T5 - Initiation to security

T-SEC-500

You shall not pass

A Hobbit's tall

+ ONCE UPON A TIME

You have just arrived on an infrastructure that has no notion of security. You will need to set up network and system security.
To do this, you are asked to set up an architecture of 3 virtual machines (1 client, 1 gateway, 1 server).

+ HOBBITS

First, prepare a diagram of the requested architecture:

- 1 “client” VM in a network
- 1 “server” VM in another network
- 1 “gateway” VM with access to both network AND configured in NAT with the external network (internet)
- List of all the services for each VMs

The “client” VM will be the one used to access services of the “server” ones with all requests resolved by the gateway.

Then, install these virtual machines using VMare or VirtualBox and setup the following services:

- SSH
- DNS (master for the “server”, slave for the “gateway”)
- DHCP
- NAT
- Apache
- MySQL
- 3 users (Victor, Jonathan and Marc)

All your VMs must use debian 10 “Buster” as operating system. Neither the server nor the gateway must have a graphical interface.

Think about which services must go on which virtual machine(s).

+ YOU'VE A PAIR OF SNEAKERS, STAY OUT

Now it's time to do add some system level security :

- SSH access for each user
- No way to directly SSH into a server as "root"
- Block the access for 30 seconds after 3 failed attempt
- Only "Jonathan" should be able to become execute commands as "root"
- Log the connection history

And some network level security :

- To external networks:
  - all access to the EPITECH network
  - http and https only for all other external networks
- To the "server":
  - only allow http, https, ftp, ssh and dns
- To the "gateway":
  - only allow dhcp and dns