

[TOOL] Linux Security Protection System

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0069.html>

From: support@securiteam.com

Date: 10/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Oct 2002 00:22:13 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Linux Security Protection System

DETAILS

LinSec, as the name says, is Linux Security Protection System. The main aim of LinSec is to introduce Mandatory Access Control (MAC) mechanism into Linux (as opposed to existing Discretionary Access Control mechanism). LinSec model is based on:

- * Capabilities
- * Filesystem Access Domains
- * IP Labeling Lists
- * Socket Access Control

As for Capabilities, LinSec heavily extends the Linux native capability model to allow fine grained delegation of individual capabilities to both users and programs on the system. No more almighty root!

Filesystem Access Domain subsystem allows restriction of accessible filesystem parts for both individual users and programs. Now you can restrict user activities to only its home, mailbox etc. Filesystem Access Domains works on device, dir and individual file granularity.

IP Labeling lists enable restriction on allowed network connections on per program basis. From now on, you may configure your policy so that no one except your favorite MTA can connect to remote port 25.

Securiteam: [TOOL] Linux Security Protection System

Socket Access Control model enables fine grained socket access control by associating, with each socket, a set of capabilities required for a local process to connect to the socket.

LinSec consists of two parts: kernel patch (currently for 2.4.18) and user space tools.

ADDITIONAL INFORMATION

Detailed documentation, download & mailing list information –
<<http://www.linsec.org>> <http://www.linsec.org>

The information has been provided by <<mailto:bole@bolex.bolex.co.yu>>
Bosko Radivojevic.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] PHPNuke AddOn PHPToNuke Allows Remote File Retrieving"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)