

Sofistikovanější útok

PV173 Programování v C++11

Vladimír Štill, Jiří Weiser

Fakulta Informatiky, Masarykova Univerzita

22. září 2014

Problémy na stacku II.

Ukázka zneužití situace, kdy dochází ke kopírování dat bez zajištění velikosti dat.

Zadání úlohy pochází z kurzu na Univerzitě v Kodani.

Řešení vypracoval Jiří Weiser.

Problémy na stacku II.

Soubory, které jsou k dispozici

- sortfile – spustitelný program, který obsahuje bezpečností problém.
- sortfile.c – rekonstrukce programu na základě assembleru.
- exploit.c – program, který po kompilaci a spuštění provede útok.
- shellcode.asm – assembler, který způsobí spuštění */bin/sh*.

Problémy na stacku II.

Popis situace před útokem.

Problémy programu **sortfile**

- Nekontrolovaný buffer délky 4096.
- Neuzavřený file descriptor po volání funkce *mmap*.

Komplikace při vedení útoku

- ASLR – při každém spuštění programu má zásobník jinou počáteční adresu.
- DEP – nelze předat řízení (**eip** registr) na zásobník.

Problémy na stacku II.

Idea útoku

- Lze přepsat návratovou adresu na zásobníku, pokud řádek bude delší jak 4096 znaků.
- Nelze předat řízení okamžitě na zásobník – ASLR a DEP.
- Využitím funkce *mmap* lze obejít tyto komplikace
 - Zvolí se pevná adresa, na kterou se namapuje soubor.
 - Otevřený file deskriptor má číslo 3.
 - Nastaví se mapované stránce příznak spustitelnosti.

Problémy na stacku II.

Idea útoku

- Po namapování lze již **eip** registr nasměrovat na nově alokovanou oblast.
- Následně se spustí kód, který má za úkol škodit.
 - V tomto případě se spustí shell.

Problémy na stacku II.

Problémy při útoku

- Funkce *mmap* potřebuje ke svému běhu správně nastavený zásobník.
- Pomocí buffer overflow se ale přepíše uložená hodnota **ebp** registru.
- → Je potřeba upravit uloženou hodnotu **ebp** registru.
 - Jako zásobník se použije nově namapované stránky.

Problémy na stacku II.

Shellcode

Je potřeba spustit nový program – pomocí funkce `execve`.

- Systémové funkce se v Linuxu spouští nastavením hodnot v registrech a následným přerušením.
- Id funkce `execve` je 11 (registr **`eax`**).
- První parametr je ukazatel na cestu ke spustitelnému souboru – cesta je v namapované stránce (registr **`ebx`**).
- Druhý a třetí parametr necháme nulové (registry **`ecx`** a **`edx`**).
- Samotné volání proběhne po přerušení 128.

Problémy na stacku II.

Další detaily si můžete nastudovat pohledem do kódu.