Module M4210 - Architecture de sécurité des réseaux

TD 1 : Sécurité des réseaux

11 février 2015

Questions de cours

1. Rappeler les principales propriétés requises d'un système de gestion de la sécurité des réseaux.
2. Quelles sont les principales étapes d'un cycle PPR ?
3. Quelles sont les principales différences entre un virus informatique, un ver et un *wabbit* ? Donner un exemple d'un *wabbit*.
4. Citer deux attaques ciblées différentes de réseaux

Attaques

1. Donner des exemples d'attaques basées sur l'usurpation d'adresses.
2. Donner deux exemples d'attaques par saturation.
3. Donner des exemples d'attaques de type *déni de service*.
4. Pourquoi un paquet mal-formé peut-t-il provoquer l'arrêt de la machine réceptrice ?
5. Afin de restreindre la visibilité d'une machine A, l'administrateur met en œuvre une politique de filtrage des paquets `ICMP` de type `echo-request` à destination de A. Comment peut-on faire pour tester l'atteignaibilité de la machine ?
6. Le `RFC 864` spécifie le service `chargen` qui permet de générer des chaînes de caractères aléatoirement à destination d'un client qui en fait la demande. Le service, associé au port `19` est destiné initialement à des fins de tests et des mesures des protocoles `UDP` et `TCP`. Donner un schéma qui permet de détourner ce service pour attaquer une cible A.
7. Rappeler le principe de l'attaque `ARP spoofing`. Donner deux manières différentes pour se protéger contre cette attaque.
8. Comment intercepter des messages entre deux hôtes en utilisant le protocole `RIP`.

NAT

On considère le cas d'un particulier qui possède trois machines et un abonnement d'accès à Internet auprès d'un fournisseur d'accès (FAI). L'accès se fait via une ligne téléphonique. Le FAI attribue au particulier l'adresse IP fixe suivante : `138.76.29.7/24`. Les trois machines sont reliées entre-elles par un réseau local de type `10baseT`. Une des machines sert comme une passerelle pour permettre le partage de l'accès à l'Internet entre les trois machines.

1. Afin de partager l'accès à l'Internet, le particulier attribue à ces machines les adresses suivantes : `138.76.29.7, 138.76.29.8 et 138.76.29.9` . Qu'en pensez-vous de cette solution ?
2. Proposer un plan d'adressage pour le réseau du particulier.
3. Proposer deux méthodes différentes pour partager l'accès au WEB entre les trois machines.
4. A quel niveau opère le service NAT ? Que peut-on conclure ?
5. Quelle est la différence entre un service NAT statique et un service NAT dynamique ? Quel type de service proposez vous d'utiliser dans ce cas ?

Pare-feux

1. Qu'est-ce qu'un pare-feu ? Quelle sont ses principales fonctions ? Et à quels niveaux un pare-feu peut-il opérer ?
2. Quelle est la différence entre un pare-feu à filtrage statique et un pare-feu à filtrage dynamique ?
3. Un pare-feu est un équipement nécessaire mais non suffisent pour assurer la sécurité d'un réseau. Justifier.
4. Qu'est-ce qu'un DMZ ? Quelle est son utilité ?
5. Une règle de filtrage dans votre pare-feu permet de bloquer un certain type de trafic. Un audit de sécurité de votre système montre que ce n'est pas le cas. Quel peut être le problème ?
6. Donner les principales règles à appliquer par un pare-feu concernant le filtrage du trafic sortant du réseau protégé.

IPTables

Expliquer l'effet des règles de filtrage suivantes :

1. `iptables -A INPUT -s 193.48.143.10 -j ACCEPT`
2. `iptables -A INPUT -i lo -j ACCEPT`
3. `iptables -A INPUT -p udp -dport 22 -j ACCEPT`
4. `iptables -A INPUT -p tcp -tcp-flags SYN FIN-j Drop`
5. `iptables -A INPUT -p tcp -tcp-flags SYN ACK,SYN, FIN-j Accept`
6. `iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP -sport 1024:65535 -dport 80 -j ACCEPT`
7. `iptables -A INPUT -j LOG -log-level debug -log-prefix "PAQUET ENTRANT "`
8. `iptables -t nat -A POSTROUTING -o eth0 -j SNAT -to 1.2.3.4`
9. `iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT -to 1.2.3.4 :1-1023`
10. `iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE`

En utilisant la syntaxe `iptables`, donner les règles de paramétrage d'un pare-feu pour réaliser les tâches suivantes :

1. La machine ne peut qu'envoyer des paquets `ICMP echo-request` vers les autres machines du réseau. Elle peut répondre aux messages de même type.
2. La machine peut seulement accéder à des serveurs web sans pouvoir utiliser la commande `ping` ni répondre à des messages `ECHO-request`.
3. Donner à la machine la capacité de servir comme un serveur web seulement, sans rien d'autres !
4. Limiter l'effet d'une attaque par saturation de messages `ICMP request` tout en répondant de temps à autres à des messages de ce type.
5. Sauvegarder dans un fichier log tous les paquets refusés.