

Laborator II: Suprascrierea Stivei. *Shellcodes I*

Iosif George-Andrei

Tabelă de Conținut

Tabelă de Conținut

1. Suprascrierea Stivei

Tabelă de Conținut

1. Suprascrierea Stivei
2. *Shellcodes I*

Tabelă de Conținut

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, suprascrind 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.


```
sketch();
```

Rezultatele Suprascrierii Stivei

- ❖ 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

- Impunerea unei lungimi maxime la copierea în *buffer*

- ❖ 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

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

- ❖ *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

```
sketch();
```

Limitări în Scrierea *Shellcode*-urilor

Limitări în Scrierea *Shellcode*-urilor

- ❖ Dimensiunea *buffer*-ului

Limitări în Scrierea *Shellcode*-urilor

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

Limitări în Scrierea *Shellcode*-urilor

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

Exerciții

1. Suprascrierea Stivei

1. Suprascrierea Stivei
2. Crearea și Testarea unui *Shellcode*

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

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

Exemplu Concret

RCE în Aplicația Client Steam

- ❖ Vulnerabilitate raportată în 2019, pe HackerOne

RCE în Aplicația Client Steam

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

RCE în Aplicația Client Steam

- ❖ 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

RCE în Aplicația Client Steam

- ❖ 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

RCE în Aplicația Client Steam

- ❖ 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`

RCE în Aplicația Client Steam

- ❖ 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

Recapitulare

