NetBSD

— Secure by Default —

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. NetBSD supports PROT_EXEC permission via mmap() for all platforms where the hardware differentiates execute access from data access, though not necessarily with single-page granularity. 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.

Third Party Packages

Many of the most important and well-engineered security software packages available can be installed flawlessly via NetBSD's pkgsrc. Some of those packages are snort, Tripwire, CFS, Nessus, Amap, GnuPG and honeyd.

1.4 2007-4-7 Created by Stefan Schumacher `<stefan@net-tex.de>`