TP AISE — *Reverse* & SUID

Exercice : Programme SUID

Pour cet exercice, l'idéal est de disposer de deux utilisateurs (A et B) sur la même machine (voir « useradd » pour en créer un) . **Il est déconseillé, pour des raisons de sécurité et de stabilité, d'utiliser « root » à cette fin**. Voici la démarche à suivre pour la réalisation de cet exercice :

1. Remplir un fichier (type `.secret`), et le mettre en permission uniquement pour l'utilisateur A
2. Ecrire un code C appelant la fonction « `system( « ls /path/to/secret » )` »
3. Compiler le code et créer un binaire dont le propriétaire est l'utilisateur A
4. Attacher le bit SUID (« sticky-bit ») à ce binaire.
5. Exécuter le binaire en tant que A
6. Exécuter le binaire en tant que B
7. Compiler le code une seconde fois pour un créer un binaire dont le propriétaire est B.
8. Exécuter B, que se passe-t-il ?
9. **BONUS** : Trouver un moyen de lire le contenu de .secret depuis l'utilisateur B.

Exercice : Dépassement de pile

Dans un premier temps, compilez le code ci-dessous (en mode 32 bits si possible, `-m32`, ce sera plus simple). Bien penser à désactiver la protection de pile, active par défaut pour des raisons de sécurité (flag `-fno-stack-protector`). Ensuite, votre mission est de n'utiliser que ce binaire : **interdiction de modifier le code source !** (note : vous pouvez passer le binaire en root ou en un autre utilisateur (`chown`). Pensez à mettre le binaire en SUID pour l'exécuter ou à vous octroyer les droits d'exécution (`chmod`) :

```c
#include <stdlib.h>
#include <stdio.h>
/* gcc -m32 -o stack stack.c -fno-stack-protector */
int main()
{
  int var;
  int check = 0x04030201;
  char buf[40];

  fgets(buf,45,stdin);

  printf("\n[buf]: %s\n", buf);
  printf("[check] %p\n", check);

  if (check == 0xdeadbeef) {
     printf(« You Win !\n »);
     system("/bin/sh");
   }
   return 0;
}
```

Reproduire l'exercice avec les autres binaires à disposition sur le dépôt Github.

Exercice : Debugging

Mettez en pratique GDB dans la recherche de bug des binaires du projet Github. Vous pouvez aussi le mettre en pratique dans vos projets respectifs.