

How to Secure your Network Workshop

Introduction

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

Objectives

At the end of this course, participants will be familiar with new ways and methods to help them to secure their networks. The course is taught "hands-on" in a virtualised FreeBSD environment. Participants will configure some tasks and will learn to analyze and debug common mis-configurations 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.

Participants

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

Workshop Requirements

- 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 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"> • Introduction to security • Network layers • Defence in depth • Basic physical layer security | <ul style="list-style-type: none"> • Firewalls • Inclusive and exclusive policies • Simple ACLs | <ul style="list-style-type: none"> • Securing websites: HTTP and HTTPS • Configuring Apache and nginx |
| 11:15 – 11:30 (15 minutes) | Coffee break | Coffee break | Coffee break |
| 11:30 – 13:00 (90 minutes) | <ul style="list-style-type: none"> • Layer 1 and layer 2 • Ethernet: VLANs • Wireless basics | <ul style="list-style-type: none"> • Statefull firewalls • pf: the BSD packet filter | <ul style="list-style-type: none"> • Introduction to cryptography • PKI, basics of letsencrypt.org |
| 13:00 – 14:00 (60 minutes) | Lunch | Lunch | Lunch |
| 14:00 – 15:30 (90 minutes) | <ul style="list-style-type: none"> • Wireless: WEP, WPA, WPA2? • Captive portals • Ethernet 802.1x | <ul style="list-style-type: none"> • Securing higher layers (applications) • E-mail: what about spam? • Sensible outbound filtering | <ul style="list-style-type: none"> • Generating letsencrypt.org certificates • Configuring nginx and Apache with HTTPS • Using SSL in other applications |
| 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 firewalls (more tomorrow!) • Discussion and Q&A | <ul style="list-style-type: none"> • Configuring postfix and dovecot to protect against spam (abuse) • Discussion and Q&A | <ul style="list-style-type: none"> • Mitigation: what if it all goes wrong? • Discussion and Q&A |

Revision #1

Created 28 October 2024 13:01:13 by sara

Updated 28 November 2024 13:10:52 by sara