Mittuniversitetet
MID SWEDEN UNIVERSITY

DT149G Administration of UNIX-like systems

# Laboratory Assignment: tutis ad absurdum (working title)

Lennart Franked*

lab_assgn6.tex 2071 2014-11-05 10:14:51Z lenfra

## Contents



## 1 Introduction

This laboratory assignment will cover firewall configurations, and adding DNSSEC support to your bind server.

## 2 Aim

After completion of this assignment you will:

- Have the knowledge of setting up an IPTables firewall.
- Have basic understanding of DNSSEC.

*E-post: lennart.franked@miun.se.

# 3 Reading instructions

Before starting this assignment you should have read chapter 22 and chapter 17.13 in Nemeth et al. [3]. You should also read the Internet System Consortiums document about DNSSEC and BIND [1].

# 4 Tasks

Perform the following tasks and document all the steps taken to complete them

## 4.1 IPTables

Linux use the Netfilter framework to filter packages, enable NAT or PAT and perform other forms of packet mangling, see [2] for more information about netfilter. In this section we are going to work with IPTables, which is a text based front-end for Netfilter. In the previous assignments you have set up an FTP, NFS, SAMBA/CIFS server, also DNS and email server, we must therefore make sure that our firewall will let these services through. We also want to be able to connect to FTP servers to retrieve files, and to connect to our server using SSH and browse the Internet. Last but not least we would like to make sure that we can send and receive ICMP echo and request packets to and from our server, but nothing else.

With this in mind we can create the following firewall policy:

- Drop all incoming packets by default.
- Allow all traffic to and from the local network.
- Allow all incoming packets using transport protocol TCP and port 137-139, 445 (SAMBA/CIFS).
- Allow all incoming packets using transport protocol TCP and port 20,21 (FTP).
- Allow all incoming packets using transport protocol UDP and port 53 (DNS).
- Allow all incoming packets using transport protocol TCP and port 25 (SMTP).
- (If applicable) Allow all incoming packets using transport protocol TCP 465 (Secure SMTP).
- Allow all incoming packets using transport protocol TCP and port 110(POP).
- (If applicable) Allow all incoming packets using transport protocol TCP and port 995 (Secure POP3).
- Allow all incoming packets using transport protocol TCP and port 143.
- (If applicable) Allow all incoming packets using transport protocol TCP and port 993 (secure IMAP).

- Allow all incoming packets using transport protocol TCP and port 53 (DNS).
- Allow all incoming packets using transport protocol TCP and port 80 (HTTP).
- Allow all incoming packets using transport protocol TCP and port 443 (HTTPS).
- Allow all incoming packets using transport protocol ICMP of type echo-request.
- Allow all incoming packets using transport protocol ICMP of type echo-reply.
- Allow all outbound packets.
- Enable stateful packet inspection

Since the rules for IPTables are added with the help of the `iptables(8)` command, the best way to set up your firewall is by adding the commands in a shell script. Therefore create a file named `iptables.sh` and add the following lines at the beginning of the file:

```
#!/bin/sh
#
#IPTABLES SCRIPT
#<COURSE NAME> <COURSE CODE> - ASSIGNMENT 6
#<YOUR NAME>
#
#Creating a macro that specifies the location of iptables.
IPTABLES=/sbin/iptables

echo ‘‘Flushing existing tables and setting default
    policies’’
$IPTABLES -F
$IPTABLES -P INPUT DROP
#Make sure that you replace iptables with $IPTABLES, this
    way you
#will use the macro defined above.
echo "Setting up INPUT chains"
#Add your input and output chains below
```

Replace everything that is written within <>, then add your iptables commands after ‘Add your input and output chains below‘.

## 4.2 Securing DNS

In this section you will further secure your DNS-server by setting up DNSSEC. This security service that is based on an asymmetric encryption scheme and chain of trust, will among other things make your domain less susceptible to DNS cache poisoning attacks.[1]

[1] An attack that can send false DNS replies about your domain redirecting the traffic to another host.

1. Start by enabling DNSSEC by adding the `dnssec-enable yes` option to your named.conf file.

2. (Optional.) Enable the `dnssec-validation` option as well to make your DNS server validate received signatures from other servers.

3. Generate your zone signing key (ZSK) and key signing keys( KSK) with the help of the `dnssec-keygen(8)`. What key size did you choose for the ZSK and KSK? Motivate your choice.

4. `dnssec-keygen(8)` generated two files per key pair, *.key* and *.private*. Explain the contents of these files.

5. Include your KSK and ZSK public keys in your domain zone file using the `$include <public key>` syntax to ensure that your public keys will be self-signed.

6. Now that you have your ZSK and KSK its time to sign your zone with the help of the `dnssec-signzone(8)` command.

7. What must be added in the parent zone to ensure that your signed zone can be validated through a chain of trust?

8. Explain why DLV-servers (DNSSEC Look-aside Validation) and the corresponding DLV records exist and how they work.

9. When is it necessary to set the `dnssec-lookaside` option in `named.conf`?

10. Present the difficulties with key rollover for both ZSK and KSK and how to achieve this in a secure manner.

# 5 Examination

Hand in a report containing all your solutions to the questions in section 4.

# References


[1] DNSSEC and BIND, 2010. URL `http://www.isc.org/software/bind/dnssec`.

[2] Netfilter, 2012. URL `http://www.netfilter.org`.

[3] Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley. *UNIX and Linux system administration handbook*. Prentice Hall, Upper Saddle River, NJ, 4th ed. edition, 2011. ISBN 978-0-13-148005-6 (pbk. : alk. paper).