TP 4IF SERE - Sécurité Réseau
Attaques
antoine.boutet@insa-lyon.fr

Objectif : L'objectif de ce premier TP est de mettre en oeuvre différentes attaques de cyber-sécurité, afin de vous faire prendre conscience des failles les plus répandues et des risques qu'elles représentent. Un compte rendu vous sera demandé incluant la réponse aux questions posées ainsi que votre analyse personnelle. Dans un second temps, il vous sera demandé de préparer une ou deux attaques que vous aurez choisi, de la mettre en place dans la plate-forme de virtualisation et de préparer une présentation d'introduction et un exercice guidé. Un présentation de votre / vos attaques sera réalisée semaine 13.

Moyens mis en oeuvres : Pour ce TP, vous disposez de 5 machines virtuelles. Les machines sont isolées dans un sous-réseau afin que le TP n'interfère pas avec l'extérieur.

Chaque binôme dispose de 5 machines :

- Hacker : C'est la machine que vous allez utiliser pour faire vos attaques. Elle fonctionne sous KALI Linux, une distribution Linux équipée de tous les outils nécessaires aux attaques, et dont la vocation est de tester la sécurité des systèmes informatiques.
  Nom d'utilisateur : root - mot de passe : 000000
- Serveur 1 : Ce serveur ne comporte rien de particulier, il sert à l'exercice de prise en main du TP.
- Serveur 2 : Ce serveur héberge plusieurs sites web sur un serveur apache, ainsi qu'un serveur MySQL. Chaque site sers à mettre en évidence une faille précise de sécurité. Leur contenu est détaillé dans les exercices.
- Client : Il s'agit d'un client Windows qui sera victime d'une de vos attaques.
- Android : Un client Android qui sera aussi victime d'une de vos attaques.

Partie 1 : Sniffing

Machines nécessaires : hacker – server1

Exercice guidé : Une machine de votre réseau ouvre toute les minutes une connexion (root) TELNET avec le Serveur 1. Utilisez cette connexion pour trouver le mot de passe root du serveur.

Comment faire ? :

1. Si ce n'est pas déjà fait, lancez l'interface graphique de kali : startx

   Faire un schéma du réseau : Tout au long de ce TP, vous aurez besoin de connaître les IP des différentes machines présentes sur le réseau.
   On peut scanner le réseau grace à nmap :
   ```
   # nmap -sP <ip réseau>
   # soit dans notre cas :
   nmap -sP 10.101.101.0/24
   ```

2. Lancez Wireshark : Application > Renifler et Usurpation > Wireshark

3. Sélectionnez votre interface réseau (eth0)

4. Wireshark espionne actuellement tout les paquets. Vous pouvez filtrer uniquement les telnet en précisant telnet dans la barre des filtres.

5. Lorsque wireshark a intercepté une connexion TELNET, des paquets apparaissent. Néanmoins, le mot de passe est difficile à reconstituer car il a pu être découpé en plusieurs paquets. La meilleur solution est de demander à Wireshark de reconstituer le flux associé à ces paquets. Pour ce faire : clic droit sur un paquet > suivre > flux tcp

6. Vous devriez maintenant avoir trouvé le mot de passe.

Question : Expliquez l'intéret d'une connexion SSH par rapport à une connexion TELNET. Que se serait-il passé dans le cas d'une connexion SSH ? Faire un schéma expliquant les échanges SSH de paquet lors de la première connexion entre deux machines.

Partie 2 : Vulnérabilités Serveur

Machines nécessaires : hacker – server2

2.1) XSS : Cross Site Scripting et SQL Injection

Suivre le diapo XSS-SQL.pdf, le site web associé est disponible sur http://ip-server2/sql/.

2.2) RFI : Remote File Inclusion

Suivre le diapo RFI.pdf, le site web associé est disponible sur http://ip-server2/rfi/.

2.3) FUV : File Upload Vulnérability

Suivre le diapo FUV.pdf, le site web associé est disponible sur http://ip-server2/fuv/.

2.4) DOS : Denial Of Service

Machines nécessaires : hacker - server1 - client

Question : Rappelez comment fonctionne l'établissement d'une connexion TCP. Que se passe-t'il si on bloque l'émission du ACK ?

Cette attaque s'appelle un SYN flood, et vise à forcer le serveur à maintenir un maximum de connexion ouvertes. Un outil integré à KALI permet justement d'effectuer une telle attaque :

```
hping3 --flood -p <port> -S <ip victime>
```

Votre victime sera le client Windows sur votre réseau. Pour voir l'impact d'une telle attaque, connectez vous sur le client (mot de passe : Ku5632) et ouvrez le gestionnaire des taches, onglet performances.

On peut lister les ports ouverts de la victime grace à nmap. Sur la machine hacker :

```
#scan tous les ports compris entre 1 et 500
nmap -p 1-500 <ip cible>
```

Une fois que vous avez déterminé l'ip de la victime et un port pour attaquer, lancez l'attaque via la machine hacker.

Question : Qu’observez-vous sur l’utilisation du processeur et l’utilisation réseau de la victime ? Pour renforcer l’attaque, vous pouvez lancer la même attaque depuis le serveur 1 cette fois, dont vous avez pu obtenir l’accès grace à l’introduction.

Question : Qu’observez-vous cette fois ? Que pouvez-vous dire sur la capacité d’une telle attaque ?

Remarque : Le client Windows devrait de nouveau répondre lorsque vous cessez l’attaque (Crtl+C). Si ce n’est pas le cas, vous pouvez redémarrer la machine virtuelle.

Partie 3 : Vulnérabilités Client

3.1) Client Macros Office

Machines nécessaires : hacker - server1 – client

Suivre le diapo Macros.pdf.

Dans cet exercice, vous allez mettre en evidence une faille de sécurité que constituent l’inclusion de macros dans un document .odt.

3.2) Android Repackaging Attack

Machines nécessaire : android

Suivre le diapo Android.pdf.

Réinitialisation de la plate-forme :

Avant de partir, merci de réinitialiser la plate-forme en exécutant le script reinit.sh dans le home du root :

```
#>sh reinit.sh
```

Ressources

- Les guides et recommandations de l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information) : https://www.ssi.gouv.fr/