

# Hardening a web-server for the modern internet

## Introduction

Hands on how to secure your network Three day course – [Philip Paeps](#)

## Objectives

By the end of the workshop, everyone should know how to run secure services in jails on FreeBSD and use the pf firewall to keep malicious people on the internet out of their jails.

## Prerequisites

Participants should be familiar with Unix-style operating systems. The course is taught on FreeBSD but the environment will be familiar to people with a systems administration background on Linux or Solaris. Participants should bring their own laptops.

## Participants

Systems administrators and network operators who are running Network services in their organization.

## Workshop Requirements

- Knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access. You cannot use a tablet for this workshop.

## Instructors

[Philip Paeps](#)

## Agenda

Time	Day 1: Sunday 14 August	Day 2: Monday 15 August	Day 3: Tuesday 16 August
08:30 – 09:15 (45 minutes)	Registration and coffee	Registration and coffee	Registration and coffee

09:15 – 11:15 (120 minutes)	<ul style="list-style-type: none"> <li>• Installing FreeBSD in a VM</li> <li>• Where to find installation media</li> <li>• Which installation to choose</li> <li>• Installing on a clean machine</li> </ul>	<ul style="list-style-type: none"> <li>• Advanced jails</li> <li>• Installing a jail from scratch</li> <li>• Isolating jails with pf</li> <li>• Nested jails</li> </ul>	<ul style="list-style-type: none"> <li>• Jailing the Postfix mailserver</li> <li>• Installing Postfix from a package</li> <li>• Configuring a basic Postfix in a jail</li> <li>• letsencrypt.org certificate for SMTP</li> </ul>
11:15 – 11:30 (15 minutes)	Coffee break	Coffee break	Coffee break
11:30 – 13:00 (90 minutes)	<ul style="list-style-type: none"> <li>• FreeBSD is not Linux</li> <li>• Filesystem overview</li> <li>• init(8) and rc(8) (NO SYSTEMD!)</li> <li>• Starting and stopping processes</li> <li>• Package management with pkg(8)</li> </ul>	<ul style="list-style-type: none"> <li>• Using ezjail for easier management</li> <li>• Installing a dozen jails in two minutes</li> <li>• Upgrading jails</li> <li>• Deleting and archiving jails</li> <li>• Package management across many jails</li> </ul>	<ul style="list-style-type: none"> <li>• Hardening Postfix against spammers</li> <li>• DNS blacklists and whitelists</li> <li>• Sender and recipient restrictions</li> <li>• Fun tricks with multiple IP addresses</li> </ul>
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	<ul style="list-style-type: none"> <li>• pf: the BSD firewall</li> <li>• Default-deny ruleset</li> <li>• Allowing services</li> <li>• NAT and port forwarding</li> </ul>	<ul style="list-style-type: none"> <li>• Jailing and securing nginx</li> <li>• Installing nginx in a fresh jail</li> <li>• Tuning nginx for maximum security</li> <li>• Obtaining and managing letsencrypt.org certificates</li> <li>• Online tools for confirming webserver security</li> </ul>	<ul style="list-style-type: none"> <li>• Building your own custom packages</li> <li>• Introduction to Poudriere</li> <li>• Installing Poudriere in a jail</li> </ul>
15:30 – 15:45 (15 minutes)	Coffee break	Coffee break	Coffee break
15:45 – 16:30 (45 minutes)	<ul style="list-style-type: none"> <li>• Introduction to jails</li> <li>• Lightweight virtualisation</li> <li>• Jails vs. virtual machines</li> <li>• Mention bhyve</li> </ul>	<ul style="list-style-type: none"> <li>• Exercises with nginx</li> <li>• Reverse proxies across multiple jails</li> <li>• Dodgy services locked up in nested jails</li> </ul>	<ul style="list-style-type: none"> <li>• Putting it all together</li> <li>• ezjail, poudriere, nested jails</li> <li>• Mostly automated installations</li> <li>• Using multiple package repositories</li> </ul>

Revision #1

Created 28 October 2024 12:54:01 by sara

Updated 28 October 2024 15:25:01 by sara