Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - Entrainement

Le but de cet exercice est d'arriver à ouvrir une connexion à distance depuis syl vers opeth.

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

Le contexte

Les mécanismes de *Single Packet Authorization* (ou SPA) sont des méthodes permettant de modifier le comportement d'un firewall en temps réel en provoquant l'ouverture de ports permettant la communication, grâce à l'envoi, au préalable, d'un paquet authentifiant la machine voulant accéder au service considéré.

les mécanismes de type SPA consistent à vérifier le caractère sain du client avant toute action de sa part (le client étant une machine qui tente d'ouvrir une connexion vers notre serveur). La question est donc : Comment vérifier qu'on peut faire confiance au client ? SPA y répond en disant qu'il faut que le client entre "le bon mot de passe" ou "la bonne clé". Le principe est le suivant, dès que le client cherche à se connecter à un service protéger par SPA, il doit tout d'abord montrer à ce dernier qu'il est légitime. Pour se faire, il crée un paquet (généralement UDP), contenant :

- 16 octets de données aléatoires
- nom d'utilisateur (pour différencier les utilisateurs)
- horrodatage
- version du logiciel (nécessaire pour garantir la compatibilité)
- mode (ouverture de connexion dans notre cas)
- requête (le/les port(s) qu'on cherche à ouvrir)
- somme de hachage (porte sur tous les champs précédents)

Ce message est ensuite chiffré à l'aide d'une clé (souvent symétrique) partagée par le serveur et ses différents clients. À la réception du message d'authentification, le serveur SPA va le déchiffrer avec la clé correspondante et vérifier la validité du message. Ensuite, si toutes les vérifications sont positives, il donne l'accès au client aux ports demandés pendant une courte période (30 secondes en général). Au bout de cette période, le port est de nouveau fermé. Bien entendu, si un attaquant intercepte le paquet, il ne peut pas le rejouer puisque le serveur est capable de detecter le rejeu. Si cette technique est appliquée à tous les services tournant sur notre serveur, vu de l'extérieur, notre serveur ressemblera de plus en plus à un client tout ce qu'il y a de plus quelconque.

Prenons un petit exemple pour en expliquer le fonctionnement. Initialement tous les ports du serveur sont fermés par un firewall. Il est possible d'accéder à l'un d'entre eux (par exemple le port ssh) grâce à un message SPA. Pour se faire, il faut générer le message décrit ci-dessus et l'envoyer au serveur. Si l'authentification réussit, le serveur reconfigure le firewall pour autoriser ce client en particulier ouvrir une connexion sur le port 22. Cette autorisation temporaire et expire au bout d'un certain temps. Il est donc nécessaire dans ce cas de refaire l'étape de *port-knocking*.

En résumé, SPA est donc une méthode "simple" pour autoriser un accès distant sur un port qui n'est pas constamment ouvert. Cela permet d'éviter les scans de ports et certaines attaques.

Dans notre cas, il faut, au préalable à toute tentative de connexion, trouver le mot de passe SPA qui fera office de de clé.

Challenge

Dans ce qui suit, il est **interdit** de reconfigurer les interfaces réseaux des machines faisant partie du réseau.

1. Expliquer pourquoi en quoi le principe du SPA présenté ci-dessus peut améliorer la sécurité. Est-il possible avec une technique de brute-force de découvrir la clé SPA permettant de débloquer un port ? Expliquer comment le rejeu peut être détecté.
2. Déterminer les adresses IP de toutes les interfaces réseau de toutes les machines. (celles qu'il est possible de trouver).
3. opeth est protégée par un mécanisme de SPA sur le port `telnet` (port 23). nile, quant à elle, joue le rôle de client et se connecte régulièrement à opeth sur ce même port. L'objectif ici est de parvenir à partir de syl à ouvrir une session `telnet` sur le port correspondant d'opeth. Expliquer de manière détaillée les étapes que vous allez suivre pour y arriver.

Remarques :

— Sur la machine dt s'exécute un démon qui écoute sur un port dont le numéro est comprisentre 40000 et 50000. À toute connexion sur ce dernier, le serveur répondra en envoyant le mot de passe SPA. Il vous sera donc nécessaire au préalable de trouver la clé SPA fournie par ce serveur.

— Dans le cas où vous ayez forger le message SPA à partir syl, il vous est demandé d'utiliser la commande `fwknop` :
`fwknop -A 'tcp/port' -s -D @ip_machine_distante`
Dans cet example, nous demandons l'accès au port `port` de la machine distante. Attention, fwknop va vous demander de fournir un mot de passe !

— L'adresse IP de dt est 104.85.39.23.

— Le compte de l'utilisateur qui se connecte périodiquement depuis nile vers opeth existe aussi sur grave.