Séance 2
Une première attaque : Attaque MITM d'un service SSH

Objectifs de la séance

- Découverte de concepts de sécurité basiques
- Mise en oeuvre d'un protocole de transmission de données sécurisé
- Compréhension et mise en oeuvre d'un premier type d'attaque : Man-in-the-Middle

Email pour le rapport : romain.dulout@u-bordeaux.fr

A. Un Besoin Importante en Sécurité

L'apparition des premiers Unix et systèmes d'information communicants s'est accompagnée de l'émergence de piles protocolaires visant l'échange de données entre machines comme FTP (File Transfer Protocol), TELNET (TELetype NETwork) ou encore RSH (Remote SHell).

Q1 : RSH et TELNET ont-ils un objectif commun ? Si oui, quel est-il ?

Bien qu'encore largement utilisés aujourd'hui, ces protocoles n'ont pas été conçus pour être sécurisés ; leurs fonctionnalités sont particulièrement pauvres lorsqu'il s'agit d'authentifier la source ou l'émetteur, ou encore de garantir l'intégrité et la confidentialité des flux.

Q2 : A quoi correspondent les termes de chiffrement, intégrité, non répudiation et disponibilité des données ? Parmi ces différentes fonctions, pour lesquelles l'authentification est-elle utile ?

Leur usage est même devenu problématique d'un point de vue filtrage. FTP nécessite par exemple une ouverture dynamique de port sur une passerelle utilisant du NAT. Pour ces raisons, le besoin d'un protocole applicatif sécurisé capable de remplacer ces briques logicielles s'est fait rapidement sentir : SSH est né.

Q3 : Que permet de faire SSH par rapport à ces précédentes solutions ? Est-ce que cette solution est aujourd'hui toujours d'actualité ? Quelles sont ses potentielles limites ?

(Source possible : https://locall.host/is-ssh-deprecated/)

B. OpenSSH

OpenSSH (OpenBSD Secure Shell) est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH. Créé comme alternative Open Source à la suite logicielle proposée par la société SSH Communications Security, OpenSSH est développé depuis 1999 par l'équipe d'OpenBSD, dirigée par son fondateur, Theo de Raadt, et diffusé sous licence BSD.

OpenSSH est à la fois une brique logicielle du système OpenBSD et l'implémentation SSH la plus utilisée sur les systèmes BSD et GNU/Linux. OpenSSH utilise la cryptographie comme mécanisme d'authentification. Contrairement à TLS, le modèle de sécurité de ce service n'utilise pas par défaut une infrastructure à clés publiques mais la méthode Trust on the first use (Vu plus tard dans cette séance).

OpenSSH couvre les mécanismes suivants :

- le chiffrement ;
- l'authentification ;
- l'intégrité des données transmise.

Le fonctionnement d'OpenSSH s'appuie sur un chiffrement asymétrique (authentification) ainsi qu'un chiffrement symétrique (chiffrement des données).

Q4. Différentes questions à ce sujet :

- **Quel est l'intérêt du chiffrement ?**
- **Quelle différence entre un chiffrement symétrique et asymétrique ?**
- **Quelle est la solution la plus légère ? Si je dois réaliser un transfert volumineux, est-il préférable d'utiliser un chiffrement symétrique ou un chiffrement asymétrique ?**
- **Dans le cas du SSH, à quelle fin est utilisé le chiffrement asymétrique ? Et le chiffrement symétrique ?**

(Source potentielle : https://www.lebigdata.fr/ssh-tout-savoir
Autre Source utile : Le point 4 de la Ressource située dans le même dossier)

C. Première utilisation d'OpenSSH

Depuis le client, connectez-vous au serveur SSH à l'aide de la commande ssh à taper dans un émulateur de terminal. Un message proche de celui présenté ci-dessous apparaît :

```
etusio@clissh:~$ ssh etusio@srvssh.local.sio.fr
The authenticity of host 'srvssh.local.sio.fr (192.168.56.10)' can't be established.
ECDSA key fingerprint is SHA256:lPIxEKxsYHPP3i7iMiZZXLYUoW9viLwSfF39MNoWM4.
Are you sure you want to continue connecting (yes/no)?
```

Q5. Que signifie cette alerte qui est affichée à l'écran ?

- **Devez-vous continuer l'opération ? Pourquoi ?**
- **Lors d'une prochaine connexion depuis le même client sur ce serveur, ce message apparaîtra-t-il à nouveau ? Pourquoi ?**

(Source potentielle : Le point 1 de la Ressource située dans le même dossier)

Q6. Sur la machine virtuelle cliente, expliquez à quoi sert le fichier /home/etusio/.ssh/known_hosts.
(Source potentielle : Le point 2 de la Ressource située dans le même dossier)

À ce stade du TP, supprimez le contenu du fichier known_hosts (**attention, ne pas supprimer le fichier**).

```
etusio@clissh:~$ echo > ~/.ssh/known_hosts
```

D. Découverte des hôtes et services présents sur un réseau local

Nous allons maintenant nous connecter à l'attaquant présent sur le réseau (KaliAttaquant1).

Q7. Qu'est ce que Kali Linux ? Qu'est ce que permet de faire cette distribution ?

En tant qu'attaquant, la première étape consiste à recueillir des informations sur le réseau dans lequel nous nous trouvons. Pour ce faire, nous allons utiliser l'outil nmap.

Q8. Que permet de faire cet outil ?

Entrez la commande ci-dessous :

```
etusio@kali:~$ nmap -sP 192.168.56.0/24
```

Puis cette seconde commande :

```
etusio@kali:~$ nmap -sV 192.168.56.10
etusio@kali:~$ nmap -sV 192.168.56.11
etusio@kali:~$ nmap -sV 192.168.56.254
```

Q9. Que permettent de faire chacune des commandes ci-dessus ? Quels semblent être les services et les ports ouverts sur le réseau ? Listez les pour chacun des hôtes du réseau.

L'analyse des résultats permet à l'attaquant de cibler plus particulièrement le serveur SSH.

E. Simulation d'une attaque de l'homme du milieu entre votre client et votre serveur SSH

Une personne malveillante s'est introduite sur votre réseau dans le but de récupérer entre autres des informations confidentielles dont des noms d'utilisateurs et mots de passe disposant de privilèges sur le réseau.

Après avoir analysé l'architecture réseau et découvert l'existence d'un serveur SSH, elle décide de réaliser une attaque Man-in-the-Middle (MitM) afin d'obtenir un accès sur ce dernier.

Q10. Expliquez les principes généraux d'une attaque de l'homme du milieu. Expliquez à quoi elle pourrait spécifiquement correspondre dans le contexte SSH.

(Source potentielle : Le point 3 de La Ressource située dans le même dossier)

Dans un premier temps, sur le client et le serveur SSH, analysez les caches ARP respectifs des deux machines à l'aide de la commande suivante (pour avoir des informations dans le cache arp, vous devrez peut-être au préalable lancer un ping sur chaque machine présente dans le réseau ou relancer la commande « nmap ») :

```
etusio@clissh:~$ ip neigh show
etusio@srvssh:~$ ip neigh show
```

Q11. Notez les associations adresse IP / adresse MAC présentes sur les deux machines.

Nous allons maintenant tenter de simuler une première attaque. Pour ce faire, sur l'attaquant, il va nous être nécessaire d'installer un nouvel outil : ssh-mitm.

Vous pourrez procéder à cette installation à l'aide de la commande suivante :
git clone https://github.com/ktux/ssh-mitm

Vous allez maintenant pouvoir lancer l'installation.

```
etusio@kali:~$ cd ssh-mitm/
etusio@kali:~/ssh-mitm$ export LANG=en_US.utf-8
etusio@kali:~/ssh-mitm$ sudo ./install.sh
```

Note : La commande « export LANG=en_US.utf-8 » sert à exporter, via une variable d'environnement, la langue par défaut utilisée au moment de l'installation de l'outil (anglais avec un encodage UTF-8). Sans cet export, un message d'erreur empêche l'installation.

Lors de cette installation, il vous est proposé d'installer AppArmor pour restreindre les droits de ssh-mitm. Acceptez la proposition.

Vous allez maintenant pouvoir lancer ssh-mitm :

```
etusio@kali:~/ssh-mitm$ sudo ./start.sh
```

L'attaquant sera ainsi positionné entre le client et le serveur SSH. Il se fera passer pour le serveur légitime auprès du client, il recevra et journalisera toutes les informations transmises par le client avant de les transmettre au serveur légitime

La machine attaquante doit donc être en mesure de router les paquets le temps de l'attaque. Ainsi le script start.sh exécute la commande suivante automatiquement afin d'activer le routage (sysctl -w net.ipv4.ip_forward=1).

Q12. Pourquoi l'activation du routage sur la machine de l'attaquant est indispensable au bon fonctionnement de l'attaque MITM ?

Puis le script réalise à l'aide de NETFILTER/IPTABLES une redirection de ports afin de rediriger tous les flux à destination de la machine attaquante sur le port 22/TCP vers le port 2222 du système Kali Linux (iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2222).

Notez qu'il est possible d'observer quel service écoute sur le port 2222 en localhost à l'aide de la commande (etusio@kali:~$ ss -ltnp). Il est également possible d'observer quelles sont les règles de filtrage et de NAT en cours d'utilisation sur la distribution Kali Linux (sudo iptables -L).

F. Mise en place d'une attaque ARP Spoofing afin d'obliger le client et le serveur SSH à faire transiter les trames Ethernet échangées par l'attaquant.

Q13. Indiquez en quoi une attaque de type ARP Spoofing peut être utile ici à l'attaquant ?

(Source potentielle : Le point 3 de la Ressource située dans le même dossier)

Réalisez cette attaque sur la machine Kali Linux à l'aide de la commande ettercap :

sudo ettercap -i eth0 -T -M arp /IP_SERV// /IP_CLI//

- -T : lance ettercap en mode texte ;
- -M : indique que l'on veut une attaque de type "Man in the middle" ;
- IP_* les adresses IP des victimes. Notes : les / et // doivent être utilisés dans la commande.

À nouveau sur le client puis le serveur SSH, analysez le cache ARP respectif des deux machines à l'aide de la commande :

```
etusio@clissh:~$ ip neigh show
etusio@srvssh:~$ ip neigh show
```

Q14. Comparez les caches ARP du client et du serveur avec les associations notées précédemment (au niveau de la question 9). Qu'en concluez-vous ?

Sur la machine cliente et sur Kali Linux, exécutez le logiciel de capture de trame Wireshark et réalisez une capture de trames d'une vingtaine de secondes et enregistrez-les (ou visualisez les juste en temps réel). Analyser plus particulièrement les trames ARP émises et reçues.

Pour lancer Wireshark sur le client, cliquer sur Applications>Internet>Wireshark puis sélectionner l'interface Ethernet qui se nomme enp0s3 (contrairement à la machine Kali Linux qui utilise une carte Ethernet nommée eth0).

Q15. À partir de ces différentes observations, expliquez en détails comment fonctionne une attaque ARP Spoofing.

Envoyez une requête ping (icmp-écho) depuis le client vers le serveur (192.168.56.10). Puis vérifiez à l'aide d'une capture de trame sur la machine Kali Linux que ces dernières passent effectivement bien par l'attaquant.

Q16. Quels éléments démontrent que l'attaque se déroule correctement ?

G. Mise en œuvre et exploitation de l'attaque Man-in-the-Middle

Depuis le poste client, reconnectez-vous sur le serveur avec le protocole SSH.

```
etusio@clissh:~$ ssh etusio@srvssh.local.sio.fr
The authenticity of host 'srvssh.local.sio.fr (192.168.56.10)' can't be established.
ED25519 key fingerprint is SHA256:ehuFqeaDT90nXN8dY1a6HYuOoDouws5z693TOfU1dXs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.10' (ED25519) to the list of known hosts.
```

Une fois sur le serveur SSH, tapez les commandes suivantes :

```
etusio@srvssh:~$ sudo cat /etc/shadow
etusio@srvssh:~$ sudo iptables -L
```

Sur le poste de l'attaquant (Kali), il est maintenant possible d'arrêter l'attaque ARP Spoofing, tapez la touche Q pour arrêter. Puis arrêter le service ssh-mitm :

```
etusio@kali:~/ssh-mitm$ sudo ./stop.sh
```

Récupérez le login et le mot de passe tapés par la victime de l'attaque :

Q17. Que contient le fichier *~~/home/ssh-mitm/shell_session_0.txt~~* présent sur Kali Linux ? Que contient le fichier *~~/var/log/auth.log~~* ?

Note : L'accès à ces fichiers nécessite l'utilisation de la commande sudo.

Sur le poste de la victime, videz le cache ARP puis tentez de vous reconnecter à nouveau sur le serveur SSH :

- sudo ip neigh flush all
- ssh etusio@srvssh.local.sio.fr

Un message d'erreur devrait apparaître.

Q18. Expliquez pourquoi ce message d'erreur apparaît ? Proposez une solution afin de pouvoir à nouveau se connecter au service SSH depuis le client.