GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Printer Security Essentials

© SANS Institute 2000 - 2002, Author retains full rights.

By Andrew Rikarts

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I. Introduction…….. 3

A. Overview: What is this paper all about?
1. Intended Audience
2. About the Author
3. General Preview
4. Definition of Terms

B. Defining the Problem: Are printers a security risk?

II. Vulnerability Assessment……. 6

A. What are the vulnerabilities associated with printers?
1. Security Scans
2. Scan Analysis
3. Physical Analysis

B. Vulnerabilities examined

III. Vulnerability Fixes and Risk Mitigation…… . 37

A. What can be done to fix the problems?

B. What can be done to lower the risk on things that can't be fixed?
1. Mitigation Methods
2. Physical Policy

C. What can be done in the future?

IV. Summary: What have we learned? …….. 40

V. References …… 41

VI. Test Questions ……. 42

A. Multiple Choice

B. True & False

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I. Introduction

A. Overview: What is this paper all about?

1. Intended Audience

This paper is intended to heighten the awareness of the reader to the often-overlooked consequences of adding printing devices to a network. While the content is intended for the network administration professional it could valuable to wide range of skill levels ranging from manager to end-user. Security is something everyone needs to be conscious of in their daily use of information systems and the admittedly esoteric content to follow can at least serve to widen the scope of thought given to information security and assurance. This document could be viewed as the foundation for a "best practices" policy for printer security.

2. About the Author

Andrew Rikarts has over 20 years of computer experience beginning with coding BASIC on TRS-80 model I's and hacking CompuServe using his Apple][+ and Hayes Micromodem II at 300 baud when escape characters could take down a BBS and phone phreaking was "safe". Several years of schooling later landed him in a PC analyst and COBOL programmer spot at an insurance company. This then lead to a seven year sentence as an IT Manager position where he moved his company from Data General Mini computers to the realm of a completely re-engineered client-server system on the Internet in time for Y2K. Through that time VPN's, Firewalls, and Anti-virus programs all became required technology. After working himself out of a job in the privately held company he finds himself in his current position as an Enterprise Operations Engineering (EOE) Information Assurance Center (IAC) engineer (what a mouthful) working on an extremely large enterprise (~400K end users). All those bits and pieces of experience and adaptability are now an everyday demand of the critical mission. His daily focus ranges from resolving deployment issues, trade studies, meetings and obscurities such as securing printers.

3. General Preview

In this document the reader will be made aware of potential security implications related to the deployment of printers attached computers connected to a network or connected directly to a network as a network print device. The reader will be made aware of methods used to determine vulnerabilities and results of those methods from real world scenarios. The reader will be presented with ways to secure and mitigate vulnerabilities experienced by the author and be presented with a proactive approach to future printer procurement.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. Definition of Terms

Several terms used throughout this paper are defined below:

ACL – Access Control List – A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

FTP – File Transfer Protocol - Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

HTTP - Hypertext Transfer Protocol - The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

IEEE - Institute of Electrical and Electronics Engineers – A professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.

LAN – Local Area Network – A high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

MAC Address – Media Access Control Address - Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a *hardware address*, *MAC layer address*, and *physical address*.

Port Security - Port security prevents unauthorized access of a port by "securing" a specific MAC address on a port. For example, if you enable port security, the switch will remember the first MAC address it sees on the port. If that MAC address changes, the switch will disable the port, preventing the device from seeing the rest of the network. You can also manually specify a MAC address.

RFC - Request For Comments - Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.

Telnet - Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

TCP/IP - Transmission Control Protocol/Internet Protocol - Common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.

VLAN – Virtual Local Area Network – Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Definitions by

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

B. Defining the Problem: Are printers a security risk?

An often-overlooked process in the overall defense-in-depth approach to Information Assurance is peripheral security analysis. In this case of this document we will be focusing on a specific peripheral, the printer. At first thought, printers appear to be an innocuous output-only device. While that may appear to be case to the everyday user, the truth is that there is a lot more to it. Set aside for a moment the fact that the mission of a printer is create a hardcopy of potentially critical information and the physical security involved with that hard output and begin to think about the advances technology that have transformed these simple output devices into web/enterprise-manageable document distribution centers capable of all sorts of nifty tricks. A majority of today's business printers have transcended from simple output devices into fully capable servers with operating systems and built-in webservers. All of these integrations can and often are prone to all of the vulnerabilities that we should all be familiar with regarding these types of separate systems. Even the smallest of networked or non-networked printers have security implications, some more serious than others, but all need to be addressed, secured and/or mitigated.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

II. Vulnerability Assessment

C. What are the vulnerabilities associated with printers?

1. Security Scans

The typical first step in securing network devices is using a network security assessment "scan" tool such as ISS, Nessus, Netrecon, Cybercop, Superscan, etc. to determine any well-known vulnerabilities that the device may possibly have to be exploited. It is best to use more than one tool to get more confident feeling that all the bases are covered. No one tool seems to ever be perfect. Here are some actual scans from some production printers. The scan data output has been trimmed and cleaned for sensitive information.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ISS – Internet Security Scanner Output

Network Vulnerability Assessment Report Sorted by Vulnerability Severity

10/22/2001

Report Description

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	Session1	**Session ID:**	91
File Name:	Session1_011022	**Template:**	production
Comment:	Network Printing Solution	**Termination Status:**	Finished

Scan Summary Information

Hosts Scanned:	13	**Scan Start:**	2001/10/22 09:39:35
Hosts Active:	13	**Scan End:**	2001/10/22 10:11:09
Hosts Inactive:		**Elapsed:**	00:31:34

Vulnerability Name	Severity
HTTP proxy penetrated	High

Description:

The web (HTTP) proxy allowed access through the proxy server. If the test was conducted from outside the firewall, an attacker could use the proxy to access any portion of the network inside the firewall.

False Positives: If the test was conducted from inside the firewall, no risk is indicated.

Fix

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Review the proxy server's settings. Refer to your firewall's documentation for more information.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.241		N/A		91
x.x.x.243				91

Vulnerability Name	Severity
TCP sequence prediction (CAN-2001-0328)	Medium

Description:

The TCP sequence was found to be predictable. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets can compromise services, such as rsh and rlogin, because their authentication is based on IP addresses. Attackers can also perform session hijacking to gain access to unauthorized information.

Some Microsoft patches for this did not completely resolve the sequence predicability. The following information explains the varying levels of TCP sequence predictability in Windows operating systems:
- Windows NT 4.0 pre-SP3 systems are highly predictable.
- Windows NT 4.0 SP4 through SP6 use a different algorithm to reduce sequence predictability, but the systems remain predictable.
- Microsoft released patch MS99-046, which uses the same algorithm as Windows 2000, to fully fix the problem.
- Windows 2000 is not TCP predictable.

Internet Scanner users: Please note that this check can potentially be time consuming, and may greatly increase the time required to perform a scan.

Fix

Ask your vendor for patches to correct TCP sequence prediction. Note that some patches make sequence prediction more difficult, but still possible. As a result, the host may continue to report this vulnerability.

For Windows NT 4.0:
Apply the latest Windows NT 4.0 Service Pack (SP4 or later), available from the Windows NT Service Packs Web page. Note that Windows NT system may continue to report this vulnerability. After you successfully apply the Service Pack, apply the patch referenced in Microsoft Security Bulletin MS99-046. See References.

For HP-UX 9.0:
Apply the appropriate patch for your system, as listed in CERT advisory CA-2001-09. See References.

For FreeBSD 3.x:
Upgrade to the latest version of FreeBSD (3.5.1-STABLE dated after 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For FreeBSD 4.x:
Upgrade to the latest version of FreeBSD (4.1.1-STABLE dated after 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

For FreeBSD 5.x:
Upgrade to the latest version of FreeBSD (5.0-CURRENT dated 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

For Cisco IOS 11.x and 12.x:
Apply the latest patch for this vulnerability, as listed in Cisco Security Advisory: Cisco IOS Software TCP Initial Sequence Number Randomization Improvements. See References.

For Cisco CBOS 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7 and 2.3.8:
Upgrade to the latest version of CBOS (2.42 or later), as listed in Cisco Systems Field Notice, May 22, 2001. See References.

For other distributions:
Contact your vendor for upgrade or patch information.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.247			x.x.x.247: TrivialGuess: 24 out of 24 (100.00%)	91
x.x.x.250			x.x.x.250: TrivialGuess: 24 out of 24 (100.00%)	91
x.x.x.248			x.x.x.248: TrivialGuess: 23 out of 23 (100.00%)	91
x.x.x.249			x.x.x.249: TrivialGuess: 24 out of 24 (100.00%)	91

Vulnerability Name	Severity
Finger service (CVE-1999-0612)	Low

Description:

The finger service or daemon was detected as running. Finger can give an attacker information, such as logon accounts and trusted hosts. This information could be useful to an attacker in performing an attack.

Internet Scanner users: Please note that this check can potentially be time consuming, and may greatly increase the time required to perform a scan.

Fix

Disable finger, or install a finger service or daemon that limits the type of information provided.

Windows: The finger service is not native to Windows, but may be present. To stop or disable the service in Windows NT:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Open the Services control panel. From the Windows NT Start menu, select Settings, Control Panel, Services.
2. Select the service.
3. Click Stop.
4. When the service has stopped, click Startup.
5. Choose one of these options:
- To permanently disable the service, click Disabled.
- To turn the service off unless manually activated by the user or a program, click Manual.
6. Click OK, then click Close.

Unix: Disable the finger daemon or configure the type of information available from finger. Unix systems can use GNU finger available from the GNU finger 1.37 download site. See References.

To disable the finger daemon when started from inetd:
1. Edit the /etc/inetd.conf (or equivalent) file.
2. Locate the line that controls the daemon.
3. Type a # at the beginning of the line to comment out the daemon.
4. Restart inetd.
--OR--
For more information on GNU finger, download the compressed file from the GNU finger 1.37 download site. See References. You will need decompression and untarring utilities to use this file.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.244				91
x.x.x.241				91
x.x.x.242				91
x.x.x.243				91
x.x.x.246				91

Vulnerability Name	Severity
HTTP proxy detected	Low

Description:

A web (HTTP) proxy has been identified. Some older proxy servers may have vulnerabilities that let an attacker execute commands remotely. If the web proxy can be penetrated, it could lead to unauthorized access to the network.

Fix

Disable the service or review your proxy rules. See your firewall's documentation for more information.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Unix: Do not run your web server as a proxy. Refer to your web server's documentation, and disable the proxy, if possible.

Windows: From the Services control panel, disable the HTTP service:
1. Open the Services control panel. From the Windows NT Start menu, select Settings, Control Panel, Services.
2. Select the service.
3. Click Stop.
4. When the service has stopped, click Startup.
5. Choose one of these options:
- To permanently disable the service, click Disabled.
- To turn the service off unless manually activated by the user or a program, click Manual.
6. Click OK, then click Close.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.241				91
x.x.x.243				91

Vulnerability Name	Severity
HTTP server with unresolvable local links	Low

Description:

An unresolved link was detected. Web browsers will receive an error when accessing this link. This issue does not indicate a serious vulnerability, and is only noted as a courtesy.

Fix

Notify your Webmaster, since this dead link represents a bug in the web page.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.249		Port 80	Url missing: JavaScript:Help('http://help.networkprinters.com/n2825/en/java/s_gen.htm') Url referring: /TAState/0/s_gen.htm	91

Vulnerability Name	Severity
ICMP netmask request response	Low

Description:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A response was received to an Internet Control Message Protocol (ICMP) netmask request. By determining the netmasks of various computers in your network, an attacker can better map your subnet structure and infer trust relationships.

Fix

Configure your firewall or filtering router to block outgoing ICMP packets.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.247		N/A		91

Vulnerability Name	Severity
ICMP timestamp requests	Low

Description:

The target computer responded to an ICMP timestamp request. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

Fix

Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 13 or 14 and/or code 0.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.32	<printer name>			91
x.x.x.33	<printer name>			91
x.x.x.34	<printer name>			91
x.x.x.31	<printer name>			91

Vulnerability Name	Severity
Stock fingerd running (CVE-1999-0612)	Low

Description:

The finger service or daemon was detected as running. Finger can give an attacker information, such as login accounts and trusted hosts.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Fix

Disable finger, or install a finger daemon that limits the type of information provided.

Unix: Disable the finger daemon, or configure the type of information available from finger. Unix systems can use GNU finger available from the GNU finger 1.37 download site. See References.

To disable the finger daemon started from inetd:
1. Edit the /etc/inetd.conf (or equivalent) file.
2. Locate the line that controls the daemon.
3. Type a # at the beginning of the line to comment out the daemon.
4. Restart inetd.
--OR--
For more information on GNU finger, go to the GNU finger 1.37 download site. See References.

Windows: The finger service is not native to Windows, but may be present.

Note: The finger service may be included as part of another application, such as Netscape Mail Server.

CAUTION: Repeated use of finger can cause a system to become overloaded, which can cause it to stop responding. An attacker can use this susceptibility to disrupt the network.

To stop or disable the service in Windows NT:
1. Open the Services control panel. From the Windows NT Start menu, select Settings, Control Panel, Services.
2. Select the service.
3. Click Stop.
4. When the service has stopped, click Startup.
5. Choose one of these options:
- To permanently disable the service, click Disabled.
- To turn the service off unless manually activated by the user or a program, click Manual.
6. Click OK, then click Close.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.244			Integrated port Printer Type: Lexmark T622 Print Job Status: No Job Currently Active	91
x.x.x.242			Integrated port Printer Type: Lexmark T522 Print Job Status: No Job Currently Active	91
x.x.x.246			Integrated port Printer Type: Lexmark Optra W810 Print Job Status: No Job Currently Active Printer Status: 0 Ready	91

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

x.x.x.241	Integrated port Printer Type: Lexmark T520 Print Job Status: No Job Currently Active Service Device Error	91
x.x.x.243	Integrated port Printer Type: Lexmark T620 Print Job Status: No Job Currently Active	91

Vulnerability Name	Severity
Traceroute can be used to map network topologies	Low

Description:

Traceroute is a utility used to determine the path a packet takes between two endpoints. Traceroute does this by sending a series of packets with particular TTL (Time To Live) values and examining the ICMP replies seen.

Sometimes, when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall to gain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information.

Internet Scanner users: If traceroute is active on an internal network, this message does not represent a vulnerability. If tracerouting is possible through the firewall, your network is vulnerable.

Fix

Prevent or limit external tracerouting into internal networks using packet filtering.

Unix: The Unix version of Internet Scanner uses UDP packets to conduct a traceroute. Disallow incoming UDP packets with high-numbered destination ports. For more information, refer to your firewall documentation. ICMP packets are not found by Unix.

Windows NT: The Windows NT version of Internet Scanner uses ICMP to conduct a traceroute. Disallow incoming ICMP packets with high-numbered destination ports. For more information, refer to your firewall documentation. UDP packets are not found by Windows NT.

Note: Because the Unix and NT versions of Internet Scanner use different methods for traceroute, this vulnerability may occasionally be found by one version and not the other.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.32		<printer nbname>	Route: x.x.x.55 -> x.x.x.1 -> x.x.x.32	91
x.x.x.31		<printer name>	Route: x.x.x.55 -> x.x.x.1 -> x.x.x.31	91

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

x.x.x.33	<printer name>	Route: x.x.x.55 -> x.x.x.1 -> x.x.x.33	91
x.x.x.246		Route: x.x.x.55 -> x.x.x.1 -> x.x.x.246	91
x.x.x.34	<printer name>	Route: x.x.x.55 -> x.x.x.1 -> x.x.x.34	91

Vulnerability Name	Severity
Windows local user on workstation	Low

Description:

A local user account has been found on a non-domain controller. Some sites require that all user accounts on workstations and standalone servers be managed through the domain.

Fix

Remove the local user. To delete (permanently remove) a user account, follow the steps below appropriate for your platform.

For Windows NT:
1. Open User Manager. (From the Windows NT Start menu, select Programs, Administrative Tools (Common), User Manager.)
2. Select the local user from the list.
3. Press Delete and confirm the removal.

For a Windows 2000 domain:
1. Start Active Directory Users and Computers Management Console (dsa.msc) from a command prompt.
2. Double-click on the Users folder.
3. Right-click on the user of interest.
4. Select Delete to remove the user permanently.

For stand-alone Windows 2000 machines:
1. Start Local Users and Groups Management Console (lusrmgr.msc) from a command prompt.
2. Double-click on the User folder.
3. Right-click on the user of interest.
5. Select Delete to remove the user permanently.

IP Address	DNS Name	Additional Info	More Info	Session ID

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

x.x.x.32	<printer name>	TsInternetUser	91
x.x.x.33	<printer name>		91
x.x.x.34	<printer name>		91
x.x.x.31	<printer name>		91

Vulnerability Name	Severity
WWWBoard default administration accounts	Low

Description:

WWWBoard is a cgi based Web message board. It contains a default account that can be used for remote administration: WebAdmin / WebBoard. If not changed, remote users can access the message boards with full access.

Fix

Change the password to the WebAdmin account.

IP Address	DNS Name	Additional Info	More Info	Session ID
x.x.x.243		N/A		91
x.x.x.241				91

Technician **1**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Nessus Scan Report

Number of hosts which were alive during the test : 13
Number of security holes found : 14
Number of security warnings found : 45
Number of security notes found : 37

List of the tested hosts :

- x.x.x.32**(Security holes found)**
- x.x.x.31**(Security holes found)**
- x.x.x.247**(Security holes found)**
- x.x.x.248**(Security holes found)**
- x.x.x.249**(Security holes found)**
- x.x.x.250**(Security holes found)**
- x.x.x.34**(Security holes found)**
- x.x.x.33**(Security holes found)**
- x.x.x.241 **(Security warnings found)**
- x.x.x.243 **(Security warnings found)**
- x.x.x.246 **(Security warnings found)**
- x.x.x.242 **(Security warnings found)**
- x.x.x.244 **(Security warnings found)**

---

x.x.x.32 :

List of open ports :

- *netbios-ssn (139/tcp) (Security hole found)*
- *unknown (3460/tcp) (Security hole found)*
- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port netbios-ssn (139/tcp)

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

. All the smb tests will be done as "/"

Warning found on port netbios-ssn (139/tcp)

Here is the browse list of the remote host :
<printer names in extensive browse list –deleted->
This is potentially dangerous as this may help the attack
of a potential hacker by giving him extra targets to check for

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Solution : filter incoming traffic to this port
Risk factor : Low

Warning found on port netbios-ssn (139/tcp)

The host SID can be obtained remotely. Its value is :
<printer name>: 5-21-1606980848-299502267-725345543
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low

Vulnerability found on port unknown (3460/tcp)

It *may* be possible to make this web server execute
arbitrary code by sending it a too long argument to
a POST command.

Risk factor : High

Solution : Upgrade your web server.

Warning found on port unknown (3460/tcp)

a web server is running on this port

Information found on port unknown (3460/tcp)

The remote web server type is :
RADSTGMS/1.1
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Information found on port general/udp

For your information, here is the traceroute to x.x.x.32 :
x.x.x.1
x.x.x.32

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is
possible to predict the next value of the ip_id field of
the ip packets sent by this host.

An attacker may use this feature to determine if the remote
host sent a packet in reply to another request. This may be
used for portscanning and other things.

Solution : Contact your vendor for a patch
Risk factor : Low

Information found on port general/tcp

QueSO has found out that the remote host OS is
* WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch

CVE : CAN-1999-0454

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Warning found on port general/icmp

The remote host answers to an ICMP timestamp
request. This allows an attacker to know the
date which is set on your machine.

This may help him to defeat all your
time based authentifications protocols.

Solution : filter out the icmp timestamp
requests (13), and the outgoing icmp
timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

---

x.x.x.31 :

List of open ports :

- netbios-ssn (139/tcp) (Security hole found)
- unknown (3460/tcp) (Security hole found)
- general/udp (Security notes found)
- general/tcp (Security warnings found)
- general/icmp (Security warnings found)

Vulnerability found on port netbios-ssn (139/tcp)

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

. All the smb tests will be done as "/"

Warning found on port netbios-ssn (139/tcp)

Here is the browse list of the remote host :
<printer names in extensive browse list –deleted->
This is potentially dangerous as this may help the attack
of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port
Risk factor : Low

Warning found on port netbios-ssn (139/tcp)

The host SID can be obtained remotely. Its value is :
<printer name> : 5-21-117609710-2077806209-682003330
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low

Vulnerability found on port unknown (3460/tcp)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

It *may* be possible to make this web server execute
arbitrary code by sending it a too long argument to
a POST command.

Risk factor : High

Solution : Upgrade your web server.

Warning found on port unknown (3460/tcp)

a web server is running on this port

Information found on port unknown (3460/tcp)

The remote web server type is :
RADSTGMS/1.1
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Warning found on port general/tcp

The remote host uses non-random IP IDs…

Information found on port general/tcp

QueSO has found out that the remote host OS is
* WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch
CVE : CAN-1999-0454

Warning found on port general/icmp

The remote host answers to an ICMP timestamp
request…

x.x.x.247 :

List of open ports :

- *http (80/tcp) (Security hole found)*
- *unknown (631/tcp) (Security hole found)*
- *general/tcp (Security notes found)*
- *general/udp (Security notes found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port http (80/tcp)

The remote host seems to be vulnerable to the Cross Site Scripting vulnerability. The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request).
The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code.
Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high).

Solution:
Depending on the type of Web Server software install the appropriate patch, see the URLs below.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk Factor: Medium

Additional information:
IIS:
http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html

Allaire:
http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html

Apache:
http://www.apache.org/info/css-security/

General:
http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html

Information found on port http (80/tcp)

The remote web server type is :
Allegro-Software-RomPager/3.10
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Vulnerability found on port unknown (631/tcp)

The remote host seems to be vulnerable to the Cross Site Scripting vulnerability. The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request).
The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code.
Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high).

Solution:
Depending on the type of Web Server software install the appropriate patch, see the URLs below.

Risk Factor: Medium

Additional information:
IIS:
http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html

Allaire:
http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html

Apache:
http://www.apache.org/info/css-security/

General:
http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html

Warning found on port unknown (631/tcp)

a web server is running on this port

Information found on port unknown (631/tcp)

The remote web server type is :
Allegro-Software-RomPager/3.10

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

Information found on port general/tcp

Nmap found that this host is running VxWorks 5.3.x bases system (usually an ethernet hub or switch) or BayNetworks MicroAnnex XL term server

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request…

x.x.x.248 :

List of open ports :

- *http (80/tcp) (Security hole found)*
- *unknown (631/tcp) (Security hole found)*
- *general/tcp (Security notes found)*
- *general/udp (Security notes found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port http (80/tcp)

Vulnerability found on port unknown (631/tcp)

Warning found on port unknown (631/tcp)

a web server is running on this port

Information found on port unknown (631/tcp)

The remote web server type is :
Allegro-Software-RomPager/3.06b1
We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

Information found on port general/tcp

Nmap found that this host is running Accelerated Networks - High Speed Integrated Access VoDSL

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request…

x.x.x.249 :

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

List of open ports :

- *http (80/tcp) (Security hole found)*
- *unknown (631/tcp) (Security hole found)*
- *general/tcp (Security notes found)*
- *general/udp (Security notes found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port http (80/tcp)

Information found on port http (80/tcp)

Warning found on port unknown (631/tcp)

Information found on port unknown (631/tcp)

Information found on port general/tcp

Nmap found that this host is running Accelerated Networks - High Speed Integrated Access VoDSL

Warning found on port general/icmp

---

x.x.x.34 : (*big listening ports violator*)

List of open ports :

- *sunrpc (111/tcp)*
- *unknown (135/tcp)*
- *netbios-ssn (139/tcp) (Security hole found)*
- *microsoft-ds (445/tcp)*
- *unknown (1027/tcp)*
- *unknown (1034/tcp)*
- *unknown (1035/tcp)*
- *unknown (1037/tcp)*
- *unknown (1053/tcp)*
- *unknown (3372/tcp)*
- *unknown (3389/tcp)*
- *unknown (3460/tcp) (Security warnings found)*
- *unknown (3465/tcp)*
- *unknown (5000/tcp)*
- *unknown (6389/tcp)*
- *unknown (8007/tcp)*
- *unknown (9180/tcp)*
- *unknown (9188/tcp)*
- *unknown (9189/tcp)*
- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port netbios-ssn (139/tcp)

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

. All the smb tests will be done as "/"

Warning found on port netbios-ssn (139/tcp)

The host SID can be obtained remotely. Its value is :

<printer name> : 5-21-117609710-2077806209-682003330

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low

Warning found on port unknown (3460/tcp)

a web server is running on this port

Information found on port unknown (3460/tcp)

The remote web server type is :
RADSTGMS/1.1
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Warning found on port general/tcp

The remote host uses non-random IP IDs…

Information found on port general/tcp

QueSO has found out that the remote host OS is
* WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch

CVE : CAN-1999-0454

---

x.x.x.33 :

List of open ports :

- *netbios-ssn (139/tcp) (Security hole found)*
- *unknown (3460/tcp) (Security warnings found)*
- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*

Vulnerability found on port netbios-ssn (139/tcp)

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

. All the smb tests will be done as "/"

Warning found on port netbios-ssn (139/tcp)

The host SID can be obtained remotely. Its value is :

<printer name> : 5-21-117609710-2077806209-682003330

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low

Warning found on port unknown (3460/tcp)

a web server is running on this port

Information found on port unknown (3460/tcp)

The remote web server type is :
RADSTGMS/1.1
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Warning found on port general/tcp

The remote host uses non-random IP IDs…

Information found on port general/tcp

QueSO has found out that the remote host OS is
* WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch

CVE : CAN-1999-0454

---

x.x.x.241 :

List of open ports :

- *finger (79/tcp) (Security warnings found)*
- *http (80/tcp) (Security warnings found)*
- *unknown (631/tcp) (Security warnings found)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*
- *general/icmp (Security warnings found)*

Warning found on port finger (79/tcp)

The remote finger daemon accepts
to redirect requests. That is, users can perform
requests like :
finger user@host@victim

This allows crackers to use your computer
as a relay to gather information on another
network, making the other network think you

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

are making the requests.

Solution: disable your finger daemon (comment out
the finger line in /etc/inetd.conf) or
install a more secure one.

Risk factor : Low
CVE : CAN-1999-0105

Warning found on port finger (79/tcp)

There is a bug in the finger service
which will make it display the list of the accounts that
have never been used, when anyone issues the request :

finger .@target

This list will help an attacker to guess the operating
system type. It will also tell him which accounts have
never been used, which will often make him focus his
attacks on these accounts.

Solution : disable the finger service in /etc/inetd.conf, or
upgrade your finger daemon.

Risk factor : Medium
CVE : CAN-1999-0198

Warning found on port http (80/tcp)

The remote web server appears to be running with
Frontpage extensions.

You should double check the configuration since
a lot of security problems have been found with
FrontPage when the configuration file is
not well set up.

Risk factor : High if your configuration file is
not well set up
CVE : CVE-1999-0386

Warning found on port unknown (631/tcp)

a web server is running on this port

Warning found on port unknown (631/tcp)

The remote web server appears to be running with
Frontpage extensions.

You should double check the configuration since
a lot of security problems have been found with
FrontPage when the configuration file is
not well set up.

Risk factor : High if your configuration file is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

not well set up
CVE : CVE-1999-0386

Information found on port general/tcp

QueSO has found out that the remote host OS is
* Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

CVE : CAN-1999-0454

Warning found on port general/icmp

The remote host answers to an ICMP timestamp
request. …

This file was generated by Nessus, the open-sourced security scanner.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Superscan results on a HP4500N

```
* + x.x.x.x (IP Removed)
   |___   21  File Transfer Protocol [Control]
            |___ 220 JD FTP Server Ready..
   |___   23  Telnet
            |___ ...
   |___   80  World Wide Web HTTP
            |___ HTTP/1.0 200 OK..Server:HTTP/1.0..Content-Type:text/html....
   |___  280  http-mgmt
   |___  515  spooler
   |___ 9100  HP JetDirect Printer Server
```

Superscan results on a HP5000N

```
* + x.x.x.x (IP Removed)
   |___   21  File Transfer Protocol [Control]
            |___ 220 JD FTP Server Ready ..
   |___   23  Telnet
            |___ ...
   |___   80  World Wide Web HTTP
            |___ HTTP/1.1 200 OK ..Server: Agranat-EmWeb/R5_2_0..Content-Type:
text/html..Cache-Control: no-cache..Pragma: no-cache....
   |___  280  http-mgmt
   |___  515  spooler
   |___ 9100  HP JetDirect Printer Server
```

While a one-time scan will tell you the vulnerabilities you have today, periodic follow-up scans are highly recommended because new firmware upgrades, changes in configuration and software updates can exposed new holes that will need to be addressed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Scan Analysis

The next logical step is to do an analysis of the tool output data. You need to understand that when a tool finds "vulnerabilities" they are always "potential" vulnerabilities and may not be truly exploitable. Each item must be examined for validity and addressed if found valid. Here is an example of one basic vulnerability analysis focused on valid issues:

Level	Issue	IP	Port	Comments	Potential Mitigation
Serious	The remote printer has no password set.	252	23	This allows anyone to change its IP, thus to generate problems on your network.	Solution : telnet to this printer and set a password
High	It seems possible to overflow the remote MSQL cgi by making a request like : GET /cgi-bin/w3-msql/AAAA...AAAA	252	80	This allows an attacker to execute arbitrary code as the httpd server (nobody or root).	Disable webserver/ACL access
High	SNMP_Set guessed Community Name and changed system information	242, 243, 244, 245, 246, 247, 248, 249, 250, 252		SNMP_Set guessed Community Name and changed system information	If you need SNMP for network management, make sure it is properly configured with private community names.
High	There's a buffer overflow in the remote web server.	252	80	It is possible to overflow the remote web server and execute commands as user SYSTEM.	Upgrade or disable webserver
High	It may be possible to make the web server execute arbitrary code or crash by sending it a too authorization.	252	80		Upgrade or disable webserver.
High	This FTP server accepts any login/password combination.	252	21	Anyone can browse the FTP section of your disk without consent.	Disable FTP, passwords sent in clear
High	The remote FTP server closes the connection when one of the commands USER, PASS or HELP is given with a too long argument.	252	21	This probably due to a buffer overflow, which allows anyone to execute arbitrary code on the remote host. Attackers don't need an account to exploit this flaw.	Disable FTP server

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

High	It is possible to log into the remote FTP server as ' '/' '.	252	21	If the remote server is PFTP, then anyone can use this account to read arbitrary files on the remote host.	Disable FTP server
High	It is possible to get root privileges over FTP.	252	21	There is a backdoor in the old ftp daemons of Linux, which allows remote users to log in as 'NULL', with password 'NULL',	Disable FTP server
Medium	The remote host uses non-random IP IDs,	252, 31, 32, 247, 248, 249, 250, 245, 246, 241, 244, 242, 243, 251		It is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things	Contact your vendor for a patch
Medium	The remote host seems to be vulnerable to the Cross Site Scripting vulnerability.	247, 248, 249, 250	80	The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request). The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code.	Disable webserver.
Medium	There is a bug in the finger service	245, 246	79	It will display the list of the accounts that have never been used, when anyone issues the request: finger .@target This list will help attackers guess the operating system type. It will also tell them which accounts have never been used, which will often make them focus their attacks on these accounts.	Disable finger service

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Low	The Telnet service is running.	252	23	Anyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.	Disable telnet service.
Low	It is possible to connect directly on this port, and it is very likely that it is possible to make the printer print the data we will sent to it, thus overriding lpd authority.	252		An attacker may connect to this printer, force it to print pages of garbage, and make it run out of paper. If this printer is used relied on to print security logs, then this will be a problem.	Filter incoming traffic to this port.
Low	It was possible to log into the remote host using a NULL session	31, 32	139	The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access	Filter incoming traffic to this port.
Low	The remote host answers to an ICMP timestamp request.	31, 32, 247, 248, 249, 250, 245, 246, 241, 244, 242, 243	ICMP	This allows an attacker to know the date which is set on your machine. This may help defeat all time based authentifications protocols.	Disable service/filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).
Low	The remote finger daemon accepts to redirect requests.	245, 246, 241, 244, 242, 243	79	Users can perform requests like: finger user@host@victim. This allows crackers to use your computer as a relay to gather informations on another network, making the other network think you are making the requests.	Disable service/filter port
Low	The 'echo' port is open.	245, 246, 251	7	This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denial of service.	Disable service/filter port

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Low	The chargen service is running.	251	19	Chargen responds with some random (something like all the characters in the alphabet in row). It will continue spewing characters until the client closes the connection. An easy attack is 'pingpong' which IP spoofs a packet between two machines running chargen. They will commence spewing characters at each other, slowing the machines down and saturating the network.	Disable service/filter port
Warning	The FTP service allows anonymous logins.	252	21		Disable FTP

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After a thorough analysis we find that the majority of issues revolve around services provided by the printer manufactures that are intended to enhance workgroup type productivity with very little attention to impact on security. We see many webserver-based vulnerabilities exposed by the addition of web-based management facilities. Most often these services prove to be stripped-down versions of popular webservers that are at revision levels that have many well-known problems. We also see lots of exposed services that offer the malicious scanner from as little as configuration data to pathways such as FTP that can easily be exploited to reveal the contents of the hard disk storage facilities of the device.

3. Physical Analysis

This brings us to examining the device itself to see in what ways it stores and processes data. This analysis should involve intense scrutiny of the documentation provided and all technical references available for not only the printer, but also the devices it may use that are optional accessories such as a network interface. Many vendors provide their technical data via their Internet presence support areas:

Hewlett-Packard Printers: http://welcome.hp.com/country/us/eng/support.htm
Xerox Printers:
http://www.xerox.com/go/xrx/template/020.jsp?view=Support&Xcntry=USA&Xlang=en_US&Xseg=corp
Lexmark: http://support.lexmark.com/cgi-bin/jaguar/jaguar.cgi?ccs=229:1:0:0:0:0
Epson Printers: http://support.epson.com/

The key in dealing with these support sites is to not let the absence of available documentation deter you from your mission. Do not hesitate to call the support lines and query the support technicians until they give you the data you need. After enough pounding by security conscious consumers they should hopefully make the information more readily available. The absence of best practices and guidelines was a portion of the motivation behind the creation of this document. Although a valid point to the absence of such data or the limited access to this data to actual customers is that to a certain degree it limits the exposure of the security limitations and workarounds that can be devised with access to such documentation. The real answer should be that even if the documentation is available (and to think it isn't to anyone determined enough is ludicrous) the consumer should not be concerned if the device is properly configured and managed.

A few examples of things that should stand out in your physical analysis and that may help you realize how all-encompassing security analysis needs to be:

1. Internal hard disks that store queued or FTP'd document files that can be accessed by users and although it deletes "references to the file on the hard disk" [1] it leaves the actual file contents "on the hard disk drive until overwritten by the next job"[1] rather than deleting the entire contents. It is amazingly touted as a security feature.
2. Hardware configuration resets such as pressing a function button while powering up that resets the configuration of the printer to factory default settings allowing user manipulation.
3. Ribbons and Color film that are left with an imprint or can act as a stencil to recreate printed output.
4. Service access ports that may not have passwords enabled allowing complete access to printer storage and configuration.
5. Modem/Faxing functionality that may facilitate unauthorized transport of output from the facility.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Infrared (Ir) ports that may allow walk-by, unauthorized printing.
7. Vendor Maintenance personnel exposure to sensitive materials via user printing and hard disk access during scheduled maintenance and off-site repairs.
8. Unauthorized user access to printed output that might be waiting in the output bin.

[1] - DCInfoSecurityCertDocumentv2.pdf provided upon request from Xerox Corporation.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

B. Vulnerabilities examined.

While you find too many vulnerability listings specific to printers, what you need to focus on are the ones that are related to services that are incorporated in the specific printer. As we said earlier we have found telnet, FTP, and webserver services and researching the vulnerabilities common to these services will give us a feel for what will be security concerns. It stands to reason that if it is known that FTP authentication is passed unencrypted or "in clear text" between client and server that this vulnerability will exist in the FTP implemented in the printer. Denial of Service and information gathering exploits can also easily be transferred to the services involved.

Lets take a look at a Bugtraq listing detailing a vulnerability in add-on print-servers in some HP printers. You should notice this obvious example of the lack of attention to detail regarding security that most printer vendors have had until recent. The mentality of providing the benefits of technology without concern for potential security implications is far too common. Many printer and device configurations, which include security settings, can be too easily reset or negated by simple manipulation. Vendors have relied on a "you have to know how" attitude when all it takes is opening a on-line user-manual provided to the world by the Internet.

http://www.securityfocus.com/bid/3132

HP JetDirect JetAdmin is the installation and management software for HP's line of commercial print servers.

HP JetDirect devices configured using the JetAdmin web interface do not set a password for telnet access when the administrator password is chosen. As a result, the telnet port will be left exposed to unrestricted remote access. Remote users with malicious intent will be able to access the device to cause a denial of service, or potentially monitor printer activity to gather information that may be used to compromise systems.

Additionally, this problem is compounded by the fact that the admin password is reset when the device is rebooted.

Workaround: Set the telnet password manually.

Currently the SecurityFocus staff are not aware of any vendor-supplied patches for this issue. If you feel we are in error or are aware of more recent information, please mail us at: vuldb@securityfocus.com <mailto:vuldb@securityfocus.com>.

HP JetAdmin 4.0: HP JetAdmin 4.1.2: HP JetAdmin 5.1: HP JetAdmin 5.5: HP JetAdmin 5.5.177: HP JetAdmin 5.6: HP JetAdmin 6.0: HP JetAdmin 6.1: HP JetAdmin 6.2:

Credit:

This vulnerability was submitted to BugTraq on August 1st, 2001 by Will Backman <whb@ceimaine.org>.

References:

Message: Re: HP Jetdirect passwords don't sync http://www.securityfocus.com/archive/1/201224
Message: HP Jetdirect passwords don't sync http://www.securityfocus.com/archive/1/201160

Web page: HP JetAdmin Product Support Page http://www.hp.com/cposupport/nonjsnav/hpprinterm28673.html

You, as the reader, should be as amazed as the Author that as of the writing of this paper there is still no patch for this issue.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

III. Vulnerability Fixes and Risk Mitigation

A. What can be done to fix the problems?

Now that we have determined there really are problems and we have done our research we need to see what steps we can take to fix them. Our first look should be at what the manufacturer may have in the way of fixes or security setting suggestions. Below we can see what HP's website has to say about the issue covered in the last section.

http://www.hp.com/cposupport/networking/support_doc/bpj05999.html#P87_10006

They suggest we follow this list of steps.

Security step 1 - Upgrade the Jetdirect firmware to the highest level
Security step 2 - Specify a telnet password
Security step 3 - Disable all unused protocols
Security step 4 - Disable all unused print and management services
Security step 5 - Specify an SNMP set community name
Security step 6 - Specify an access control list

Basically they have the BugTraq workaround and a few other good suggestions that should be used unilaterally across all printer/print-server platforms. The latest firmware is most likely going to ensure you have access to the most configuration features and contain potential fixes. Specifying strong passwords is Security 101 item that everyone should know. Disabling unused protocols and print/management services is the best advice to give on any platform, not just printers. If you are not using it, why on earth expose yourself to the potential vulnerability?!?!

B. What can be done to lower the risk on things that can't be fixed?

The question to ask at this point is "Did I fix all the problems?", and nine times out of ten the answer will be "No". The next question that needs to be asked is "Given what remains is the risk acceptable?" and less security driven environments the answer may be "Yes". Unfortunately, in the Author's world it's not that easy. Some printers have imbedded NIC's that have SNMP functionality that cannot be disabled or configured (community name cannot be made private). FTP and web management services may be required and the exposed vulnerabilities are unacceptable. What can be done?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Mitigation Methods

Well from very recent experience one solution can be to severely limit the network access to the devices to management. In this extreme case scenario the implementation requires the use of a switch capable of implementing Virtual LAN's (VLAN's), Access Control Lists (ACL's), Port Security and the use of print-servers. The available ports and protocols that can be used between the Print Server and Printer VLAN's need to be controlled through Access Control List's (ACL's) and settings on the router. These ACL's will also prevent unauthorized traffic on to, and from, the Printer VLAN's.

Here is an example of how a problem and mitigation can be summarized for enterprise approval.

Problem
The Network Administrators cannot remotely manage printers without using HTTP. Lack of a remote printer management capability creates a very high cost on-site manpower and travel requirement. The SNMP community string protocols are written to the printer firmware and are required for most Xerox and Lexmark printers to operate.

> *· The HTTP configuration (as far as security) on most Xerox and Lexmark printers is minimal/non-existent.*
> *· Currently, HTTP port 80 and 631 have a medium risk issue (Cross Site Scripting) that must be mitigated.*
> *· SNMP public community string has a low risk issue that must also be mitigated.*

Background *– The use of HTTP and SNMP Public strings were identified during security scans conducted prior to implementation. The security analysts determined the need to develop a solution to limit port and protocol traffic and still allow the use and remote management of these printers at the growing number of enterprise sites.*

Mitigation
To mitigate these issues, network administration will implement an ACL on the router/switch on the Print Server/Printer VLAN. The ACL will protect the printers from external attack (probes, scans and possible exploit) much like a firewall blocking TCP traffic. This mitigation has been tested and passed in the development lab. Hardware addresses should be attained from all printers and print-servers and port security should be implemented at the switch to further secure these predominantly static networks.

The security analysts will conduct a follow-up scan and review of this Print Server/Printer VLAN mitigation solution plan in the development and production test labs. The Printer Solution and all related network architecture documents will be updated to reflect this change.

Recommendations
Final approval should be given for this Print Server/Printer VLAN ACL mitigated solution for remote printer management

A follow-up scan should be performed after all configuration and mitigation steps have been implemented to ensure that all issues have been properly addressed. It may take a few to get it right.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Physical Policy

The last step is to protect the physical environment. A solid, ever-evolving with new discovery and technology, physical policy needs to be in place to act as the law dictating the proper use of all devices including printers. You need to list out all of the specific considerations that must be made in the use of device. You must clearly outline methods of configuring and securing the device as well as keeping the data secure from the time it enters the device and even after it is printed. Here is a list of many of things that should be considered and answered by your policy:

- Is the area where the printer is located secure? Who has access? Can anyone walking by grab the output or manipulate the configuration settings? What must be in place to make the area secure? Locks? Cabinets? What prevents the printer default settings from being reset by a malicious individual?

- Is a "secure print" feature enabled? This is a feature that inhibits the printing of a document by anyone other than the person that sent the file. It does this by queuing the file until a PIN number is entered that was negotiated at the time it was sent by user to print.

- What is the procedure for accompanying maintenance personal when they are making repairs or maintaining the equipment? What procedure should be followed for wiping the data on the internal hard disk if the machine is to leave the building? What kind of checks and assurances are in place regarding the maintenance vendors?

- What is the policy for printed documents? How and where are they stored? What about the procedure for destroying sensitive documents and the ribbons (check your fax machine!!!!) and film (some color printers use this method) used to print them?

- What are your network implementation policies as detailed by your approved mitigations? It is good to note that the same analysis and fix/mitigation process can be followed in the physical real as well as the network.

C. What can be done for the future?

Now that we have addressed what we have we need to make a requirements document for future printer purchases. This document should be a checklist as to what functionality is desired, such as a "secure print" option, and be specific as to what can be items that eliminate a printer for selection such as non-configurable SNMP.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IV. Summary: What have we learned?

We set out to discover the potential security risks related to printers. We covered known vulnerabilities and more importantly the four step process of how to assess, fix, mitigate and attempt to prevent as many as possible when in the procurement process. We also presented the need for solid physical policy and how to view security comprehensively in the "big picture". Through the application of the basic processes discussed in the document, the reader should have a good portion of fundamentals needed to examine other peripheral devices. This document was not meant to be the end-all, but merely an eye-opening detail of experiences that opened the eyes of the Author.

[1] - DCInfoSecurityCertDocumentv2.pdf provided upon request from Xerox Corporation.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

V. Reference Section

DCInfoSecurityCertDocumentv2.pdf and Document Centre Security White Paper v1-17.pdf provided upon request from Xerox Corporation

http://www.hp.com/cposupport/networking/support_doc/bpj05999.html#P87_10006

BugTraq #3132 - http://www.securityfocus.com/bid/3132

The CERT® Coordination Center (CERT/CC) (www.cert.org)

Hewlett-Packard Printers: http://welcome.hp.com/country/us/eng/support.htm

Xerox Printers:
http://www.xerox.com/go/xrx/template/020.jsp?view=Support&Xcntry=USA&Xlang=en_US&Xseg=corp

Lexmark: http://support.lexmark.com/cgi-bin/jaguar/jaguar.cgi?ccs=229:1:0:0:0:0

Epson Printers: http://support.epson.com/

Software

Foundstone (www.foundstone.com) – Superscan 3.0

The "Nessus" Project (www.nessus.org) - Nessus 1.0.9

Internet Security Systems (www.iss.net) - ISS 6.2

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

VI. Test Questions

Multiple Choice Questions

1. All of the following can be used as part of an enterprise printing mitigation solution except:

a) VLAN
b) ACL
c) HIDS
d) Port Security

2. _____ provide the best first step in determining the potential network related printer vulnerabilities:

a) multimeters
b) scan tools
c) vendor web sites
d) network administrators

3. The four step process for securing printers and other network devices are:

a) discover, secure, mitigate and prevent
b) discover, fix, mitigate and prevent
c) assess, isolate, repair and prevent
d) assess, fix, mitigate and prevent

4. All of these are common printer vulnerabilities except:

a) web management interface
b) telnet
c) OSPF
d) FTP

5. A physical policy should be _____ .

a) ever-changing
b) ever-lasting
c) user-configurable
d) static-routed

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

True or False Questions

1. After the initial scan is performed, configurations are finalized and mitigation steps are implemented the printer is secure and a follow-up security scan is not necessary.

__ True
__ False

2. A physical policy should include all the steps necessary to secure a printer.

__ True
__ False

3. Manufacturer websites will have all the information you need to properly secure a printer.

__ True
__ False

4. The "secure print" option encrypts data from the user to printer and therefore provides a secure method of printing.

__ True
__ False

5. Any of the popular scan tools are complete and would be sufficient to determine printer vulnerabilities.

__ True
__ False

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Answers

Multiple Choice

1. c

2. b

3. d

4. c

5. a

True or False

1. False

2. True

3. False

4. False

5. False

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.