Workshop in Information Security – Homework #1

*First step: setup the environment*

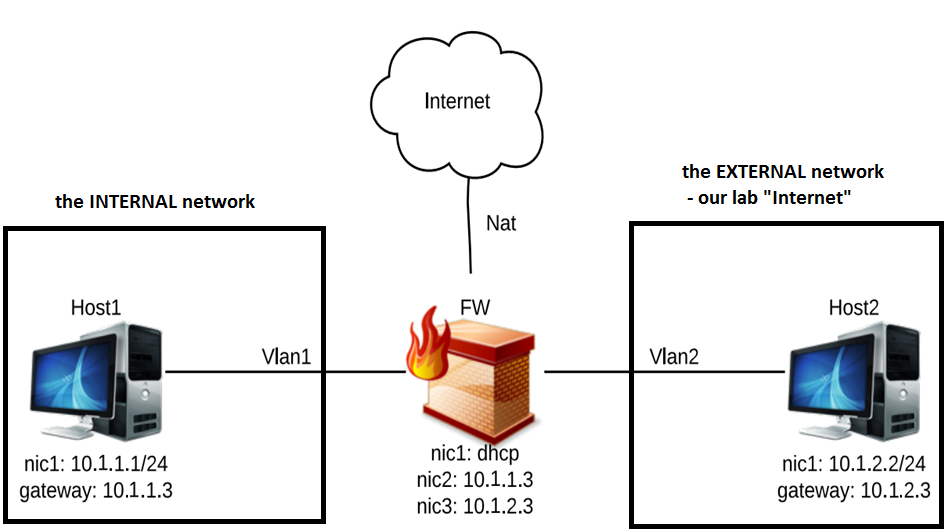
We want to setup an environment, to illustrate the real world networks.

This is very common practice in network security research. It’s make things easier and gives us the full control on our lab. Also, in case of real vulnerability testing, it’s promise no computer will affect.

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

It’s 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:

* All the subnets are 255.255.255.0, AKA x.x.x.x/24
* On FW machine, nic2 is connected to vlan1, and nic3 to vlan2
* You have to clone the “host” to create 2 machines, one for host1 and one for host2
* Enable (make it constant) IP forwarding on FW machine, otherwise you will not be able to pass traffic through this machine
* 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, that make a verdict on a packet (accept/drop) based on their type (and not their 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 “accet”, 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!