Computersicherheit und SATAN

Was ist SATAN ?

SATAN (Security Analysis Tool for Auditing Networks) ist ein Programmpaket, das SystemadministratorInnen beim Auffinden von Sichertsmängeln in UNIX-Systemen unterstützen soll. In Umkehrung der Absichten der Entwickler kann SATAN natürlich auch "Computer-Hacker" beim Aufspüren eben dieser Mängel behilflich sein. Im Vorfeld der Verfügbarkeit von SATAN entspann sich daher auch eine Diskussion, ob solch ein Programm der Öffentlichkeit zugänglich gemacht werden sollte. Schließlich herrschte aber doch Konsens darüber, daß es notwendig sei, etwas gegen mangelndes Interesse und Fachwissen in Sicherheitsfragen, selbst routinierter SystemadministratorInnen, zu unternehmen, was den Entwicklern gemessen an dem großen Interesse offensichtlich geglückt ist. Der Umstand, daß damit auch minderbegabte "Amateur-Computer-Hacker" leichteres Spiel haben könnten, wird in Kauf genommen.

Wie funktioniert SATAN ?

SATAN ist eine Sammlung von Einzelprogrammen, mit deren Hilfe Informationen über UNIX-Computer - typischerweise alle UNIX-Workstations eines Instituts - über das Netz ermittelt werden sollen. Überprüft werden Services wie NIS, finger, NFS, ftp, sendmail u.ä., also über das Netz aufrufbare Programme, die von "Hackern" oft zum Eindringen verwendet werden. Ziel ist, unzureichende Konfigurationen bzw. veraltete Versionen mit Sicherheitsmängeln zu entdecken.

SATAN verwendet einen WWW-Browser (Netscape, Mosaic) oder Lynx als Benutzerschnittstelle und ermöglicht so einfache Bedienung über eine graphische Oberfläche mittels der Maus.

Ironie des Schicksals ist wohl, daß in der ersten Version des Sicherheitswerkzeuges SATAN (Version 1.0) ein gravierender Sicherheitsmangel gefunden wurde. Manche WWW-Browser (z. B. Netscape) schicken unter gewissen Umständen einen geheimen "session key", auch "magic cookie" genannt, über das Netzwerk. Wer in Besitz dieses Schlüssels gelangt, kann Programme auf dem Computer ausführen, auf dem SATAN läuft (siehe CERT Satan Advisories 95:06 und 95:07a). In neuere SATAN-Versionen (ab 1.1) sind mehrere Mechanismen eingebaut, die ermöglichen, daß diese generelle Schwachstelle mancher WWW-Browser während der Sicherheitstests - und nur während dieser (!) - nicht zum Tragen kommt. CERT empfiehlt daher, auch für die neuen Versionen von einer SATAN-Session aus keine auswärtigen URL'S (WWW-Seiten) zu öffnen. Als Ergebnis einer Sicherheitsüberprüfung mit SATAN werden gefundene Schwachstellen aufgelistet und (!) außerdem auch Lösungsvorschläge angeboten.

Ist SATAN gefährlich ?

Grundsätzlich kann SATAN zum Ausforschen von Schwachstellen eingesetzt werden, nicht aber zum unerlaubten Eindringen. Weiters ist SATAN so programmiert, daß seine Anwendung leicht zu verfolgende Spuren hinterläßt, von einer/m erfahrenen AdministratorIn also bemerkt wird. Sind die Schwachstellen erst einmal bekannt, so ist das Eindringen allerdings selbst mit Standardprogrammen möglich. Für die/den SystemadministratorIn bringt die Installation von SATAN naturgemäß einen gewissen Aufwand mit sich, sie/er erhält dafür aber auch ein Werkzeug, mit dem regelmäßige Checks schnell und bequem durchzuführen sind, ein gravierender Unterschied zu seinen Vorgängern. Ein wichtiger Aspekt ist die Erhöhung der Sensibilität für Sicherheitsfragen, die durch die Aufregung über SATAN sicherlich erreicht wurde. Für SystemadministratorInnen an der TU Wien möchte ich nochmals auf die Aktion des EDV-Zentrums hinweisen. Wir überprüfen Ihre UNIX-Workstations mit SATAN. Nötig ist dafür eine Anforderung von der/dem EDV-Beauftragten oder Institutsvorstand mit den Namen der zu überprüfenden Rechner an die Adresse

`root@shiva.tuwien.ac.at.`

Wo bekommt man Informationen zum Thema Sicherheit ?

Eine Auswahl:

Newsgroup: `comp.security.unix`

CERT (Computer Emergency Response Team) informiert über gefundene Sichertslücken, in der Regel sobald ein Patch zur Behebung existiert. Die Publikationen sind erhältlich über ftp

`<URL:ftp://ftp.cert.org/pub/cert_advisories>`

oder Mail: schreiben Sie eine Email an `cert@cert.org` mit Bitte um Aufnahme auf die Liste (subscribe).

"Public domain"-Programme und Publikationen zum Thema Sicherheit sind stets in neuester Version auf dem ftp-Server der Universität Wien zu finden:

`<URL:ftp://ftp.univie.ac.at/security>`

Schließlich ist auf unserem ftp-Server der sehr gute, kompakter Text "Improving the Security of Your Site by Breaking Into it" der SATAN-Entwickler Dan Farmer and Wietse Venema unter

`<URL:ftp://ftp.tuwien.ac.at/Sources/Security/satan/satan.ps>`

zu finden.

Udo Linauer