ROP (Return Oriented Programming)

Aleknight

Securimag

6 Février 2020

In French please!

- Exploitation logicielle
- Buffer overflow

Quelques rappels

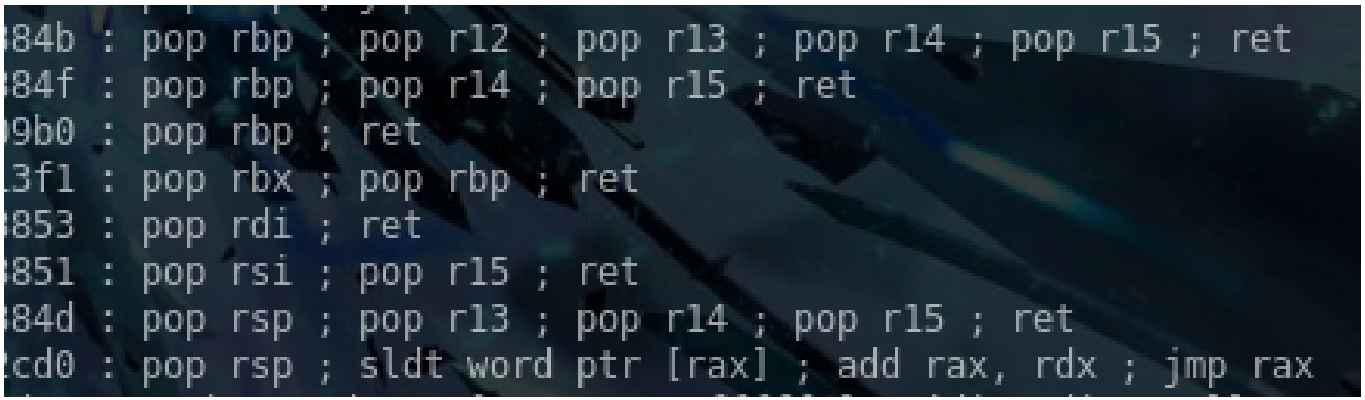
- Exploitation de la mauvaise gestion de la mémoire (scanf, gets, strcpy)
- Réecriture d'adresses en mémoire

Origine et concept

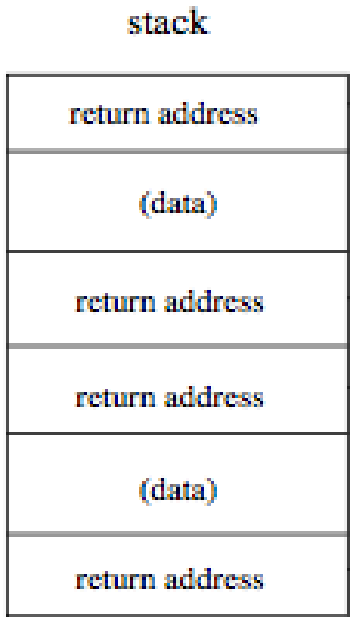
- ASLR & NX
- Utilisation du code source pour créer notre exploit
- Des instructions importantes : **ret**, **call** et **jmp**

En pratique

- Utilisation de gadgets



En pratique


stack
return address
(data)
return address
return address
(data)
return address

Un peu d'aide svp

ROPgadget

Les gadgets c'est bien mais ...

- Utilisation des fonctions
- Rappels sur les conventions d'appel

Les gadgets c'est bien mais ...

- Adresse de la fonction
- Gadget pour passer les arguments après le ret
- Sert aussi d'adresse de retour pour la fonction.

Une solution

PIE (Position Independant Executable)

The end

Des questions ?