

# DNSSEC Workshop

## Introduction

Hands on DNS and DNSSEC Three day course – [Philip Paeps](#)

## Objectives

At the end of this course, participants will be familiar with the Domain Name System and Security Extensions to the Domain Name System (DNSSEC). The course is taught "hands-on" in a virtualised FreeBSD environment. Participants will configure authoritative and recursive domain name servers and will learn to analyse and debug common misconfigurations and bugs

## 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. The virtualised lab environment is hosted on a server in Germany. Reliable internet connectivity with reasonable latency is required

## Participants

Systems administrators and network operators responsible for the DNS services in their organisation.

## Workshop Requirements

- Some understanding of DNS is required (for example, operational experience managing DNS servers is useful)
- Some 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 23 August	Day 2: Monday 24 August	Day 3: Tuesday 25
------	-------------------------	-------------------------	-------------------

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>• Introduction to DNS</li> <li>• Resource records</li> <li>• Delegation</li> <li>• Queries, responses and flags</li> </ul>	<ul style="list-style-type: none"> <li>• Configuring authoritative nameservers</li> <li>• Setting up DNS zonefiles</li> <li>• Delegating authority</li> <li>• Debugging common zonefile problems</li> </ul>	<ul style="list-style-type: none"> <li>• Introduction to DNSSEC</li> <li>• New resource records and flags in DNSSEC</li> <li>• Validating a domain from the root step by step</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>• DNS packet analysis</li> <li>• DNS data flow</li> <li>• DNS vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Very brief introduction to cryptography</li> <li>• Using TSIG to secure queries</li> </ul>	<ul style="list-style-type: none"> <li>• Key management: ZSKs and KSKs</li> <li>• Theory of key rollover and best practices</li> </ul>
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	<ul style="list-style-type: none"> <li>• Tools: dig, drill, host, nslookup, tcpdump</li> <li>• Tools exercises</li> <li>• Resolving a domain from the root by hand</li> </ul>	<ul style="list-style-type: none"> <li>• Configuring secondary nameservers</li> <li>• Configuring TSIG to secure zone transfers</li> <li>• Debugging common zone transfer issues</li> </ul>	<ul style="list-style-type: none"> <li>• Manually signing a zone with BIND 9</li> <li>• Configuring automatic DNSSEC with BIND 9</li> <li>• Brief introduction to OpenDNSSEC</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 the lab environment</li> <li>• Discussion and Q&amp;A</li> </ul>	<ul style="list-style-type: none"> <li>• Configuring unbound as a recursive resolver</li> <li>• Discussion and Q&amp;A</li> </ul>	<ul style="list-style-type: none"> <li>• Configuring unbound with trust anchors</li> <li>• Demo with SSHFP and TLSA</li> <li>• Discussion and Q&amp;A</li> </ul>

Revision #1

Created 28 October 2024 12:44:18 by sara

Updated 28 November 2024 13:10:52 by sara