B2 – SÉCURITÉ: PEPITO

Par: ploujo_c, pidjot_a, rakoto_m, sayyou_y

- Retours de fonctions non vérifiés

Description: Rajouter la fonction *die* sert à vérifier que le processus se termine correctement.

Ancien code: (daemon.c)

```
fprintf(stderr, "Process received SIGTERM.\n" \
        "Exiting\n");
```

Nouveau code: (daemon.c)

```
if (fprintf(stderr, "Process received SIGTERM.\n" \
        "Exiting\n") < 0)
die("fprintf()");
```

- Augmentation du buffer

Description: Il est nécessaire d'augmenter le buffer pour éviter le *buffer overflow.* En cas de *buffer overflow*, le processus écrit en dehors de son espace alloué.

Ancien code: (main.c)

```
char        savePassword[64] = {0};
```

Nouveau code: (main.c)

```
char        savePassword[420] = {0};
```

- Changement de fonction

Description: Les fonctions *strcmp* et *strcpy* deviennent *strncmp* et *strncpy* car il faut comparer le nombre exact de caractères entrés dans le buffer, notamment grâce à la fonction *strlen*.

Ancien code: (main.c)

```
if (!strcmp(password, userPassword))
  isUser = 1;
strcpy(savePassword, password);
```

Nouveau code: (main.c)

```
if (!strncmp(password, userPassword, strlen(password)))
  isUser = 1;
strcncpy(savePassword, password, strlen(savePassword));
```

- Rajout de paramètres

Description: La fonction système fprintf prend par défaut une chaîne de caractères. Cependant, si le paramètre entré n'est pas une chaîne de caractères, il est nécessaire de le signaler.

Ancien code: (network.c)

```
fprintf(stderr, msg);
```

Nouveau code: (network.c)

```
if (fprintf(stderr, "%s", msg) < 0)
  die("fprintf()");
```

- Vérification d'un mot de passe non nul

Description: La vérification qu'un mot de passe a été rentré est nécessaire.

Ancien code: (main.c)

```
if (!strcmp(password, userPassword))
```

Nouveau code: (main.c)

```
if (password != NULL && strlen(password) <= 512 && !strcmp(password,
userPassword, strlen(password)))
```

- Changement du 2e paramètre de la fonction *fopen*

Description: Le fichier *pepito.pid* ne peut pas être lu par l'utilisateur normalement.

Ancien code: (daemon.c)

if (!(pidFile = fopen("pepito.pid", "w")))

Nouveau code: (daemon.c)

if (!(pidFile = fopen("pepito.pid", "rw")))