Université M'hamed Bougara Boumerdes / Faculté des Sciences / Département d'Informatique

Module : Sécurité informatique | **Niveau :** L3 ISIL/SI (S6) | **Date :** 13.06.2023
Examen : ETLD | **Documents :** non autorisés | **Durée :** 1h30

Matricule : Nom : Prénom : Groupe :

Exercice 01 (10 points) : Cochez la ou les bonnes réponses

1. Une méthode de chiffrement symétrique :
   - ☐ Permet de compresser les données en plus du chiffrement.
   - ☐ Consiste à communiquer la clé à son interlocuteur pour que celui-ci puisse décrypter les données
   - ☐ Est plus rapide qu'une méthode de chiffrement asymétrique
   - ☐ Aucune bonne réponse
2. Les serveurs de messagerie sont surchargés suite aux spams à cause de :
   - ☐ Leurs espaces de stockage sont saturés de mails d'erreurs
   - ☐ Le compte de l'administrateur est saturé de messages d'erreurs
   - ☐ La bande passante du réseau est plus large
   - ☐ Les équipements d'interconnexion sont saturés
3. Le rôle de la sécurité en entreprise est :
   - ☐ Réduire le risque à un niveau acceptable
   - ☐ Prévenir tout risque
   - ☐ Empêcher les employés de travailler correctement
   - ☐ Surveiller le bon fonctionnement des systèmes
4. Un screenlogger est :
   - ☐ Une préparation d'une attaque spam
   - ☐ Un cheval de Troie
   - ☐ Une préparation d'une porte dérobée
   - ☐ Un Ransomware
5. Je trouve une clé USB dans ma boîte à lettres. Quelle est la meilleure action ?
   - ☐ Je la connecte à mon ordinateur pour en voir le contenu.
   - ☐ Je l'analyse avec un anti-virus, on ne sait jamais.
   - ☐ Je la jette, une clé peut contenir un virus.
6. Un cheval de Troie est :
   - ☐ Programme keylogger
   - ☐ Programme screenlogger
   - ☐ Une porte dérobée
   - ☐ Une préparation d'une attaque spam
7. Une signature numérique permet de :
   - ☐ S'assurer qu'un message provient de la bonne personne
   - ☐ S'assurer que le message n'a pas été modifié durant un transfert
   - ☐ S'assurer que le message n'a pas été lu par une personne non autorisée
   - ☐ Détecter une personne qui nie avoir fait une action
8. L'attaque smurf est :
   - ☐ Une attaque qui utilise le protocole ICMP pour effectuer une attaque DOS
   - ☐ Une attaque qui exploite la faille du protocole ARP pour espionner un réseau
   - ☐ Une attaque qui vie à casser la confidentialité des messages
   - ☐ Une attaque qui détermine les machines actives dans un réseau local
9. Quelles sont les caractéristiques de cross site Scripting (CSS) et l'injection SQL ?
   - ☐ Une attaque vise le client et l'autre le serveur
   - ☐ Les deux peuvent être utilisées dans une architecture 3 tiers
   - ☐ Les deux attaques visent un serveur Web
   - ☐ Toutes les réponses sont correctes
10. Citez-le(s) principe(s) de sécurité traité(s) par une fonction de hachage
    - ☐ Disponibilité, intégrité, authentification.
    - ☐ Confidentialité, intégrité, non-répudiation.
    - ☐ Authentification, intégrité, non-répudiation.
    - ☐ Respect de vie privée, intégrité, authentification

Exercice 01 : Soit le programme C suivant.

```
1   #include <stdio.h>
2   #include <string.h>
3   void foo (char * message1, char* message2, int a)
4   {
5       char c[12];
6       message2 = “remplis”;
7       strcpy(c, message2);
8       strcpy(c, message1);
9   }
10  void main(int argc, char **argv)
11  {
12      char *message1 = argv[1];    //récupérer la première entrée de l’utilisateur
13      char *message2 = argv[2];    //récupérer la deuxième entrée de l’utilisateur
14      foo(message1, message2, 1) ;
15  }
```

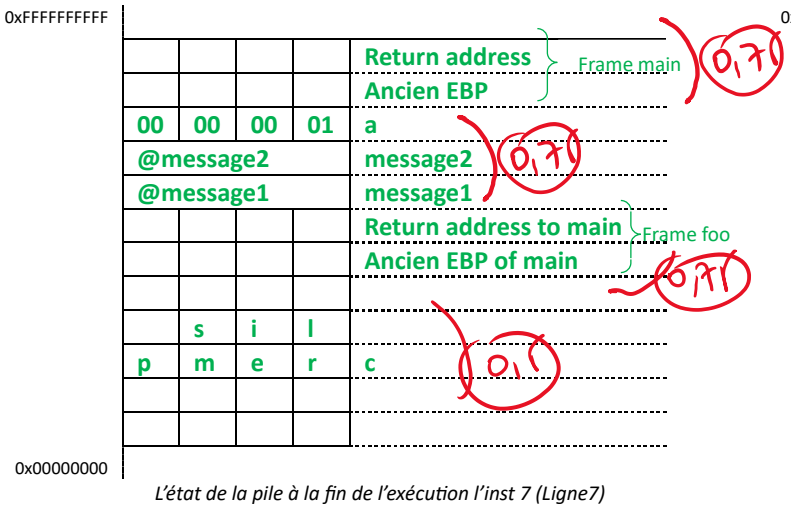
1. Si on veut abuser d’un programme en C, quelle est la technique fréquemment utilisée ?
   La technique du buffer overflow ……
2. Le programme C ci-dessus est il vulnérable à ce type d’abus ? oui ……
3. Si oui, précisez l’instruction (numéro de ligne) dans le programme qui est responsable de cette vulnérabilité ?
   strcpy(c, message1); (ligne 8) ……

En tant qu’un attaquant, vous voulez abuser de ce programme pour activer un shellcode(virus) qui est stocké sur la mémoire à l’adresse **0x41 62 75 73. (Cette adresse est équivalente en ASCII à « A B U S »).**

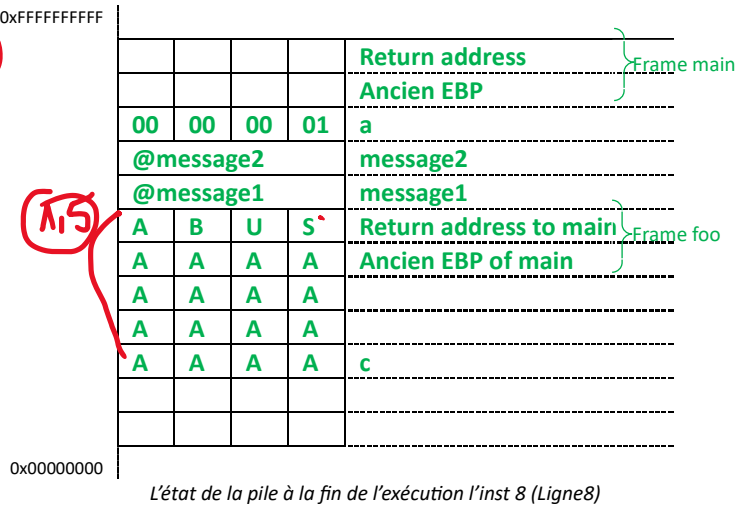
4. Précisez quelle est la variable (nom de la variable) que vous allez abuser pour effectuer cet abus ?
   message1 ……
5. Préciser la taille de l’entrée que vous allez utiliser pour effectuer cet abus ?
   20 caractères ……
6. Préciser la valeur de l’entrée que vous allez utiliser pour effectuer cet abus ?

A A A A A A A A A A A A A A A A **S U B A**

7. Compléter les diagrammes de la pile en considérant que toutes les variables sont alignées sur des multiples de 4 octets, et que les adresses sont stockées sur 4 octets. Les instructions (ligne 12 et 13) peuvent être ignorées lors de la représentation sur la pile.
   Donner l’état de la pile en prenant en considération les valeurs à utiliser pour chaque entrée afin de réaliser l’abus :
   7.1. à la fin de l’exécution de l’instruction 7 (ligne 7).
   7.2. à la fin de l’exécution de l’instruction 8 (ligne 8).



L’état de la pile à la fin de l’exécution l’inst 7 (Ligne7)



L’état de la pile à la fin de l’exécution l’inst 8 (Ligne8)

8. Que doit faire le programmeur pour éliminer cette vulnérabilité ?
   Vérifier la taille des entrées.
   Utiliser la fonction sécurisée de la fonction strcpy. (strncpy)

Bon courage.