Bezpieczeństwo komputerowe

Laboratorium - lista nr 6 [D]

Zadanie 1 (100 pkt) Poniższy program:

login.c

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


int auth(char *code) {
    int ret, cmp;
    cmp = strcmp(code, "haslo");
    if (cmp == 0) {
        ret = 1;
    } else {
        ret = 0;
    }
    return ret;
}

void login(char *code) {
    int secret = 9;
    int authenticated = auth(code);
    char pass[10];
    strcpy(pass, code);
    if (authenticated) {
        printf("The secret is: %d\n", secret);
    } else {
        printf("Unauthorized\n");
    }
}

int main(int argc, char *argv[]) {
    char code[10];
    strcpy(code, argv[1]);
    login(code);
    return 0;
}
```

został skompilowany za pomocą komendy:
`gcc login.c -o login -fno-stack-protector -z execstack`
Program jest uruchamiany w linii poleceń: `$ ./login pass`.

1. Znajdź jakie ciągi wejściowe (poza ciągiem: *haslo*) powodują wyświetlenie sekretu i dalsze poprawne działanie programu. Wyjaśnij dlaczego się tak dzieje (musisz umieć przedstawić jak wygląda pamięć procesu w zależności od danych wejściowych i wykonywanej instrukcji).
2. Wyjaśnij znaczenie parametrów kompilatora. Które z nich są potrzebne, aby osiągnąć efekt opisany w poprzednim punkcie?

Zadanie 2* Poniższy program:

smartnot.c

```c
#include <unistd.h>

char shellcode[]= "???";
int main(int argc, char* argv[])
{
    int *ret;
    ret = (int *)&ret +2;
    (*ret) = (int) shellcode;
}
```

zostanie skompilowany za pomocą komendy:
`gcc smartnot.c -o smartnot -m32 -fno-stack-protector -z execstack`

Wyjaśnij jakie znaczenie ma każda z podanych opcji kompilatora.

Znajdź taką wartość zmiennej shellcode, aby:

1. (40 pkt) został wyświetlony Twój numer indeksu,
2. (60 pkt) została uruchomiona powłoka (np. /bin/sh).