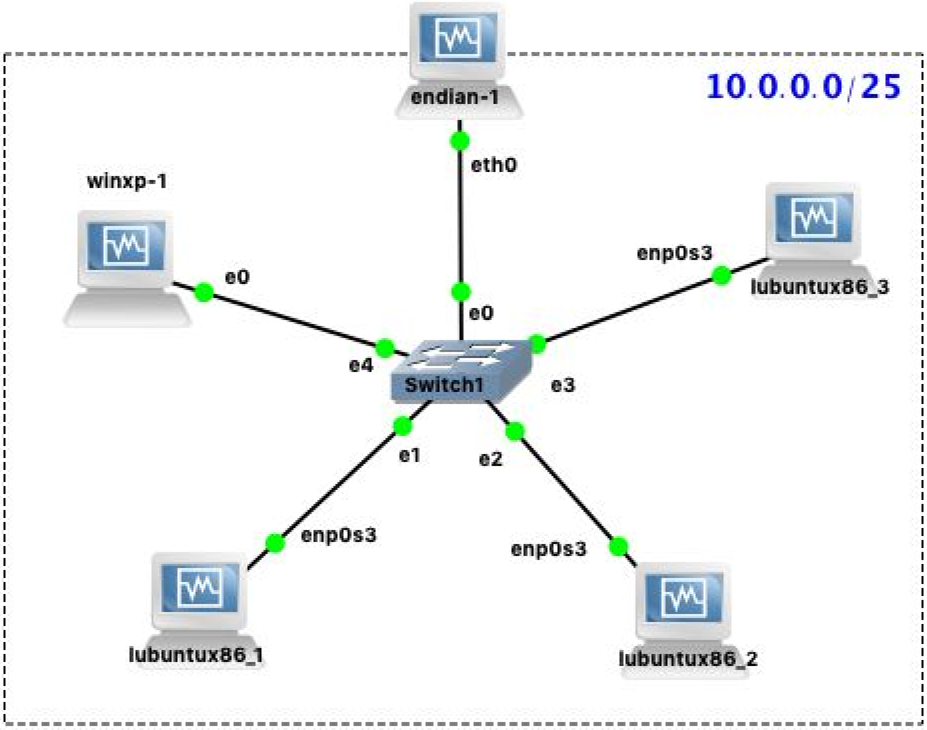
CPSC 456 **Assignment 3: Python Worm Program** Fall 2020

Due: Saturday, December 12th @ 11:59 PM



Complete the skeleton Python program called worm.py. Run in on a similar GNS3 topology shown above using 3 Lubuntux86, WinXP, and an Endian VMs. Copy the worm.py in one of the three Lubuntu VM where it will be executed and infect the other two Lububtux86 VMs using SSH dictionary attack. If the program is not launched from /tmp, then copy it to this directory and mark it as infected (see isInfectedSystem and markInfected functions). Note that 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 endian VM in the process.

Provided Files:

- `getip.py` : Shows how to retrieve the IPv4 address(es) of a given host's network interface(s) except the localhost (127.0.0.1). *Do not submit this file.*

- `hostscan.py` : This file illustrates how to scan the LAN for other hosts running SSH server (on port 22). *Do not submit this file.*

- `worm.py` : Main code to implement the worm program for the assignment.

Python modules on Lubuntux86 VMs: paramiko, netifaces, nmap, & pynetinfo

Grade Breakdown

- 95 % - The completion of a Python worm program (`worm.py`) using the provided skeleton code to infect and self-replicate to other potential victim systems on the same network.

- 5 % - Proper documentations in `README` file

Important: Grading the assignment shall be based on the VMs provided in class. Be sure to also test it to ascertain that your program works just as expected.

You may copy the VirtualBox OVA files at the class Google shared folder or download from http://tech.ecs.fullerton.edu/cslabs/vms. Import (3) `lubuntux86.ova, winxp.ova` and `endian324.ova` to start your environment. You do not need to change the network settings as all should be pre-configured as it is on the server.

What to turn in on Titanium?

- 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, 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.

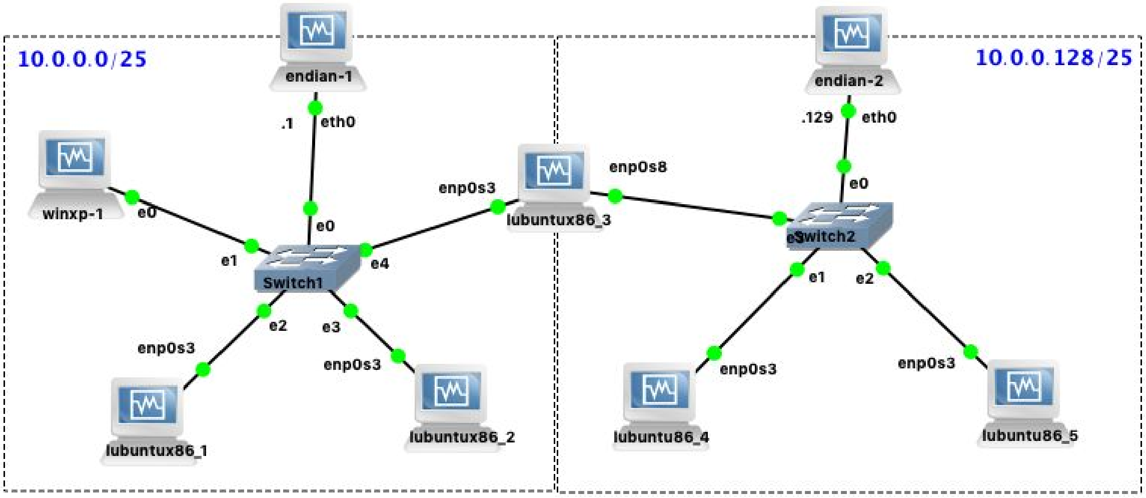
(Optional) **Extra Credit 1: 10%**

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`).

(Optional) **Extra Credit 2: 20%**

Make the worm program spread to other systems connected to another network using multiple network interfaces on one host that is connected to two different networks.

- Extend the primary GNS3 topology with another network consisting of an endian and two additional Lubuntu VMs.
- Setup up Lubuntux86_3 VM to connect to both networks. (i.e. Network #1: 10.0.0.0/25; Network #2 10.0.0.128/25)


10.0.0.0/25
endian-1
.1
eth0
winxp-1
e0
e1
e0
Switch1
e4
enp0s3
lubuntux86_3
enp0s8
e2
e3
enp0s3
enp0s3
lubuntux86_1
lubuntux86_2
endian-2
.129
eth0
10.0.0.128/25
e0
e3
Switch2
e1
e2
enp0s3
enp0s3
lubuntu86_4
lubuntu86_5