Commencé le	lundi 22 avril 2024, 09:34
État	Terminé
Terminé le	lundi 22 avril 2024, 09:36
Temps mis	1 min 59 s
Points	9,00/9,00
Note	**10,00** sur 10,00 (**100**%)

Question 1

Correct

Note de 1,00 sur 1,00

Lors d'un débordement de pile (« stack overflow »), que cherche-t-on à écraser ?

Veuillez choisir une réponse.

a. Pointeur d'environnement

b. Argument d'appel de fonction

c. Tampon d'environnement

d. Pointeur de retour ✓

Votre réponse est correcte.

La réponse correcte est : Pointeur de retour

Question 2

Correct

Note de 1,00 sur 1,00

Lors d'un débordement du tas (« heap overflow »), que cherche-t-on à écraser ?

Veuillez choisir une réponse.

a. Pointeur d'environnement local

b. Argument d'appel de fonction

c. Données stockées en mémoire ✓

d. Pointeur de retour

Votre réponse est correcte.

La réponse correcte est : Données stockées en mémoire

Question 3

Correct

Note de 1,00 sur 1,00

Quelle utilisation de ces fonctions C++ est la plus susceptible d'être vulnérable à une attaque de débordement de mémoire tampon :

Veuillez choisir une réponse.

- a. strcpy (copie la chaine de caractères) ✓
- b. memchr (trouve un caractère dans un bloc de mémoire)
- c. time (affiche le temps)
- d. rand (produit un nombre aléatoire)
- e. strlen (obtenir la longueur d'une chaîne)

Votre réponse est correcte.

La réponse correcte est : strcpy (copie la chaine de caractères)

Question 4

Correct

Note de 1,00 sur 1,00

Quelle approche n'est pas une technique de protection contre les stack overflow :

Veuillez choisir une réponse.

- a. ALSR (Address space layout randomization)
- b. Les Canaries
- c. ROP (Return Oriented Programming) ✓
- d. Utiliser des langages typés comme JAVA

Votre réponse est correcte.

La réponse correcte est : ROP (Return Oriented Programming)

Question 5

Correct

Note de 1,00 sur 1,00

Quelle approche n'est pas une technique de protection contre les heap overflow :

Veuillez choisir une réponse.

- a. ALSR (Address space layout randomization)
- b. Les Canaries ✓
- c. ESP (Executable-space protection)
- d. Utiliser des langages typés comme JAVA

Votre réponse est correcte.

La réponse correcte est : Les Canaries

Question 6

Correct

Note de 1,00 sur 1,00

Que se passe-t-il si un stack overflow parvient à écraser l'adresse de retour mais la nouvelle adresse ne pointe pas vers le shell code :

Veuillez choisir une réponse.

- a. Rien, le programme va continuer à s'exécuter
- b. En général, cela va causer une erreur « segmentation fault » ✓

Votre réponse est correcte.

La réponse correcte est : En général, cela va causer une erreur « segmentation fault »

Question 7

Correct

Note de 1,00 sur 1,00

La solution StackShield permet en général d'éviter les « segmentation fault »

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 8

Correct

Note de 1,00 sur 1,00

En sécurité informatique le terme « exploit » (en anglais) fait référence à :

Veuillez choisir une réponse.

a. Un outil qui permet de pirater des machines à distance en faisant la reconnaissance sur le réseau et découvrant les vulnérabilités qui y sont présentes

b. Au code machine qui est inséré via le réseau ou via une page Web sur une machine afin de l'infecter

c. Une prouesse informatique réalisée par un pirate qui aurait réussi à devenir « root » sur une machine particulièrement bien protégée

d. Une méthode qui permet de prendre le contrôle d'une machine étant donnée l'existence d'une vulnérabilité sur un de ses logiciels ✓

Votre réponse est correcte.

La réponse correcte est : Une méthode qui permet de prendre le contrôle d'une machine étant donnée l'existence d'une vulnérabilité sur un de ses logiciels

Question 9

Correct

Note de 1,00 sur 1,00

On considère le programme suivant :

```
void func(int n)
 {        char* chunk = (char*) malloc(32);
          memset(chunk, 'A', n);
          printf("%s\n", chunk);
          free(chunk);
          chunk = NULL; }
int main(int argc, char *argv[])
 {        func(argv[1]);
          return 0;  }
```

Quelle vulnérabilité identifiez-vous dans ce programme ?

Veuillez choisir une réponse.

- a. Stack overflow
- b. Heap overflow ✓
- c. Race condition
- d. Format string vulnerability
- e. Fuite de mémoire

Votre réponse est correcte.

La réponse correcte est : Heap overflow