Lab Sheet 4

Security

In our fourth lab, we will implement a virus in Python. The virus will be a Python script which infects other Python scripts and copies its payload into them. This is very much the same way as any virus would attack executable files and infect them with malicious code.

1 Task 1: Directory and Files

Create some dummy Python script files (e.g. hello world programs or programs with random code, just make sure it's nothing important that you would like to keep) in a directory in your home folder. Then create a new Python script called `virus.py` in the same safe directory. HINT: Dont' forget to add the "shebang" to your Python files (i.e. the first line in a Python script should always be `#!/usr/bin/env python`.

2 Task 2: Prepare Virus Code

To implement the virus, we will follow these steps:

- Clearly mark where the virus starts (use `### VIRUS BEGIN ###` and `### VIRUS END ###` comments.
- The virus will have to access files and directories, copy itself, etc. Therefore we will need to import the libraries `sys, glob, re` (make sure you know what these libraries offer and what they are here for). So import these libraries.
- Our virus (same as every other virus) has the following major functionality:
    1. Makes a copy of itself.
    2. Finds potential victims.
    3. Checks and infect.
    4. Optional payload.

3 Task 3: Copy the Virus

To copy the virus, we will need to read in the file that is running (i.e. the virus file) and search for the virus code. Then we will save every line in a list. So this is the code where the virus copies itself. (HINT: Look for your begin and end comments).

4 Task 4: Find potential victims

Use the `glov` library to look for other Python files in the same directory and save them to a list.

5 Task 5: Check and infect

Go through the list of Python files in the directory and for each do the following:

1. Open the file in reading mode.
2. Read the lines and save them to a list.
3. Close the file.
4. Check if the file is already infected.
5. If not, look for the "shebang" and add the virus code between it and the original program code to a list of code lines.
6. Open the file in write mode this time and overwrite the contents with the content of your list.
7. Close the file.

6 Task 6: Add Payload and Run the Virus

Add the payload to your virus (this is the code that does the damage). In our case it is sufficient to just print something like "Infected!!!".

After you did this, run the `virus.py` script and watch what happens to your hello world program. Can you explain what the virus did?