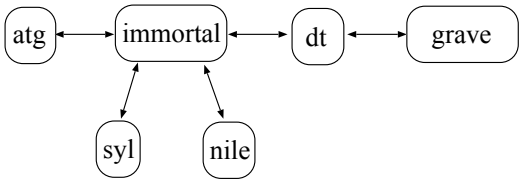
Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - A l'abordage !

Le but de ce TP est de vous mettre dans la situation d'un attaquant. Vous avez uniquement accès aux machines `dt` et `nile` en tant que `root`. Le but est de trouver les identifiants (login/mot de passe) qui vous permettront d'ouvrir une session sur atg à partir de nile. Pour vous "simplifier" la vie, `syl`, se connecte périodiquement à atg en utilisant le protocole `telnet` à l'aide des identifiants recherchés (le dialogue se fait donc en clair).



La topologie réseau correspondante peut être obtenue en lançant le script de démarrage `/net/stockage/aguermou/SR/TP/5/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/5/; ./qemunet.sh -x -t topology -a archive_tp5.tgz
```

Indications :

- immortal et grave font office de serveur dns pour toutes les machines du réseau. De plus lorsqu'une requête concernant atg est envoyée à immortal, cette dernière la fait suivre au serveur légitime qu'est grave.
- Dans le cas ou sur une machine vous avez besoin de répondre à un trafic que vous recevez mais qui ne vous est pas destiné, pensez à utiliser l'action `REDIRECT` de la table nat d'iptables. Un exemple d'utilisation de ce type de règle est fourni ici : `http://www.thoughtcrime.org/software/sslsniff/`.
- Un serveur dns simple (`dnsmasq`) est intallé sur dt. Il vous permettra de répondre simplement à des requêtes dns (en modifiant le fichier `/etc/dnsmasq.hosts` et en redémarrant le service). Une documentation peut-être trouvée ici : `http://blog.philippheckel.com/2013/07/18/how-to-dns-spoofing-with-a-simple-dns-server-using-dnsmasq/`.
- Enfin, dans le cas ou vous auriez besoin de faire suivre un traffic depuis nile vers une autre machine, un script redirect.sh vous est fourni (`/net/stockage/aguermou/SR/TP/5/redirect.sh`). Il fonctionne de la manière suivante : `./redirect.sh [numero_port] @IP`.