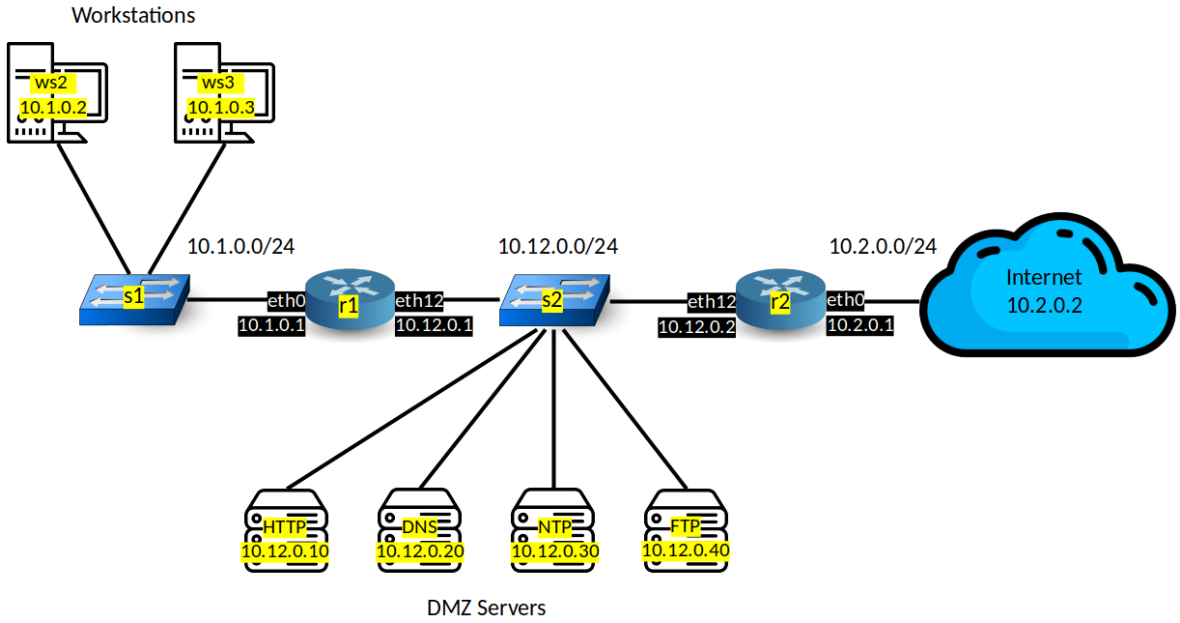
LINFO2347 – Project Network Attacks

The goal of this project is to develop network attacks, as well as a protection against them, on a given network topology, emulated with the `mininet` tool. This project must be done by **groups of 2 students**. The deadline is **Friday, May 19, 18:00**.

Mininet topology

`mininet` is a powerful tool to emulate networks. It has a Python API, making it easy to configure and deploy. Documentation is available here.

We will give you a (vulnerable) `mininet` network topology as a playground to implement your attacks and protections. This topology mimics a typical enterprise network:



More precisely, the servers run the following services:

- HTTP: Apache2 HTTP server
- DNS: dnsmasq
- NTP: OpenNTPD
- FTP: vsftpd

For ease of deployment, this topology is embedded into a VM, that you can download here.
The credentials are mininet/mininet.

To run the topology, execute the following command:

```
sudo -E python3 ~/LINFO2347/topo.py
```

You can run a `pingall` test on the topology, i.e. a test that checks connectivity between all devices in the network, by running the following command:

```
sudo -E python3 ~/LINFO2347/topo.py -p
```

Basic enterprise network protection

As a preliminary step, you must make the topology a bit more secure. Currently, any host in the topology can initiate a connection with any other. To make it more similar to an actual enterprise network topology, you must deploy firewall rules (using nftables) which implement the following policies:

- Workstations can send a ping and initiate a connection towards any other host (other workstations, DMZ servers, internet).
- DMZ servers **cannot** send any ping or initiate any connection. They can only respond to incoming connections.
- The Internet can send a ping or initiate a connection **only** towards DMZ servers. They cannot send a ping or initiate connections towards workstations.

For the rest of this document, the functionality of this more secure network will be considered as the **normal operation** of the network. Naturally, once this protection is enabled, the `pingall` test will not succeed anymore.

Network attacks

Throughout the course, you have seen the functioning of multiple network attacks, as well as means of protection against them. For this project, we ask you to implement at least 3 network attacks seen in the course, with a way to protect against them.

Examples of attacks include, but are not limited to:

- Network scans (with any protocol)
- SSH/FTP brute-force attack
- (Reflected) DDoS
- DNS/ARP cache poisoning
- Botnet

Your attacks must take the form of runnable scripts, which can be executed on one of the topology's hosts. Consider the scapy tool to forge and send network packets. The attacks must be implemented by yourselves, which means you **may not** use a tool to perform specific tasks (e.g. you may not use Hydra for password brute-forcing).

Your means of protection must take the form of network firewalls, implemented with nftables.
You can implement the firewall rules on any host of the topology (workstations, servers, routers), depending on the attack you want to prevent.
Warning: blocking traffic only based on specific IP addresses is not considered as a solution !

You must provide separate scripts for attacks and protection, such that we can test them separately.

Make sure that normal operation of the topology, i.e. connectivity between any pair of devices, is still possible when your means of protection are active.

Report

You must write a small report, detailing the functioning of your attacks and your means of protection. Additionally, the report must contain instructions on how everything can be executed on the project VM. Ideally, this report should be written as a GitHub README, in the **md** format. Please be straightforward and keep it short.

Summary

Here are the project's intended objectives:

- Basic enterprise network protection
- 3 attacks successfully implemented (+ up to 2 more for additional grades)
- Protection successfully implemented (while not disrupting normal operation)
- Report describing your attacks and protection means
- Instructions on how to launch topology, attacks and protection

Deliverable

The INGInious task for submission is accessible at https://inginious.info.ucl.ac.be/course/LINFO2347/project-network-attacks. You must register to a group on INGInious with your partner to be able to submit.

You must submit a ZIP archive containing:

- The mininet topology.
- Firewall rules for basic enterprise network protection.
- A folder containing your attack scripts.
- A folder containing your protection scripts.
- A report, as a README in the md format, which describes your attacks and means of protections, as well as instruction on how to launch both.