NetBSD

— Sicherheit frei Haus —

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 www.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 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.

NetBSD

— Built-In Security —

Secure by default

The NetBSD Project adopts the same approach to security as it does to the the rest of the system: *Solutions and not hacks*. Security issues in NetBSD are handled by the NetBSD security officer and the NetBSD security alert team. As well as investigating, documenting and updating code in response to newly reported security issues, the team also performs periodic code audits to search for and remove potential security problems.
NetBSD has integrated Kerberos IV (KTH-KRB), Kerberos 5 (Heimdal), and ssh. In addition, all services default to their most secure settings, and insecure services are disabled by default for new installations. NetBSD also contains full support for IPSEC for both IPv4 and IPv6.

Security Advisories

When security problems are discovered and corrected, we issue a security advisory, describing the problem and containing a pointer to the fix. These are announced to our netbsd-announce mailing list as well as to various other mailing lists and websites.

Checking for Vulnerabilities in Installed Packages

The NetBSD Security-Officer and Packages Groups maintain a list of known security vulnerabilities to packages which are (or have been) included in pkgsrc. Through audit-packages, this list can be downloaded automatically, and a security audit of all packages installed on a system can take place.
One can set up audit-packages to download the vulnerabilities list and run a package audit in the daily security script.

File Flags and Security Levels

File flags allow the administrator and users to protect programs and data from being altered even by root. If a file is marked with the *sappnd* flag, data can only be appended to the file, but it cannot be altered anymore. The *schg* flag protects a file from being altered even by root.
Security levels restrict several system functions, according to the level. The system can be set to a stricter level, but not to a lower level, while running in multiuser mode. So the system is protected even against an intruder with superuser access.

Checking for Manipulated Files

The mtree utility compares a file hierarchy against a specification read from a file. By using a specification that collected sufficent attributes of files like ownership, mode and cryptographic message digests, any manipulation of a file can be revealed – uncovering threats like rootkits or trojans.

Non-Executable Stack and Heap

NetBSD supports non-executable mappings on platforms where the hardware allows it. Process stack and heap mappings are non-executable by default. This makes exploiting potential buffer overflows harder. When the hardware has a larger granularity, the rule is that if any page in the larger unit is executable, then the entire larger unit is executable, otherwise the entire larger unit is not executable.
No compile-time option is needed to enable this software support, it's always available.

Locking Out Trojans

Veriexec adds a new function to the exec-Path of the kernel, thus allowing the kernel to check a cryptographic hash for a binary. With this feature, it is almost impossible to run manipulated binaries like a rootkit or a trojan.

Encrypted Partitions

The cryptographic device driver (cgd) provides functionality which allows you to use disks or partitions for encrypted storage. After providing the appropriate key, the encrypted partition is accessible using cgd pseudo-devices just like a normal data partition. Cgd can also be used to encrypt /tmp and swap-space or file systems residing in a file, creating an encrypted container.

Controlling System Calls

Niels Provos' systrace provides a way to monitor, intercept, and restrict system calls. Systrace acts as a wrapper to the executables, controlling their access of system calls.

File System Extended Attributes

Extended Attributes allow one to add meta data to vnodes of files and directories. This can be used to keep user defined information (eg. a checksum) connected to a file/directory.

Daily Security Checks

NetBSD comes with two shell scripts, `daily.conf` and `security.conf`. The scripts are used to do daily maintenance and security checks of the system. They can be started via cron each night and generate a verbose report of the system's security status.

Packet Filter

NetBSD comes with two mature TCP/IP packet filters in the base system. Ipf or pf enable any NetBSD machine to work as a well-engineered and sophisticated firewall.

Version 1.3 as of 2007-4-7. See `http://www.net-tex.de/netbsd/advocacy` Created by Stefan Schumacher (`http://www.net-tex.de`)