Université FERHAT ABBAS SETIF I
Faculté des sciences
Département d'informatique
Sécurité des Applications Web
1ère année Master GL, IDTW

TP n°4

Objectif

L'objectif de ce TP est :

- de compléter le TP n°3 en menant d'autres types d'attaques sur l'application web DVWA
- d'utiliser **Burp Suite** et **netcat** qui sont des outils très utilisé dans le monde des tests de pénétration ainsi que quelques scripts PHP permettant d'ouvrir des accès dérobés au serveur pour y exécuter des commandes.

Outils utilisés

Les outils que nous utiliserons dans ce TP sont :

- la machine virtuelle Kali Linux qui servira de **client et/ou de serveur web pour l'attaquant (hackeur)**
- la machine virtuelle Metasploitable2 disposant de l'application web Damn Vulnerable Web Application (DVWA) qui servira de **serveur cible**
- la machine hôte (physique) qui servira de **client cible**

Burp Suite

Burp Suite est un outil permettant entre autres choses de réaliser des tests de pénétration sur des applications web en offrant un grand nombre d'outils. La version **Community Edition** de Burp Suite qui est installée sur Kali Linux n'offre pas toutes les fonctionnalités des version Entreprise et Professional. Nous utiliserons l'outil **proxy** de Burp Suite.

Pour rappel, un proxy est un serveur intermédiaire entre deux machines. Dans notre cas, chaque requête émise par le navigateur du client sera destinée au proxy qui la retransmettra vers le serveur web destinataire. Chaque réponse du serveur passera également par le proxy qui la transmettra ensuite au navigateur.

Burp Suite permet d'**intercepter** les **requêtes HTTP** et les **réponses** avant leur retransmission et éventuellement de les **modifier "à la volée"** avant qu'elles ne soient acheminées vers le destinataire.

1. Lancer la machine virtuelle Metasploitable2 et récupérer son adresse IP.
2. Lancer la machine Kali linux et récupérer son adresse IP.
3. Lancer le navigateur de la machine hôte et se connecter à l'application DVWA avec le compte **admin** (admin/password).

   Cross Site Request Forgery (CSRF)

4. Positionner le niveau de sécurité à **low**.
5. Cliquer sur l'item de menu **CSRF**.
6. La page affichée permet de changer le mot de passe de l'utilisateur courant.

7. Afficher le code source pour visualiser les informations sur le formulaire de demande de modification de mot de passe (script action, méthode d'envoi, noms des paramètres).

8. Construire (sur une feuille) l'URL de la requête permettant de changer le mot de passe de l'utilisateur en **1234**.

9. Cliquer sur l'item de menu **XSS stored** et ajouter un commentaire contenant une redirection vers l'URL construite à la question précédente.

10. Le mot de passe de l'utilisateur admin a été modifié en **1234**.

11. Remettre le mot de passe de l'utilisateur admin à **password**.

12. Se déconnecter de l'application DVWA et s'y reconnecter sous le compte **smithy** (smithy/password).

13. Positionner le niveau de sécurité à **low**.

14. Cliquer sur l'item de menu **XSS stored**.

15. Vérifier que le mot de passe de **smithy** a été changé en 1234.

16. Remettre le mot de passe de **smithy** à sa valeur initiale **password**.

17. Se reconnecter à l'application DVWA en tant que **admin**.

18. Réinitialiser la base de données de l'application DVWA.

Téléversement (upload) de fichier

19. Lancer le navigateur FireFox sur Kali Linux.

20. Se connecter à l'application DVWA avec le compte admin.

21. Positionner le niveau de sécurité à **low**.

22. Cliquer sur l'item de menu **Upload**.

23. Afficher le script de traitement en appuyant sur le bouton **view source**.

24. Dans quel répertoire sont stockés les fichiers téléversés.

25. Cliquer sur le bouton **Browse** et téléverser le fichier **/usr/share/webshells/php/php-backdoor.php**

26. Aller à l'URL :

http://[ADRESSE IP KALI LINUX]/dvwa/hackable/uploads/php-backdoor.php

27. Que permet de faire cette backdoor ?

28. Positionner le niveau de sécurité à **medium**.

29. Cliquer sur l'item de menu **Upload**.

30. Afficher le script de traitement en appuyant sur le bouton **view source**.

31. Quels fichiers téléversés sont acceptés par ce script ?

32. Utiliser Burp Suite pour intercepter les requêtes HTTP et changer "à la volée" le type de fichier téléversé.

33. Sur Kali Linux, ouvrir le fichier **/usr/share/webshells/php/php-reverse-shell.php**, modifier la ligne $ip = "127.0.0.1" en remplaçant 127.0.0.1 par l'adresse IP de Kali Linux.

34. Téléverser le fichier **/usr/share/webshells/php/php-reverse-shell.php**

35. Sur Kali Linux, ouvrir un terminal et utiliser l'utilitaire réseau **netcat** pour se mettre à l'écoute sur un port (TCP **1234**), puis une fois qu'un client s'y connecte, d'échanger des données au format texte avec ce client. La commande à taper est la suivante :

    nc -l -v -p 1234

36. Aller à l'URL :

    http://[ADRESSE IP KALI LINUX]/dvwa/hackable/uploads/php-reverse-shell.php

37. Le script PHP s'est connecté au serveur créé par **netcat** et permet d'exécuter des commandes envoyées par **netcat** sur le serveur distant.

38. Pourquoi appelle-t-on ce script un **reverse** shell (pas un shell) ?

39. Positionner le niveau de sécurité sur **high**.

40. Afficher le script de traitement en appuyant sur le bouton **view source**.

41. Quels fichiers téléversés sont acceptés par ce script ?

    Vol de cookies (et de sessions)

42. Sur Kali Linux, lancer les serveurs Apache et MySQL (ou plutôt MariaDB) grâce aux commandes :

    sudo service apache2 start

    sudo service mysql start

43. Créer une base de données **tp4** contenant une table **cookie** qui servira de stocker les cookies volés **(voir vidéo dédiée)**.

44. Créer un script PHP permettant de stocker une chaine de caractères reçue en paramètre (cookie volé) dans la table **cookie** de la base de données **tp4 (voir vidéo dédiée)**.

45. Créer un script permettant à l'attaquant de visualiser les cookies stockés dans la table **cookie** de la base de données **tp4(voir vidéo dédiée)**.

46. Lancer le navigateur sur la machine Kali Linux.

47. Se connecter à DVWA avec le compte **admin**.

48. Ajouter un commentaire redirigeant l'utilisateur vers le script de vols de cookies et avec comme paramètre les cookies obtenus sur l'application DVWA.

49. Lancer le navigateur sur la machine hôte.

50. Se connecter à DVWA avec le compte **smithy**.

51. Positionner le niveau de sécurité à **low**.

52. Cliquer sur l'item de menu **XSS stored**.

53. Sur Kali Linux, récupérer le cookie de session (**PHPSESSID**) se trouvant dans la base de données **tp4**.

54. Utiliser Burp Suite pour remplacer son cookie de session par la cookie de session volé et prendre l'identité de **smithy**.