BOP Pwn

Dice CTF 2023

Pwn Presentation/My real pwn presentation

Challenge

- For this challenge, we are only given the binary and the connection details
- We can tell by looking at the binary and playing around with it a bit that it is a stack based buffer overflow and it has seccomp enabled.
- Seccomp basically means that you can only do certain syscalls, in this case open, read, write
- We also don’t have much gadgets except a pop rdi, and printf

What makes a good pwn challenge

- The three things that you should focus on in a pwn challenge is either
  - Making the vulnerability novel and/or interesting
    - One that makes you have to think and reverse the binary
  - Making the exploit novel and/or interesting
    - Maybe you have to learn and implement a new pwning technique
    - Maybe you have to get by a new mitigation
  - Making the program something novel and/or interesting, but easy
    - Make the ctfers learn a new platform
      - Kernel Exploitation, Browser Exploitation, Hypervisor Exploitation

The Exploit

1. Leak libc using pop rdi, (got address) printf
    a. Find the right libc version by doing this three times and using the libc database
2. Find a writable address in memory that is big enough > 64 bytes
3. Then put flag.txt into the binary with a read(0, &writable_memory, 8)
4. Open flag.txt with syscall open syscall(2, &writable_memory, read_only)
5. Read flag into writable memory read(3, &writable_memory, 70)
6. Print out flag with pop rdi, writable_memory printf

The Good and Bad

- The good part of this challenge is that the steps needed to take to get the flag lead you there
  - Do I have enough gadgets? No -> Libc Leak
  - Do I have “flag.txt” in the binary? No -> put flag.txt into binary
  - Can I use system or an execve syscall? No -> do a open, read, write chain
- The bad parts of this challenge is that the binary itself is very bland and boring
  - It doesn’t have any theme and literally just asks something stupid for the prompt
    - No ascii art, or interesting quotes to make the binary exciting
- The challenge itself was also a bit tedious
  - Since they didn’t give you a libc version you have to hunt it which is just time consuming.
- Not much was learned.
  - I only really learned that printf can be used the same way puts does.