CISC 367 – Spring 2016

Team Assignment – Python Worm

In this assignment, you are to develop a worm in Python which

1. Scans a new IP address and if SSH daemon is running, tries and bruteforces the login/password (brute-force attack),
2. If the worm succeeds, then upload a copy of the worm *itself* and the *dictionary* file to the host, and
3. Runs the copy, so it can now do 1–3.

To implement the port scanning part, please refer to Port scanner in Python.

To implement brute-force attack and worm propagation, please refer to
Simulating an SSH Worm using Python .

In particular, `SSHDictionaryAttack.py` is a Python program that does brute-force attack, and `UploadAndExecute.py` is a Python program that **upload** *a copy of itself* to the host hacked.

To make a copy of a program itself, you may need to refer to the Python program in `How to Make a Simple Computer Virus with Python`.

The dictionary file would be in the following format.

```
[/Users/cshen/PythonWorm 577] more dictionary
hello               world
happy               happy
<your-username>     <your-password>
sad                 veryverysad
```

You are to develop this worm in one single Python program termed `PythonWorm.py`. Test your implementation on your laptop with two other Linux VMs running. On your laptop, do

```
$ python PythonWorm.py IP-addr-1 IP-addr-2 dictionary
```

For instance, the worm should propagate from my laptop to user `cshen` on VM_1 with IP-addr-1, and then from VM_1 to user `cshen` on VM_2 with IP-addr-2.

To use the SSH protocol, you will need to install the paramiko library on your laptop and the Linux VMs via `sudo pip install paramiko`.

Extra credits: Add a *signature* into the worm itself so that when it hacks into a host that had been hacked before, the propagation stops.

You may refer to the virus Python program in `How to Make a Simple Computer Virus with Python`. to see how to check for signature.