04/18/95

Preparing Your AIX System for SATAN

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

About This Document

This document from the AIX Security Response Team (security@austin.ibm.com) contains tips to help users prepare their systems for vulnerabilities probed by the tool called SATAN. This document applies to AIX 3.2 and 4.1.

Purpose of This Document

Everyone is becoming increasingly aware of computer security issues. No one wants to lose valuable information to unwanted intruders. The SATAN tool was developed to help system administrators secure all computers on their networks. The danger exists that this tool could be used for unlawful purposes.

We want to help AIX users secure their systems so SATAN will not cause any problems. This document is intended to help AIX users understand each of the vulnerabilities probed by SATAN and learn what they can do to secure their systems in each of these areas. Many books and articles have been written on computer security configuration issues and we will refer you to these articles when appropriate.

AIX Vulnerabilities Probed by SATAN

NFS Export to Unprivileged Programs

If the nfs mount daemon, rpc.mountd, is started with the -n flag it allows mount requests to come from non-privileged ports. This is used to allow some older versions of NFS to perform mounts. It should not be used. The AIX default is to not use the -n flag.

For additional security use the nfso utility to turn on kernel port checking. The command would be:

```
nfso -o nfs_portmon=1 (in AIX version 3 )
nfso -o portcheck=1   (in AIX version 4 )
```

The default in AIX is to NOT do kernel portchecking.

NFS Export via Portmapper

Access to file systems via portmapper is disabled by default in recent versions of AIX. To make sure you have a later version of portmapper that fixes this problem, check to make sure your machine has the fix for APAR IX32328. That fix has been included in PTFS U419992 U419994 U419995.

Use the following aix cmd to determine if you have applied these ptfs:

```
lslpp -al U419992 U419994 U419995
```

Unrestricted NFS Export

Entering a directory or filesystem in the /etc/export list without specifying an access list allows any host who's IP address can be resolved to mount the directory. This is not secure. The access list should be specified when exporting filesystem objects.

Exports specifying root access or read/write access also are inherently lower security and should be implemented with caution.

NIS Password File Access

The ability to view encrypted passwords when NIS is being used and the ability to exploit the information can be curtailed and to some extent prevented in a number of ways.

- Use a /var/yp/securenets file to restrict the NIS services to trusted networks. (see the notes on securenets below).
- Make the NIS domain name hard to guess and non-obvious. Employee turn-over or other security concerns may require domain renaming. (use the chypdom command or smit chypdom to change domain names and move the /var/yp/<domain_name> directory to the new name)
- Require users to use non-trivial passwords.

Use of the /var/yp/securenets file:

The implementation of ypserv and ypxfrd that utilize the securenets file was shipped in response to APAR ix32328 Some PTF's that contain that fix are: U419992 U419994 and U419995.

Use the following aix cmd to determine if you have applied these ptfs:

```
lslpp -al U419992 U419994 U419995
```

Both the "ypserv" and "ypxfrd" use a /var/yp/securenets file and, if present, only responds to IP addresses in the range given. This file is only read when the

daemons (both ypserv & ypxfrd) start. To get a change in /var/yp/securenets to take effect, one must kill and restart the daemons. The format of the file is one or more lines of:

```
netmask netaddr
```

For example:

```
255.255.0.0 128.30.0.0
255.255.255.0 128.311.10.0
```

In the second example, the netmask is 255.255.255.0 and the network address is 128.311.10.0 . This setup will only allow the ypserv to respond to those IP addresses which are within the subnet 128.311.10 range.

An additional NIS security note is that allowing ypset to reset ypbind binding lowers security. ypbind daemons shipped in the fix for APAR IX43595 (in PTF U431006) disallow ypset's as their default behavior and this is strongly recommended.

Use the following aix cmd to determine if you have applied this ptf:

```
lslpp -al U431006
```

Rexd Access

The rexd server allows users to execute commands on remote servers in an environment similar to that of the local system. No validation of identity or access permission is performed. This behavior leads many people to believe that the use of rexd is a security vulnerability.

There are currently no known defects in the rpc.rexd command which adversely affect the security of the system. rpc.rexd is contained in the bosnet.nfs.obj.client subsystem. The most recent PTF for that subsystem as of the writing of this document is U436781.

Use the following aix cmd to determine if you have applied this ptf:

```
lslpp -al U436781
```

The lack of authentication of the identity of the invoker may present a security exposure in an untrustworthy environment. You should weigh the risks of a security exposure against the functionality provided when you consider enabling this service.

The problems with rexd are inherent in the design of the server and cannot be corrected easily. The security problems can be limited by careful use of NFS exports on the client system and by disabling rexd on the server.

IBM issued CA-92:05 on March 5, 1992 describing a problem with the initial configuration of rexd on AIX 3.1 and AIX 3.2 systems. APAR IX21353 was opened to correct this problem. The problem corrected by this APAR no longer exists in AIX 3.2.5 or AIX 4.1.

In AIX 3.2.5 and 4.1 rexd is disabled by default when shipped.

Sendmail Vulnerabilities

All AIX versions of /usr/sbin/sendmail are vulnerable to some of the attacks described in CA-95:05. The official APARs resolving ALL known AIX sendmail vulnerabilities are IX49257 (version 3.2) and IX49604 (version 4.1).

AIX users should obtain the emergency patch from Internet ftp site software.watson.ibm.com. The file is located in /pub/aix/sendmail/sendmail.tar.Z in compressed tar format. Please follow the installation instructions in the sendmail.readme file located in this same directory.

Currently, AIX versions 3.2 and 4.1 are based on sendmail version 5.64. Although this is an old version of sendmail, all known sendmail security bugs are fixed by the emergency patch mentioned previously.

If you permit automatic mail forwarding or programs that accept mail messages, please be sure there is no way for these programs to create a shell or send commands. This type of configuration can create a security hole that could be exploited by an unfriendly user.

TFTP File Access

The tftpd server allows users to retrieve files without requiring an account on the remote server. Tftpd is commonly used by diskless systems and X-stations as well. Tftp does not require the use of a user name or password and therefore may grant access to system data when the identity of the requestor has not been established. This may allow unknown users to acquire restricted data or to modify user files.

There are currently no known defects in tftpd which adversely affect the security of the system. The tftpd command is contained in the bosnet.tcpip.obj.client subsystem. The most recent PTF for that subsystem as of the writing of this document is U435114.

The lack of any authentication or identification of the requestor should be considered when configuring tftpd. The tftp service may be restricted using the /etc/tftpaccess.ctl file. This file is documented in InfoExplorer under the tftpd command. This function was added to AIX v3.1 by APAR IX22628 and is available in the 2014 level PTF.

Tftp should be configured in /etc/inetd.conf to run as the user "nobody". The following line is an example of how to do this.

```
tftp    dgram   udp     wait    nobody  /etc/tftpd tftpd -n
```

This example will allow remote users to write files on the local system. If you have no requirement for granting write permission to remote users you should consider removing the "-n" flag from the command line given above.

The user "nobody" should own no files or directories on the system. The only files or directories which the user "nobody" should be able to read are those with read or write (and execute for directories) permission to "other". Refer to the chmod command in InfoExplorer for details on how to manage file and directory permissions. By properly restricting access to "other", you will effectively limit the files and directories which tftpd may access and modify.

IBM released CERT advisory CA:91-19 on October 17, 1991 for the tftpd daemon. The vulnerability described in that advisory is corrected in all releases of AIX v3.2 and AIX v4.

Remote Shell Access

The rsh and rlogin commands are used to establish sessions on remote servers. Both commands operate in a similar manner from an access perspective. The file /etc/hosts.equiv or a .rhosts file in the user's home directory may be consulted to determine if access is granted. When access is not automatically granted for the rlogin command the remote user is prompted for a password.

The rshd server has had one security related defect. APAR IX45182 corrected a defect in which the "-l" option (used to control operation of the server) did not work properly. This APAR was first delivered in PTF U432655. This PTF should be applied to any system which has been configured according to the instructions given below. This problem does not exist on any release of AIX v4.

The rlogind server has had one significant security related defect. APARs IX44254 and IX44367 corrected a defect in which any network user was able to gain access to the remote system as any user. These APARs were first delivered in PTFs U431620 and U431622 respectively. Both of these PTFs or their superceding PTFs should be installed on all systems. This problem does not exist on any release of AIX v4.

Two significant enhancements have been made to the rshd server. APAR IX45701 added a facility for restricting use of rshd and rexecd on a user by user basis. This feature may be useful for critical system accounts which might be subject to attack via a network connection. This APAR was first delivered in PTF U434068. APAR IX48235 added additional auditing capability. This feature may be useful when connecting to unsecure networks or when you are interested in monitoring rshd usage. A USER_Login audit event will be created for each rshd invocation. This may be used in conjunction with the TCPIP_access event to determine local user and remote hostname for each rshd and rexecd. As of the writing of this document this APAR has not been packaged into a PTF.

Both rshd and rlogind are subject to security violations related to use of the /etc/hosts.equiv and $HOME/.rhosts files. This exposure can be removed by adding the "-l" flag to the rshd and rlogind command lines in /etc/inetd.conf. The following two lines are an example of how you might do this.

```
shell    stream   tcp   nowait  root    /etc/rshd       rshd -l
login    stream   tcp   nowait  root    /etc/rlogind    rlogind -l
```

If you do not wish to grant remote network access to your system, you may disable this facility entirely with lines similar to the following.

```
#shell    stream   tcp   nowait  root    /etc/rshd       rshd
#login    stream   tcp   nowait  root    /etc/rlogind    rlogind
```

Please refer to InfoExplorer for additional information on configuring the /etc/inetd.conf file and the inetd daemon.

Should you choose to enable rshd and/or rlogind, the use of the /etc/hosts.equiv and $HOME/.rhosts files creates a dependency on the information in those files and the information which the servers use being accurate. Errors in either file or spoofing of host addresses or names are common causes of security exposures. When the network is not secure or trustworthy, consider disabling these services for some or all users or enabling the auditing subsystem to track possible attacks. You may also wish to consider use of a firewall or some other form of packet filter to restrict access to trustworthy hosts or networks.

InfoExplorer describes the proper configuration of the /etc/hosts.equiv file. As a general rule, grant access to specific users and specific hosts. You should monitor the existence of .rhosts files and insure that users are educated about their proper use.

The telnet service may be more appropriate in an unsecured network environment as it does not support the pre-authentication of users.

CERT advisory CA-94:09 was released on May 23, 1994 describing the security exposure in the rlogin service.

Use the following aix cmd to determine if you have applied one of these ptfs:

```
lslpp -al U43xxxx
```

Unrestricted X Server Access

In 1993 CERT issued advisory CA-93:17 which documented a xterm vulnerability in X11R5 and earlier versions of X11. This problem was resolved by the following apars:

```
aixterm X11r4 : ix34738 - resolved by U417488 and U419246
aixterm X11r5 : ix40275 - resolved by ptf U425631
xterm   X11r4 : ix40279 - resolved by ptf U425255 and U425228
xterm   X11r5 : resolved by U493250 (3.2.5 Gold)
```

Use the following aix cmd to determine if you have applied these ptfs:

```
lslpp -al U4xxxxx
```

If you are using AIX 3.2, please make sure you have all these ptfs applied to avoid potential security problems. These fixes are shipped as part of the GOLD version of AIX 4.1. Because of X11's design, the client/server can be accessed by any other host on the network. If you are on the Internet, your display can be accessed by any machine in the world. X11 security issues for AIX are similar to the X11 security problems facing other X11 vendors. It is difficult to make X completely secure. However, there are access control mechanisms which can be put in place to help make your environment more secure. You should never use the "xhost +" cmd because this will enable any remote user to read/write screen information. Please remove all "xhost +" cmds from any file or program on your system. For a useful tool for limiting X access, see the /usr/bin/xauth.

The best source of information on securing X is in : O'Reilly & Associates,Inc. "X Window System Adminstrator's Guide". Specifically chapter 4 which goes into detail about X security. The discussion in this chapter applies to the AIX environment. In additon, the Common Desktop Enviroment (CDE) interface available on AIX 4.1 uses XDMCP protocol discussed in this chapter.

Writable FTP Home Directory

In 1992, CERT issued advisory CA-92:09 about an AIX Anonymous FTP Vulnerability. This problem was resolved by apar ix23944, which was included in the GOLD release of AIX 3.2. Thus, AIX 3.2 and 4.1 systems are not vulnerable to this problem. The original problem was discovered on AIX 3.1. If you are running AIX 3.1, please update to the latest release of 3.1, which resolves this problem.

The following information can be very helpful:

- The ftpd man page has explicit instructions for securely configuring your anonymous FTP user and subtree.
- The /usr/lpp/samples/tcpip/anon.ftp file can be used to securely set up your anonymous account. (/usr/samples/tcpip/anon.ftp in AIX 4.1)
- The CERT tip found at ftp://info.cert.org/tech_tips/anonymous_ftp contains applicable information.

Wu-ftpd Vulnerability

This problem only affects users running the wuarchive-ftpd. If you do not have this modified version of ftpd, then you are not vulnerable to this specific attack. If you are running the wuarchive-ftpd, and your version is dated prior to April 8, 1993, please take corrective action or remove this daemon.

You can obtain more information about this service via anonymous ftp from wuarchive.wustl.edu (128.252.135.4).

This service is NOT distributed with AIX.

More Information on AIX Security

We publish an AIX security newsletter that is updated whenever we have security information that affects AIX users.

To subscribe to the newsletter:

```
mail -s "subscribe security" aixserv@austin.ibm.com < /dev/null
```

If you have comments or questions about AIX security, or you would like to notify us of a potential problem, please send mail to security@austin.ibm.com.

To order an APAR from IBM in the U.S. call 1-800-237-5511. APARs may be obtained outside the U.S. by contacting a local IBM representative.

More Information on Internet Security Topics

One of the best ftp sites for computer security information is ftp://coast.cs.purdue.edu/pub. You might also want to check out their WWW home page at http://www.cs.purdue.edu/coast. Their hotlist of other security home pages is also very helpful.

Other WWW sites with pointers to useful security info:

```
http://csrc.ncsl.nist.gov/first
http://ciac.llnl.gov
```

There are many listservers and newsgroups that are completely dedicated to the topic of computer security. You can find more information about these by looking at some of the WWW sites mentioned above.

CERT Advisory on SATAN

CERT Advisory
CA-95:06
April 3, 1995
Security Administrator Tool for Analyzing Networks (SATAN)

The CERT Coordination Center staff has examined beta version 0.51 of the Security Administrator Tool for Analyzing Networks (SATAN). This advisory contains information based on our review of this pre-release version. When the official release is available, we will distribute an updated advisory. SATAN is scheduled for release on April 5, 1995, at 14:00 GMT.

What is SATAN?

SATAN is a testing and reporting tool that collects a variety of information about networked hosts. The currently available documentation can be found at

```
ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z
```

SATAN gathers information about specified hosts and networks by examining network services (for example, finger, NFS, NIS, ftp, and rexd). It can then report this data in a summary format or, with a simple rule-based system, investigate potential security problems. Problems are described briefly and pointers provided to patches or workarounds. In addition to reporting vulnerabilities, SATAN gathers general network information (network topology, network services run, types of hardware and software being used on the network). As described in the SATAN documentation, SATAN has an exploratory mode that allows it to probe hosts that have not been explicitly specified. Thus, SATAN could probe not only targeted hosts, but also hosts outside your administrative domain.

Section 4 below lists the vulnerabilities currently probed by SATAN.

Potential Impact of SATAN

SATAN was designed as a security tool for system and network administrators. However, given its wide distribution, ease of use, and ability to scan remote networks, SATAN is also likely to be used to locate vulnerable hosts for malicious reasons. It is also possible that sites running SATAN for a legitimate purpose will accidentally scan your system via SATAN's exploratory mode.

Although the vulnerabilities SATAN identifies are not new, the ability to locate them with a widely available, easy-to-use tool increases the level of threat to sites that have not taken steps to address those vulnerabilities. In addition, SATAN is easily extensible. After it is released, modified versions might scan for other vulnerabilities as well and might include code to compromise systems.

How to Prepare for the Release of SATAN

- Examine your systems for the vulnerabilities described below and implement security fixes accordingly.
- In addition to reading the advisories cited for specific vulnerabilities below, consult the following documents for guidance on improving the security of your systems:

  ```
  ftp://info.cert.org/tech_tips/security_info
  ftp://info.cert.org/tech_tips/anonymous_ftp
  ftp://info.cert.org/tech_tips/packet_filtering
  ```

- Contact your vendor for information on available security patches, and ensure that all patches have been installed at your site.
- Use the tools listed in Section 5 to assist you in assessing and improving the security of your systems.

Vulnerabilities Probed by SATAN

Listed below are vulnerabilities that beta version 0.51 of SATAN tests for, along with references to CERT advisories and other documents where applicable.

Administrators should verify the state of their systems and perform corrective actions as necessary. We cannot stress enough the importance of good network configuration and the need to install all available patches.

1. NFS export to unprivileged programs
2. NFS export via portmapper
3. Unrestricted NFS export

   See CERT advisory CA-94:15 and CA-94:15.README for security measures you can take to address NFS vulnerabilities.

   The following advisories also address problems related to NFS:

   ```
   CA-94:02.REVISED.SunOS.rpc.mountd.vulnerability
   CA-94:02.README
   CA-93:15.SunOS.and.Solaris.vulnerabilities
   CA-92:15.Multiple.SunOS.vulnerabilities.patches
   CA-92:12.REVISED.SunOS.rpc.mountd.vulnerability
   CA-91:21.SunOS.NFS.Jumbo.and.fsirand
   ```

4. NIS password file access

   See CERT advisory CA-92:13 for information about SunOS 4.x machines using NIS, and CA-93:01 for information about HP machines.

5. rexd access

   We recommend filtering the rexd service at your firewall and commenting out rexd in the file /etc/inetd.conf.

   See CERT advisory CA-92:05 for more information about IBM AIX machines using rexd, and CA-91:06 for information about NeXT.

6. Sendmail vulnerabilities

   See CERT advisory CA-95:05 and CA-95:05.README for the latest information we have published about sendmail.

7. TFTP file access

   See CERT advisory CA-91:18 for security measures that address TFTP access problems. In addition, CA-91:19 contains information for IBM AIX users.

8. Remote shell access

   We recommend that you comment out rshd in the file /etc/inetd.conf or

   protect it with a TCP wrapper.

9. Unrestricted X server access

We recommend filtering X at your firewall. Additional advice about packet filtering is available by anonymous FTP from

```
ftp://info.cert.org:/pub/tech_tips/anonymous_ftp
```

10. Writable FTP home directory

    See CERT advisory CA-93:10. Guidance on anonymous FTP configuration is also available from

    ```
    ftp://info.cert.org:/pub/tech_tips/anonymous_ftp
    ```

11. Wu-ftpd vulnerability

    See CA-93:06, CA-94:07, and CA-94:07.README for more information about ftpd.

Note: In addition to our FTP archive at info.cert.org, CERT documents are available from the following sites, and others which you can locate by using archie:

```
ftp://coast.cs.purdue.edu:/pub/mirrors/cert.org/cert_advisories
ftp://unix.hensa.ac.uk:/pub/uunet/doc/security/cert_advisories
ftp://ftp.luth.se:/pub/misc/cert/cert_advisories
ftp://ftp.switch.ch:/network/security/cert_advisories
ftp://corton.inria.fr:/CERT/cert_advisories
ftp://ftp.inria.fr:/network/cert_advisories
ftp://nic.nordu.net:/networking/security/cert_advisories
```

Currently Available Tools

The following tools are freely available now and can help you improve your site's security before SATAN is released.

COPS and ISS can be used to check for vulnerabilities and configuration weaknesses. COPS is available from:

```
ftp://info.cert.org:/pub/tools/cops/*
```

ISS is available from:

```
ftp://ftp.uu.net:/usenet/comp.sources.misc/volume39/iss
```

CERT advisory CA-93:14 and CA-93:14.README contain information about ISS.

TCP wrappers can provide access control and flexible logging to most network services. These features can help you prevent and detect network attacks. This software is available by anonymous FTP from:

```
ftp://info.cert.org:/pub/tools/tcp_wrappers/*
```

The TAMU security package includes tools to check for vulnerabilities and system configuration weaknesses, and it provides logging and filtering of network services. This software is available by anonymous FTP from:

```
ftp://net.tamu.edu:/pub/security/TAMU/*
```

The Swatch log file monitor allows you to identify patterns in log file entries and associate them with actions. This tool is available from:

```
ftp://ee.stanford.edu:/pub/sources/swatch.tar.Z
```

Detecting Probes

One indication of attacks by SATAN, and other tools, is evidence of a heavy scan of a range of ports and services in a relatively short time. Many UNIX network daemons do not provide sufficient logging to determine if SATAN is probing the system. TCP wrappers, the TAMU tools, and Swatch can provide the logging you need.

Using SATAN

Running SATAN on your systems will provide you with the same information an attacker would obtain, allowing you to correct vulnerabilities. If you choose to run SATAN, we urge you to read the documentation carefully. Also, note the following:

- It is easy to accidentally probe systems you did not intend to. If this occurs, the probed site may view the probe(s) as an attack on their system(s).
- Take special care in setting up your configuration file, and in selecting the probe level when you run SATAN.
- Explicitly bound the scope of your probes when you run SATAN. Under "SATAN Configuration Management," explicitly limit probes to specific hosts and exclude specific hosts.
- When you run SATAN, ensure that other users do not have read access to your SATAN directory.
- In some cases, SATAN points to CERT advisories. If the link does not work for you, try getting the advisories by anonymous FTP.

Getting More Information about SATAN

As noted above, SATAN documentation is available from:

```
ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z
```

Additional documents are available through a mail server set up by one of the authors.

Send mail to:

```
majordomo@wzv.win.tue.nl
```

Put the following text in the body (not in the subject line):

```
get satan mirror-sites
get satan release-plan
get satan description
get satan admin-guide-to-cracking.101
```

The last document contains "Improving the Security of Your Site by Breaking Into It," a 1993 paper in which the authors give their rationale for creating SATAN.

The CERT Coordination Center staff thanks Dan Farmer and Wieste Venema for the the opportunity to examine pre-release versions of SATAN. We also appreciate the interaction with the response teams at AUSCERT, CIAC, and DFN-CERT, and feedback from Eric Allman.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the e-mail be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT staff for details).

```
Internet E-mail: cert@cert.org
Telephone: +1 412-268-7090 (24-hour hotline)
   CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
   and are on call for emergencies during other hours.
Fax: +1 412-268-6989
Postal address:  CERT Coordination Center
                 Software Engineering Institute
                 Carnegie Mellon University
                 Pittsburgh, PA 15213-3890
                 USA
```

CERT advisories and bulletins are posted on the USENET newsgroup comp.security.announce. If you would like to have future advisories and bulletins mailed to you or to a mail exploder at your site, please send mail to cert-advisory-request@cert.org.

Past advisories, CERT bulletins, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from info.cert.org.

Copyright Notice

Copyright 1995 Carnegie Mellon University This material may be reproduced and distributed without permission provided it is used for noncommercial purposes and the copyright statement is included.

CERT is a service mark of Carnegie Mellon University.

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (satan.tips.cmd, 4FAX# 3199)