B2 - Lab 4

Instructions

This lab should be done by groups of 1 or 2 people.

Your markdown document will be used the generate a pandoc pdf so respect the markdown spec and use previews (available in any decent text editor).

the following header should be present at the top of your markdown document (obviously adapted to match your group).

```
---
title: ”B2 - Lab 4 - GROUP X”
author:
-  GROUP MEMBER 1
-  GROUP MEMBER 2
output:
  pdf_document: default
---
```

Only ONE file drop will be allowed per group so verify that your document contains VALID markdown and image links.

When unziped in a new folder the output the following file structure SHOULD be followed.

```
lab4.GROUP_NB.zip
lab4.GROUP_NB
├── images
│   ├── bar.jpeg
│   ├── foo.png
│   └── ...
└── lab4.GROUP_NB.md
```

Replace GROUP_NB by your group number. Penalties will be applied if the required format is not respected.

the pdf corresponding your exercise will be generated as follow

```
unzip lab4.GROUP_NB.zip
cd lab4.GROUP_NB
pandoc lab4.GROUP_NB.md -o lab4.GROUP_NB.pdf
```

Your explanations will be followed strictly and should be precise enough in order to be able to redo the full exercice. Exercices should be done with GNS3 using only the following appliances: ethernet switches, alpine linux, OpenWRT.

During thoses exercices you will see sometimes see that you should allow tcp, udp or both. You are encouraged to test your trafic rules with a client and a server for that use. On alpine you should use https://pkgs.alpinelinux.org/package/v3.3/main/x86/netcat-openbsd On openwrt GNU netcat should work as well.

Part 1: Lan One

Create a network with the following topology:

- 1 openwrt router connected to a NAT network
- 1 ethernet switch connected to the lan port
- 2 alpine linux connected to the switch (`m1` and `m2`)

Remote management interface

Allow remote access to LuCI interface from outside. From now on, LuCI or the cli could be used to do the same tasks.

Network configuration

Use and configure the following subnet (`LAN`) 192.168.XX.0/24 where XX is your group number. Use 192.168.XX.1 for openwrt. Change the configuration of the DHCP server to give addresses from 2 to 200 One alpine linux (`m1`) should use dchp, the other one (`m2`) should get one of the remaining ip not in the previous range.

`m2` should be configured to use the default openwrt DNS.

Find the netcat commands used to listen to udp and tcp. For TCP and UDP give the netcat commands to:

- on `m2` listen on port 88XX where XX is your group number (if your group number is single digit, prefix it with a 0)
- on `m1` connect to the following server
- the server should not die when a client disconnects

Part 2: Subnet

Activate one of the 2 remaining network interfaces on openwrt, call this interface `LAN2`. Choose a 2 host subnet in the private ip range (different from the previous subnet), assign the first one to the router interface. Connect a new alpine linux `m3` this network take the other available address, this machine should have a static ip and use the DNS available with openwrt.

Part 3: Firewall

Tweaking a firewall zone associated with `LAN2` allow machines in this subnet to access to the internet. Allow machines from `LAN` to communicate with machines in `LAN2` the reverse should not be possible. Connections from wan on port 77XX (TCP only) should be redirected to `m3` on port 63XX where in both cases XX is your group number (if your group number is single digit, prefix it with a 0) Connections from wan on port 63XX (UDP only) should be redirected to `m2` on port 63XX. Do this using port forwarding and using NAT (one for each). Explain the differences between those 2 methods.

Confirm that your setup is working by doing the following:

- creation of a new nat network
- an alpine linux `m4` in dhcp mode connected to this new nat.
- connect `m4` to `m3` with netcat
- connect `m4` to `m2` with netcat

Part 4: Misc

fun with pipes

Using netcat client in tcp on `m1` talk to `m2` and then forward the messages in udp to `m4`.

SSH access

Configure dropbear or openssh server, login with password should be disabled. An ssh client on `m4` should be able to connect.

Make luCI only accessible by `LAN` network only or by using an ssh tunel. To test this you could use your host or `m4` using wget to verify that the login mage is loaded.