

Tema 3

- Deadline Soft: 19.01.2016 23:55
- Deadline Hard: 19.01.2016 23:55
- Data publicării: 09.01.2016 01:15
- Data ultimei modificări: 09.01.2016 18:30
- Responsabili:
 - [Vladimir Diaconescu](#)
 - [Adrian Bogatu](#)

Enunț

Să se compileze un program scris în limbaj C și să se rezolve următoarele:

1. Identificați posibilele vulnerabilități ce s-ar putea găsi în program (analiză statică).
2. Determinați userul și parola pentru login.
3. Creați o suită de intrări pentru program astfel încât:
 1. Programul să ajungă să execute funcția `secret_func1`.
 2. Programul să "apeleze" funcția `secret_func2` cu argumente valide de intrare.
 3. Programul să "apeleze" din biblioteca standard C funcția `fopen( '<prenume>', 'w' )` pentru a crea un fișier local având prenumele vostru.

Setup

Pentru dezvoltarea temei recomandăm să folosiți mașina virtuală de Windows descrisă în secțiunea [Mașini virtuale](#) din pagina de resurse. Mașina virtuală de Windows este numită SSS - Windows 7 32bit. Această mașină virtuală este folosită și pentru verificarea temei pe [vmchecker](#).

În [arhiva de resurse a temei](#) veți vedea că există fișierul `seed.c`, precum și scriptul Python `mangle.py`.

Pentru a genera fișierul sursă C plecând de la `seed.c`, rulați comanda:

```
python mangle.py <nume> <prenume> <a treia cifră din numărul grupei>
```

unde:

- `<nume>` este numele vostru de familie (începeți cu majusculă)
- `<prenume>` este prenumele vostru (unul dintre ele dacă aveți două, începeți cu majusculă)
- `<a treia cifră din numărul grupei>` este ceea ce spune 😊; pentru grupa 324CA este cifra 4, iar pentru grupa 322CA este cifra 2

De exemplu, pentru Ionescu Anca-Monica de la grupa 323CA, modul de rulare a comenzii de generare a fișierului sursă C va fi

```
python mangle.py Ionescu Anca 3
```

Comanda de mai sus va genera fișierul `tema3.c`. Acesta este fișierul propriu-zis al temei care trebuie compilat.

Înainte de toate, recomandăm să adăugați în variabila `PATH` calea pentru `gcc/gdb` și alte utilitare, precum și pentru Python. Pentru aceasta, în Command Prompt, rulați comanda

```
set PATH=%PATH%;C:\Python27;C:\MinGW\bin
```

Acum puteți să compilați fișierul temei generat mai sus:

```
gcc -o tema3.exe tema3.c
```

Implementare

La nivelul implementării, aveți de scris câteva fișiere de intrare pentru programul compilat care să rezolve câte una din cerințele din enunț (de la punctul 3).

Recomandăm să generați aceste fișiere de intrare folosind un script Python sau orice alt limbaj de programare.

Trimitere și notare

Temele vor trebui încărcate pe platforma [vmchecker](#) (în secțiunea IOCLA) și vor fi testate automat. Arhiva încărcată va fi o arhivă `.zip` care trebuie să conțină:

- fișierele sursă/script-urile ce generează intrările pentru program: `payload_a`, `payload_b`, `payload_c`
- fișierul sursă aferent: `tema3.c`
- fișier `README` ce conține descrierea implementării
 - analiza statică (pe scurt)
 - cum ați determinat userul și parola de login
 - cum v-ați gândit să faceți programul să ajungă în `secret_func1`, `secret_func2`, `fopen`

Punctajul este repartizat în felul următor:

- 20% `README`, cu pașii urmați pentru a rezolva cerințele, explicați în detaliu
- 25% analiză statică
- 25% determinare user și parola, și trecerea de procesul de login
- 30% cele trei exploatări

Precizări suplimentare

În cadrul corectării, vom verifica dacă `tema3.c` este într-adevăr fișierul generat pornind de la `seed.c` și datele voastre. Dacă există diferențe, nu se merge mai departe în procesul de corectare.

Din moment ce programul de intrare scris în C este dat, analiza statică presupune să interpretați cod C, nu assembly.

Arhivă temă

Arhiva de resurse a temei, ce conține `mangler.py` și `seed.c` (în curând și checker-ul) o puteți descărca de [aici](#).

Resurse ajutătoare

- [Laborator 9](#): Gestiunea bufferelor. Buffer overflow
- [Laborator 10](#): Exploatarea memoriei. Shellcodes
- [Performing a ret2libc attack](#)

From:

<http://elf.cs.pub.ro/asm/wiki/> - Introducere în organizarea calculatorului și limbaj de asamblare

Permanent link:

<http://elf.cs.pub.ro/asm/wiki/teme/tema-3?rev=1452452928>

Last update: **2016/01/10 19:08**

