Exploitation de binaire

Jean V.

C’est quoi l’exploitation de binaire ?

- Manipuler et modifier l’exécution d’un binaire

- Exemple :
- Binaire ls : list directory contents
- Binaire ls exploité : list directory contents + exec rm -rf *

Sommaire

I. Rappel Binaire

II. Buffer overflow

I. Rappel binaire

I. Rappel binaire

Rappel binaire

- Langage machine
- x86/x86_64

- rip/eip : instruction pointer
- rsp/esp : stack pointer

- Gdb: debugger linux https://darkdust.net/files/GDB%20Cheat%20Sheet.pdf

II. Buffer overflow

II. Buffer overlow

- Principe : déborder un buffer.
- Exemple :

```c
int main(int argc, char *argv[])
{
    char value = 'A';
    char toto[4];
    printf("Value: %c\n", value);
    strcpy(toto, "buf");
    toto[4] = 'B';
    printf("Value: %c\n", value);
}
```

```
azazhel@locahost:~$ ./toto
Value: A
Value: B
```

Stack avant toto[4] =’B’

A	0x8ff4
buf\0	0x8ff0
.	
.	
.	

Stack après

B	0x8ff4
buf\0	0x8ff0
.	
.	
.	

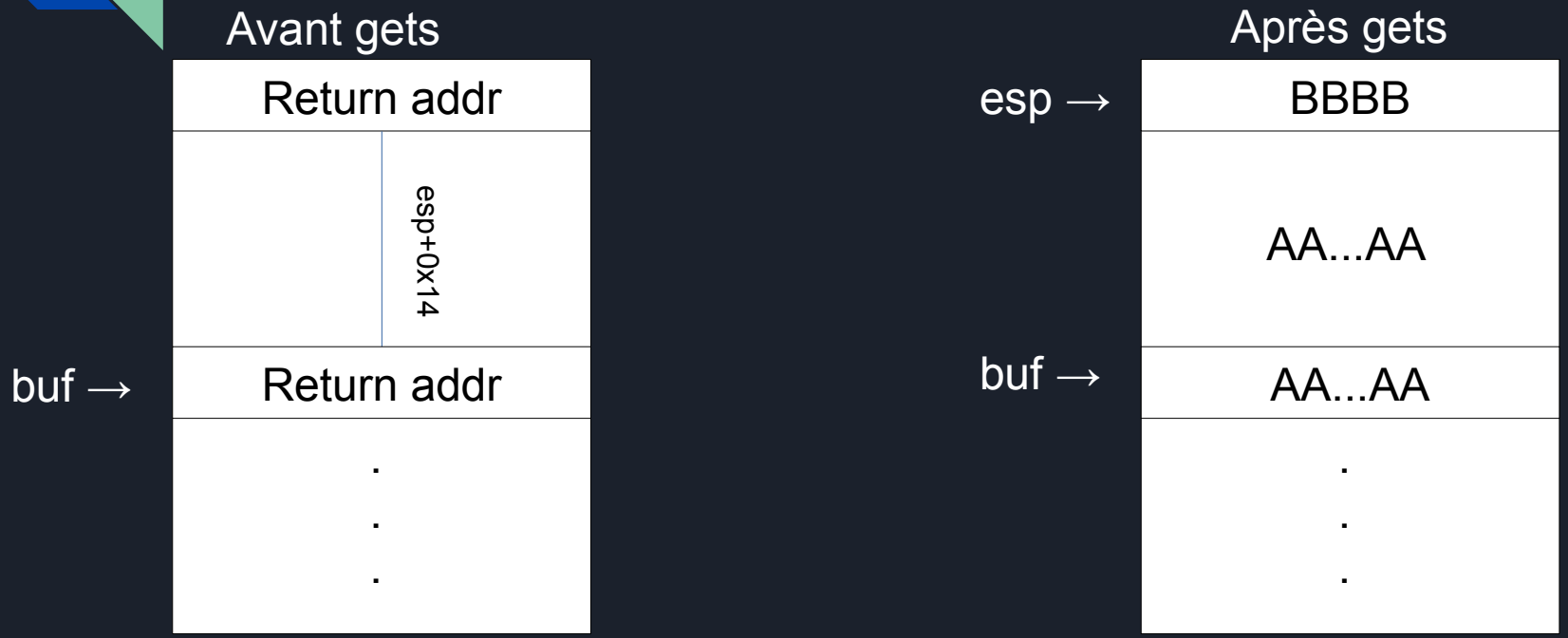
‘b’ : @0x8ff0 ‘A’ : @0x8ff4
‘u’ : @0x8ff1
‘f’ : @0x8ff2
‘\0’ : @0x8ff3

toto+4 = 0x8ff4

Contrôle de l’exécution

- Registre eip : Instruction pointer.
- Registre esp : stack pointer.
- Quand on sort d’une fonction *esp=eip, soit return value_at_esp
- Objectif : overflow esp, puis return

Contrôle de l’exécution



Exécution de code

- Utilisation d’un shellcode
- Exécution du shellcode dans la stack
- https://shell-storm.org/shellcode/

Contre mesure :

- Rendre la stack non exécutable, bit NX (activé par défaut).
- Activer l’ASLR

Formats string bug

- Printf("%s", var) vs printf(var)

```c
void vuln()
{
    char buf[10];
    gets(buf);
    printf("%s\n", buf);
    printf(buf);
    printf("\n");
}

int main(int argc, char *argv[])
{
    vuln();
}
```

```
[azazhel@kubuntu] demo$ ./demo2
%p
%p
0x5555555596b0
```

- Dans printf(var), %p sera interprété comme un format et non comme une chaîne à afficher.
- Print le sommet de la stack

- Bypass ASLR et PIE

Exploitation de la libc

- Exploiter la libc pour appeler les fonctions qu'on veut.
- Bypass NX et ASLR

Idée : trouver l'adresse de system dans la libc et faire un call avec les bon arguments (ex : system('/bin/bash'))

Problème : Ne fonctionne pas si c'est compilé en static

Ressources

- ROP Emporium : https://ropemporium.com/
- Root Me - App - Système : https://www.root-me.org/fr/Challenges/App-Systeme/
- TryHackMe PWN101 : https://tryhackme.com/r/room/pwn101
- Hackropole - pwn : https://hackropole.fr/fr/pwn/

\ Faites des CTF /