Pwn-ing Linux x86/x64 2019
Zadania kwalifikacyjne

Grzegorz Uriasz — gorbak25@gmail.com

27 maja 2019

Ostateczną wersję rozwiązań zadań proszę przesłać mailowo do mnie w formacie pdf, w terminie podanym na stronie WWW. Zachęcam do wcześniejszego przesłania mi rozwiązań zadań na mój adres mailowy – będę wtedy w stanie powiedzieć, co jest źle i podpowiedzieć jak dopracować finalną wersję. Nie wymagam wykonania dużej ilości zadań – większa ich ilość wymagana będzie dopiero przy dużej ilości uczestników. Tak więc wyślij mi to co udało ci się wykonać. Jeżeli coś nie jest jasne, to napisz do nas – z chęcią nakieruję na literaturę bądź wytłumaczę.

Aby zakwalifikować się na warsztaty wystarczy zrobić obowiązkowe zadanie nr. 2 oraz jedno zadanie z grupy 3-6.

1 Korzystanie z Windowsa

Nie polecam korzystania z Windowsa, ponieważ na warsztatach skupiamy się na exploitacji programów działających na Linuxie. Dlatego zachęcam do zainstalowania dystrybucji Linuxa na swoim komputerze w konfiguracji dual boot(wybór systemu przy starcie komputera), np. Linux Mint, Antergos, Ubuntu lub maszyny wirtualnej z Linuxem (w razie czego podczas warsztatów będzie dostępny przygotowany obraz Ubuntu, z którego jednak lepiej korzystać w ostateczności). Ze względu na charakter warsztatów nie polecam korzystać z Windowsowego WSL-a chyba że ktoś czuje się pewny że wszystko będzie mu działało (ssh, gcc, nasm, objdump, assembler, python2, pwntools)

2 Dlaczego chcesz uczestniczyć w tych warsztatach? - Obowiązkowo

Odpowiedz na to pytanie ściśle i zwięźle. Nie jest to zadanie typu "Gdybyś był owocem, to jakim? Uzasadnij twoje stanowisko na minimalnie dwudziestu stronach A4" - oczekuję tylko krótkiego opisu. Oczekuję odpowiedzi o długości maksymalnie 2 zdania :)

3 Captcha - Na rozgrzewkę

Udowodnij mi że jesteś człowiekiem przepisując treść poniższego obrazka:

4 SSH – Instalacja i Przetestowanie

Zainstaluj SSH (zobacz opis warsztatów) i prześlij mi zrzut ekranu, co się wyświetli jak połączysz się z github.com na koncie git (komenda: `ssh git@github.com`, należy zaakceptować certyfikat githuba). Jeżeli wyświetli się permission denied, należy sprawdzić czy wygenerowało się swój klucz oraz czy dodało się go do konta na githubie (które warto założyć, bo nawet jeżeli na tych warsztatach się nie przyda, to później na pewno).

5 Operacje logiczne

Odpowiedz na pytania i rozwiąż poniższe równania.

5.1 W jaki sposób można odejmować używając dodawania?

Dodawanie na bramkach logicznych jest o wiele łatwiejsze do zrealizowania niż odejmowanie. A więc w jaki sposób używając operacji logicznych typu and, xor, or ... uzyskać odejmowanie dwóch liczb binarnych mając układ dodający dwie liczby binarne do siebie?
Porada: Poczytaj o reprezentacjach binarnych liczb ze znakiem.

5.2 Operacje bitowe

Masz do dyspozycji 8-bitową zmienną liczbową bez znaku o nazwie Adam. Zaproponuj działania dzięki których ustawisz i-ty bit Adama na 1 oraz j-ty bit Adama na 0. W jaki sposób sprawdzić czy n-ty bit Adama jest jedynką?

Oblicz na kartce(bez pomocy komputera) poniższe dwa działania:
((24 and 101) or (132 xor 241)) nor 5 = ?
(123 xor 153) xor (246 and 235) = ?

6 Błąd w kodzie C

Poniższy kod zawiera wywołanie funkcji system która otwiera powłokę systemową. Na pierwszy rzut oka dotarcie do tej linijki kodu jest niemożliwe ze względu na sprawdzenie, czy pole casual w strukturze state jest różne od 1. Otóż poniższy kod w języku C zawiera błąd który pozwala przejąć Tobie kontrolę nad polem casual. Twoim zadaniem jest przeanalizowanie kodu, znalezienie wspomnianego błędu i opisanie mi go w rozwiązaniu. W rozwiązaniu podaj przykładowe wejście które pozwala na wywołanie funkcji system oraz sposób naprawy tego błędu.

```c
#include <stdio.h>
#include <stdlib.h>

typedef struct
{
        char tab[100];
        char casual;
} state;

state s;

int main()
{
        int ans, i;
        printf("How many times to loop: ");
        scanf("%d", &ans);
        if(ans<0 || ans>100)
        {
                printf("Invalid number\n");
                return 0;
```

```
        }

        s.casual = 1;

        for(i = 0; i<=ans; i++)
        {
                s.tab[i] = i;
        }

        if(s.casual != 1)
        {
                printf("YOU SHALL NOT CALL ME!\n");
                system("/bin/sh");
                return 0;
        }
        printf("No shell for you\n");

        return 0;
}
```

Powodzenia i do zobaczenia w Zabrzu!