Write-up (version en français) machine : Crocodile.

Introduction

La machine Crocodile(ip pour cet exercice : 10.129.22.186) est un excellent exemple de situation où plusieurs failles se rejoignent pour permettre à un attaquant de prendre le contrôle d'un service à distance. Dans ce cas, nous examinerons deux points faibles principaux : d'abord, un accès FTP mal configuré qui autorise les connexions anonymes, et ensuite, une application web vulnérable qui expose son interface d'administration. En combinant ces deux failles, nous verrons comment des données en clair et un contrôle d'accès insuffisant peuvent être exploités pour pénétrer plus profondément dans le système et obtenir un contrôle total. Ce rapport détaillera chaque étape, de la phase de reconnaissance initiale jusqu'à l'élévation des privilèges, en mettant en lumière les vulnérabilités exploitées pour parvenir à nos fins.

Reconnaissance

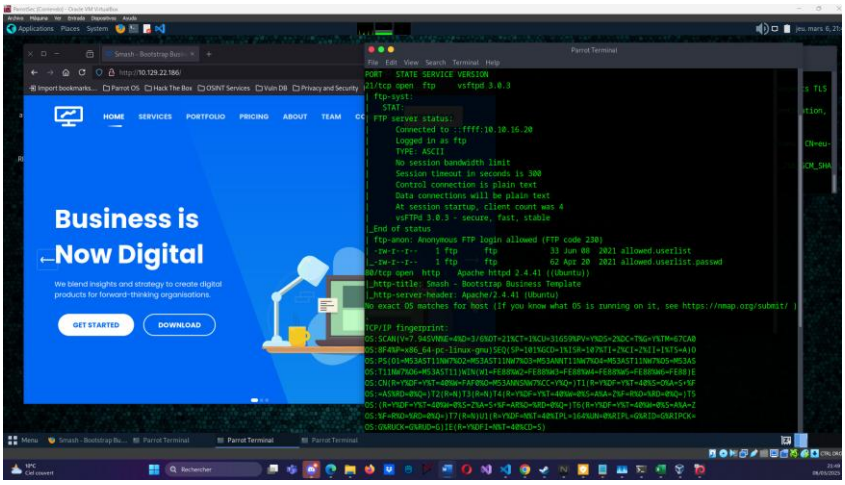
On commence par réaliser un scan avec nmap avec la commande suivante :

```
sudo nmap -sS -sV -A 10.129.22.182
```

On observe deux ports ouverts :

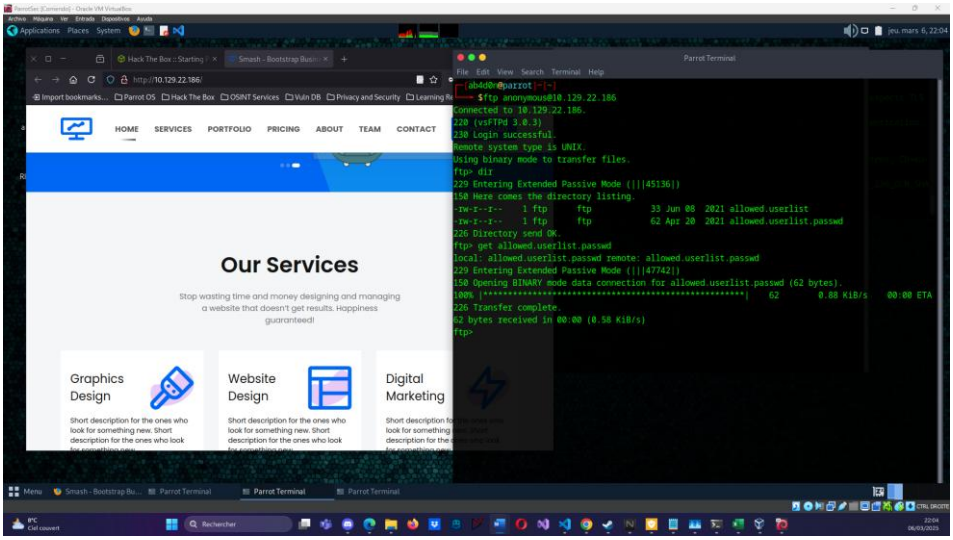
```
21/tcp open  ftp    vsftpd 3.0.3

80/tcp open  http   Apache httpd 2.4.41 ((Ubuntu))
```

On continue donc notre reconnaissance sur le navigateur web, l'application semble être une plateforme de design pour des sites web. Cependant le service FTP (port 21) a attiré notre attention car il est configuré pour permettre une connexion anonyme, ce qui pourrait être exploité.

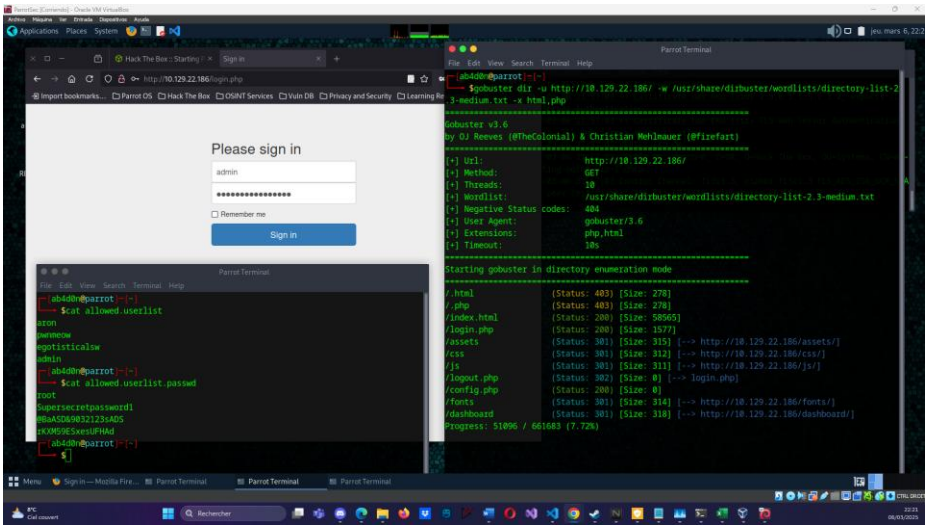


Identification des vulnérabilités

On sait qu'on peut se connecter anonymement sur le serveur ftp , une foie dedans on voie directement deux fichier, on prend les deux.



On ne trouve pas d'autres informations intéressantes sur le serveur ftp donc on maintenant on ce centre sur le site. On va donc énumérer les fichiers du site en cherchant des fichiers php et html intéressant.



On voit déjà un fichier nommé login.php, on utilise donc les identifiants et mots de passe qu'on a trouvé et on trouve tout de suite le flag

Leçons apprises

Ce scénario démontre l'importance d'une bonne configuration des services réseau. Les principales leçons tirées sont:

1. **Ne jamais laisser un accès anonyme activé sur des services comme FTP** : Cela peut exposer des informations sensibles à toute personne ayant accès à l'IP du serveur.
2. **Vérifier et sécuriser les interfaces administratives** : Un simple formulaire de connexion sans vérification adéquate peut être un point d'entrée pour un attaquant.
3. **Utiliser des outils d'énumération et de découverte** : Des outils comme **nmap** et **gobuster** sont essentiels pour identifier des services et des répertoires cachés qui peuvent être exploités.

L'attaque réussie sur cette machine a mis en lumière la vulnérabilité des configurations mal sécurisées et l'importance de la gestion des accès dans le maintien de la sécurité d'un réseau.