Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - Scanner des ports, forger des paquets, ...

Le but de ce TP est d'étudier des outils de diagnostics ainsi que d'utiliser des techniques de scan de ports simples.

Dans ce TP, nous nous concentrerons sur deux outils :

— `nmap` qui est un outil de diagnostic puissant permettant de scanner des ports d'une manière plus ou moins sophistiquée et plus encore.

— `scapy` qui est un outil permettant de forger soi-même ses propres paquets.

Remarque : La majorité des techniques que nous verrons nécessitent les droits `root`.

La topologie réseau correspondante peut être obtenue en lançant le script de démarrage `/net/stockage/aguermou/SR/TP/2/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
cd /net/stockage/aguermou/SR/TP/2/; ./qemunet.sh -x -t topology -a archive_tp2.tgz
```

1. Nous allons nous intéresser maintenant à une attaque simple dans un réseau local : l'*ARP cache poisonning*. Il s'agit d'usurper les adresses MAC de certaines machines pour mettre en place une attaque de type *man in the middle*.
   (a) Mettre en place le spoofing à l'aide d'arpspoof. Quel est le mécanisme utilisé ?
   (b) La détection de ce genre d'attaque peut se faire assez simplement en surveillant le réseau. L'outil `arpwatch` permet de faire ce genre de choses. Essayer de detecter l'attaque avec cet outil.
2. Un utilisateur se connecte périodiquement depuis `syl` sur `grave`. Il vous est demandé de trouver ses identifiants et de les utiliser pour ouvrir une session (en local) sur `grave`.
3. Une *backdoor* (*rwwwshell*) a été mise en place sur `syl`. Son principe est simple : périodiquement (toute les deux secondes) syl essaye de se connecter à la machine attaquante (opeth) pour lui permettre de lancer un shell à distance. Il vous est demandé d'une part de lancer rwww-shell sur opeth pour valider le fonctionnement de l'attaque et d'autre part d'identifier le processus responsable de l'ouverture de la backdoor sur syl.
4. À l'aide de `nmap` essayer de déterminer le système d'exploitation de nile.
5. Toujours à l'aide de `nmap` faite un balayage d'adresses IP (*ping sweep*).
6. Mettre en place, à l'aide de `nmap`, différents scans allant du *SYN scan* au *XMAS scan*. Modifier le firewall au niveau de la passerelle pour voir l'évolution du résultat.
7. Répeter la question précédente mais cette fois-ci avec `scapy`. Penser à réinitialiser les règles du firewall modifiées dans la question précédente.