Université Batna-2
Faculté Math Informatique
Département informatique

le : 29 Mai 2016
Durée : 1h30
Licence 3 SI

Examen final Module Sécurité Informatique

Documents et ***téléphones*** non autorisés

Exercice1

1- Dans un réseau sans fil, l'administrateur remarque au bout d'un certain temps après la mise en marche du réseau, que le taux de perte des paquets est très élevé (nombre de paquets perdus par unité de temps) ! quelles sont, à votre avis, les attaques possibles qui ont pu causer ce taux élevé de perte de paquets ? (citez au moins 3 possibles)

2- Après vérification, il s'est avéré que tous les nœuds du réseau sont des nœuds de confiance : qui se sont authentifiés avant de rejoindre ce réseau sécurisé. Est-ce qu'il reste un doute qu'il peut exister un attaquant(s) qui cause(ent) ces pertes de Paquets parmi ces nœuds ou ça doit surement être un disfonctionnement du réseau ? expliquer.

Exercice2

1- Qu'est-ce qu'un Déni de Service ? Donnez une attaque qui puisse le causer dans un réseau local filaire? une autre pour un réseau sans fil ?
2- Un serveur **S** et un client **C** communiquent sans aucun souci. Un autre nœud **X** s'introduit dans le réseau : il se présente comme étant le serveur **S** par rapport à **C**, et se présente comme étant le client **C** par rapport au serveur **S**. Le VRAI **S** et le VRAI **C** continuent à communiquer avec **X** sans se rendre compte qu'ils communiquent avec un faux **S** et un faux **C**.
    a. Qu'appelle-t-on cette attaque ?
    b. Est-ce qu'elle peut mener à un DoS ? Expliquez.
    c. Comment se protéger de cette attaque (dans ce cas de figure)?

Exercice3 (IDS)

1- Un nœud malveillant s'introduit dans le réseau mais ne se fait pas détecter par l'IDS car il ne fait qu'analyser le trafic discrètement. Est-ce un faux positif ou un faux négatif ?
2- A votre avis, de quoi dépend le nombre de sondes placées dans un réseau ?
3- Quelle est la différence entre un IPS et un IDS ?

Exercice4 (WireShark)

1- Wireshark est un analyseur de trafic qui peut servir à mieux sécuriser le réseau. citez et expliquer une fonction de Wireshark que l'administrateur peut exploiter dans ce but (sécurité).
2- Comment un attaquant peut exploiter Wireshark pour un acte malveillant ? Citez un seul exemple en expliquant.

Bon courage
Dr. S. BOUAM

Corrigé type avec barème :

Exercice1 (5pts)

1- Dans un réseau sans fil, l'administrateur remarque au bout d'un certain temps après la mise en marche du réseau, que le taux de perte des paquets est très élevé (nombre de paquets perdus par unité de temps) ! quelles sont, à votre avis, les attaques possibles qui ont pu causer ce taux élevé de perte de paquets ? (citez au moins 3 possibles)

Si ces paquets sont perdus à cause d'une attaque (car ça peut être un disfonctionnement du réseau lui-même), il existe plusieurs attaques qui peuvent être en cause (les paquets peuvent être routés ailleurs que sur le bon chemin, supprimés du réseau, altérés à cause de brouillages, …..Ce qui donne comme attaques possibles (trois suffisent) :

-Trou noir (Blackhole) (qui englouti les paquets)

- Trou de ver (qui les route ailleurs)

- Attaques par brouillage (Jamming) (qui détruit les paquets)

-Attaque par collisions (qui annule les paquets)

(Chaque attaque sera notée sur 1pt : 1pt * 3= 3pts)

Ce sont les attaques les plus évidentes qui causent les pertes de paquets dans un réseau, spécialement sans fil, mais on peut citer aussi : boucle de routage, inondation qui causent une élimination automatique des paquets donc une attaque qui mène indirectement à la suppression des paquets…….etc

2- Après vérification, il s'est avéré que tous les nœuds du réseau sont des nœuds de confiance : qui se sont authentifiés avant de rejoindre ce réseau sécurisé. Est-ce qu'il reste un doute qu'il peut exister un attaquant(s) qui cause(ent) ces pertes de Paquets parmi ces nœuds ou ça doit surement être un disfonctionnement du réseau ? expliquer.

On ne pourra jamais écarter la possibilité qu'il existe un ou plusieurs attaquants *internes* au réseau qui se sont introduits (malgré l'authentification) suite à une usurpation d'identité ou une attaque physique (tampering) car on est dans un réseau sans fil et c'est facile de voler ou contrôler un dispositif sécurisé et d'en extraire les clés secrètes, la suite de l'attaque pour causer des pertes importantes sera alors facile !

(citer au moins une attaque qui rende la possibilité de perte des paquets possible malgré une authentification vérifiée est notée sur 2pts)

Exercice2 (7pts)

1- Qu'est-ce qu'un Déni de Service ? Donnez une attaque qui puisse le causer dans un réseau local filaire? une autre pour un réseau sans fil ?

Un Dos : est une attaque ou l'objectif d'un ensemble d'attaques qui vise à mettre à plat une partie ou tout le système informatique. ……. 1pt

***DoS filaire : ex : Sniffing, smurfing, flooding, …etc (une seule attaque =1pt)**

***DoS sans fil : ex Jamming, collisions, tampering, flooding, …etc(une seule attaque =1pt)**

2- Un serveur **S** et un client **C** communiquent sans aucun souci. Un autre nœud **X** s'introduit dans le réseau : il se présente comme étant le serveur **S** par rapport à **C**, et se présente comme étant le client **C** par rapport au serveur **S**. Le VRAI **S** et le VRAI **C** continuent à communiquer avec **X** sans se rendre compte qu'ils communiquent avec un faux **S** et un faux **C**.

a. Qu'appelle-t-on cette attaque ?

La réponse correcte est : Cette attaque est une attaque Man In the Middle ……1pt

Mais également ceux qui m'ont mis spoofing, usurpation d'identité, attaque sybille, seront notés car ce sont des attaques qui mènent à l'attaque Man in the middle et qui passent dans ce scénario.

b. Est-ce qu'elle peut mener à un DoS ? Expliquez.

Oui, absolument ……0.5pt car tout le trafic passe par X et il pourra alors extraire des informations qui puissent l'aider à aboutir à un DoS, il pourra injecter de fausses informations, causer une congestion, supprimer des messages importants…. Et tout ça peut mener à un DoS partiel ou total. ……1pt

c. Comment se protéger de cette attaque (dans ce cas de figure)?

L'authentification est la clé de base pour contrer à cette attaque……1pt
Le cryptage peut être complémentaire, l'identification, signature numérique……0.5pt

Exercice3 (IDS) (6pts)

1- Un nœud malveillant s'introduit dans le réseau mais ne se fait pas détecter par l'IDS car il ne fait qu'analyser le trafic discrètement. Est-ce un faux positif ou un faux négatif ?

Un faux négatif. ……2pt

2- A votre avis, de quoi dépend le nombre de sondes placées dans un réseau ?

Le premier paramètre de base est : le niveau de sécurité qu'on veut assurer : plus le niveau est élevé, plus le nombre de sondes va augmenter ……1pt
Le deuxième paramètre de base est : la taille du réseau : plus le réseau est peuplé, plus il y aura de sondes, moins de nœuds il y aura, moins de sondes existeront ! ……1pt
Rq : d'autres paramètres peuvent jouer sur le nombre de sondes mais les plus évidents sont ces deux-là.

3- Quelle est la différence entre un IPS et un IDS ?

Tout simplement : un IPS sert à Prévenir les intrusions *avant* qu'elles ne s'infiltrent dans le système et l'IDS sert à Détecter les intrusions une fois elles se sont introduites dans le système……2pt

Exercice4 (WireShark) (2pts)

1- Wireshark est un analyseur de trafic qui peut servir à mieux sécuriser le réseau. citez et expliquer une fonction de Wireshark que l'administrateur peut exploiter dans ce but (sécurité).

Il existe plusieurs fonctions Wireshark qui servent à sécuriser le réseau : filtrage, statistique, analyse des paquets….(citer une seule avec explication suffit)……..1pt

2- Comment un attaquant peut exploiter Wireshark pour un acte malveillant ? Citez un seul exemple en expliquant.

On peut citer par exemple l'analyse des paquet, qui pourra permettre de récupérer des mots de passe par exemple et de casser l'authentification (tout autre exemple correct sera noté)……1pt