SATAN

Security Administrator’s Tool for Analyzing Networks

Overview and Installation
{Running the SATAN Security Tool under Linux}

© by stan reichardt
St.Louis UNIX Users Group
Introduction

- SCOPE: Very simple tutorial for the un-initiated.
- LEARN: About SATAN security software and installation on a Linux PC.
- CONSIDER: Audience's needs and level of proficiency.
Agenda

Topics:
- About SATAN
- Installing SATAN

Schedule:
- Disclaimer
- Query Audience
- Overview
- Terms and definitions
- About SATAN
- Installing SATAN
- Related/Further Information
- Summary
Overview

PROBLEM:
General Lack of Sys Admin Security Knowledge

APPROACH:
Freely available teaching tool

Written by Wietse Venema & Dan Farmer

(ftp sites & mirrors will be given later)
Terms and Definitions

- **SATAN** - remote network auditing tool
- **SANTA** - nice name for above
- **Hacker** - expert computer explorer
- **Cracker** - short for system cracker
- **Security** - warm and fuzzy
- **Trojan Horse** - does unexpected things
About SATAN

- Explain the topic in detail:
  - who
  - what
  - where
  - when
  - why
  - how
Who wrote SATAN

- Wietse Venema
  - formerly @ Eindhoven Univ of Tech
  - author TCP Wrapper
  - numerous security papers

- Dan Farmer
  - worked on COPS @ Carnegie Mellon U
  - formerly with SUN Inc.
What does SATAN do

- scans for erroneous configurations
- scans for known software errors
- outputs warning message with explanation of WHY there is a problem and provides info on how to correct problems
- provides GUI output
- provides tutorial documentation
What does SATAN not do

- NOT for ordinary user
- NOT silent – easily detected
- NOT without solutions
- NOT really an attack tool
Where SATAN...

- was written
- is used
- is available  (more later)
When was SATAN written

- released April 5th 1995
- Current version 1.1.1
- update?
Why write SATAN

GOAL - to provide a tool that conducted Network Security audits and offers tips for correcting frequent vulnerabilities
How was SATAN done

- source code
- C language
- perl 5.001+
- modular design (modify & extend)
Installing SATAN

/ Explain the topic in detail:
/ requirements
/ process
/ results
Prep for SATAN

- UNIX operating system
- minimum hardware (color monitor)
- root authority
- X Windows
- WWW browser
- network connection
- source code
- C compiler & Perl 5.001+
Compiling SATAN

- general procedure
  - run the "reconfig" script
  - run the "make" command
  - If behind firewall
    - unset proxy environment variables
    - configure browser
      - to NOT use SOCKS
      - to NOT use HTTP proxy
  - run the "satan" script in a xterm
Compiling SATAN

- special LINUX problems
  - originally not quite "standard"
  - missing items...
  - patch files
- special NETSCAPE problems
  - need current release
  - disable pearl helper
Compiling SATAN

- hostname MUST match in files:
  - /etc/hosts
  - /etc/HOSTNAME (may not exist)

- trouble shooting
  - run "dmesg"
  - view /var/log/secure file
  - run "script" to capture responses
Resulting SATAN

- precautions
- running program
- interpreting results
Related Information

\- Documentation:
  \- Readme file
  \- Protecting Networks With SATAN by Martin Freiss – O'Reilly
    {105 pgs}
  \- Hacker Proof by Lars Klander – Jamsa Press {15 pgs}
  \- Maximum Security by Anonymous – Sams.net Pub. {5 pgs}

\- Other related training:
  \- rs.internic.net/nic-support/15min {free}
  \- www.data.com/Tutorials {free}
  \- www.cbt.sys.com – TCP/IP course {$$$$$}
For Further Information

Other Books

- Unix System Security by Rik Farrow - Addison Wesley {'91}
- TCP/IP Network Admin by Craig Hunt - O'Reilly {'92}
- Computer Crime by Icove, Seger & VonStorch - O'Reilly {'95}
- Practical UNIX & Internet Security (2nd Ed) by Simpson Garfinkle & Gene Spafford - O'Reilly {'96}
- The Cuckoo's Egg by Cliff Stoll - Pocket Books/Bantam {'89}
- Terminal Compromise {'93?} /archive/doc/misc/termcomp.zip
- Wyrm by Mark Fabi - Bantam {Science Fiction '98}

Magazine Articles:

- Scientific American - Oct '98 "How Hackers Break In..."
- Sys Admin - Jan '99 "Freeware-Based Security"
Other Resources:

Consulting services -- ?

World Wide Web sites:
- http://wzv.win.tue.nl/satan/
- http://www.cs.purdue.edu/coast/
- http://www.infilsec.com/vulnerabilities/

Newsgroups:
- comp.security_unix
- comp.os.linux
Other Software

- SAINT - Security Administrator's Integrated Network Tool
- COPS - Computer Oracle Password & Security
- ISS - Internet Security Scanner
- Courtney - SATAN detector
- Gabriel - SATAN detector
- Strobe -
- NSS - Network Security Scanner
- identTCPscan -
- Jakal -
- Netlog -
- NETMAN -
- NID - Network Intrusion Detector - *req DES key from DOE*
- NOCOL - Network Operations Center Online
- SPI-NET - Security Profile Inspector for Networks
Summary

- Recap the key points
- Suggestions and observations
- Questions, comments and other feedback on these materials to: stan@michelob.wustl.edu