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.

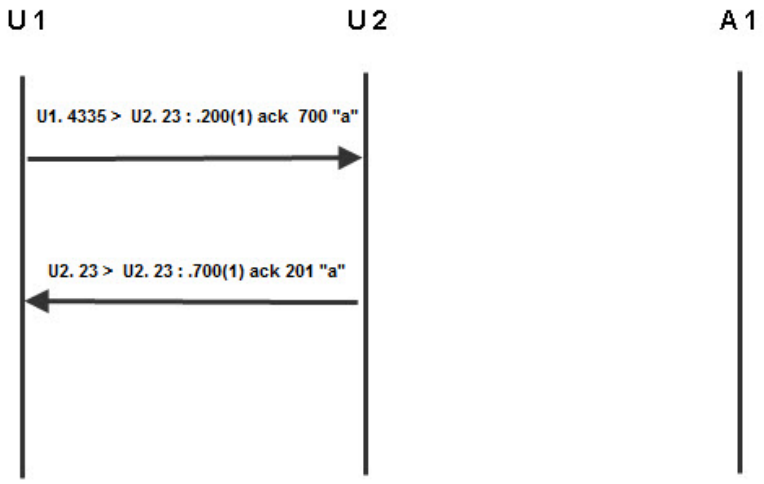

Figure 4.1 Vol de session TCP (à compléter)

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).

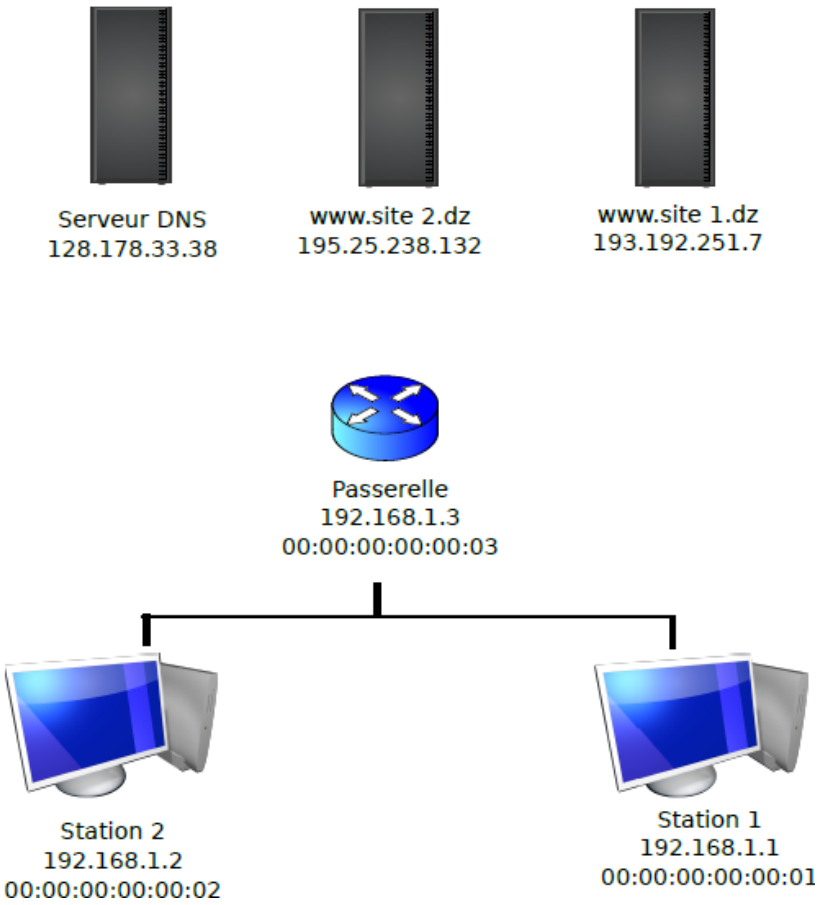

Figure 4.2 architecture d'un réseau attaqué par empoisonnement du cache ARP (à compléter)