Rechnernetze

Security Tools: SATAN

Bernd Lehle / Oliver Reutter

Security Tools: SATAN

Bernd Lehle / Oliver Reutter

In letzter Zeit tauchte das Thema Sicherheit immer wieder in allen möglichen Schlagzeilen auf und sorgte stellenweise für größere Unruhe. Auch an der Universität Stuttgart wurden bereits einzelne Rechner Opfer von elektronischen Eindringlingen, die sich über das Netz unerlaubten Zugriff verschafft hatten. Damit die Systembetreuer hier auf dem Campus dieser wachsenden Bedrohung leichter begegnen können, haben wir uns entschlossen, eine Artikelserie zu starten, die mit zuverlässigen Informationen und handfesten Rezepten Hilfestellung leis-ten soll. Den Anfang macht ein Bericht über das wohl bekannteste Tool, das dem Systembetreuer zur Verfügung steht - SATAN.

Die Geschichte von SATAN

SATAN steht für Security Administrator Tool for Analyzing Networks (Wer mit diesem Namen Probleme hat, kann es mit einem perl-Skript leicht in SANTA umbenennen, was Security Analysis Network Tool for Administrators heißt).

Die geistigen Väter dieses Tools sind in der Netzwerk-Security-Gemeinde keine unbeschriebenen Blätter. Dan Farmer, ein junger Amerikaner mit feuerroten langen Locken hat sich durch das Sicherheitspaket cops einen Namen gemacht. Er war Sicherheitsberater bei Sun, ging dann zu Silicon Graphics, wo er nach der Veröffentlichung von SATAN wieder gehen mußte und ist jetzt wieder bei Sun. Wietse Venema ist ein holländischer Kernphysiker, der äußerlich durch ein geheimnisvoll-verschmitztes asiatisches Lächeln auffällt. Er arbeitet an der Technischen Universität Eindhoven; sein bekanntestes Sicherheitsprodukt ist der tcp-Wrapper, mit dem man Netzwerkverbindungen leicht regulieren und mitprotokollieren kann. Der tcp-Wrapper wird in der nächsten Ausgabe unserer Benutzerinformationen genauer beschrieben.

Die gemeinsame Arbeit der beiden reicht weit zurück: Als erstes gemeinsames Produkt erschien im Dezember 1993 der Admin`s Guide to Cracking, ein knapp 20-seitiges Dokument, das einem Systemverwalter helfen soll seine Maschinen abzusichern, indem er sie durch die Augen eines Eindringlings betrachtet. In diesem Text wurde SATAN erstmals angekündigt.

Im Januar 1995 war dann der Kern von SATAN geschaffen und der 5. April 1995 wurde als Datum für die erste Veröffentlichung festgelegt. Im Vorfeld wurde gleichzeitig umfangreiche Dokumentation verteilt. Die eigentliche Veröffentlichung wurde sorgsam geplant und vorbereitet.

Interessanterweise erzeugte die Ankündigung von SATAN in den USA einen starken Medienrummel und selbst angesehene Blätter wie die New York Times zeichneten Schreckensbilder von Hacker-Heeren, die nun per Knopfdruck in bisher sichere Rechner einbrechen und prophezeiten wieder einmal das Ende des Internets. Seit der Veröffentlichung wurden allerdings keine erhöhten Einbruchaktivitäten festgestellt, die auf SATAN zurückzuführen sind. Im Vergleich dazu legte im November 1988 der Internet-Wurm von Robert Morris das komplette, damals noch auf die USA beschränkte Internet für einige Tage lahm.

Wietse Venema kommentierte den Presserummel mit den Worten: "Free publicity is worth every penny You pay for it." :-)

SATAN-Installation

Um SATAN auf der eigenen Workstation benutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Etwa 4 MByte Speicher auf der Festplatte im gewünschten Filesystem
- Perl 5.000 oder später sollte entweder lokal oder in /sw installiert sein
- Aus Sicherheitsgründen sollte der gewünschte WWW-Browser (Netscape, Mosaic, Lynx) lokal installiert sein
- Man muß das root-Passwort besitzen.

Die aktuellen Quellen besorgt man sich am besten aus:

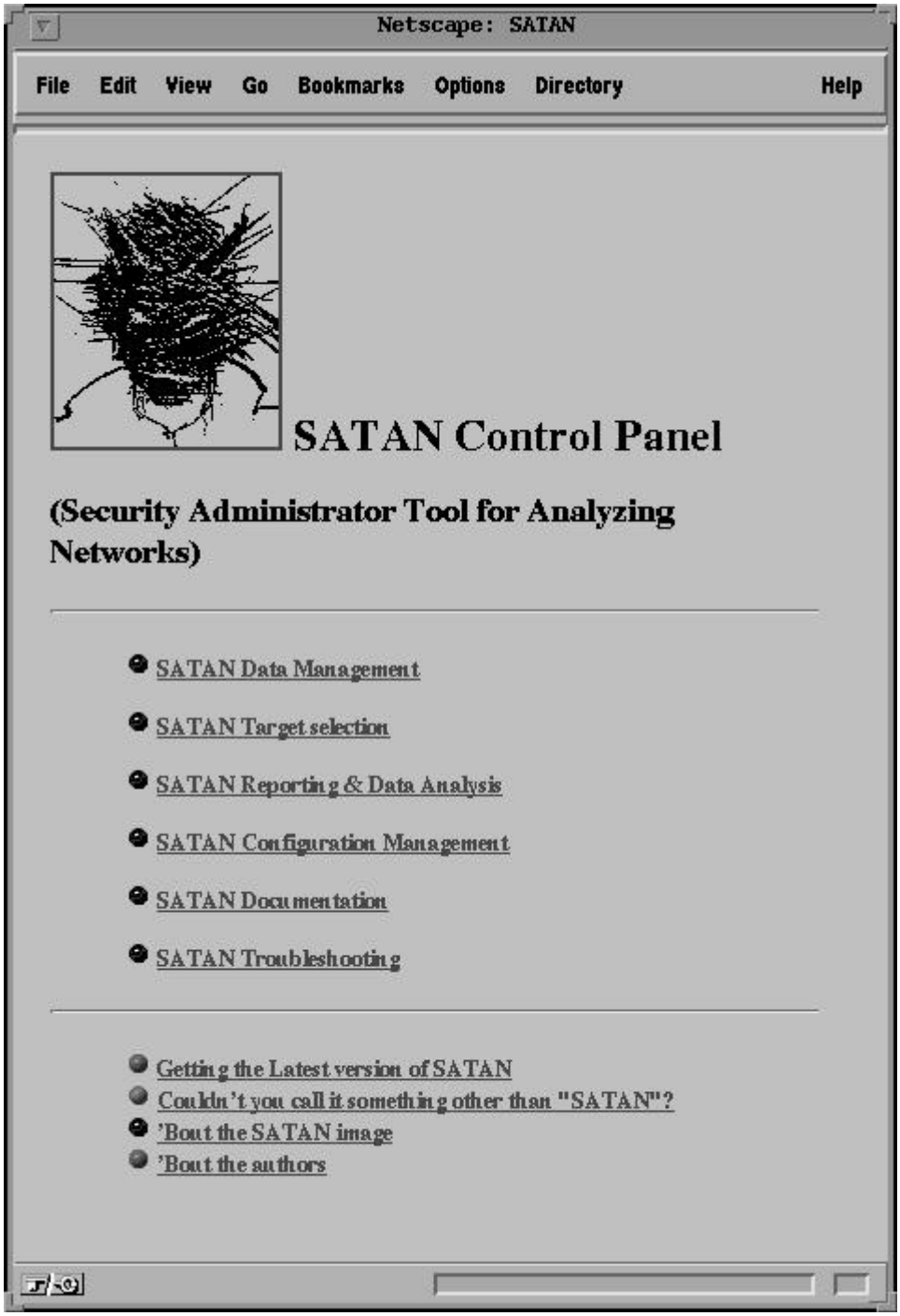
`ftp.uni-stuttgart.de : /pub/unix/security`
`ftp.cert.dfn.de : /pub/tools/net/satan`

Das Script `reconfig` sollte nach dem Auspacken des Quellcodes mit dem Befehl `compress -d < satan-1.1.1.tar.Z|tar xvf -` gestartet werden. Es bestimmt die Pfade benötigter Kommandos und trägt sie in die entsprechenden Programme ein. Wird der gewünschte WWW-Browser von SATAN nicht gefunden, muß er in der Datei `satan-1.1.1/config/paths.pl` in der Zeile `$MOSAIC="program_name";` von Hand ergänzt werden. Abschließend muß nur noch das Kommando `make` ausgeführt werden. `make` fragt nach dem verwendeten Betriebssystem und übersetzt danach die Quellen. Damit ist die Installation eigentlich abgeschlossen.

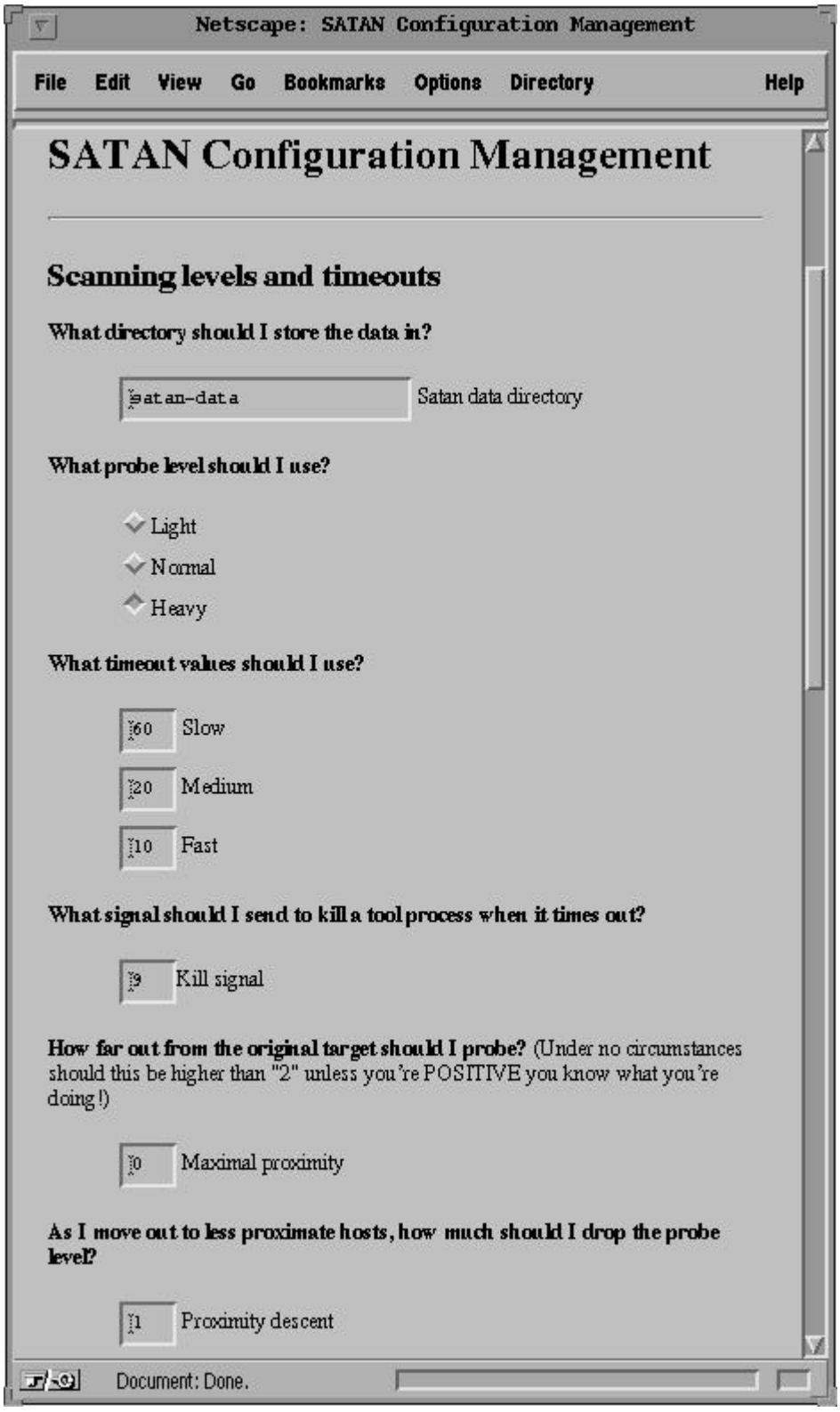
Nun kann SATAN von der Kommandozeile aus gestartet werden. Wird SATAN ohne Parameter aufgerufen, startet er eine WWW-Browser Session. Die Kommandozeilen- optionen stehen in `satan.8` im üblichen `nroff -man`-Format.

SATAN-Konfiguration

Nach dem Start von SATAN erscheint das Hauptmenü (**SATAN Control Panel**):

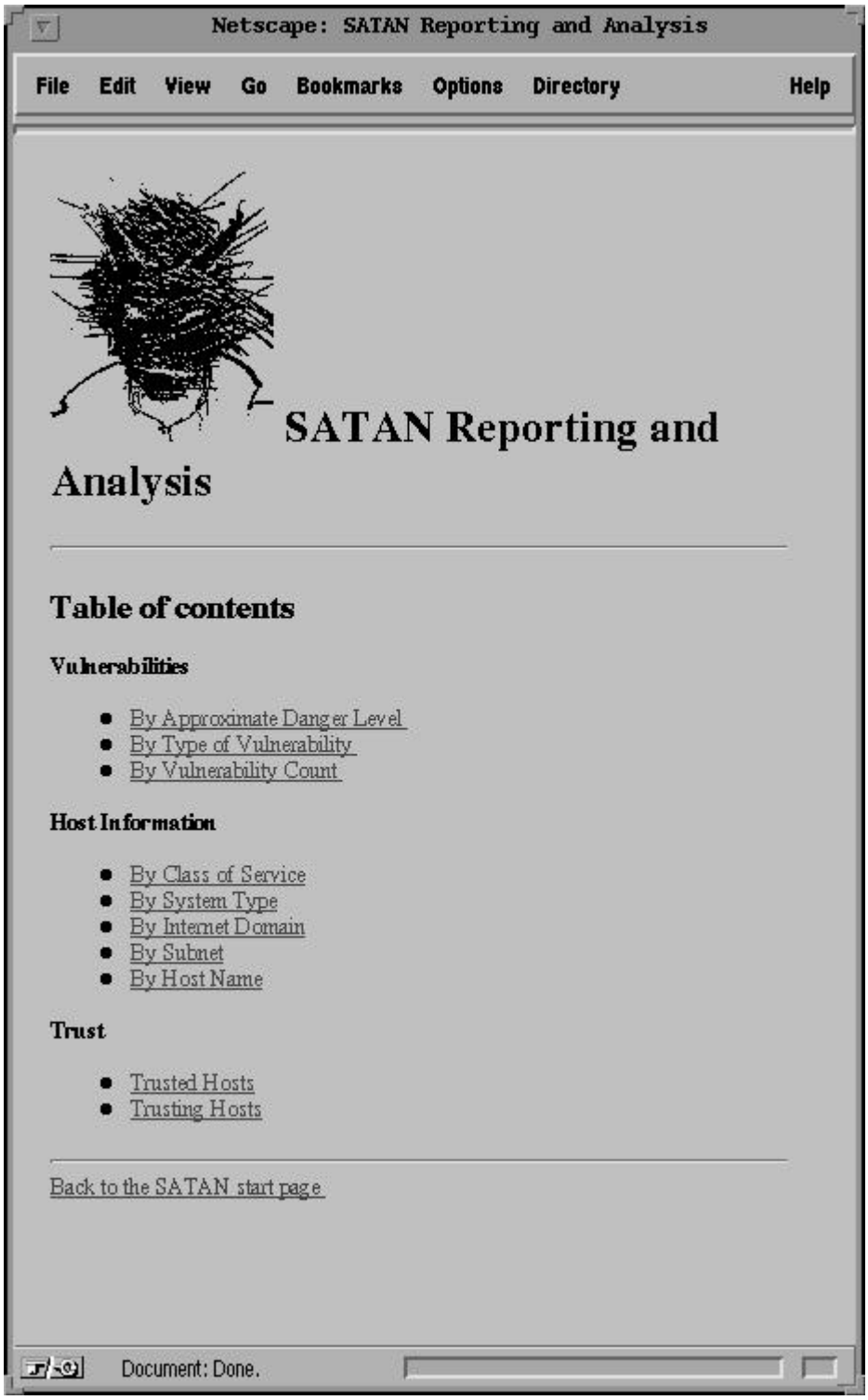


Aus diesem Menü heraus können alle Aktionen gesteuert werden. Zuerst sollten die von Haus aus mitgelieferten Grundeinstellungen den eigenen Bedürfnissen angepaßt werden. Dazu wird der Menüpunkt **SATAN Configuration Management** angewählt:



Hier werden die Einstellungen zu Verzeichnissen, wie intensiv SATAN die einzelnen Rechner untersuchen soll, die Adresse des zu untersuchenden Subnetzes und Rechner, die bei der Suche ausgelassen werden sollen, vorgenommen. Sind sämtliche Einstellungen erfolgt, wird im Menüpunkt **SATAN target selection** das primäre Ziel des Scans angegeben und der Scan gleich gestartet.

Im Menüpunkt **SATAN Reporting and Analysis** können die Ergebnisse übersichtlich dargestellt werden. Bei Sicherheitsproblemen bietet SATAN eine ausführliche Problembeschreibung, zeigt mögliche Lösungswege auf, bietet aber keine Anleitung zum Einbruch in die betroffenen Rechner.



Wie merke ich, daß jemand meine Maschine mit SATAN angreift?

Je nach Angriffsstärke geben die Autoren folgende Spuren an, die SATAN hinterläßt:

- **Light:** Kaum Spuren. Wir konnten leichte Scans nur durch einen extrem paranoid eingestellten Portmapper und genaues Studium der Logfiles nachweisen. Obwohl dieser Scan bereits schwere Löcher aufzeigen kann (z.B. unbeschränkte NFS-exports) ist er praktisch nicht feststellbar

- **Medium:** Eigentlich sollten bei dieser Einstellung irgendwelche Spuren in den Logs auftauchen,

bei einem Test stellten wir allerdings fest, daß SATAN auch hier kaum Spuren hinterließ

- **Heavy:** Fehlermeldungen können auf Systemkonsolen auftauchen, was bei uns bisher aber noch nie der Fall war. Lediglich einige seltsame Effekte auf den Ausgangs- und Zielrechnern konnten beobachtet werden:
  - Verlust der Umgebungsvariablen von eingeloggten Benutzern
  - Deaktivierung von bootp auf dem Ausgangsrechner
  - Änderungen in Konfigurationsdateien auf dem Ausgangsrechner.

In den Logfiles fallen bei einem Heavy Scan fast immer Connects in äußerst kurzen Abständen (bis zu 20 pro Sekunde) auf, die mit Ausnahme eines sehr wortkargen Loggings auffallen sollten.

Zum Beispiel:

```
Nov 24 15:42:50 :victim.edu fingerd[9286]:connect from evil.host
Nov 24 15:42:51 :victim.edu fingerd[9288]:connect from evil.host
Nov 24 15:42:51 :victim.edu fingerd[9290]:connect from evil.host
Nov 24 15:42:52 :victim.edu fingerd[9292]:connect from evil.host
Nov 24 15:42:52 :victim.edu fingerd[9294]:connect from evil.host
Nov 24 15:42:52 :victim.edu fingerd[9296]:connect from evil.host
```

Ebenso auffällig sind Login-Versuche auf privilegierte Standard Accounts wie root oder bin sowie auf Guest Accounts oder anonymous ftp:

```
Nov 24 16:20:30 :victim.edu rshd[9357]:root@evil.host as root: permission denied.
cmd=`file /bin/sh`
Nov 24 16:25:11 :victim.edu rshd[9358]:bin@evil.host as bin: permission denied.
cmd=`file /bin/sh`
Nov 24 16:30:01 :victim.edu ftpd[9360]:ANONYMOUS FTP LOGIN REFUSED FROM evil.host

Nov 24 16:37:16 :victim.edu rshd[9363]:guest@evil.host as guest: permission
denied. cmd=`file /bin/sh`
```

Dies sind leicht modifizierte Original Logfiles von einer Indigo R3000 unter IRIX 5.3. Bei anderen Betriebssystemen sehen die Logs anders aus. Die Einstellung des Syslog- Daemons entnehmen Sie bitte der Manual Page zu `syslog(1)`. Ebenso informativ ist das Header File `/usr/include/sys/syslog.h`

Mit Hilfe von courtney und gabriel - beide Programmpakete finden Sie auf `ftp.uni-stuttgart.de` und `ftp.cert.dfn.de` - kann man die Suche nach SATAN-Spuren in den Syslogs automatisieren.

Ansprechpartner in sicherheitsrelevanten Fragen

An wen kann ich mich in so einem Fall wenden? Hier zwei wichtige Adressen und Ansprechpartner:

- `sneakers@rus.uni-stuttgart.de`
- `dfncert-request@cert.dfn.de`

Bernd Lehle, NA-5531
E-Mail: `Lehle@rus.uni-stuttgart.de`

Oliver Reutter, NA-4513
E-Mail: Oliver.Reutter@rus.uni-stuttgart.de