Université de Bordeaux — année 2020-2021

Master CSI/Master Info. — Sécurité des réseaux

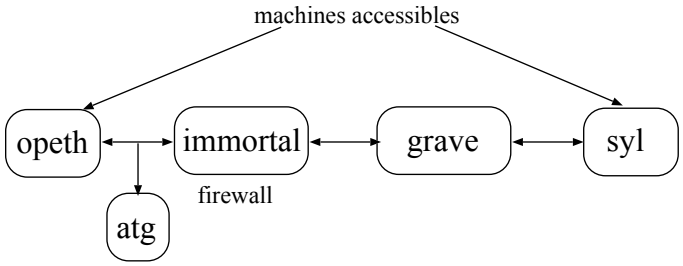
TD - TP noté (1h)

— Les réponse doivent être saisies sur l'activité rendre le TP (https://moodle1.u-bordeaux.fr/mod/vpl/view.php?id=318934) du moodle de l'UE de sécurité des réseaux.
— Lancer le script de démarrage `/net/stockage/aguermou/SR/devoir/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 initiale des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
user@machine# cd /net/stockage/aguermou/SR/devoir/2/; ./qemunet.sh -d tmux -b \
                  -t topology -a archive_devoir.tgz;
user@machine# tmux a
```

Le contexte

Le but du challenge est de récupérer un code secret fournit par atg depuis une des machines que vous contrôlez. Malheureusement, opeth a été installée de façon très restrictive (très peu d'outils sont installés, pas de dossier de partage `/mnt/host`, etc.). Le but est donc d'utiliser opeth comme pivot pour accéder à atg depuis syl. immortal quant à elle, joue le rôle d'un firewall très restrictif qui ne laisse passer que le trafic IPSec.



Du point de vue du rendu moodle, il vous est demandé de rendre :
— Décrire ce que vous faites dans en remplissant le fichier de commentaires
— Saisir le flag qui vous est fournit par grave lorsque vous arrivez à configurer IPSec. Ce flag est disponible soit à l'écran ou dans un fichier flag contenu dans le dossier de partage de grave.
— Saisir le code secret.

Une fois le code secret (resp. flag) saisi, vous avez la possibilité de vérifier la saisie en cliquant sur le bouton run de moodle.

Configuration IPSec

Afin de pouvoir utiliser opeth comme pivot, il est nécessaire de pouvoir communiquer avec elle depuis syl. Il faut donc mettre en place une communication IPSec entre opeth et syl.

Récupération du secret

Le code secret que vous devez récupérer est fournit par atg en utilisant une simple connexion TCP sur un port dont le numéro est entre 40000 et 45000.

Indications : L'utilisation d'opeth comme pivot être fait en établissant un tunnel `ssh` avec choix dynamique de port et d'utiliser un outil de tunneling avancé tel que `proxychains`.