CERT Advisory CA-1995-06 Security Administrator Tool for Analyzing Networks (SATAN)

Original issue date: April 3, 1995
Last revised: September 23, 1997
Updated Copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center staff examined beta version 0.51 of the Security Administrator Tool for Analyzing Networks (SATAN). This advisory initially contained information based on our review of this pre-release version. When the official release became available, we updated the advisory based on version 1.1.1.

1. 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.

After the release of SATAN 1.0, we published a separate advisory describing a vulnerability in SATAN. If you do not already have a copy of CA-95.07a, we strongly urge you to obtain a copy from

www.cert.org/advisories/CA-95.07a.REVISED.satan.vul.html

As we receive new information about SATAN, we will update advisories CA-95.06 (SATAN in general) and CA-95.07a (vulnerability in SATAN). We encourage you to check our advisories regularly for updates to relating to your site.

2. 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.

3. 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://ftp.cert.org/pub/tech_tips/intruder_detection_checklist
  ftp://ftp.cert.org/pub/tech_tips/UNIX_configuration_guidelines
  ftp://ftp.cert.org/pub/tech_tips/anonymous_ftp_config
  ftp://ftp.cert.org/pub/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.

4. 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 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-93.15.SunOS.and.Solaris.vulnerabilities
   CA-92.15.Multiple.SunOS.vulnerabilities.patched
   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 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. A TCP/IP wrapper program is available from
   ftp://ftp.cert.org/pub/tools/tcp_wrappers/
9. Unrestricted X server access
   We recommend filtering X at your firewall. Additional advice about packet filtering is available by anonymous FTP from
   ftp://ftp.cert.org/pub/tech_tips/packet_filtering
10. Writable FTP home directory
    See CERT advisory CA-93.10.
    Guidance on anonymous FTP configuration is also available from
    ftp://ftp.cert.org/pub/tech_tips/anonymous_ftp_config
11. wu-ftpd vulnerability
    See CA-93.06 and CA-94.07 for more information about ftpd.
12. Unrestricted dial-out modem available via TCP.
    Place modems behind a firewall or put password or other extra authentication on them (such as S/Key or one-time passwords). For information on one-time passwords, see CERT advisory CA-94.01, Appendix B.

Note: In addition to our FTP archive at ftp.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

5. 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//ftp.cert.org:/pub/tools/cops/*

ISS is available from
ftp://ftp.uu.net/usenet/comp.sources.misc/volume39/iss
CERT advisory CA-93.14 contains 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://ftp.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

6. 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.

New tools are becoming available on the network to help you detect probes, but the CERT staff has not evaluated them.

Although detection tools can be helpful, keep in mind that their effectiveness depends on the nature and availability of your logs and that the tools may become less effective as SATAN is modified. The most important thing you can do is take preventive action to secure your systems.

7. 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.
- Install all relevant security patches for the system on which you will run SATAN.
- Ensure that the SATAN directory tree cannot be read by users other than root.
- Execute SATAN only from the console of the system on which it is installed (e.g., do not run SATAN from an X terminal, from a diskless workstation, or from a remote host).
- Ensure that the SATAN directory tree is not NFS-mounted from a remote system.
- It is best to run SATAN from a system that does not support multiple users.

8. Getting more information about SATAN

The SATAN authors report that SATAN 1.1.1 is available from many sites, including:

ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.README
ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan_doc.README

To get a current list of sites, send mail to:

majordomo@wzv.win.tue.nl

and put in the body of your message

get satan mirror-sites

You can also use archie to locate sites that have SATAN.

MD5 checksums for SATAN:

satan-1.1.1.README = 3f935e595ab85ee28b327237f1d55287
satan-1.1.1.tar.Z = de2d3d38196ba6638b5d7f37ca8c54d7
satan-1.1.1.tar.Z.asc = a9261070885560ec11e6cc1fe0622243
satan_doc.README = 4ebe05abc3268493cdea0da786bc9589
satan_doc.tar.Z = 951d8bfca033eeb483a004a4f801f99a
satan_doc.tar.Z.asc = 3216053386f72347956f2f91d6c1cb7c

Also available is "Improving the Security of Your Site by Breaking Into It" (admin-guide-to-cracking.101), 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.

UPDATES

Note to users of LINUX SATAN: There was a posting to USENET that a Trojan horse was introduced into a version of LINUX SATAN binaries archived on ftp.epinet.com. CERT staff have not verified that this Trojan horse exists; however, if you are using LINUX SATAN and believe your version may be compromised, we suggest you obtain additional information from

ftp://ftp.epinet.com/pub/linux/security

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted into
               the advisory. Updated tech tip references.
Apr. 11, 1995  Updated information based on SATAN 1.1.1 (original advisory
               was based on beta version 0.51):
                 Introduction - added reference to CA-95.07a
                 Sec. 4 - added information on SATAN probe for unrestricted
                          modems
                 Sec. 6 - added a note on tools for detecting probes
                 Sec. 7 - added five additional precautions
                 Sec. 8 - where to get a copy of SATAN
                          checksums for SATAN and documentation
                          where to send comments about SATAN
Apr. 11, 1995  Sec. 3 - pathnames corrected in Sec. 3
               Sec. 4-5 - colons noted in (and subsequently removed from) URLs
Apr. 11, 1995  Updates section - added a note on LINUX SATAN
```