

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"> • Introduction to DNS • Resource records • Delegation • Queries, responses and flags 	<ul style="list-style-type: none"> • Configuring authoritative nameservers • Setting up DNS zonefiles • Delegating authority • Debugging common zonefile problems 	<ul style="list-style-type: none"> • Introduction to DNSSEC • New resource records and flags in DNSSEC • Validating a domain from the root step by step
11:15 – 11:30 (15 minutes)	Coffee break	Coffee break	Coffee break
11:30 – 13:00 (90 minutes)	<ul style="list-style-type: none"> • DNS packet analysis • DNS data flow • DNS vulnerabilities 	<ul style="list-style-type: none"> • Very brief introduction to cryptography • Using TSIG to secure queries 	<ul style="list-style-type: none"> • Key management: ZSKs and KSKs • Theory of key rollover and best practices
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	<ul style="list-style-type: none"> • Tools: dig, drill, host, nslookup, tcpdump • Tools exercises • Resolving a domain from the root by hand 	<ul style="list-style-type: none"> • Configuring secondary nameservers • Configuring TSIG to secure zone transfers • Debugging common zone transfer issues 	<ul style="list-style-type: none"> • Manually signing a zone with BIND 9 • Configuring automatic DNSSEC with BIND 9 • Brief introduction to OpenDNSSEC
15:30 – 15:45 (15 minutes)	Coffee break	Coffee break	Coffee break
15:45 – 16:30 (45 minutes)	<ul style="list-style-type: none"> • Introduction to the lab environment • Discussion and Q&A 	<ul style="list-style-type: none"> • Configuring unbound as a recursive resolver • Discussion and Q&A 	<ul style="list-style-type: none"> • Configuring unbound with trust anchors • Demo with SSHFP and TLSA • Discussion and Q&A

Revision #1

Created 28 October 2024 12:44:18 by sara

Updated 28 November 2024 13:10:52 by sara