Malices et espièglerie

Fil d'étincelles n°4

Définitions

Hacker (Petit Robert) Pirate informatique qui agit par jeu, goût du défi, sans intention de nuire. Recommandation officielle de traduction française : *fouineur*.

Pirate informatique (Petit Robert) Qui pirate les logiciels ou s'introduit dans un système informatique par défi pour en tirer profit.

Cryptographie (Petit Robert) Procédé (signes conventionnels, modification de l'ordre, de la disposition des signes, remplacement des signes…) permettant de rendre un message inintelligible, de protéger des données.

À ce propos, on parle plutôt de « chiffrement » et l'on « chiffre un message » plutôt que de « cryptage » et de « crypter un message ». Décrypter correspond plutôt à comprendre le message sans comprendre la façon dont il a été chiffré.

Hachage

On va commencer par s'intéresser à un problème assez général : comment trouver un mot de passe ?

Commencer par une petite précision : les démonstrations que nous allons faire aujourd'hui ne sont surtout pas à reproduire chez soi, car cela peut entraîner de lourdes amendes et des peines de prison. Dans notre cas, les comptes que nous allons utiliser et le site que nous allons pirater sont factices, et ne sont mis en place que pour cette démonstration.

Basculer sur l'affichage HDMI. Ouvrir le terminal, lancer le serveur. Je crée le compte « Johanne » sans qu'elle ne puisse en connaître le mot de passe, le chat non plus. Le défi sera de se connecter à ton compte.

Heureusement, on peut lire directement la base de données. Ouvrir la base de données avec « DB Sqlite Browser ». Présenter rapidement les tables qui la composent, en faisant une analogie avec un tableur Excel. Ouvrir la table « `auth_user` ». On y retrouve notamment l'user `johanne`. On peut essayer de copier-coller le contenu du champ « `password` », mais l'authentification ne fonctionne pas.

La raison, c'est le hachage. En présenter le principe. Montrer quelques exemples de hachage : https://www.tools4noobs.com/online_tools/hash/. Insister sur l'asymétrie de l'opération : on peut facilement hacher des données, mais il est très difficile de retrouver les données à partir du hash. Cette protection est-elle suffisante ?

Regarder les autres utilisateurs dans la base. Ils possèdent le même hash de mot de passe. Ils ont donc le même mot de passe. Et on va pouvoir le deviner : « Michael Jackson », « Fan de film », « Halloween ». On peut essayer par exemple « thriller » et Ô miracle, le mot de passe fonctionne.

Stocker les mots de passe en clair, c'est terrible. Mais les hacher, ce n'est pas suffisant. Voir la vidéo de Tom Scott « How NOT to store passwords » https://www.youtube.com/watch?v=8ZtInClXe1Q.

Là on a directement accès à la base de données. Dans la réalité, on se contente souvent d'une fuite partielle et recopiée. Ce sont ces fuites de données qui se retrouvent en vente sur des forums pas

très nets. Avec le nouveau règlement européen RGPD, les administrateurs des systèmes d'information que nous utilisons sont tenus de nous notifier en cas de fuite de données. Ce n'est pas toujours le cas. On peut vérifier à l'aide de :

- https://haveibeenpwned.com/
- https://monitor.firefox.com/

Attaque par force brute

Si les systèmes sont correctement protégés, on ne peut pas ruser pour deviner un mot de passe depuis ce que l'on connaît de la base de données. La seule option qui reste à l'attaquant c'est l'attaque par force brute, ie. essayer tous les mots de passe jusqu'à que l'un fonctionne. Ce qui va compter, c'est la robustesse du mot de passe.

Une fois Johanne connectée à son compte, lui demander de changer son mot de passe, en lui demandant d'utiliser une date (donc 8 chiffres) **BIEN PRÉCISER DE NE PAS UTILISER UNE DATE QUI LUI EST RELIÉ**. Je ne saurai pas lequel est-ce. En vérifiant dans la base de données, on verra bien que le hash a changé. On ne peut donc pas le deviner, il va falloir brute-force.

Montrer le code source du script qui essaye tous les mots de passe. On essaye tous les mots de passe possible. On le hache. Si les hash correspondent, bingo ! Lancer le script.

```
python manage.py crack johanne 8 0123456789
```

En 2/3 minutes, le mot de passe est trouvé.

Compter le nombre de possibilités : 10x10x10… = 10^8. Diviser par le nombre d'essais à la seconde (on tourne autour des 60k/s, une attaque réelle serait plutôt autour des 1k/s). Estimer le temps qu'il faut pour trouver la solution.

Comparer à un mot de passe aléatoire avec des chiffres minuscules / majuscules, des nombres, etc… Une bonne pratique : le diceware. Présenter le XKCD. https://www.passwordmonster.com/.

Présentation des gestionnaires de mot de passe. Mot de passe avec https://privacycanada.net/strong-password-generator/.

Attention, un bon mot de passe ne protège pas de tout. Utiliser des mots de passe différents fait que si un site fuite, les autres ne sont pas compromis. Attention aussi : si tous les comptes utilisent une même adresse mail, si un attaquant obtient l'accès à la boîte mail, il peut utiliser la procédure « mot de passe oublié » pour tous les comptes reliés !

Écoute d'un réseau

Ouvrir le point d'accès WiFi du Toshiba. Démarrer la tablette, et la connecter au point d'accès. Afficher l'écran de la tablette sur le PC, à l'aide de `srcpy`. Trouver l'adresse IP du serveur, changer l'adresse d'écoute du site. Donner la tablette à Johanne, lui demander de s'y connecter.

En feutré, ouvrir WireShark (`sudo`) et capturer les données.

Demander à Johanne d'écrire quelque chose dans la boîte de la page d'accueil du site, je ne regarde pas ce que c'est. Elle valide. En analysant le réseau, je retrouve ce dont il s'agit.

Montrer ma démarche en affichant WireShark. Montrer tout le flux réseau. Parler de paquet qui s'échangent entre des adresses. Filtrer par adresse IP du destinataire, 10.42.0.1 (donc l'adresse du serveur qui héberge le site).

```
ip.dst==10.42.0.1
```

On voit tout un tas de paquets, en provenance de la même source. On suppose qu'il s'agit de l'adresse IP de la tablette. On peut le vérifier depuis la tablette en allant sur « Paramètres » « Connexions » « Wi-Fi » « Avancé » et c'est écrit en bas. Dans tous ces paquets, il y a une colonne nommée « protocole ». On voit TCP, DNS, HTTP, … Est-ce qu'il y a un paquet en particulier intéressant ? Oui, le http, c'est le même que ce que l'on écrit dans les barres d'adresses. Filtrer les paquets http.

```
ip.dst==10.42.0.1 and http
```

Il ne reste plus que quelques requêtes. Certaines sont « GET » d'autres « POST ». Les requêtes GET sont plutôt utilisées pour lire du contenu. Lorsque c'est l'utilisateur qui envoie des informations au serveur, on a plutôt une requête POST. On regarde la POST. Dedans, il y a le texte écrit par Johanne.

Là j'écoute le réseau car j'en suis le maître (l'ordinateur qui écoute est celui qui propose le point d'accès WiFi. C'est le cas si l'attaquant arrive à avoir un accès direct à un routeur par exemple, ou à un serveur. Mais en réalité, l'attaque qui arrive plutôt est l'attaque de l'homme-du-milieu. (Faire un schéma sur Paint). En utilisant des failles de sécurité, on détourne le traffic classique, on intercepte et on retransmet.

Détournement de session

Sur la tablette, Johanne se connecte à son compte et change son mot de passe. Elle en met un compliqué (mélange de deux mots par exemple). Retrouver les requêtes dans le réseau. On peut y lire le mot de passe en clair, notamment. Mais admettons que le système soit plus sécurisé et que l'on ne puisse pas lire le mot de passe. On peut quand même accéder à la session de Johanne.

Dans la requête il y a un cookie nommé sessionid. Copier sa valeur. Ouvrir Firefox, aller sur le site, se connecter en tant que yohan, et changer le cookie sessionid. Rafraîchir la page : je suis connecté en tant que Johanne. Tada !

Explications sur les cookies.

Chiffrement asymétrique et SSL

Tout ceci est possible parce que notre traffic réseau n'est pas sécurisé. Le site est en effet en http. Donc les paquets http sont en clair, non chiffrés.

C'est à ça que sert le HTTPS : chiffrer les paquets pour qu'on n'en inspecte pas le contenu. Essayer, depuis la tablette, d'aller sur YouTube / et de regarder une vidéo (par exemple, le dernier Fil d'étincelles) / ou trouver une notice de document sur le site de la bibliothèque. Dans la capture, on pourra voir que des requêtes se font à un serveur nommé youtube.com, mais on ne pourra pas trouver de paquet « http » ou « https », que des paquets TLS.

```
frame contains "youtube"
```

```
frame contains "rlv.eu"
```

```
dns
```

Donc on peut avoir une certaine idée du traffic des gens : on voit que la tablette s'est connectée à YouTube, mais on ne sait pas ce qu'elle y a fait. C'est tout le rôle du S dans httpS : c'est pourquoi,

pour éviter que n'importe qui d'autre que la banque puisse connaître nos informations bancaires sur le réseau, il faut veiller à ce qu'il y ait bien le S dans la barre d'adresse.

Pour chiffrer les paquets, on utilise le chiffrement asymétrique.

Voir le « Guide d'autodéfense numérique » : https://guide.boum.org/tomes/2_en_ligne/1_comprendre/6_chiffrement_asymetrique/2_principe_asymetrique/

Le navigateur a une clé publique et une clé privée (faire un schéma sur paint). Le serveur connaît la clé publique du navigateur, chiffre le paquet, et seul un connaisseur de la clé privée peut déchiffrer ce message. Donc, tant qu'on ne connaît pas la clé, on ne peut pas savoir quelle vidéo YouTube a été visionnée.

Éditer > Préférences > Protocoles > TLS > (Pre)-Master-Secret log filename

Recommencer l'expérience en utilisant le raccourci Firefox sur le bureau du PC Toshiba, et en se rendant sur https://reseaubibliotheques.rlv.eu/. Johanne fait une recherche et consulte la notice d'un ouvrage. Là on peut retrouver toutes les informations à propos de la notice (en recherchant un paquet http2 avec le mot « notice »).

Montrer le fichier `/home/atelier/sshkey.log`. C'est dans ce fichier que Firefox enregistre la clé qu'il utilise pour déchiffrer le contenu du serveur.

Capture de drapeau

Si ça vous intéresse, on a plein de ressources documentaires à la médiathèque. En termes de connaissances, il faut connaître le fonctionnement d'un réseau et comment utiliser un terminal. C'est le début. Il existe ensuite de nombreux sites permettant de s'exercer au hacking (virtuellement, il s'agit de machines virtuelles, donc factices, pas de problème juridique). C'est ce qu'on appelle le Capture The Flag (capturer le drapeau). Les participants sont mis dans un environnement (le plus souvent, un ordinateur / smartphone / …) et doivent trouver un mot de passe caché quelque part dedans. En voici quelques exemples :

- https://overthewire.org/wargames/bandit/bandit1.html
- https://www.root-me.org/
- https://www.hackthebox.com/
- https://tryhackme.com/

Sur Twitch, je regarde de temps en temps la chaîne de Khaos Farbauti (https://www.twitch.tv/khaos_farbauti) qui fait ce genre de chose en live. Il y en a d'autres mais je n'ai pas retenu les noms, surtout des petits streamers.

Sur YouTube, il y a beaucoup de contenu anglophone de qualité. Notamment la chaîne YouTube Computerphile https://www.youtube.com/user/Computerphile qui a fait plusieurs vidéos à propos du hacking. Et pour celles et ceux qui aiment la technique, il y a la chaine YouTube de LiveOverflow, qui documente et vlog sa participation à des compétitions de CTF, et qui explique comment il découvre certaines failles à l'intérieur (notamment devenir sudo sur Ubuntu). https://www.youtube.com/c/LiveOverflow.