkbox"/>
Web Server Printing			
Print Demo Pages	✓	<input type="checkbox"/>	<input type="checkbox"/>



Authorization Dialog

You need to supply a username and a password to access this site.

HP Jetdirect Networking (password only, no username required) at 131.225.84.243

System Location: MW-9

HP JetDirect: J4169A

Firmware Version: L.21.11

IP Address: 131.225.176.72

Hardware Address: 0001E63D9575

Admin Password: <Set>

Refresh

```
[tarupp@catbot ~]$ telnet 131.225.84.33
Trying 131.225.84.33...
telnet: Unable to connect to remote host: Connection refused
[tarupp@catbot ~]$ ftp 131.225.84.33
ftp: connect: Connection refused
ftp> quit
```

Initiate Status Refresh	✓	<input type="checkbox"/>	<input type="checkbox"/>
Generate Reports	✓	<input type="checkbox"/>	<input type="checkbox"/>

SNMP

- Simple Network Management Protocol
- Generally not necessary that it be running on your device unless your devices are centrally managed with some other software
 - But this depends on the device!! I'm looking at you JetDirect...
- Can disclose sensitive data...

Like passwords

And system configuration

Passwords From SNMP

- 31 31 31 31 3D 31 30 38 3B
- 48 50 35 53 49 3D 31 30 38 3B
- 44 48 43 50 34 4D 45 3D 31 30 38 3B
- 55 53 4D 42 33 35 32 31 36 36 3D 31 30 38 3B
- 43 4F 4E 46 49 47 4A 44 31 37 30 3D 31 30 38 3B
- 48 44 54 56 33 32 3D 31 30 38 3B
- 42 4C 55 45 31 42 4F 58 3D 31 30 38 3B
- 43 4F 57 50 49 45 3D 31 30 38 3B
- 00 00 00 00 00 00 00 00 00 00 00

Whoops, I mean...

- 1111
- HP5SI
- DHCP4ME
- USMB352166
- CONFIGJD170
- HDTV32
- BLUE1BOX
- COWPIE
- empty password (there were lots of them)

demo: pull password from SNMP

System Configuration

Installed Software

```
HOST-RESOURCES-MIB::hrSWInstalledName.43 = STRING: "ed-0.2-36"  
HOST-RESOURCES-MIB::hrSWInstalledName.44 = STRING: "groff-1.18.1.1-3.EL  
HOST-RESOURCES-MIB::hrSWInstalledName.45 = STRING: "krb5-devel-1.3.4-33  
HOST-RESOURCES-MIB::hrSWInstalledName.46 = STRING: "libpng-1.2.7-1.el4.  
HOST-RESOURCES-MIB::hrSWInstalledName.47 = STRING: "libcroco-0.6.0-4"  
HOST-RESOURCES-MIB::hrSWInstalledName.48 = STRING: "man-1.5o1-9.rhel4"  
HOST-RESOURCES-MIB::hrSWInstalledName.49 = STRING: "Omni-0.9.1-7.1"  
HOST-RESOURCES-MIB::hrSWInstalledName.50 = STRING: "mysql-4.1.20-1.RHEL  
HOST-RESOURCES-MIB::hrSWInstalledName.51 = STRING: "bc-1.06-17.1"  
HOST-RESOURCES-MIB::hrSWInstalledName.52 = STRING: "diskdumputils-1.3.1  
HOST-RESOURCES-MIB::hrSWInstalledName.53 = STRING: "pyxf86config-0.3.19  
HOST-RESOURCES-MIB::hrSWInstalledName.54 = STRING: "foundation-redhat-4  
HOST-RESOURCES-MIB::hrSWInstalledName.55 = STRING: "psgml-1.2.5-4"  
HOST-RESOURCES-MIB::hrSWInstalledName.56 = STRING: "lockdev-1.0.1-6.2"  
HOST-RESOURCES-MIB::hrSWInstalledName.57 = STRING: "rpm-python-4.3.3-18  
HOST-RESOURCES-MIB::hrSWInstalledName.58 = STRING: "sysreport-1.3.15-6"  
HOST-RESOURCES-MIB::hrSWInstalledName.59 = STRING: "guile-1.6.4-14"  
HOST-RESOURCES-MIB::hrSWInstalledName.60 = STRING: "docbook-style-dsss1  
HOST-RESOURCES-MIB::hrSWInstalledName.61 = STRING: "gnutls-1.0.20-3.2.3  
HOST-RESOURCES-MIB::hrSWInstalledName.62 = STRING: "libxml2-2.6.16-6"  
HOST-RESOURCES-MIB::hrSWInstalledName.63 = STRING: "netpbm-progs-10.25-  
HOST-RESOURCES-MIB::hrSWInstalledName.64 = STRING: "pilot-link-0.11.8-8  
HOST-RESOURCES-MIB::hrSWInstalledName.65 = STRING: "xmlsec1-1.2.6-3"  
HOST-RESOURCES-MIB::hrSWInstalledName.66 = STRING: "anuplot-4.0.0-4"
```

System Configuration

Mountpoints; disk space

```
HOST-RESOURCES-MIB::hrDiskStorageCapacity.1536 = INTEGER: 78150744 KBy
HOST-RESOURCES-MIB::hrDiskStorageCapacity.1537 = INTEGER: 134217727 KB
HOST-RESOURCES-MIB::hrDiskStorageCapacity.1538 = INTEGER: 0 KBytes
HOST-RESOURCES-MIB::hrPartitionIndex.1536.1 = INTEGER: 1
HOST-RESOURCES-MIB::hrPartitionIndex.1536.2 = INTEGER: 2
HOST-RESOURCES-MIB::hrPartitionIndex.1536.3 = INTEGER: 3
HOST-RESOURCES-MIB::hrPartitionIndex.1537.1 = INTEGER: 1
HOST-RESOURCES-MIB::hrPartitionLabel.1536.1 = STRING: "/dev/hda1"
HOST-RESOURCES-MIB::hrPartitionLabel.1536.2 = STRING: "/dev/hda2"
HOST-RESOURCES-MIB::hrPartitionLabel.1536.3 = STRING: "/dev/hda3"
HOST-RESOURCES-MIB::hrPartitionLabel.1537.1 = STRING: "/dev/hdb1"
```

```
HOST-RESOURCES-MIB::hrFSMountPoint.1 = STRING: "/"
HOST-RESOURCES-MIB::hrFSMountPoint.2 = STRING: "/sys"
HOST-RESOURCES-MIB::hrFSMountPoint.3 = STRING: "/proc/bus/usb"
HOST-RESOURCES-MIB::hrFSMountPoint.4 = STRING: "/export/home"
HOST-RESOURCES-MIB::hrFSMountPoint.5 = STRING: "/rest"
HOST-RESOURCES-MIB::hrFSMountPoint.6 = STRING: "/proc/sys/fs/binfmt_
HOST-RESOURCES-MIB::hrFSMountPoint.7 = STRING: "/var/lib/nfs/rpc_pip
HOST-RESOURCES-MIB::hrFSMountPoint.8 = STRING: "/proc/fs/nfsd"
HOST-RESOURCES-MIB::hrFSMountPoint.9 = STRING: "/mnt"
```

System Configuration

Processes

```
HOST-RESOURCES-MIB::hrSWRunPath.210 = STRING: "kseriod"
HOST-RESOURCES-MIB::hrSWRunPath.321 = STRING: "kjournald"
HOST-RESOURCES-MIB::hrSWRunPath.1237 = STRING: "udev"
HOST-RESOURCES-MIB::hrSWRunPath.1449 = STRING: "kauditd"
HOST-RESOURCES-MIB::hrSWRunPath.1513 = STRING: "kmirrored"
HOST-RESOURCES-MIB::hrSWRunPath.1557 = STRING: "kjournald"
HOST-RESOURCES-MIB::hrSWRunPath.1558 = STRING: "kjournald"
HOST-RESOURCES-MIB::hrSWRunPath.2058 = STRING: "/opt/rocks/bin/python"
HOST-RESOURCES-MIB::hrSWRunPath.2069 = STRING: "syslogd"
HOST-RESOURCES-MIB::hrSWRunPath.2073 = STRING: "klogd"
HOST-RESOURCES-MIB::hrSWRunPath.2084 = STRING: "irqbalance"
HOST-RESOURCES-MIB::hrSWRunPath.2094 = STRING: "portmap"
HOST-RESOURCES-MIB::hrSWRunPath.2114 = STRING: "rpc.statd"
HOST-RESOURCES-MIB::hrSWRunPath.2144 = STRING: "rpc.idmapd"
HOST-RESOURCES-MIB::hrSWRunPath.2311 = STRING: "/usr/sbin/automount"
HOST-RESOURCES-MIB::hrSWRunPath.2359 = STRING: "/usr/sbin/automount"
HOST-RESOURCES-MIB::hrSWRunPath.2374 = STRING: "/usr/sbin/smartd"
HOST-RESOURCES-MIB::hrSWRunPath.2384 = STRING: "/usr/sbin/acpid"
HOST-RESOURCES-MIB::hrSWRunPath.2405 = STRING: "/usr/sbin/sshd"
HOST-RESOURCES-MIB::hrSWRunPath.2491 = STRING: "rpc.rquotad"
HOST-RESOURCES-MIB::hrSWRunPath.2508 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2509 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2510 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2511 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2512 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2513 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2514 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2515 = STRING: "nfsd"
HOST-RESOURCES-MIB::hrSWRunPath.2516 = STRING: "lockd"
HOST-RESOURCES-MIB::hrSWRunPath.2517 = STRING: "rpciod"
HOST-RESOURCES-MIB::hrSWRunPath.2521 = STRING: "rpc.mountd"
HOST-RESOURCES-MIB::hrSWRunPath.2676 = STRING: "crond"
HOST-RESOURCES-MIB::hrSWRunPath.2707 = STRING: "xfs"
HOST-RESOURCES-MIB::hrSWRunPath.2726 = STRING: "/usr/sbin/atd"
HOST-RESOURCES-MIB::hrSWRunPath.2742 = STRING: "dbus-daemon-1"
HOST-RESOURCES-MIB::hrSWRunPath.2752 = STRING: "cups-config-daemon"
HOST-RESOURCES-MIB::hrSWRunPath.2756 = STRING: "/usr/sbin/snmpd"
HOST-RESOURCES-MIB::hrSWRunPath.2763 = STRING: "hal"
HOST-RESOURCES-MIB::hrSWRunPath.2763 = STRING: "hal"
```

Cmon, where's the risk?

- It's not about getting root
- Because I can embarrass the heck out of your organization and abuse your resources
 - Software/music/image drops
 - Upload my own watermarks, so I can include inappropriate content in everything that is printed...use your imagination.
 - Change your print banners
 - FTP bounce attacks so I can scan behind your firewalls
- Provides valuable reconnaissance info for use in larger attacks

demo: FTP bounce

Being a jerk

- `cat /dev/hda | nc -c 192.168.1.2 9100`
- FTP your swapfile to the printer
- Change the LCD display
- `nmap -P0 -sI printer_ip target_ip`
- `telnet localhost 19 | nc printer_ip 9100`



So what do you recommend we do then?

- Disable unnecessary services and protocols if possible
- Ask Data Comm to filter services that cannot be disabled
- Get rid of your old printers. Yeah, I said it

If you're feeling geeky

- <http://www.irongeek.com/i.php?page=security/networkprinterhacking>
- yum install net-snmp-utils
provides snmpget and snmpwalk
- telnet to your printer and see what I saw
- decode your own hex
<http://nickciske.com/tools/hex.php>

Further Reading

- Information and Recommendations for Securing Printers on Site
 - CD-DocDB # 2072
 - KCA required to view
 - Additions and corrections welcome

Questions?

