University of Stuttgart
Institute of
Information Security

Grundlagen der Informationssicherheit
Winter Term 2017/18
Prof. Dr. Ralf Küsters

Homework 5

Submission into the *green SEC mailbox* in front of Room 2.041 until January 16, 2018, 17:30.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants in the tutorial sessions.
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk loosing points.

Problem 1: Firewalls with nftables (10 points)

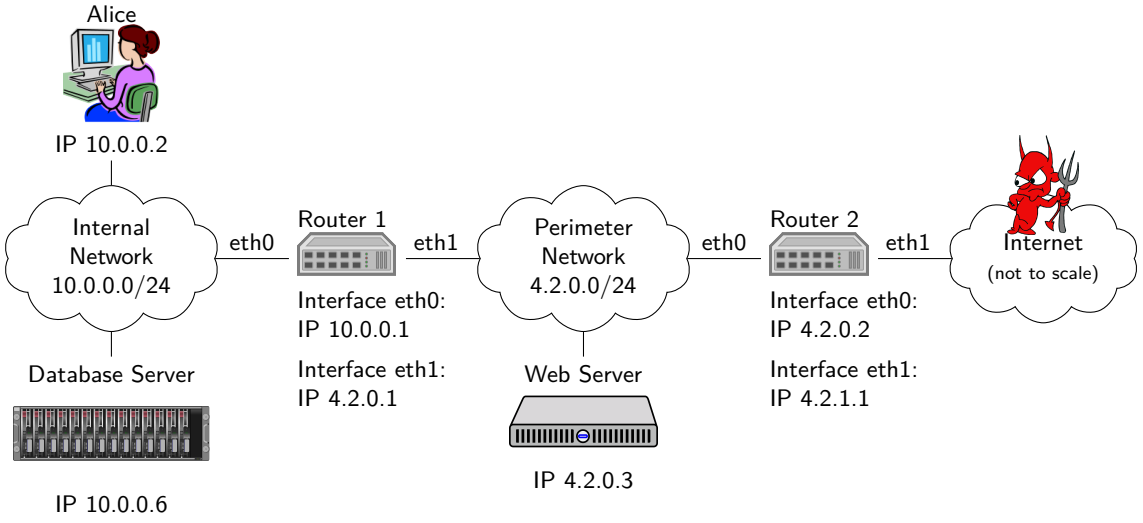

Figure 1: Network Setting

In Figure 1 you see a network setting with a perimeter network structure. Both routers can run an nftables firewall. Your task is to write two nftables configurations (one for each router). You need to write a chain for the forward hook (for each router) that allows

- Alice to start and use connections to the web server and the Internet (using TCP and UDP with arbitrary port numbers),
- the web server to start and use connections to the database server's TCP port 3306, and
- everyone in the Internet to start and use connections to the web server's TCP port 443.

Note that none of the servers shall be allowed to access the Internet (with exceptions that follow from the requirements above). Your firewall configuration must prevent the attacker (located in the Internet)

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

to access any device connected to the internal network and the perimeter network (with the exception stated above). If the attacker takes over the web server, your configurations must still prevent the attacker from accessing Alice or the database server (with the exception that the web server may access TCP port 3306 of the database server).

Write your firewall configurations in nftables syntax such that the configurations can be deployed into a real-world Linux system. Researching the syntax of nftables is part of this problem.

Problem 2: Web of Trust and PGP

In ILIAS you can find the ZIP archive `gis-homework-05-problem-2.zip`. This archive contains the files that are referred to in this problem.

(a) The file `pubkeys.asc` has been created with the tool GnuPG[2] (a PGP implementation). This file contains several public keys for which the key binding has been verified by various users (representing a web of trust). (5 points)

Who certified which key binding? Draw a picture analogous to the lecture (Slide Set 11, Slide 44)! (Only consider signing/certification keys, you can ignore encryption (sub)keys that are also listed in GnuPG's output.)

Hint: You need to install the tool GnuPG on your computer and you need to import the file into the tool. Finding out how to use GnuPG is a major part of this problem.

(b) In the ZIP archive you can find five signed messages. Who created the signatures? (5 points)

Assume that Alice trusts every key binding for which she finds a valid certification chain. Which of these signatures are trusted by Alice?

[2] `https://www.gnupg.org/`