Td ARP Hack

16 octobre 2017

1

ARP Poisoning

L'objectif de ce `td` est de mettre en place plusieurs techniques de *hack* dans un réseau, pour notamment apprendre à se protéger.

1. Configurer `GNS3` en mode serveur avec une machine virtuelle.

2. On souhaite, dans un premier temps, créer une topologie simple basée sur le réseau IP 192.168.0/24 avec plusieurs noeuds `docker`

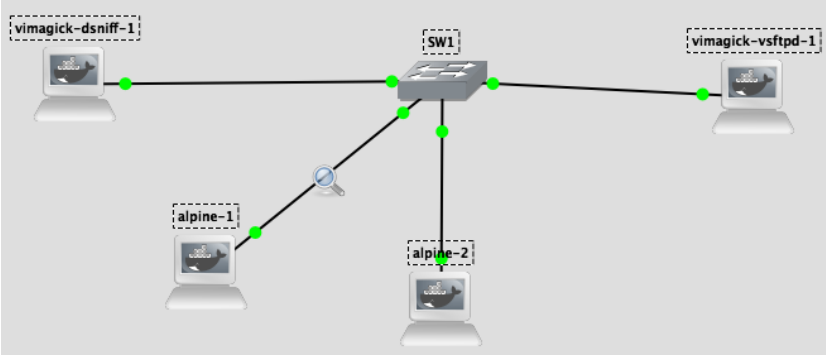

FIGURE 1 – Topologie elementaire

Base revision e844974, Wed Apr 6 11:51:50 2016 +0200, David Bromberg.

3. Créer plusieurs `template` de noeuds docker. En particulier, les conteneurs suivants :
   - `vimagick-dsniff`, contient tous les outils de l'attaquant
   - `vimagick-vsftpd`, contient le serveur ftp
   - `alpine:3.3`, contient le conteneur linux de base
   - `gns3-dhcp`, contient un serveur dhcpd basé sur dnsmasq
4. Il est possible de vérifier l'existence et le contenu de tous ces conteneurs *via* le site https://hub.docker.com/
5. Pour forcer un commutateur à se comporter comme un hub, on peut utiliser l'outil `macof`. Rappeler comment fonctionne `macof` en détaillant son fonctionnement. Tenter de saturer votre commutateur. Faire une capture de trafique pour illustrer son fonctionnement.
6. Pour indiquer à votre station que vous souhaitez faire une redirection de trafic, faire un `echo 1 > /proc/sys/net/ipv4/ip_forward`
7. Inspecter le cache `arp` de chacune de vos stations grâce à la commande `arp`.
8. L'objectif va être d'utiliser l'utilitaire `arpspoof` enfin d'envoyer à une cible, c'est à dire à la victime, de fausses réponses `ARP` afin de contaminer son cache `ARP`. L'objectif est en particulier d'intercepter le traffic de la victime. En particulier, l'`arp spoofing` permet de mettre en place une attaque de type *man in the middle* (si couplé avec la redirection de traffic).
   `arpspoof -t` $IP_{machine1}$ $IP_{machine2}$ permet de se faire passer auprès de `machine1` comme étant `machine2`

   

   Poison bidirectionnel

   Pour faire une redirection bi-directionnelle, penser à contaminer également le cache arp de la machine 2.
   `arpspoof -t` $IP_{machine1}$ $IP_{machine2}$
   `arpspoof -t` $IP_{machine2}$ $IP_{machine1}$
9. Tester le fonctionnement de l'outil `arpspoof`, illustrer son fonctionnent en capturant le trafique et en regardant l'évolution du cache arp de vos machines.
10. Comment peut-on d'après vous se protéger de ce type d'attaque ?