Laborator II: Suprascrierea Stivei. Shellcodes I

Iosif George-Andrei

1. Suprascrierea Stivei

- 1. Suprascrierea Stivei
- 2. Shellcodes I

- 1. Suprascrierea Stivei
- 2. Shellcodes I
- 3. Exemplu Concret

Suprascrierea Stivei

Suprascrierea Buffer-ului

Suprascrierea Buffer-ului

Buffer: Zonă temporară de memorie, folosită la un moment dat pentru procesarea sau mutarea datelor.

Suprascrierea Buffer-ului

- Buffer: Zonă temporară de memorie, folosită la un moment dat pentru procesarea sau mutarea datelor.
- Suprascrierea Buffer-ului: Scrierea într-un buffer a unor date care depășesc limitele acestuia, suprascriind astfel zone de memorie vecine. Poate apărea la limbaje de programare care nu efectuează o verificare automată a limitelor zonelor de memorie în care se scrie (de exemplu, Assembly, C și C++).

• **În Stivă**: Zona de memorie suprascrisă aparține de stiva procesului, *buffer*-ul fiind o variabilă locală.

- În *Stivă*: Zona de memorie suprascrisă aparține de stiva procesului, *buffer*-ul fiind o variabilă locală.
- În *Heap*: Zona de memorie suprascrisă aparține de *heap*, buffer-ul fiind o variabilă alocată dinamic.

- În *Stivă*: Zona de memorie suprascrisă aparține de stiva procesului, *buffer*-ul fiind o variabilă locală.
- În *Heap*: Zona de memorie suprascrisă aparține de *heap*, buffer-ul fiind o variabilă alocată dinamic.
- La Nivel de Tip de Date: Efectuarea de operațiuni care rezultă într-o valoare ce nu poate fi salvată într-un anumit tip de date. De exemplu, (char) (2 ★ 128) e egal cu 0.

Funcționare

Funcționare

sketch();

Modificarea unor variabile

- Modificarea unor variabile
 - Referințe către funcții

- Modificarea unor variabile
 - Referințe către funcții
 - Canarii

- Modificarea unor variabile
 - Referințe către funcții
 - Canarii
- Modificarea adreselor de retur

Protecții

Protecții

▶ Impunerea unei lungimi maxime la copierea în *buffer*

Protecții

- Impunerea unei lungimi maxime la copierea în buffer
- Folosirea unor **mecanisme de securitate** impuse de compilator (canarii), la nivel de sistem de operare (Data Execution Prevention pe Windows) sau *hardware* (bitul NX în intrările din tabelele de pagini ale procesorului)

Shellcodes I

Shellcodes

Shellcodes

➤ **Shellcode**: Secvență de coduri de operații folosită în exploatarea de programe pentru efectuarea unor sarcini (de obicei, deschiderea unui shell).

Shellcodes

- ► Shellcode: Secvență de coduri de operații folosită în exploatarea de programe pentru efectuarea unor sarcini (de obicei, deschiderea unui shell).
- Scris în Assembly (recomandat datorită controlului mai mare), eventual în C (rezultatul depinde de compilator)

Funcționare

Funcționare

sketch();

Dimensiunea buffer-ului

- Dimensiunea buffer-ului
- Posibilitatea interpretării unor octeți ca terminator de șir

- Dimensiunea buffer-ului
- Posibilitatea interpretării unor octeți ca terminator de șir
- Detectabilitatea operațiunilor efectuate de către soluțiile de securitate

Exerciții

Exerciții 11/16

Recomandări

Exerciții 12/16

Recomandări

 Folosiți comanda man pentru a primi ajutor la rularea anumitor comenzi.

Exerciții 12/16

Recomandări

- Folosiți comanda man pentru a primi ajutor la rularea anumitor comenzi.
- Folosiți documentația pwntools pentru a identifica metodele de care aveti nevoie.

Exerciții 12/16

Exemplu Concret

Exemplu Concret

Vulnerabilitate raportată în 2019, pe HackerOne

- Vulnerabilitate raportată în 2019, pe HackerOne
- Protocol proprietar pentru descoperirea serverelor de jocuri

- Vulnerabilitate raportată în 2019, pe HackerOne
- Protocol proprietar pentru descoperirea serverelor de jocuri
- Fuzzing efectuat pe protocol pentru a identifica un câmp vulnerabil, specific numelui de utilizator

- Vulnerabilitate raportată în 2019, pe HackerOne
- Protocol proprietar pentru descoperirea serverelor de jocuri
- Fuzzing efectuat pe protocol pentru a identifica un câmp vulnerabil, specific numelui de utilizator
- Suprascrierea buffer-ului la nivel de stivă

- Vulnerabilitate raportată în 2019, pe HackerOne
- Protocol proprietar pentru descoperirea serverelor de jocuri
- Fuzzing efectuat pe protocol pentru a identifica un câmp vulnerabil, specific numelui de utilizator
- Suprascrierea buffer-ului la nivel de stivă
- Folosirea unui shellcode pentru lansarea cmd.exe

- Vulnerabilitate raportată în 2019, pe HackerOne
- Protocol proprietar pentru descoperirea serverelor de jocuri
- Fuzzing efectuat pe protocol pentru a identifica un câmp vulnerabil, specific numelui de utilizator
- Suprascrierea buffer-ului la nivel de stivă
- Folosirea unui shellcode pentru lansarea cmd.exe
- Depășirea unor limitări provocate de conversia Unicode a numelui (în acest caz, a payload-ului) și de caracterele NULL

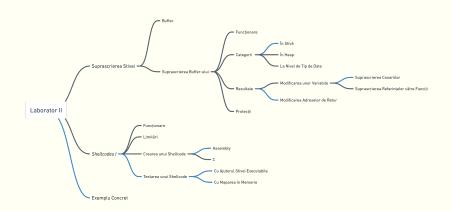
Recapitulare

Recapitulare 15/16

Recapitulare

Recapitulare 16/16

Recapitulare



Recapitulare 16/16