HOWTO articles - Security

Securing your computer is an ongoing process. The following guides will help you secure your Slackware installation, be it for server, workstation or laptop needs. Make sure you subscribe to the slackware-security mailing list. All security announcements since 1999 are available on http://www.slackware.com/security/.

This section contains articles related to securing your Slackware based system and network.

Inspired? Want to write a Security HOWTO page yourself?
Type a new page name (no spaces - use underscores instead) and start creating! You are not allowed to add pages

Security

Physical security

Network security

- Firewall
- Protecting SSH connections from brute-force attacks:
- Use only SSH keys instead of passwords for SSH connections: Using SSH keys
- Network services: the following services can be tweaked:
  - inetd
  - OpenSSH

File System Security

- Encryption
  - Encrypt swap space to protect sensitive contents Enabling Encrypted Swap
- File Permissions
- Track system changes with OSSEC

Overview of Security HOWTOS

Page	Description	Tags

Enabling Encrypted Swap	Enabling Encrypted Swap When available memory drops below a certain point, the Linux kernel will swap the contents of memory pages to swap space. This content may include sensitive information such as passwords, usernames, PINS, banking or other identity information. This data is usually in plain text and so can be read without effort. Encrypting the system swap space protects its contents against unauthorized access and attack should access to the hard drive be compromised or physically remov…	howtos, security, encryption, swap
Enabling Secure Boot on Slackware	Enabling Secure Boot on Slackware On Unified Extensible Firmware Interface (UEFI) based hardware, a system can operate in Secure Boot mode. In Secure Boot mode, only EFI binaries (i.e. boot managers, boot loaders) that are trusted by the platform owner, either explicitly or via a chain of trust, are allowed to run at boot time. This prevents unauthorised EFI binaries and operating systems from running on your system, which can improve security.	howtos, security, secure boot, uefi, author turtleli
hosts.allow, hosts.deny	hosts.allow, hosts.deny These two files in /etc are a common place for storing rules about who you want to allow to connect to the services on your machine. While a firewall can be considered as hiding a door, these files control who is allowed to open the door.	howtos, security, slackware allversions, inetd
Installing Tor Using a SlackBuild Script	Installing Tor Using a SlackBuild Script Overview From torproject.org: Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.	howtos, software, tor, slackbuild, author nocturnal.slacker
Loading Intel Microcode	Loading Intel Microcode Introduction Due to revelations the last years of hardware vulnerabilities with processors using speculative execution and various “threading” techniques, the Kernel has implemented a range of mitigations for these issues to eliminate the issue or reduce the potential problem. Alot of these solutions are included in the Kernel and can be/are activated in various ways.	howtos, security, cpu, microcode, spectre, meltdown
OpenVPN	OpenVPN OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (	howtos, openvpn, slackbuild, security
Improving OpenSSH security	Improving OpenSSH security OpenSSH is the swiss-army knife of remote-access programs: it provides you with a shell on your distant machine, and transmits data in a secure and encrypted way - including commands, file transfer, X11 and VNC sessions, rsync data, etc.	howtos, security, ssh, author noryungi

How to use SSH keys to connect without a password.	How to use SSH keys to connect without a password. OpenSSH is a very secure way to connect remotely to a Slackware machine. But the easiest way to use SSH is to use its key facility. The concept of public/private keys can be hard to explain, we will try to go through it in as simple a manner as possible.	howtos, security, ssh, sshkeys, author noryungi
Mandatory Access Control - Getting started with Tomoyo Linux on Slackware	Mandatory Access Control - Getting started with Tomoyo Linux on Slackware Introduction There are a few different tools in the Tomoyo family. Mainly Tomoyo 1, Akari and Tomoyo 2. There is also CaitSith, but this guide is dealing with Tomoyo 2.x. And at the time of writing Tomoyo 2.6.x for Kernel 5.1 and later.	howtos, security, lsm, mac, tomoyo

howtos, topic page