

Projet Sécurité: CTF



GROUPE	BACKDOOR	SCENARIO 21/10
PHASE 1	DEVELOPPEMENT CTF	SYSTEME
NIVEAU	MOYEN	

Un expert en sécurité informatique est engagé pour pénétrer un serveur FTP et un serveur SSH afin de récupérer des informations d'une entreprise. Le défi consiste à naviguer à travers ces systèmes en utilisant des techniques d'exploitation et d'escalade de privilèges.

Temps estimée: 1h

Acte 1 : La Porte du Serveur FTP

1. Introduction

- Le protagoniste découvre l'existence d'un serveur FTP avec une adresse IP spécifique, accessible avec un nom d'utilisateur mais sans mot de passe.
- Le client FTP est utilisé pour établir une connexion.

2. Exploration FTP

- À l'intérieur, le protagoniste découvre un fichier nommé "passwd.txt" contenant une liste de mots de passe pour un service particulier.
- Une lettre énigmatique rédigée par une personne inconnue est également trouvée.

Acte 2 : L'Étape Cruciale - Serveur SSH

1. Utilisation des Renseignements

- En utilisant les informations obtenues grâce au fichier "passwd.txt", le protagoniste tente d'accéder au serveur via SSH.

2. Connexion Réussie

- Après une série de tentatives, le protagoniste établit enfin une connexion SSH réussie.

3. Chasse au trésor - user.txt

- À l'intérieur du serveur SSH, le protagoniste recherche le fichier "user.txt" qui contient l'information cruciale qu'il recherche.

Acte 3 : L'Escalade des Privilèges

1. Enquête sur les Privilèges

- Le protagoniste explore le serveur SSH à la recherche de programmes ou de services qui peuvent s'exécuter avec des privilèges élevés.

2. Découverte de l'Exploit

- Une vulnérabilité est trouvée et exploitée pour acquérir des privilèges élevés.

3. L'Ascension au Sommet - root.txt

- Le protagoniste utilise cette nouvelle position pour accéder au fichier "root.txt" qui détient les informations les plus sensibles.