Master 2 SeCReTS

TP Sécurité Réseau

Première partie
Généralités

1 Manipulations basiques

Vous devez utiliser **deux machines virtuelles**.

Consulter la documentation de VirtualBox (ou VMware Player) pour bien comprendre les différentes options possibles en termes de configuration réseau.

- La première machine virtuelle (`VM1`) devra avoir deux interfaces réseaux : l'une sera connectée au système hôte en mode *host-only* et l'autre sera rattachée à un réseau interne (« *intnet* » sous VirtualBox) dédié aux machines virtuelles.
- La deuxième machine virtuelle (`VM2`) devra être uniquement connectée au réseau interne des machines virtuelles.

1.1 Choix des sous-réseaux

Choisissez deux sous-réseaux :

- l'un en `/24` pour l'interconnexion *host-only* ;
- l'autre en `/28` pour la communication interne entre les machines virtuelles.

Dessiner un schéma réseau détaillé de cette mini architecture pour avoir les idées bien claires et vérifier ensuite que tout fonctionne correctement.

1.2 Modification du système

La configuration réseau des différentes interfaces doit être fixée dans les fichiers de configuration de manière à ne pas perdre le paramétrage en cas de *reboot* des machines virtuelles (se reporter à la documentation Debian pour connaître les fichiers de configuration à modifier).

1.3 Affichage des tables ARP

Consulter la page de manuel du programme `arp`. Comment cet outil fonctionne-t-il ? Est-ce que son utilisation génère du trafic réseau ?

.

A l'aide de ce programme, afficher la table ARP sur les machines virtuelles et vérifier ainsi qu'elles sont bien connectées sur un même support de niveau 2.

1.4 Ajout d'une adresse IP supplémentaire

Paramétrer une deuxième adresse IP associée à l'interface côté réseau interne (appelée adresse IP *alias*) de `VM2`.

Vérifier que cela fonctionne et que la nouvelle adresse IP est bien accessible. Quels sont les différents mécanismes réseaux qui rendent possible l'association de plusieurs adresses IP à une même interface physique ?

1.5 Capture du trafic réseau

1.5.1 Utilisation de `tcpdump`

Consulter la page de manuel de `tcpdump`.

Afficher les paquets de données transitant par votre interface réseau. Essayer d'exécuter `tcpdump` avec différents arguments afin de faire varier le mode d'affichage des paquets réseaux (décodage plus ou moins détaillé).

Enregistrer quelques secondes de trafic réseau sur le disque dans un fichier de capture et essayer de relire ce fichier (toujours à l'aide de `tcpdump`).

1.5.2 Capture du trafic ARP

Mettre en évidence un échange ARP (requête et réponse). Comment pouvez-vous forcer la génération de trafic ARP ?

1.5.3 Capture du trafic ICMP

Mettre en évidence les requêtes ICMP de type `echo-request` et `echo-reply` envoyées entre les machines virtuelles.

Quelles sont les données additionnelles contenues dans ces paquets ?

1.6 Routage

1.6.1 Tables de routage

Consulter les pages de manuel des programmes `route` et `netstat`.

En utilisant l'un ou l'autre de ces outils, afficher les tables de routage des machines virtuelles.

1.6.2 Ajout d'une route

Vérifier d'abord sur la machine `VM2` que vous **ne pouvez pas** atteindre la machine physique.

Modifier ensuite la table de routage de `VM2` pour y ajouter une route vers la machine physique. Est-ce que cela fonctionne ? Que faut-il faire en plus ?

1.6.3 Utilisation de `traceroute`

Utiliser le programme `traceroute` pour afficher le chemin réseau entre `VM2` et la machine hôte.

1.7 MTU

A l'aide de la commande `ifconfig`, modifier le MTU de l'interface de la machine virtuelle `VM1` (l'interface qui est connectée à la machine physique) pour lui donner une valeur inférieure à sa valeur initiale.

Reprendre la question précédente, et essayer d'envoyer des paquets `ICMP` *echo-request* avec une taille supérieure au MTU que vous venez de modifier. Que se passe-t-il ?

Deuxième partie

UDP et TCP

2 Utilisation de la commande `netstat`

A l'aide de la commande `netstat`, afficher les connexions réseaux actives de votre machine virtuelle.

3 Utilisation de la commande `netcat`

Consulter la page de manuel de `netcat`.

A l'aide de ce programme, essayer d'ouvrir une connexion `TCP` depuis une machine virtuelle vers une autre machine, en prenant un numéro de port destination inattribué

Que se passe-t-il ? Observer les mécanismes de retransmission de `TCP` lors de la tentative d'établissement de la connexion. Quels sont les valeurs (approximatives) des *timeouts* ?

Essayer maintenant avec un port destination en écoute et mettre en évidence l'ouverture de la connexion `TCP` (poignée de main en trois étapes).

Remarque : pour les deux questions précédentes, il faut utiliser les résultats de la commande `netstat` pour déterminer quels sont les numéros de ports que l'on peut utiliser.

3.1 Client/serveur trivial

A l'aide de `netcat` et de quelques commandes de shell, créer un serveur `TCP` trivial, acceptant les connexions sur le port 10000 et retournant au client un compteur incrémenté chaque seconde.

Troisième partie

Utilisation des outils de sécurité

Dans un premier temps, désactivez le pare-feu, `NAT`, etc.

4 Reconnaissance réseau

Prendre connaissance de la page de manuel de `hping`.

A l'aide de `hping`, essayer de mettre en évidence l'adresse d'interconnexion de la machine virtuelle de votre homologue (en jouant sur des valeurs de `TTL` bien choisies).

5 Scans de port

Prendre connaissance de la page de manuel de `nmap`.

Lancer un scan de port `TCP` (de type *SYN scan*) vers la machine virtuelle située à l'extrémité de l'architecture. Mettre en évidence avec `tcpdump` le trafic généré.

Vérifier notamment que si vous ne paramétrez pas correctement le pare-feu local, des paquets `RST` peuvent être générés en réponse à des réponses de type `SYN/ACK`.

Combien de temps faut-il pour scanner tous les ports TCP ? Refaire le test en activant le pare-feu à l'autre extrémité de l'architecture.

6 Attaques au niveau 2

6.1 Forger un paquet ARP

A l'aide de `scapy`, forger une réponse `ARP` pour une adresse IP inexistante de votre réseau privée.

Envoyer cette fausse réponse depuis la machine virtuelle cliente (pas la passerelle) et mettre en évidence le cache `ARP` est bien mis à jour.

Si vous avez suffisamment de mémoire, dupliquer la machine virtuelle (importer/exporter) et vérifier ainsi que vous êtes en mesure de détourner le trafic.

7 Attaques de niveau 3

Paramétrer un service `TCP` sur votre machine virtuelle (serveur web, serveur SSH, etc.). Vous pouvez aussi choisir avec `netstat` un service existant.

Depuis l'autre machine, avec le programme `hping`, essayer d'envoyer un très grand nombre de paquets de type `SYN`. En principe, la pile IP de Linux met en oeuvre les *syncookie* en cas de détection d'une attque de type *syn flooding*. Essayer de mettre en évidence cette fonctionnalité.

8 La notion de tunnel `IP`

Consulter le manuel de la commande `ip`.

Le but est de créer un tunnel de type `IP` *over* `IP`.