NetBSD

OF COURSE IT RUNS NETBSD

NetBSD - Sicherheit frei Haus

Das NetBSD Projekt verfolgt den selben Ansatz zur Sicherheit wie auch zum restlichen System: *Lösungen und keine Hacks.* Fragen zur Sicherheit werden bei NetBSD vom NetBSD Security Officer und dem NetBSD Security Alert Team behandelt. Neben der Untersuchung, dem Dokumentieren und dem Verbessern von Code bezüglich aktueller Sicherheitslücken beschäftigt sich das Team auch mit regelmäßigen Inspektionen des Codes um potentielle Sicherheitslücken zu finden und auszubessern.
NetBSD hat Kerberos IV (KTH-KRB), Kerberos 5 (Heimdal) OpenSSH und IPSEC für IPv4 und IPv6 in das System mit aufgenommen. Zusätzlich sind alle Dienste prinzipiell von vornherein bei und nach der Installation abgeschaltet.

Sicherheitshinweise

Wenn ernsthafte Sicherheitsprobleme in NetBSD gefunden und verbessert werden, wird ein „Security Advisory“ veröffentlicht, daß das Problem beschreibt und einen Verweis auf die Lösung enthält. Diese Anweisungen werden im weiten Kreise angekündigt und auf der Projektseite archiviert.
Das NetBSD-Projekt verwaltet eine Liste von bekannten Sicherheitslücken in Paketen die im Paketsystem vertreten sind.
Weitere Informationen finden Sie auf http://www.netbsd.org/Security und tech-security@NetBSD.org.

File Flags und Kernel Security Level

File Flags ermöglichen es den Benutzern oder dem Administrator Dateien mit bestimmten „Flags´´ zu markieren und so vor Manipulationen zu schützen. Möglich sind etwas die Optionen *sappnd* oder *uappnd*, mit der Daten an Dateien nur mehr angehängt aber nicht mehr verändert werden dürfen. Markiert man eine Datei als *schg*, kann sie überhaupt nicht mehr verändert werden.
Kernel Security Levels schränken bestimmte Systemfunktionen ein und ermöglichen den Einsatz von File Flags. Hat man z.B. Level 2 aktiviert, sind alle Datenträger nur-lesbar verfügbar und können nicht mehr ein- oder ausgemountet werden. Der TCP/IP-Filter kann nicht mehr verändert werden, und die Systemzeit lässt sich nur noch vor- nicht aber zurückstellen.

Dateimanipulationen erkennen

mtree ist ein Instrument um eine Dateihierarchie gegen eine Spezifikation abzugleichen. Eingesetzt wird es vor allem um installierte Binärdateien gegen eine vorher spezifizierte Liste abzugleichen. Ähnlich tripwire oder AIDE, kann man

mtree dazu verwenden Manipulationen an Dateien aufzudecken. Dazu erstellt man einen Fingerabdruck eines Dateisystems, in dem Informationen zu den Dateien (Prüfsummen, Zugriffsrechte) abgelegt werden. Dieser Fingerabdruck kann dann gegen das laufende System abgeglichen werden und deckt so Veränderungen an Dateien (bspw. Würmer, Rootkits oder ähnliches) zuverlässig auf.

Trojaner aussperren

Der NetBSD-Kernel unterstützt ,,verified executable“, ein System um manipulierte Binärdateien an der Ausführung zu hindern.
Hierzu wird eine Prüfsumme der Binärdateien angelegt und vom Kernel beim Aufruf der Datei mit den aktuellen Daten verglichen. Wurde die Binärdatei verändert (bspw. von einem Wurm, Rootkit oder Einbrecher), verweigert der Kernel die Ausführung des Systems.

Partitionen verschlüsseln

Mit cgd kann man beliebige Partitionen (außer / selbst) auf Blockebene verschlüsseln. Ohne Angabe des Passworts hat Niemand, auch nicht root oder jemand mit physikalischem Zugriff auf die Festplatte, eine Chance an die Daten heranzukommen.
Mit cgd kann man auch die Swap- und Temp-Partition verschlüsseln, um zu verhindern daß dort geheime Daten öffentlich werden.

System Calls kontrollieren

Niels Provos' systrace erlaubt es eine Policy zu erstellen, mit der man einzelne Syscalls eines Programms kontrollieren kann. So ist es bspw. möglich, Apache von einem normalen Benutzer aus zu starten, weil dieser Benutzer via systrace Apache an den Port 80 binden darf - so daß Apache selbst nicht mehr mit Root-Rechten läuft.

Tägliche Sicherheitsüberprüfung

Die beiden Shellskripte `/etc/daily` und `/etc/security` erlauben es das gesamte System auf Sicherheitslücken hin zu untersuchen. Sie können nächtlich von cron gestartet werden und generieren einen umfassenden Bericht zu Sicherheitsproblemen.

Software auf Sicherheitslücken prüfen

Durch das *audit-packages*-Paket kann eine vom Projekt gepflegte Liste mit Sicherheitslücken heruntergeladen werden und mit dem System verglichen werden. Es werden so alle Pakete mit Sicherheitsproblemen aufgelistet und können dementsprechend aktualisiert werden.

Paketfilter

Mit IPFilter und pf unterstützt NetBSD im Basissystem zwei ausgereifte Paketfilter für IP-Pakete, die jedes NetBSD-System zur ausgereiften und stabilen Firewall befähigen.

Umfangreiche Sicherheitspakete

Mit pkgsrc lassen sich problemlos viele der ausgereiftesten und wichtigsten Sicherheitspakete installieren. Dazu gehören u.a. snort, AIDE, Tripwire, CFS, chkrootkit, Nessus, Amap, GnuPG und honeyd.