P. Lafourcade, C. Olivier-Anclin, M. Puys

TP4 Forensic et Securité Mobile

Rappel : `proxycl.iut.uca.fr` (192.168.128.139), port 8080

Avant de commencer. Tous les exercises se feront directement sur **vdn**, sur le réseau **secure**. Pour y accéder, entrer la ligne de commande suivante dans votre home sur la machine ! Si une erreur survient, vérifier tout de même sur vdn si le réseau `secure` est disponible. Pour rappel, le réseau `secure` est disponible à `Network > Open > secure`.

```
rm -f ~/.vdnrc && vdn-set-network-dir ~vdn/vdn/networks/secure
```

Exercise 1 (Analyse d'une trace réseau post-mortem (4 points))
Une attaque informatique a touché le serveur principal de l'entreprise. Les dossiers de l'entreprise ne peuvent plus être consultés ! Heureusement, il semble que seul le serveur de fichiers ait subi des dommages. Un problème de routage a entraîné la conservation des logs réseaux. En effet, l'administrateur réseau a oublié de les désactiver car il était débordé par d'autres problèmes. L'administrateur du système avait placardé des affiches sur les murs de l'entreprise indiquant qu'il fallait débrancher les câbles en cas de cyberattaque. Après avoir remarqué des problèmes sur le réseau, un collaborateur les a déconnectés, ce qui an entraîné la déconnexion du serveur de fichiers! À l'aide de ces logs réseaux et de Wireshark, trouvez la source de l'attaque.

Téléchargez la trace PCAP et le fichier de logs suivants, puis répondez aux questions :

`https://sancy.iut.uca.fr/~lafourcade/SECWEB/data/log.pcap`
`https://sancy.iut.uca.fr/~lafourcade/SECWEB/data/arp.txt`

1. Quelle est l'adresse du serveur attaqué ?
2. Que s'est-il passé dans l'attaque ?
3. Quel est le dispositif source de l'attaque ?
4. Quels sont les identifiants permettant de se connecter au site ? Donnez le dernier login et password pour nous convaincre.
5. Quelle est la page web servant à l'authentication des utilisateurs sur le site ?

Exercise 2 (Analyse de logs (5 points))
Un service web est disponible sur le serveur central de l'entreprise après analyse du réseau. Il y a quelques années, les prestataires de services ont mis en place un ERP. Bien qu'il n'ait pas été mis à jour depuis, le directeur ne vous l'avait pas mentionné car il le considérait comme intouchable. Il semble pourtant qu'il ait été compromis, découvrez comment !

Téléchargez le logs de l'attaque suivant et ouvrez la avec votre éditeur de texte favoris :
`https://sancy.iut.uca.fr/~lafourcade/SECWEB/data/dolibarr_access.txt`

1. A quelle heure commence l'attaque bruteforce précédente ?
2. Une fois authentifié l'attaquant à cherché une vulnérabilité sur une page php du serveur cloud de l'entreprise victime. Pour cela il essaie plusieurs extensions jusqu'à en trouver une vulnérable. Quelles extensions a-t-il testé ?
3. Quelle est l'extension qu'il utilise par la suite de l'attaque ?

4. Dans la suite de l'attaque (lignes 1340-1343), l'attaquant se sert du fichier php vulnérable pour exécuter des commandes shell sur le serveur. Que fait-il ?

Exercise 3 (Analyse post-mortem d'un système de fichier Android (6 points))
On vient de vous informer que les actions malveillantes que vous venez de découvrir sur le serveur ERP de l'entreprise ont été faite par le téléphone d'une personne de l'équipe RH. Vous devez maintenant comprendre comment l'attaquant a obtenu un accès à son téléphone et déterminer comment l'identifiant ERP de l'utilisateur a fuité. Téléchargez le système de fichier du téléphone de la victime et décompressez l'archive :

`https://sancy.iut.uca.fr/~lafourcade/SECWEB/data/filesystem.tar.gz`

1. Les SMS/MMS sont toujours un bon point de départ pour chercher des informations. Quel est le chemin de la base de données dans lequel sont stockés les SMS, dans quelle table (Sqlite3 est votre ami) ?

2. Regardez le contenu des SMS/MMS de l'utilisateur et recherchez les SMS/MMS mentionnants les identifiants. Indiquez le champ "_id" du ou des messages que vous avez trouvé. Quel jour et à quel heure ont-ils été envoyés ?

3. Retrouvez les identifiants mentionnés par les SMS/MMS. Quel est le chemin du fichier les contenant ? Quel est le mot de passe associé aux RH ?

4. Quelle est le nom de l'application malveillante utilisée par l'attaquant ? A-t-elle des permissions liées à l'attaque ? A quelle date a-t-elle été installée ?

5. Essayons de comprendre comment l'application malveillante est apparue sur le téléphone de la victime. Regardez dans la base de donnée des évenements du calendrier si des rendez-vous avaient lieu à ce moment. Expliquez ce qui s'est passé.

Exercise 4 (Reverse Engineering Android (5 points))
Le but de cet exercise sera de faire une analyse de l'APK fourni, et d'en extraire le plus d'information. Téléchargez le code de l'application malveillante

`https://sancy.iut.uca.fr/~lafourcade/SECWEB/data/base.apk`

Puis installez le logiciel `aapt` avec `apt install aapt`.

Puis lancez la commande `aapt dump permissions` pour obtenir le nom de l'application et ses permissions. Ouvrez ensuite l'APK avec la commande `unzip base.apk`.

1. Regarder les fichiers et déterminer en quel language a été écrite l'application ?

2. Retrouvez les permissions dans l'archive que vous avez décompressée en utilisant `aapt` ou en regardant dans le bon fichier.

3. Trouver le numéro de version de la librairie `androidx:core:core` utilisée dans l'application, en regardant dans le répertoire `META-INF` ?

Votre objectif est maintenant de décompiler le code source de l'application. Pour cela, lancer la commande suivante, en prenant bien soin de l'exécuter à l'emplacement du fichier `classes.dex` !

```
mkdir -p output && chmod 777 output
docker run --rm -u root -v $(pwd):/data cincan/jadx -ds /data/output /data/classes.dex
```

Une fois le programme terminé, il sera désormais possible de lire le code source dans le dossier `output`. Le programme affiche un message d'erreur mais le code est quand même décompilé dans le dossier `output`.

4. Quel est le langage du programme décompilé ? Chercher en ouvrant un des fichiers de votre choix. Expliquer pourquoi le langage du code source généré soit différent ?

5. Dans le dossier `output/com/android/updateserver/server`, trouvé l'adresse du serveur sur lesquels les SMS sont envoyés, en cherchant dans un des fichiers `Java`.

6. Que fait l'autre fichier `Java`, dans ce répertoire?