Security Web
2023/2024

P.Lafourcade, G.Marcadet, M.Puys

TP2 Authentification

Avant de commencer. Un peu de préparation sera nécessaire pour les exercises suivants: Efail, Json Web Token, Brute-force en ligne et Cookie.

1. **Extraction et Installation**: Connectez-vous sur **vdn** sur le réseau `secure` (`Network > Open > secure`), puis téléchargez l'archive suivante:

   ```
   wget http://perso.limos.fr/~gamarcadet/enseignement/websec23/tp2.tar.gz
   ```

   Vous allez l'extraire avec `tar -zxvf tp2.tar.gz`. Aller dans le dossier `websec23-tp2` et lancer la commande suivante:

   ```
   apt-get install python3-venv && python3 -m venv . &&
   source bin/activate && pip3 install -r requirements.txt
   ```

   Il est impératif de lancer la commande en indiquant le bon emplacement du fichier `requirements.txt`. Vérifier que votre prompt sur le terminal commance bien par `(websec23-tp2)`.

2. **Lancement des serveurs**: Dans un *autre terminal*, lancer les serveurs avec la commande suivante, en prenant bien soin de laisser les serveurs tournés:

   ```
   docker load -i websec23-tp2.tar.xz &&
   docker run --rm -p 5001:5001 -p 5002:5002 -p 5003:5003 websec23-tp2
   ```

Exercise 1 (Brute-force locale (3 points))
Récupérer sur ce site phpbb[1] la base de donées utilisateurs (à extraire avec `bunzip2 phpbb.txt.bz2`). Vous y trouvez aussi de nombreuses bases de données de mots de passe qui ont fuité ces dernières années :

1. (1 point) `$1$AAAA$H9wXcd/WaaomJUgWKFspy.` est un mot de passe hashé et salé, retrouver l'agorithme de hachage utilisé, identifier le sel (`rtfm openssl`[2]). Avec `openssl` et la commande `passwd` vérifier que le mot de passe est `!!1331xxx`

2. (2 points) Quel sont les mots de passe associés à `$1$BABA$DOzBWHNx08SgVSX/YuYvC/` et à `$1$CACA$XLWo4OqFFCYICqYrZ0y5i/` à partir de `phpbb`.

   Vérifier avec `openssl dgst -md5 toto.txt` que vos calculs sont corrects.

Exercise 2 (Json Web Token (2 points))
Un Json Web Token (JWT) est un token d'authentification qui permet de prouver son identité. Il se décompose en trois parties: La première contient les informations de génération du token, la seconde le contenu du token en lui-même (ID du token, durée de validité, etc), et la troisième qui constitue la signature du token, qui est en fait un MAC.

1. Aller sur le site `https://jwt.io` pour construire un token JWT. Vous aurez besoin de choisir un mot de passe de votre choix (disons, un prénom de **trois ou quatres** caractères) à entrer dans "la clé secrète", dans la partie à droite en bas. Attention à bien l'indiquer dans l'emplacement de l'entrée de la clé secrète.

[1] À une de ces deux adresses: `https://wiki.skullsecurity.org/index.php?title=Passwords` ou `https://sancy.iut.uca.fr/~lafourcade/phpbb.txt.bz2`

[2] `openssl passwd -1 -salt BBBB 'Toto'`

2. Aller dans le dossier `jwtcracker`, puis trouver l'outil `jwtcrack` (compiler-le si besoin avec `apt update && apt install openssl libssl-dev && make`) pour brute-forcer le token en faisant `./jwtcrack <token>`.

3. Retrouver le mot de passe utiliser pour forger le token dans le fichier `token.txt` (Cela prendra **au plus** 1 minute).

Exercise 3 (EFAIL (3 points))
Aller dans le dossier `efail`. Votre objectif sera de modifier le mail chiffré (`mail.txt`), et de l'envoyer sur le serveur SMTP (`http://localhost:5003`) pour en révéler son contenu. Durant cet exercice, **seul** le fichier `efail_exercice.py` devra être modifié, aucune autre modification n'est nécessaire. L'objectif est de compléter le fichier `efail_exercice.py` pour monter l'attaque EFAIL vue en cours.

1. Installer les dépendances nécessaires avec `pip3 install -r requirements.txt` si ce n'est pas déjà la cas.

2. Consulter vos mails en allant sur la page `http://127.0.0.1:5003`.

3. C'est à cette étape que votre travail commence. Le mail que dont vous souhaitez voir le contenu se trouve dans `mail.txt`. Dans cet exercice, vous n'allez modifier seulement le fichier `efail_exercice.py`, qui contient la fonction

   `def efail( iv, ciphertext, known_plaintext , begin_replace, end_replace )` où `iv` est le vecteur d'initialisation, `ciphertext` est le chiffré, `known_plaintext` est le texte clair connu, tandis que `begin_replace` et `end_replace` sont respectivement le message à remplacer au début et à la fin du message.

   La fonction doit retourner un couple `(iv', ct')` où `iv'` sera le nouveau vecteur d'initialisation et `ct'` le nouveau chiffré. La fonction est partiellement codée, il ne vous faudra que remplacer les parties entre chevrons (`< .. >`).

   Pour vous éviter de prendre du temps, nous vous fournissons `efail.py`, qui se chargera de lire le fichier `mail.txt`, de parser le chiffré, et d'appeler la fonction `efail` définie plus haut avec les bons paramètres. Pour exécuter le fichier `efail.py`, entrer la commande `python3 efail.py --mail mail.txt` Si votre fonction retourne le nécessaire, `efail.py` se chargera alors de générer le nouveau mail et de l'envoie au serveur SMTP. Le message sera alors visible dans les logs du serveur. Le voyez-vous ?

Exercise 4 (Brute-force en ligne (3 points))
Aller dans le dossier `callow`, puis aller sur la page `http://localhost:5001/login` sur votre navigateur.

1. Installer les dépendances nécessaires avec la commande

   `python3 -m pip install -r requirements.txt`

2. Monter une attaque sur `http://localhost:5001/login` permettant de retrouver le mot de passe par force-brute de l'utilisateur `admin`, en utilisant le fichier `callow.py` disponible dans le dossier `callow`. Le script propose une aide, accessible via `python3 callow.py -h`

Exercise 5 (L'attaque au président (6 points))
Bienvenue dans l'entreprise **Crypto**, en tant que secrétaire. Le président est actuellement en déplacement. Dans cet exercice, vous jouerez en alternance le rôle de la secrétaire et du président, en ajoutant et retirant les clés. Le rôle que vous devrez incarner est présenté entre paranthèse au début de la question. Téléchargez l'archive à l'adresse suivante:

`http://perso.limos.fr/~gamarcadet/enseignement/gpg-president.tar.gz`

Attention ! L'outil que l'on va utiliser, `gpg`, est capable d'enregistrer plusieurs clés en même temps. Lorsque un rôle est spécifié, *seule la clé secrète associée à ce rôle* devra être présent. La

clé secrète du président se trouve dans le fichier `keys/president.prv`, tandis que sa clé publique se trouve dans le fichier `keys/president.pub`. La clé secrète de la secrétaire se trouve dans le fichier `keys/secretary.prv` tandis que la clé publique est dans `keys/secretary.pub`. La clé secrète du président est protégée par le mot de passe `president`, et la clé secrète de la secrétaire par `secretary`.

1. Ajouter la clé secrète de la secrétaire.
2. (Secrétaire) Vous recevez un message chiffré de le part du président, situé dans le dossier `q1/message1.txt.gpg`. Découvrer le contenu du message.
3. Ajouter la clé publique de la présidente.
4. (Secrétaire) Quel drôle de message ! Assurez-vous qu'il ne s'agisse pas d'une erreur, en chiffrant *et* signant le message `q2/message2.txt`.
5. Retirer la clé secrète de la secrétaire et ajouter la clé secrète du président.
6. (Président) Rien ne va pas plus, contacter immédiatement la secrétaire pour lui indiquer qu'il s'agit d'une erreur, et même d'une arnaque ! Pour cela, signez le message `q3/message3.txt`. Puisque le message ne contient pas d'information sensible, il sera inutile de le chiffrer.
7. Retirer de nouveau la clé secrète du président et ajouter la clé secrète de la secrétaire.
8. (Secrétaire) Vérifier le message que vous venez de signer.
9. Par une source anonyme, nous sommes parvenu à trouver une clé publique située dans `keys/.attacker.pub`. Par chance, le message demandé le versement de façon scrupuleuse a été signée par l'attaquant ! Avant toute chose, il convient de s'assurer qu'il s'agisse de la bonne clé. Commencer par ajouter la clé publique dans `gpg`.
10. Vérifier ensuite la signature qui se trouve dans `q4/signature.txt.sig`.
11. Quel heureux hasard, la clé publique contient beaucoup d'information ! Donnez l'adresse email, et son visage.

Pour vous aider, nous vous fournissons les commandes `gpg` essentielles:

- `gpg --list-keys`: Liste l'ensemble des clés publiques enregistrées.
- `gpg --list-secret-keys`: Liste l'ensemble des clés secrètes enregistrées.
- `gpg --import <key>`: Permet d'importer une clé (publique ou secrète) dans gpg.
- `gpg --encrypt -r alice message.txt`: Chiffre le contenu du fichier `message.txt` en utilisant la clé publique de chiffrement d'Alice. Produit le fichier `message.txt.gpg`.
- `gpg -r bob --sign --encrypt message.txt`: Chiffre et signe le contenu du message `message.txt`, en utilisant la clé de signature locale et la clé de chiffrement de bob.
- `gpg --sign message.txt`: Signe le contenu du message `message.txt`, en utilisant la clé de signature locale. Produit le fichier `message.txt.gpg`.
- `gpg --detach-sign message.txt`: Comme avant, mais la signature est déportée dans un autre fichier. Produit le fichier `message.txt.sig`.
- `gpg --verify message.txt.gpg`: Vérifie si la signature auprès de toutes les clés publiques enregistrées dans `gpg`. Si aucune clé ne correpond, la signature est considérée comme invalide. La commande ne fait que vérifier le message, pas l'afficher.

- `gpg --verify message.txt.sig message.txt`: Vérifie si la signature auprès de toutes les clés publiques enregistrées dans `gpg`. Si aucune clé ne correpond, la signature est considérée comme invalide. La commande ne fait que vérifier si la signature est valide, pas afficher le message.
- `gpg -o output.txt --decrypt message.txt.gpg`: Déchiffre et/ou vérifie la signature d'un message `message.txt.gpg` et produit le claire dans le fichier `output.txt`.
- `gpg --list-options show-photos --fingerprint keyID`: Affiche la photo associée à la clé publique, s'il y en a. Le paramètre `keyID` correspond à l'identifiant de la clé et doit être récupéré via l'option `--list-keys`.

Exercise 6 (Sécurité des mots de passe (2 points))

1. Combien y a t'il de mots de passe différents ayant exactement 8 caractères, sachant que seuls les caractères autorisés sont alphanumériques, `-` et `_` ? Expliquez votre calcul et donnez le résultat sous la forme d'une puissance de 2.
2. Combien y a-t-il de mots de passe de 8 caractères, en supposant que les 128 caractères ASCII peuvent être utilisés ? Expliquez votre calcul et donnez le résultat sous forme de puissance de 2.
3. Supposons qu'il nécessite 1 jour pour effectuer une attaque par force brute sur un mot de passe de la question 1. Combien de jours avons-nous besoin pour effectuer une attaque par force brute sur un mot de passe de la question 2 ?
4. En supposant que le processus d'authentification n'utilise pas de sel pour calculer le hachage du mot de passe, quelle méthode peut être conseillée pour casser les mots de passe plus efficacement que l'attaque par force brute ?

Exercise 7 (Adobe (2 points))

Retrouver dans cette liste d'utilisateurs l'**unique** mot de passe en vous appuyant sur les indices. Confirmer que vous possédez bien le bon mot de passe en calculant par vous-même le hash (via `MD5`) et le comparer avec ceux présents dans le tableau.

Nom d'utilisateur	Indice	Hash
Inès	Viande populaire	e6a0ec03e2438e4b0d269f90a2d43e8b
Clara	Londres	c3e3b26d5591c7fcc326a7d399d734bb
Adam	Détective	c3e3b26d5591c7fcc326a7d399d734bb
Enzo	Sentiment positif	a4731d662cca04cc4e5e0de00714a50c
Hugo	Phénomène météorologique	2d304896fb01357a2dc75ae066138ca9
Emma	Destination de vacances	d366780b44fb6a9382339429a614826b
Léa	Film de science-fiction	69fa47f2852aa102fe7a075e3f403a47
Gabriel	Animal domestique	55dcdf017b51fc96f7b5f9d63013b95d
Lucas	Watson	c3e3b26d5591c7fcc326a7d399d734bb
Sarah	Plateforme de streaming en direct	6a057ee64a34177e388abe7304fd3d78
Jules	Instrument de musique à cordes frottées	57a49eff49945af8a9c320b91180cd57
Chloé	Explorateur de l'espace	3725aaff1c293d536aed26604d874f45
Léo	J'aime les énigmes	c3e3b26d5591c7fcc326a7d399d734bb
Manon	221b	c3e3b26d5591c7fcc326a7d399d734bb
Camille	Appareil électronique	853ca16bda4f3d303e70e48db81c17c6

Remarque

Les exercices suivants traiterons des sujets différents et utiliserons des outils variés. Nous vous recommandons de faire un dossier par exercice pour mieux vous organiser.

Exercise 8 (Cookie (1 point))
Aller sur la page `http://localhost:5002` puis passer administrateur. Aucune dépendances n'est nécessaire ici, tout se fait via le navigateur !