Workshop in Information Security – Homework #1

First step: setup the environment

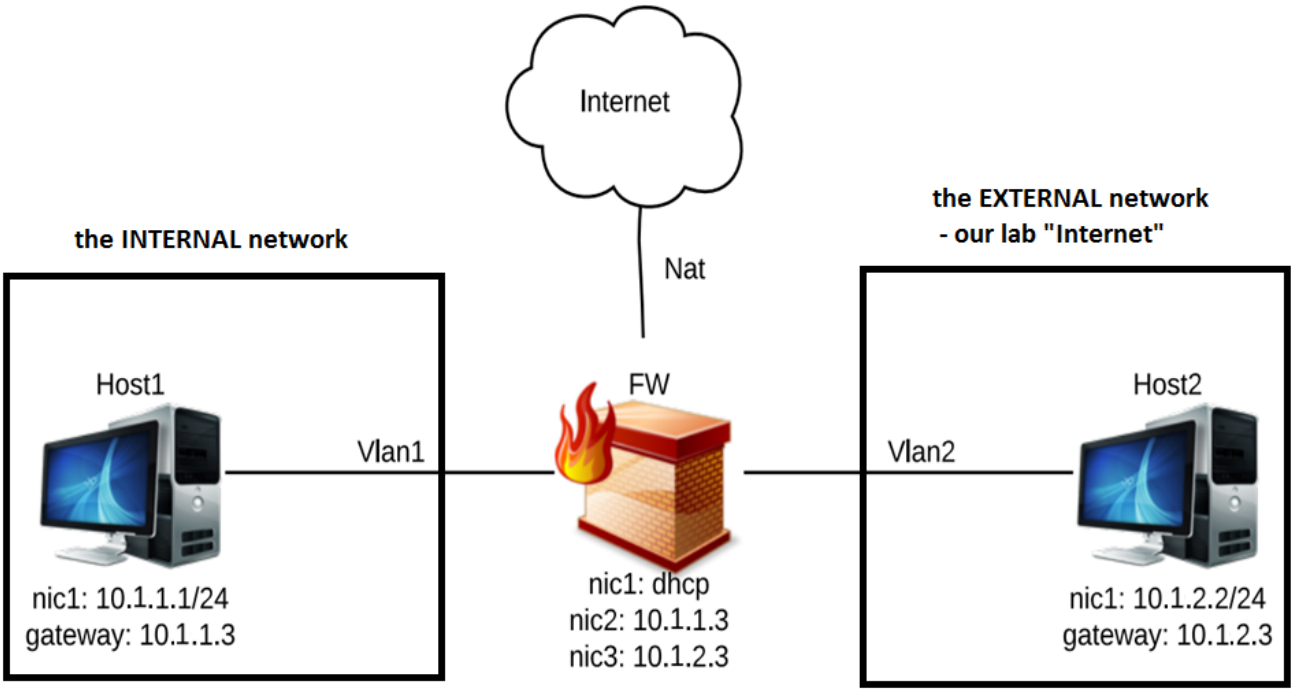
We want to setup an environment, to illustrate the real world networks.

This is very common practice in network security research. It makes things easier and gives the full control on our lab. In addition, in case of real vulnerability testing, it promises no real computer will be infected.

This setup will serve us all over the workshop, so after things are working, save your machines and take a snapshot.

It is highly recommended to save all your code on your computer (and not on the virtual machine), even better on cloud (GIT is a great solution).

Our lab:



Notes:

- In the Moodle there are client, server and FW **fully configured** machines available for you
- You only need to download, extract and add them to VirtualBox, and the lab is ready
- On FW machine, nic2 is connected to vlan1, and nic3 to vlan2
- Make sure (by “ping” Linux command) you have a stable connectivity between each host in our lab’s network
- Save your lab by taking snapshot on all the machines
- For more help with network configuration see here: https://www.cyberciti.biz/faq/setting-up-an-network-interfaces-file/

Second step: write the kernel module

In this homework, we will write a very basic kernel module, which makes a verdict on a packet (accept/drop) based on its type (and **not** its content).

The name of this module will be hw1secws.

The tasks of this module are:

- **Allow** local connection **to** the FW or **from** the FW
- **Block** connection going **through** the FW, means connection between host1 and host2 **via** the FW

Use Netfilter API as we have learned. Use the hook function smartly, and keep it simple.

Tip: you don't really need in this exercise to extract any field from the IP header, TCP header or any other data from the packet itself!

Print messages according to your verdict. When the verdict is "accept", print (using printk()):

*** Packet Accepted ***

When the verdict is "drop", print:

*** Packet Dropped ***

You will be able to see these messages via "dmesg" shell command on your terminal

Submission

Prepare a ZIP file, contains:

- "module" folder, includes hw1secws.c file (the module) and the Makefile
- Dry documentation

General rules for submission, valid for the next assignments as well:

- Document your code
- If you use a code from the internet, document it and add the source
- Individual submission
- If needed, split the files into a modular files

Good luck!

