Assignment 1: Python Worm Program

Due (Extended): *Sunday, Mar 1 @ 11:59 PM*

Provided Files:

- *getip.py* : Shows how to retrieve the IP of the network card with an IPv4 address that is not the localhost (127.0.0.1)
- *hostscan.py* : This file illustrates how to scan network for other host systems running SSH server (on port 22).
- *unittest.py* : Similar to hostscan.py, but this scans all active ports on hosts found on the network
- *worm.py* : Main code to implement the worm program for the assignment

Python modules: *paramiko, netifaces, nmap,* & *pynetinfo*

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.

- **5 %** - Proper documentations

Grading the assignment shall be based on the Multix VMs used in class. You may also copy the VirtualBox OVA files (`/home/VMs`) from the Multix server(s) and import them on your local machine. Be sure to also test it on one of the Multix servers assigned to you to ascertain that your program works just as expected.

Note*: Refer to the procedures posted on Titanium on how to connect to Multix.*

OVA files used in this assignment are: `lubuntux86.ova & endian324.ova`

What to turn in on Titanium?

- Compress both `worm.py` and `README` file to a single `zip, 7z or tar` file. (e.g. `<hmanabat_assignment2>.zip`)

    - The `README` file must include name, instructions on how to execute the worm and worm cleaner, whether any extra credit was done and any additional information.

    - The Python worm program tested on the Multix system.

(Optional) Extra Credit: 10%

A working cleaner function and logic to reverse the spread and self-clean the worm program from each host using an argument (such as **`python worm.py -c`** or **`python worm.py --clean`**).

(Optional) Extra Credit: 20%

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

- This requires setting up another network where some system(s) on another network is connected to both.
  (e.g. Network #1: 192.168.1.0/24; Network #2 192.168.2.0/24)

- The computer(s) connected to multiple networks would be infected and spread on other vulnerable hosts on another network using the other network interface.