

Hacking et Pentesting

Mars 2021 | Serie 2

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

2 Exercices 2 - Randomness

2.1 Nuclear Warhead code generator

Le code suivant a été trouvé lors du démantèlement d'un ancien sous-marin d'une puissance étrangère.

```
1 // Nuclear Warhead code generator
2
3 #define NB_NUM 10
4 #define MIN_NUM 1
5 #define MAX_NUM 9
6
7 #include <stdio.h>
8 #include <stdlib.h>
9 #include <time.h>
10
11 int main(void){
12     puts("Nuclear Warhead code generator");
13
14     time_t now;
15     srand(time(&now));
16     printf("%s", ctime(&now));
17
18     while(1) {
19         puts("Press Any Key generate new code");
20         getchar();
21
22         for(int i=0; i<NB_NUM; i++){
23             printf("%d ",rand() % (MAX_NUM - MIN_NUM +1) + MIN_NUM);
24         }
25         printf("\n");
26
27     }
28     return 0;
29 }
```

La dernière console a pu être récupérée

Pouvez-vous déduire les prochains codes ?

2.2 CardGame

Etant chaque année dernier au concours de carte de la commune, vous décidez de prendre votre revanche cette année. Vous allez tenter de prédire les cartes des futurs tirages. En discutant avec l'organisateur, vous réussissez à lui récupérer le binaire des tirages de cartes. Il vous dit qu'il a été lancé pour la première fois **cette année**.

Les lignes intéressantes du binaire vous sont données.

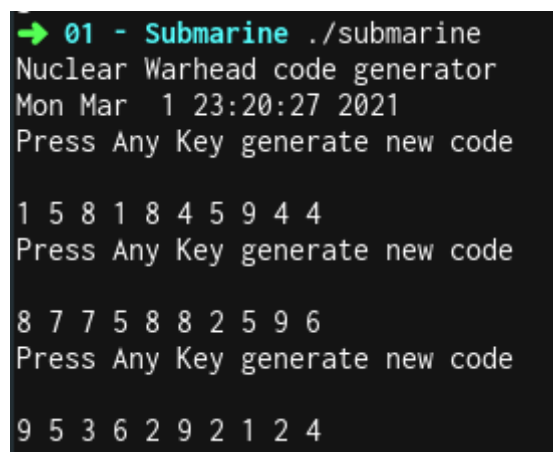
Connaissant les premiers tirages, prédisez les prochains tirages.

2.3 EuroMillions

Vous réussissez à récupérer le binaire officiel des tirages de la loterie EuroMillions.

Sachant que le jeu a été lancé au premier semestre 2020, prédisez les prochains tirages.

2.4 Annexes



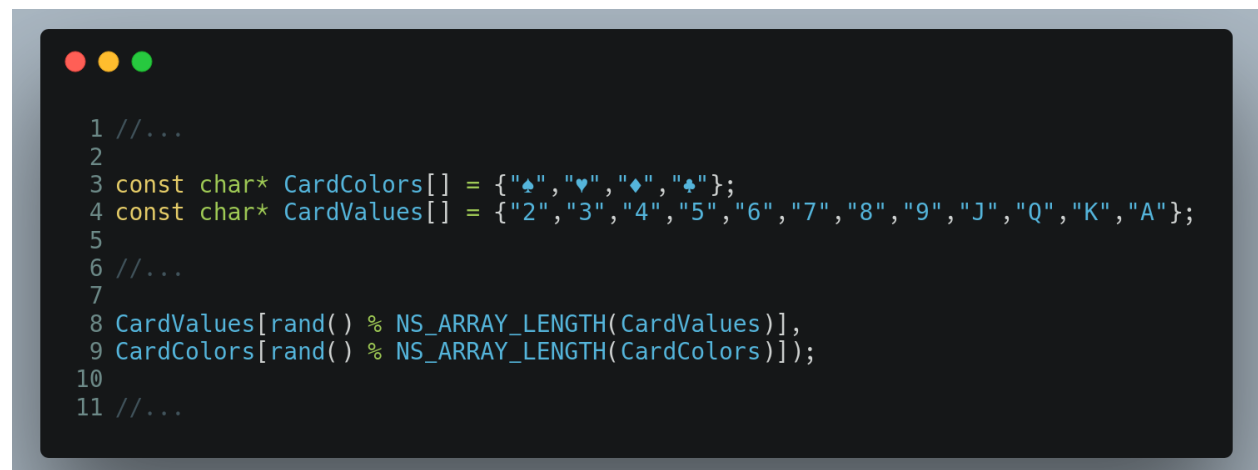
```
→ 01 - Submarine ./submarine
Nuclear Warhead code generator
Mon Mar 1 23:20:27 2021
Press Any Key generate new code

1 5 8 1 8 4 5 9 4 4
Press Any Key generate new code

8 7 7 5 8 8 2 5 9 6
Press Any Key generate new code

9 5 3 6 2 9 2 1 2 4
```

Figure 1: Exo 1 - Dernière console de bord



```
1 //...
2
3 const char* CardColors[] = {"♠", "♥", "♦", "♣"};
4 const char* CardValues[] = {"2", "3", "4", "5", "6", "7", "8", "9", "J", "Q", "K", "A"};
5
6 //...
7
8 CardValues[rand() % NS_ARRAY_LENGTH(CardValues)],
9 CardColors[rand() % NS_ARRAY_LENGTH(CardColors)]);
10
11 //...
```

Figure 2: Exo 2 - Lignes de code

```

→ 02 - CardGame ./cardgame
Press Any Key to draw new card set

4♥ Q♥ A♣ 3♠ 3♠ 4♠
5♥ A♦ 3♥ 7♥ 2♠ 6♥
7♣ J♣ Q♣ 2♣ 7♠ 9♥

```

Figure 3: Exo 2 - Derniers tirages

```

→ 03 - EuroMillion ./euromillion
Draw program for EuroMillion
Press Any Key to launch draw lots

Draw : 28 44 30 35 10 - 1 10
Press Any Key to launch draw lots

Draw : 14 46 47 28 8 - 4 12
Press Any Key to launch draw lots

Draw : 44 12 4 42 28 - 6 11
Press Any Key to launch draw lots

```

Figure 4: Exo 3 - Derniers tirages d'EuroMillions