

# 1.114.2

## Setup host security

### Weight 3

Linux Professional Institute Certification — 102

Nick Urbanik <nicku@nicku.org>

This document Licensed under GPL—see section 5

2005 October

# Outline

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

License Of This  
Document

Context

Objectives

Set up mail alias for `root`'s  
mail

Turning off unused network  
services

Some basic rules of  
security

Identify running services

Turning off services on  
Red Hat/Fedora

Turning off services on  
Debian/Ubuntu

License Of This Document

# Topic 114 Security [8]

Where we are up to

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

## Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

License Of This  
Document

1.114.1 Perform security administration tasks [4]

1.114.2 **Setup host security** [3]

1.114.3 Setup user level security [1]

# Description of Objective

## 1.114.2 Setup host security [3]

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

License Of This  
Document

Candidate should know how to set up a basic level of host security. Tasks include syslog configuration, shadowed passwords, set up of a mail alias for root's mail and turning of [sic] all network services not in use.

# Key files, terms, and utilities include:

1.114.2 Setup host security [3]

`/etc/inetd.conf` or `/etc/inet.d/*` — Where you turn off all unneeded `xinetd` services

`/etc/nologin` — only allows `root` to log in if this file exists. Other users shown contents of this file. For maintenance.

`/etc/passwd` — the file that *should not* contain passwords. See topic 1.111.1 Manage users and group accounts and related system files

`/etc/shadow` — Where shadow passwords belong

`/etc/syslog.conf` — Where `syslog` is configured. See notes for topic 1.111.3 Configure and use system log files to meet administrative and security needs

# Set up mail alias for `root`'s mail

- ▶ Many important problems are sent as mail to the `root` user
- ▶ You should *not* be logging in as `root`, use `sudo`
- ▶ You should be reading that email
- ▶ ... so you should create an alias for `root` that sends `root`'s mail to you:

```
$ grep '^root' /etc/postfix/aliases ↵  
root:                nicku
```

# Outline

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

**Some basic rules of security**

Identify running services

Turning off services on Red  
Hat/Fedora

Turning off services on  
Debian/Ubuntu

License Of This  
Document

Context

Objectives

Set up mail alias for root's mail

**Turning off unused network services**

**Some basic rules of security**

**Identify running services**

Turning off services on Red  
Hat/Fedora

Turning off services on  
Debian/Ubuntu

License Of This Document

# Some basic rules of security

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

**Some basic rules of security**

Identify running services

Turning off services on Red  
Hat/Fedora

Turning off services on  
Debian/Ubuntu

License Of This  
Document

- ▶ Use minimum privilege to do what is required
- ▶ Provide only the services your users need



# Outline

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for `root`'s mail

**Turning off unused network services**

Some basic rules of security

**Identify running services**

Turning off services on Red Hat/Fedora

Turning off services on Debian/Ubuntu

License Of This Document

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

Some basic rules of security

**Identify running services**

Turning off services on Red Hat/Fedora

Turning off services on Debian/Ubuntu

License Of This Document

# Identify running services

- ▶ See what services are configured to start:  
`$ chkconfig -list | grep on` ↵
- ▶ Determine what package each service turned on comes from with a command like  
`$ rpm -qif /etc/init.d/<service-name>` ↵
- ▶ Decide whether this service should be turned off
- ▶ You can also check running processes with `ps` and `top`

# Outline

Context

Objectives

Set up mail alias for `root`'s mail

**Turning off unused network services**

Some basic rules of security

Identify running services

**Turning off services on Red Hat/Fedora**

Turning off services on Debian/Ubuntu

License Of This Document

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

Some basic rules of security

Identify running services

**Turning off services on Red Hat/Fedora**

Turning off services on Debian/Ubuntu

License Of This Document

# Turning off services on Red Hat/Fedora

- ▶ On Red Hat/Fedora systems:
  - ▶ Remove the software package, e.g.,  
`$ rpm -e telnet ↵`  
or
  - ▶ Disable the service: `$ chkconfig -del sendmail ↵`  
or `$ chkconfig sendmail off ↵`
- ▶ Note that `chkconfig` also turns services on and off in `xinetd` as well.
- ▶ You should also be able to turn them off manually:  
`$ grep disable /etc/xinetd.d/telnet ↵`  
`disable = yes`

# Outline

Context

Objectives

Set up mail alias for `root`'s mail

**Turning off unused network services**

Some basic rules of security

**Identify running services**

Turning off services on Red Hat/Fedora

Turning off services on Debian/Ubuntu

License Of This Document

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

Some basic rules of security

Identify running services

Turning off services on Red Hat/Fedora

**Turning off services on Debian/Ubuntu**

License Of This Document

# Identify what runlevels a service starts/stops

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

Some basic rules of security

Identify running services

Turning off services on Red  
Hat/Fedora

Turning off services on  
Debian/Ubuntu

License Of This  
Document

- ▶ To find what runlevels a service  $\langle service \rangle$  will start and stop on, do:

```
$ find /etc/rc* -name '* $\langle service \rangle$ ' ←
```

- ▶ Example: to see what links exist for `squid`:

```
$ find /etc/rc* -name '*squid' ←
```

# Turning off services on Debian/Ubuntu

- ▶ See `$ man update-rc.d` ←
- ▶ To disable a service `<service>` that normally starts, do:  
`$ sudo update-rc.d -f <service> remove` ←
- ▶ For example, to disable initialisation of `squid`, do:  
`$ sudo update-rc.d -f squid remove` ←
- ▶ Turn off `xinetd` service `<service>` by editing  
`/etc/xinetd.d/<service>`, or if possible, turn `xinetd`  
off altogether:  
`$ sudo update-rc.d -f xinetd remove` ←
- ▶ Finally, if you liked `ntsysv` on Red Hat, then do  
`$ sudo apt-get install rcconf` ←

# Topics Covered

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Context

Objectives

Objectives

Set up mail alias for `root`'s mail

Set up mail alias for  
`root`'s mail

Turning off unused network services

Turning off unused  
network services

Some basic rules of security

Some basic rules of security

Identify running services

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Red  
Hat/Fedora

Turning off services on Debian/Ubuntu

**Turning off services on  
Debian/Ubuntu**

License Of This Document

License Of This  
Document



# Topics Covered

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Context

Objectives

Objectives

Set up mail alias for `root`'s mail

Set up mail alias for  
`root`'s mail

Turning off unused network services

Turning off unused  
network services

Some basic rules of security

Some basic rules of security

Identify running services

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Red  
Hat/Fedora

Turning off services on Debian/Ubuntu

**Turning off services on  
Debian/Ubuntu**

License Of This Document

License Of This  
Document

# Topics Covered

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Context

Objectives

Objectives

Set up mail alias for `root`'s mail

Set up mail alias for  
`root`'s mail

Turning off unused network services

Turning off unused  
network services

Some basic rules of security

Some basic rules of security

Identify running services

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Red  
Hat/Fedora

Turning off services on Debian/Ubuntu

**Turning off services on  
Debian/Ubuntu**

License Of This Document

License Of This  
Document

# Topics Covered

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Context

Objectives

Objectives

Set up mail alias for `root`'s mail

Set up mail alias for  
`root`'s mail

Turning off unused network services

Turning off unused  
network services

Some basic rules of security

Some basic rules of security

Identify running services

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Red  
Hat/Fedora

Turning off services on Debian/Ubuntu

**Turning off services on  
Debian/Ubuntu**

License Of This Document

License Of This  
Document

# Topics Covered

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Context

Objectives

Objectives

Set up mail alias for `root`'s mail

Set up mail alias for  
`root`'s mail

Turning off unused network services

Turning off unused  
network services

Some basic rules of security

Some basic rules of security

Identify running services

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Red  
Hat/Fedora

Turning off services on Debian/Ubuntu

**Turning off services on  
Debian/Ubuntu**

License Of This Document

License Of This  
Document

# Topics Covered

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

Some basic rules of security

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Debian/Ubuntu

License Of This Document

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
`root`'s mail

Turning off unused  
network services

Some basic rules of security

Identify running services

Turning off services on Red  
Hat/Fedora

**Turning off services on  
Debian/Ubuntu**

License Of This  
Document

# Topics Covered

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

Some basic rules of security

Identify running services

Turning off services on Red Hat/Fedora

Turning off services on Debian/Ubuntu

License Of This Document

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
`root`'s mail

Turning off unused  
network services

Some basic rules of security

Identify running services

Turning off services on Red  
Hat/Fedora

**Turning off services on  
Debian/Ubuntu**

License Of This  
Document

# Topics Covered

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

- Some basic rules of security

- Identify running services

- Turning off services on Red Hat/Fedora

- Turning off services on Debian/Ubuntu

License Of This Document

Context

Objectives

Set up mail alias for  
`root`'s mail

Turning off unused  
network services

- Some basic rules of security

- Identify running services

- Turning off services on Red  
Hat/Fedora

- Turning off services on  
Debian/Ubuntu**

License Of This  
Document

# Topics Covered

Context

Objectives

Set up mail alias for `root`'s mail

Turning off unused network services

- Some basic rules of security

- Identify running services

- Turning off services on Red Hat/Fedora

- Turning off services on Debian/Ubuntu

License Of This Document

Context

Objectives

Set up mail alias for  
`root`'s mail

Turning off unused  
network services

- Some basic rules of security

- Identify running services

- Turning off services on Red  
Hat/Fedora

- Turning off services on  
Debian/Ubuntu**

License Of This  
Document



# License Of This Document

1.114.2  
Setup host security  
Weight 3

Nick Urbanik

Context

Objectives

Set up mail alias for  
root's mail

Turning off unused  
network services

License Of This  
Document

Copyright © 2005 Nick Urbanik <nicku@nicku.org>

You can redistribute modified or unmodified copies of this document provided that this copyright notice and this permission notice are preserved on all copies under the terms of the GNU General Public License as published by the Free Software Foundation — either version 2 of the License or (at your option) any later version.