Bootcamp 2018 - Natív nyelvek

Adat alapú támadás #1

A feladat során a sérülékeny alkalmazást úgy kell megtámadni, hogy az alkalmazás memóriájában található adatok megváltoztatásával a program jóváhagyja a további hozzáférést.

Szükséges lépések:

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

Feladat: a felhasználónév megfelelő célzott módosításával érje el, hogy az "Access Granted..." sor jelenjen meg a képernyőn.

A megoldást részletes dokumentációval támassza alá, amiből látszik, hogy miért a választott bement éri el a célt. A megoldás során az alkalmazás ne álljon le hibával!

Adat alapú támadás #2

A feladat során a sérülékeny alkalmazást úgy kell megtámadni, hogy az alkalmazás memóriájában található adatok megváltoztatásával a program jóváhagyja a további hozzáférést.

Szükséges lépések:

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

Feladat: a jelszó megfelelő célzott módosításával érje el, hogy az "Access Granted..." sor jelenjen meg a képernyőn.

A megoldást részletes dokumentációval támassza alá, amiből látszik, hogy miért a választott bement éri el a célt. A megoldás során az alkalmazás ne álljon le hibával!

Controll flow alapú támadás

A feladat során a sérülékeny alkalmazást úgy kell megtámadni, hogy a controll flow úgy változzon meg az

alkalmazásban, hogy a támadó egyből az "Access granted..." sorra ugrik.

Szükséges lépések:

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

Feladat: az alkalmazás elemzése során állapítsa meg a szükséges címet, amelyre ugrani kell, majd a bemenetek ez alapján történt módosításával érje el, hogy az "Access Granted..." sor jelenjen meg a képernyőn.

A megoldást részletes dokumentációval támassza alá, amiből látszik, hogy miért a választott bement éri el a célt.

Hasznos Kiegészítés

- GDB Cheet Sheet