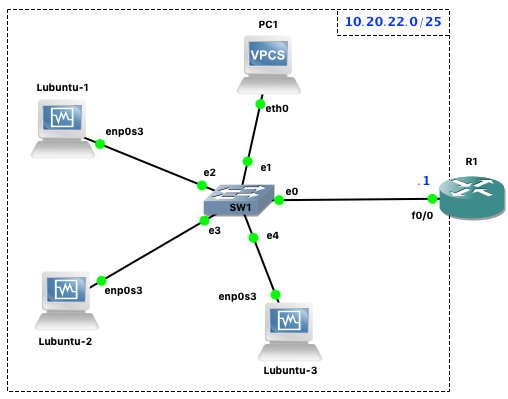
## **›**Assignment 1: Python Worm

The goal of this assignment is to create a worm program using Python to infect other similar machines on a GNS3 network. Do not run your code outside your sandbox network. You may work with a group (maximum 2 members) on this assignment.



**To Do List**:

* Create and configure a similar GNS3 topology shown above using 3 Lubuntu VMs (osboxes.org), a VPCS, and a Cisco router (as DHCP server).
  + Make sure that all the Lubuntu VMs have the required external Python modules **(**paramiko, netifaces, python-nmap, & pynetinfo) using the pip/pip3 command.  
    E.g., Python 2.x: pip install paramiko netifaces python-nmap pynetinfo
  + Install the nmap utility on all Lubuntu VMs: $ sudo apt install -y nmap
* Complete the provided skeleton Python code (worm.py) using either Python 2.x or Python 3.x. Specify which Python version you used on your README file.  
  + If the program is not launched from /tmp, then your program should copy itself to this directory and mark it as infected (see isInfectedSystem and markInfected functions).
  + The infected.txt should be created by running the worm’s markInfected(), not by transferring it by SSH File Transfer Protocol (sftp).
  + Only the worm.py itself should be copied via sftp to remote hosts. All the infected lubuntux86 hosts should have both /tmp/infected.txt and /tmp/worm.py at the end. You must also show how to handle unmatched credentials against the VPCS and router in the process.
* Copy the worm.py in one of the three Lubuntu VM where it will be executed and infect the other two Lubuntux86 VMs using SSH dictionary attack.

**Provided Files (**[**worm.zip**](https://drive.google.com/file/d/10Iee3GI_l8BeDRb-LciWVxHqepb83hXL/view?usp=sharing)**):**

*worm.py :* This is the main Python code to implement the worm program.

*getip.py :* This file shows how to retrieve the IPv4 address(es) of a given host’s network interface(s) except the localhost (127.0.0.1). *This is only a support file and does not need to be submitted*.

*hostscan.py :* This file illustrates how to scan the LAN for other hosts running SSH server (on port 22). *This is only a support file and does not need to be submitted*.

**Grade Breakdown:**

* **95%** - The completion of a Python worm program using the provided skeleton code to infect and self-replicate to other potential victim systems on the same network. All (Lubuntu) hosts should be infected and marked as such after running the worm.py.

* **5%** - Proper documentations in README file

Important: Grading the assignment shall be based on the Lubuntu VM from osboxes.org used in class. Be sure to also test it to ascertain that your program works as expected in a similar environment.

**What to turn in on Canvas?**

* Compress both worm.py and README file to a single (zip, 7z or tar) file using your name(s). (e.g.: hernan\_manabat-assign1.zip)

* + The README file must include name(s), instructions on how to execute the worm. Whether any extra credit was done and any additional information.

* + Your worm.py tested using the provided Lubuntu VMs on GNS3.

Optional)

1. Integrate a working cleaner function and logic to reverse the spread and self-clean the worm program from each host using an argument.

* (e.g., python worm.py -c or python worm.py --clean).

1. Make the worm spread to another Lubuntu system located in the adjacent network. Extend the primary GNS3 topology with another network consisting of another VPCS and a Lubuntu VM. Configure router R1 f0/1 interface to act as the DHCP server for LAN #2.

* (e.g., python worm.py -m or python worm.py --multi).

