Secure Coding 2017 - Natív nyelvek

Demo: Támadás a SimpleBOF alkalmazás ellen

- alkalmazás fordítás
- futás idejű elemzés gdb segítségével
- támadás végrehajtása

Feladat: mutassa meg, hogy mely védelmi módszerek hatékonyak a támadás ellen

Stack Smashing Protection

- Fordítsa le az alkalmazást Stack Smashing Protection-nel!

```
make withSSP
```

- gdb segítségével mutassa meg, hogy mi változtott az alkalmazás futásában!
- Tesztelje, hogy a korábban bemutatott támadás működik-e!
- Írja le, hogy miért működik még mindig, vagy miért nem működik a támadás!

NX bit

- Fordítsa le az alkalmazást NX bit alapú védelemmel!

```
make withNX
```

- gdb segítségével mutassa meg, hogy mi változtott az alkalmazás futásában!
- Tesztelje, hogy a korábban bemutatott támadás működik-e!
- Írja le, hogy miért működik még mindig, vagy miért nem működik a támadás!

ASLR

- Fordítsa le az alkalmazást ASLR-rel

```
make withASLR
```

- gdb segítségével mutassa meg, hogy mi változtott az alkalmazás futásában!

- Módosítsa a programot úgy, hogy látható legyen az ASLR hatása! (pl: `printf` segítségével)
- A módosítás miatt változtasson a támadáson, hogy az az új binárison is működjön!
- Tesztelje, hogy a korábban bemutatott támadás működik-e!
- Írja le, hogy miért működik még mindig, vagy miért nem működik a támadás!

Nyelvi megoldás

- Módosítsa az alkalmazás forráskódját, amivel javítja a sérülékenységet! (Funkcionalitás ne változzon, csak a helyes nyelvi elemeket használja!)
- Fordítsa le az alkalmazást!

```
make
```

- Tesztelje, hogy a korábban bemutatott támadás működik-e!
- Írja le, hogy miért működik még mindig, vagy miért nem működik a támadás!