SATAN und SAINT

Aufspüren und Beseitigen von Sicherheitslücken in vernetzten Umgebungen.

Christian Hofer

Als die beiden Entwickler von SATAN, Wietse Venema und Dan Farmer ihre Toolsammlung 1995 vorstellten, erregten sie damit großes Aufsehen, da es das erste einfach erhältliche Programm war, um Sicherheitslücken in vernetzten Rechnern automatisch aufzuspüren. SATAN überprüft Systeme auf Sicherheitslücken, die durch fehlerhafte Konfiguration oder Software aufgetan werden können. Es meldet aber nicht nur die problematische Stelle, sondern erklärt auch warum eine Sicherheitslücke ein Problem darstellt. Neben SATAN gibt es mittlerweile eine Reihe anderer Port-scanning- und Service-testing-tools. Im Unterschied zu den meisten vergleichbaren Programmen erlaubt SATAN aber auch die „Trust-Relationships", also die Abhängigkeiten und Vertrauensverhältnisse zwischen verschiedenen Rechnern zu untersuchen. Als Beispiel sei die „man-in-the-middle attack" genannt. Wenn ein System Ihre DNS-Anforderung für eine Telnet-Verbindung zum Server durch sich selbst schleift und alle Daten der Verbindung protokolliert, ist das natürlich ein großes Sicherheitsproblem. Der erfolgreiche Einsatz von SATAN stellt gewisse Anforderungen an die Hard-und Softwareausstattung sowie das Wissen der Benützer. So ist SATAN ausschließlich für Unix-Systeme (eingeschränkt auch für Linux) verfügbar und benötigt dort root-Rechte, Perl 5.004_004, einen C-Compiler und X-Windows.

Ein Auszug aus der Liste wichtiger, von SATAN durchsuchten Services und empfohlene Gegenmaßnahmen:

- Schreibberechtigung für anonymous-user auf FTP-Server. Abhilfe: Home- und alle Unterverzeichnisse des FTP-Server auf root als Eigentümer stellen. Kein Verzeichnis oder Datei sollte dem ftp-user gehören.
- NFS (Network File System) Freigaben können unberechtigt verbunden werden, da das NFS-Protokoll keine Authentifikation aufweist. Abhilfe: Einsatz von NFS Varianten mit Verschlüsselung, zum Beispiel Kerberos.
- Unbeschränkter rsh (remote shell) Zugang. Dieser erlaubt die Ausführung beliebiger Befehle auf dem Hostrechner. Abhilfe: Eintragungen in der Konfigurationsdatei ohne wildcards.
- X.11 Server erlaubt unbeschränkten Zugang. Abhilfe: Die „host access control" des X-Server aktivieren.

Da viele Arbeitplatzrechner als Betriebssystem MS Windows NT einsetzen, hier noch einige Sicherheitshinweise als Checkliste:

- Verwenden Sie immer das NT-Filesystem (NTFS)
- Installieren Sie immer das aktuelle Service-Pack (zur Zeit SP4) und die entsprechenden hot-fixes.
- Ändern Sie die Richtlinien für die Benutzerkonten des Rechners, so dass keine leeren oder zu kurzen Passwörter erlaubt sind. Verstecken Sie die Anzeige des letzten angemeldeten Benutzers.
- Da das Administrator-Konto sehr umfangreiche Rechte hat, sollten Sie mit dessen Rechten ein neues, unscheinbares Konto einrichten und dem „Administrator"-Konto alle Rechte entziehen. Ein Eindringling wird viel Zeit aufwenden, in dieses Konto einzubrechen. Achten Sie auch auf eine sehr sichere Verwahrung des Administrator-Passworts.
- Seien Sie mit dem Dienst NetBIOS über TCP/IP sehr vorsichtig. Besonders Rechner, die als Gateway zum Internet dienen sind anfällig auf Einbrüche darüber.
- Überprüfen Sie immer, ob Verzeichnisse freigegeben sind, die nicht mehr benötigt werden.
- Seien sie grundsätzlich bei der Rechtevergabe vorsichtig und überprüfen Sie die Notwendigkeit von Rechten regelmäßig.
- Stellen Sie immer passwortgeschützte Bildschirmschoner ein und melden Sie sich ab, wenn sie längere Zeit nicht vor dem PC sitzen. Eventuell schalten Sie den Rechner in der Nacht und am Wochenende aus.
- Wenn Sie die einfachen TCP/IP-Dienste nicht benötigen, dann deaktivieren Sie diese, um keine „Denial of Service Attacken" über diese zusätzlichen Ports zuzulassen.
- Deaktivieren Sie immer das „Gast"-Konto und alle unbenötigten Dienste.
- Nützen Sie die Systemprotokollierdienste (Audit) um die Aktivitäten am Rechner und Netzwerk zu kontrollieren.
- Überprüfen Sie regelmäßig auf Viren, Makro-Viren und sogenannter Fernsteuerungssoftware wie NetBus oder BackOrifice.
- Deaktivieren Sie die Möglichkeit beim Anmeldebildschirm den Rechner niederzufahren.
- Stellen Sie in den Netzwerkeigenschaften Zugangslisten für Systemprotokolle, Services und Ports ein.

Alle Sicherheitsvorkehrungen sind natürlich nutzlos, wenn nicht alle Benützer eines Systems die Notwendigkeit erkennen und aktiv unterstützen.

Mit diesen grundlegenden Vorsichtsmaßnahmen können Sie eine gewisse Sicherheit gewährleisten. Sie sollten aber trotzdem immer die neuesten Entwicklungen und Meldungen zur Sicherheit vernetzter Systeme und der Serversoftware mitlesen: Zwei sehr gute Mailing-Listen zu diesem Thema finden sich auf http://www.iss.net/lists und http://www.ntbugtraq.com/ntbugfaq.htm und natürlich erfahren Sie in den entsprechenden Newsgroups aktuelle und ausführliche Informationen zum Thema.

Gesamteindruck

Martin Freiss geht in „Protecting Networks with SATAN" zuerst allgemein auf die Relevanz von Sicherheitsbelangen ein und beschreibt sowohl die Installation als auch die Funktionsweise mit den entsprechenden Abwehrmaßnahmen sehr genau. Für erfahrene Benützer sind sicher auch die Ausführungen zur Erweiterbarkeit von SATAN interessant.

Das Buch richtet sich daher vor allem an Systemadministratoren von Unix-Anlagen, die eine übersichtliche Referenz zu SATAN benötigen und es regelmäßig verwenden. Inzwischen existiert eine aktualisierte Nachfolgeversion von SATAN, die sich SAINT (Security Administrator's Integrated Network Tool) nennt und über http://wwdsilx.wwdsi.com/saint zu beziehen ist. SAINT enthält eine umfangreiche Dokumentation, an den Hard-und Softwareanforderungen hat sich (leider) nichts geändert.

Freiss, M.: Protecting Networks with SATAN: Internet Security for System Administrators, 112 Seiten, O'Reilly 1998, ISBN 1-56592-425-8, ATS 320.-

Christian Hofer chofer@gmx.at