Mentoring Program

Binary-Exploitation (PWN)

/* WHERE THERE IS A SHELL, THERE IS A WAY */

TABLE OF CONTENTS

/* WHERE THERE IS A SHELL, THERE IS A WAY */

01.
Overview

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Overview

Etymology:

The original use was the word “own”, owning a system means having control over it, the word “pwn” came to be due to the adjacency of the letters P and O on a computer keyboard.

Overview

Binary-Exploitation (PWN) is the process of exploiting vulnerabilities found in compiled executable programs (due to mistakes in programming) allowing hackers to have access to secret informations, and in severe cases taking total control over the system

/* WHERE THERE IS A SHELL, THERE IS A WAY */

02.
Tools of the craft

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Tools of the craft

Disassemblers:
- GDB (extensions : pwndbg, peda, gef ..)
- Radare2

Decompilers:
- IDA
- Ghidra

Programming languages:
- Reading C / Assembly code
- Programming in Python (or another scripting language)
- Useful libraries (pwntools)
- General Linux knowledge

/* WHERE THERE IS A SHELL, THERE IS A WAY */

03.
How it works

/* WHERE THERE IS A SHELL, THERE IS A WAY */

How it works

Buffer-overflow:

When the program allocates / reserves a space of memory of size X , But the user can input data of size Y > X.

How it works

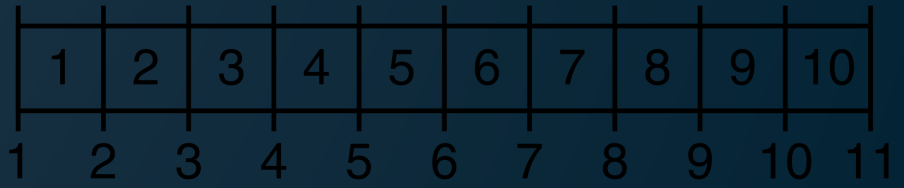
Format-string:

Format strings are a way for programmers to format the output. If controlled by the user (hacker) it can be used both in leaking and overwriting arbitrary data.

How it works

Off-By-One:

If you build a straight fence 30 feet long with posts spaced 3 feet apart, how many posts do you need?



/* WHERE THERE IS A SHELL, THERE IS A WAY */

04.
Mitigations

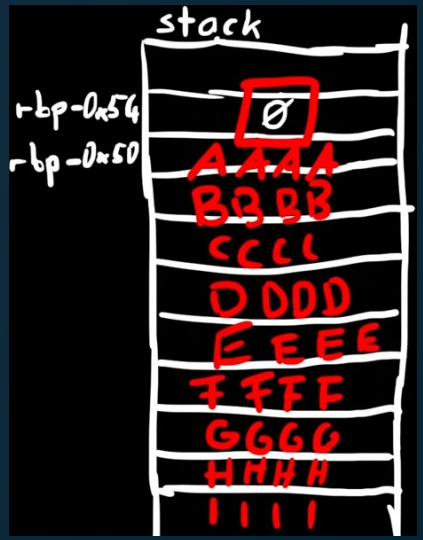
/* WHERE THERE IS A SHELL, THERE IS A WAY */

Mitigations

Stack canary
Position independent Executable (PIE)
ASLR (Address Space Layout Randomization)
Compiler optimizations (placing int before char arrays)

Bypass:

Leaking code/libc/stack/heap addresses using various techniques.



/* WHERE THERE IS A SHELL, THERE IS A WAY */

05.
Resources

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Recources

Binary-Exploitation serie (more than 50 ep)

/* WHERE THERE IS A SHELL, THERE IS A WAY */

MENTORING PROGRAM

/* WHERE THERE IS A SHELL, THERE IS A WAY */