Failles applicatives et leur exploitation

Antoxyde

Securimag

Novembre 2019

Securimag

Késako ?

Détourner l'utilisation d'un programme afin d'obtenir un accès, ou d'élever ses privilège par exemple.

Securimag

Exemples connus

- **DirtyCow** : Kernel Linux kernel, LPE (Local priv. esc.) , 2015
- **EternalBlue** : Windows (SMB) , RCE (Remote code exec.), utilisé par Wannacry , exploit crée par la NSA , 2017
- **BlueKeep** : Windows (RDP), RCE, Mai 2019
- ...

Securimag

Quelques prérequis : permissions Unix

- Un identifiant par utilisateur (0 pour root, 1000 pour le 1er user généralement).
- Un identifiant par groupe (idem).

Securimag

Quelques prérequis : permissions Unix

- Un processus possède un **UID** et un **GID**.
- Mais aussi un **EUID** et **EGID**
  Par défaut , ils ont les même valeurs qe l'UID et le GID.
- C'est celui-la qui sert pour checker les permissions.

Securimag

Le flag setuid/setgid

Sur un fichier éxécutable, le flag **setuid** (resp. **setgid**) permet de remplacer l'**euid** (resp. **egid**) par l'id de l'owner du fichier.

Exemple

Les programmes *sudo* et *passwd* utilisent ce mécanisme.

Securimag

Et donc ?

Pour élever nos privilèges :

- Soit exploiter un programme qui tourne déjà en root
- Soit exploiter un programme setuid/setgid.

Securimag

Notre premier exploit!

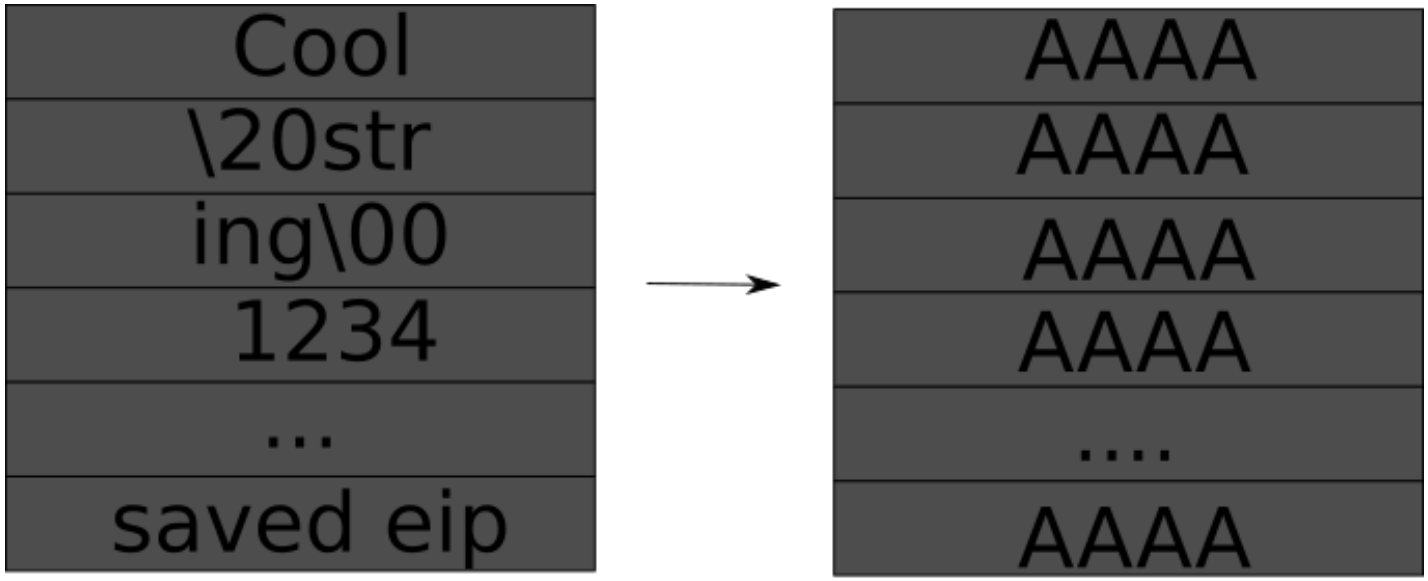
Qui saura trouver la vuln dans l'exécutable setuid appartenant à root, compilé à partir du code suivant ?

```c
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main(void) {

    setreuid(geteuid(), geteuid());
    system("ls -al");

    return 0;
}

```

Securimag

Plus compliqué : le buffer overflow (dans la stack)

Quand la taille de l'entrée utilisateur n'est pas controlée ..



Securimag

Redirection du flux d'exécution

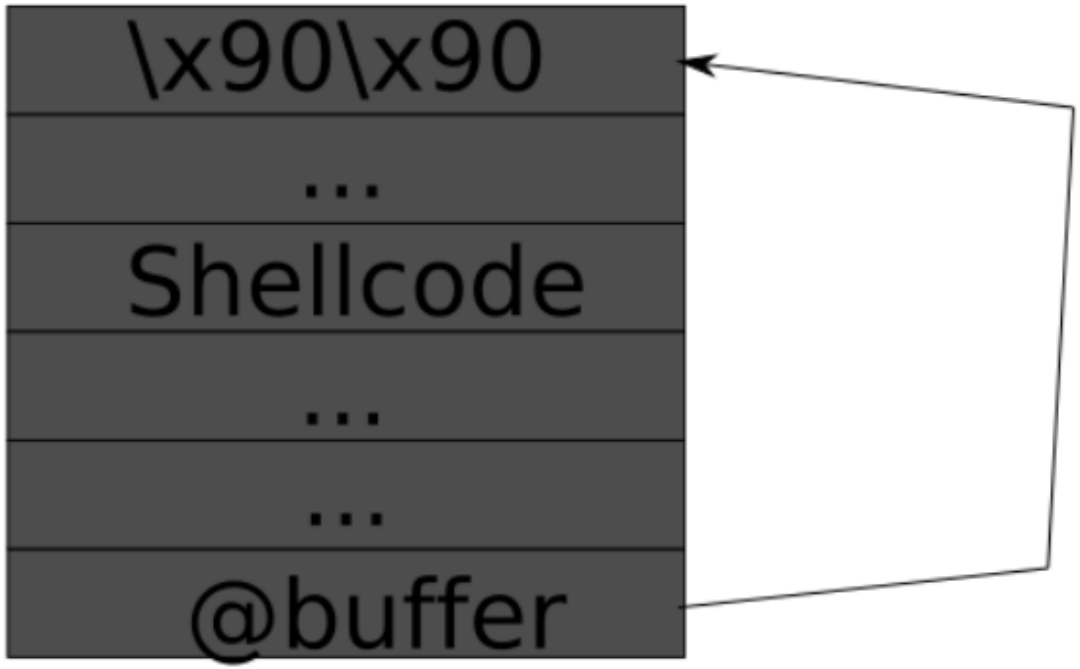
Plan d'attaque :

- Trouver le bon padding pour réécrire eip.
- Trouver vers quoi rediriger notre exécution. Ici notre super fonction win qui nous exécute un shell fera l'affaire ;).
- Réecrire le saved eip avec l'addresse de cette fonction
- ????
- Profit

Securimag

Et sans fonction "win" ?

La magie du shellcode.
Puisque aucun morceau de code de notre binaire ne fait ce qu'on veut, on a qu'a créer et injecter notre propre code.



Securimag

Mitigations

- **NX** : rends la stack non-exécutable , plus de shellcode dans la stack ...
- **ASLR** : Décale les addresses de la stack + libc d'une valeur aléatoire à l'exécution. On ne connais plus l'addresse de notre buffer à l'avance.
- **PIE** : Pareil mais pour le code du binaire. On ne connait plus par avance l'addresse de nos fonctions.
- **SSP** : Place une valeur aléatoire entre les variables locales et le saved eip et vérifie que la valeur est inchangé avant de ret.
  Sinon affiche "Stack smashing detected" et termine l'exec.
- **RelRO** : Map la GOT en read-only pour éviter qu'on puisse la réécrire.

Securimag

Mitigations

Pour voir les protections activés sur un binaire : checksec.
Attention si vous faites des tests, la plupart des protections sont activés par défaut.

- Désactivé l'ASLR : sysctl -w kernel.randomize_va_space=0
- Options GCC :
  - Désactiver NX : -z execstack
  - Désactivé PIE : -no-pie
  - Désactiver SSP : -fno-stack-protector

Securimag

Pour aller plus loin : quelques mots-clés

- La même, mais dans la heap (heap overflow).
- La même , mais au niveau du noyau (exploitation de modules kernel par ex).
- Bypass de mitigation : **ROP**, **Ret2libc**, **Ret2plt**
- Autres types de failles : **Use After Free**, **Format string bug**, **Race condition**
- Recherche de vulnérabilité automatisée (Fuzzing)
- Browser exploit : attaque des moteurs javascript
- Shellcoding (polymorphique, alphanumérique)

Securimag

Pour aller plus loin : quelques outils

- Des softs sympa : **ROPgadget**, **Pwntools**, **Ropper**, **One_gadget**, **Pwndbg**
- Quelques sites :
  - defuse.ca/online-x86-assembler.htm , un (dés)assembleur en ligne pour x86/x64
  - shellstorm-storm.org/shellcode/, une liste de shellcodes tout fait
  - w3challs.com/syscalls/, des listes de syscalls et leurs paramètres pour différentes archis.

Securimag

Merci de votre attention !

Questions ?

Securimag