acceis

Travaux Pratiques : Attaques réseaux

L'objectif de ce TP est d'appréhender certaines attaques pouvant être menées sur un réseau.

Préparation

1. Installer un outil de virtualisation (VirtualBox par exemple) : https://www.virtualbox.org/
2. Récupérer l'OVA Kali Linux (sur disque ou clé USB) et importé la machine virtuelle ;
3. Préparer la machine virtuelle Kali avec une interface en mode bridge sur la carte principale du host.

Observation de la séquence d'initialisation TCP

1. *Victime* : lancer Wireshark et filtrer les flux pour n'afficher que les échanges TCP sur le port 4242 et lancer netcat (commande « nc ») en écoute sur le port 4242.
2. *Attaquant* : A l'aide de la commande netcat, se connecter à la victime sur le port 4242.
3. *Victime* : Observer la structure des échanges.

IP Spoofing

1. *Victimes 1 & 2* : lancer Wireshark et filtrer les flux pour n'afficher que les échanges ICMP.
2. *Attaquant* : A l'aide de la commande hping3, envoyer une requête ICMP ping en usurpant l'adresse IP de la victime 2.
3. *Victimes* : Observer la structure des échanges.

SYN flooding

1. *Victime* : Faire un test de vitesse de connexion sur Internet.
2. *Attaquant* : Lancer une attaque en SYN flood via la commande hping3, sur le port TCP 21 avec une adresse IP source usurpée (random).
3. *Victime* : Refaire un test de vitesse de connexion sur Internet.

Gwenn Feunteun (**gwenn@acceis.fr**)

ARP cache poisoning

1. *Victime* : regarder le contenu du cache ARP
2. *Attaquant* :
    - Lancer wireshark ;
    - Lancer ettercap en mode graphique (option -G). Mode « unified sniff ».
    - Scanner les hôtes sur le réseau.
    - Cibler la victime et le routeur du sous-réseau.
    - Lancer une attaque d'ARP cache poisonning. « sniff remote »
3. *Victime* : Regarder le contenu du cache ARP et surfer sur le net.
4. *Attaquant* : Observer la structure des échanges.
5. Refaire la même chose, mais en python avec scapy.

Gwenn Feunteun (**gwenn@acceis.fr**)