1. Intro

Djedefre is a tool for documenting your network.

Djedefre consists of 3 parts:

- the database
- scan scripts
- the GUI

The scan scripts fill the database. The GUI displays the network in the database and allows the user to change certain values. The database is created when the GUI is first started.

Some time ago, there was a tool called Cheops, that automated network discovery and gave a nice drawing of the network. Cheops is now abandonware. Djedefre was pharao after Cheops.

2. Using Djedefre

2.1 First start

After installing or unpacking,

- Move to the directory where `Djedefre` is installed.
- Make sure that there is a directory `database` and create it if it is not there
- start the GUI with `./dedefre.pl &`

You will be greeted with a cartouche depicting the hieroglyphs for Djedefre with a number of buttons above it.

The buttons give access to functionality:

- List network provides several lists (servers, subnets, interfaces)
- Plot network provides a drawing of the network
- Options tell Djedefre to do or change something

At this point, when you press the "Plot network", you will get an empty drawing.

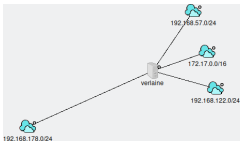
2.2 Start scanning

To get some information into the database, scan-scripts are used. These scan-scripts can be launched from the "Options" page. Although it is possible to launch the scripts in any sequence you like, some scripts rely on information in the database. For example: the "subnet" scan scans all the subnets in the database. If there are no subnets, nothing is scanned.

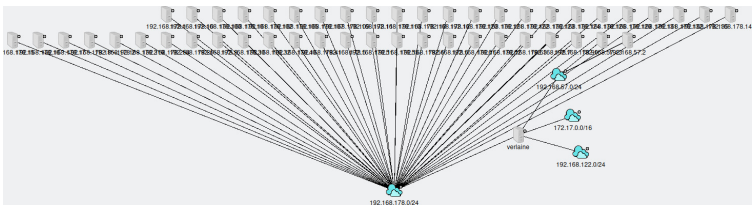
The best start would be to scab the "local system". This launches the script `scan_local_system.sh` in the `scan_scripts` directory in a separate `xterm` window.

When the scan is finished, the plot page will show the local system and the subnets that it is connected to.

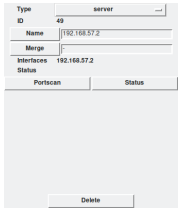
With the left mouse button, you can pick-up the server and the subnets and place them anywhere on the canvas that you like.



As there are now subnets in the database, a scan of the subnets is possible. Select "subnet" under Scan scripts in the Options page. Again, an `xterm` window opens, and when it is finished, the plot will look something like this:



Servers are placed in neat little rows and can be placed anywhere on the canvas, again with the left mouse button. With the right mouse button, a detail window opens that allows you to change the type, change the name or merge servers together. It is also possible to delete the server or do a port scan on it.



2.3 Scanning the network

You may have noticed that the scan of subnets did not provide a complete list of all the servers on the network. This is because the subnet scan uses `fping` to scan the subnet. Typically, for example, Windows 10 does not reply to a ping, so no Windows 10 machines will show up. An ARP scan however will detect those machines if they're on the same layer 2 segment.

There are a number of scan scripts available. These scripts try to find out what the network lay-out is, what the systems are.

- local_system
- subnet
- arp
- access
- type
- server
- remote_system
- cisco
- dns
- vbox
- status
- internet
- database_integrity

The scan scripts are in the diretcory `scan_scripts` and they are called `scan_xxxxx.sh` with `xxxxx` meaning the name of the scan.

2.3.1 local_system

Adds the local system to the network. Also adds the interfaces and the subnets that the system is connected to.

2.3.2 subnet

Scans all the known subnets for servers. Uses `sudo fping` for the scan.

2.3.3 arp

2.3.4 access

2.3.5 type

2.3.6 server

2.3.7 remote_system

2.3.8 cisco

2.3.9 dns

2.3.10 vbox

2.3.11 status

2.3.12 internet

2.3.13 database_integrity

CONTENTS