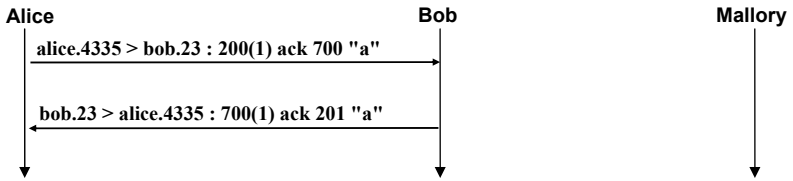
Module TR-c8

TD N° 4 – Sécurité Réseaux - Menaces

Exercice 1 – Vol de session TCP

Un pirate (Mallory) espionne une connexion **telnet**. Il forge un paquet TCP pour insérer la commande **\n écho HACKED \n** dans le flux de données. Le dernier échange de paquets avant l'insertion est illustré à la figure 1.

- Compléter cette figure avec le paquet inséré et les paquets suivants.



Exercice 2 – TCP/IP spoofing

On rappelle que l'IP *spoofing* consiste pour un pirate à se faire passer pour une machine B auprès d'une machine A (au niveau de l'adressage IP). L'attaque se compose généralement de trois étapes :

1. Le pirate paralyse la machine B.
2. Le pirate devine le procédé utilisé par A pour générer ses numéros de séquences initiaux (ISN).
3. Le pirate se fait passer pour B auprès de A.

- Quel se passerait-il si le pirate ne paralysait pas la machine B ?
- Pourquoi est-il nécessaire de déterminer la manière dont A génère ses ISN ?
- Quel peut être l'intérêt pour le pirate de se faire passer pour la machine B ?

Exercice 3 – Attaque de Kevin Mitnick

Le trafic décrit à la figure 2 a été observé dans un réseau (cas réel). De quoi s'agit-il ?

Les paquets TCP sont décrits à l'aide de lignes ayant le format suivant :
`14:18:37.26 alice.513 > bob.514: P 1382727010(2) ack 2024384001`
On y trouve :

- L'heure (**14:18:37.26**) ;
- L'adresse source (**Alice**) ;
- Le port source (**513**) ;
- L'adresse destination (**bob**) ;
- Le port destination (**514**) ;
- Un flag éventuel (**S**= syn., **P**=push, **F**=fin, **R**=reset, **.** = pas de flag) ;
- Le numéro de séquence du premier octet de données transmis dans ce paquet (**1382727010**) ;
- Le nombre d'octets transmis (**2**) ;
- Le numéro de séquence du prochain octet attendu (**2024384001**) ;

Exercice 4 – ARP/DNS spoofing

On considère un réseau local (LAN) composé de deux stations de travail et séparé de l'extérieur par un router (passerelle). Les stations de travail sont configurées pour utiliser un serveur DNS **128.178.33.38** extérieur au LAN et n'utilisant pas de cache DNS interne. On considère enfin deux serveurs HTTP extérieurs au LAN, www.site.fr et www.fakesite.fr. Les différents éléments sont représentés sur la figure 3. L'objectif de l'exercice est de proposer une attaque fondée sur le DNS spoofing, telle que lorsque l'utilisateur de **station1** (victime) tentera d'accéder au site www.site.fr, il aboutira de manière transparente sur le site www.fakesite.fr. L'attaque sera effectuée à partir de **station2**.

Lorsqu'une station souhaite communiquer avec l'extérieur du LAN, elle utilise, comme adresse MAC de destination, l'adresse MAC de la passerelle. La passerelle reçoit le paquet et le transmet 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.

1. L'utilisateur de la machine **station1** exécute la commande **ping 182.168.1.2**. Ci-dessous figurent les messages échangés sur le LAN jusqu'à l'envoi du **ping** ainsi que les adresses contenus dans le paquet **ping** ; compléter le tableau.
   - **192.168.1.1** envoie [**ARP who-has? 192.168.1.2**] à l'ensemble du LAN.
   - **192.168.1.2** répond [**ARP is-at 00:00:00:00:00:02**] à **00:00:00:00:00:01**
   - **192.168.1.1** envoie le paquet **ping 182.168.1.2**

Adresse destination dans le paquet ping	
IP Destination	
MAC Destination	

2. L'utilisateur de la machine **station1** exécute la commande **ping 128.178.33.38**. Indiquer les messages échangés sur le LAN jusqu'à l'envoie du ping et compléter le tableau ci-dessus. 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.fr.** Indiquer tous les messages échangés sur le LAN jusqu'à l'envoie du ping, puis compléter les tableaux suivants.

Adresse destination dans la requête 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 acceptent les réponses AP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment **station2** peut se faire passer pour la passerelle auprès de la **station1**.

5. L'utilisateur de la machine **`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		
	Sans attaque	Avec attaque
IP Destination		
MAC Destination		

6. On suppose que **`station2`** réussit à se faire passer pour la passerelle auprès de **`station1`**. Expliquer comment utiliser cette faille pour réaliser l'attaque initialement souhaité, à savoir que lorsque l'utilisateur de **`station1`** tentera d'accéder au site www.site.fr, il aboutira de manière transparente sur le site www.fakesite.fr 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 ci-dessous les chemins pris par les paquets transitant sur la LAN lorsque **`station1`** exécute la commande www.site.fr (on ne dessinera pas les requêtes et réponses ARP).