Writeup challenge intro - Reverse

Ce premier challenge était une introduction aux techniques de rétro-ingénieurie. Le programme était compilé avec les symbolss (noms des fonctions) et de manière dynamique, on avait donc accès à facilement aux fonctions externes telles que `strncmp`.

Solution I - Statique

En ouvrant le binaire dans un logiciel de SRE comme Ghidra, on obtenait le pseudo-code suivant:

```
undefined8 main(int param_1,undefined8 *param_2)

{
  int iVar1;
  undefined8 uVar2;

  if (param_1 == 2) {
    iVar1 = check_password(param_2[1]);
    if (iVar1 == 0) {
      uVar2 = 0;
    }
    else {
      puts("Wrong password");
      uVar2 = 0xffffffd6;
    }
  }
  else {
    printf("Usage: %s <password>\n",*param_2);
    uVar2 = 0xffffffd6;
  }
  return uVar2;
}
```

Le programme attend un paramètre passé par la ligne de commande, et le passe à la fonction `check_password`. Cette fonction contient le code suivant:

```
undefined8 check_password(char *param_1)

{
  int iVar1;
  size_t __n;
  undefined8 uVar2;

  __n = strlen("J34nn3D'h4ck_CTF_1nTr0");
  iVar1 = strncmp(param_1,"J34nn3D'h4ck_CTF_1nTr0",__n);
  if (iVar1 == 0) {
    puts("Congratulations, you can validate with:");
    printf("Flag{%s}\n","J34nn3D'h4ck_CTF_1nTr0");
```

```
    uVar2 = 0;
  }
  else {
    uVar2 = 0xffffffd6;
  }
  return uVar2;
}
```

On peut voir que si l'argument de la fonction contient la chaîne de caractères `J34nn3D'h4ck_CTF_1nTr0`, le programme affiche le message de validation, sinon il renvoie une erreur. On peut donc déduire que le flag est: `Flag{J34nn3D'h4ck_CTF_1nTr0}` !

Il est aussi possible de valider en utilisant la commande `strings` et chercher une chaîne qui ressemblerait à un flag.

Solution II - Dynamique

On peut également valider ce challenge sans même avoir besoin d'ouvrir le binaire dans Ghidra en utilisant `ltrace`. La commande `ltrace` permet d'afficher les appels aux fonctions importées par un programme tel que les fonctions de la libc. Ainsi, on peut obtenir le flag de la manière suivante:

```
ltrace ./intro test
strlen("J34nn3D'h4ck_CTF_1nTr0")                  = 22
strncmp("test", "J34nn3D'h4ck_CTF_1nTr0", 22)     = 42
puts("Wrong password")                            = 15
+++ exited (status 214) +++
```