Une image contenant cadenas, verrouiller

Le contenu généré par l’IA peut être incorrect.

|  |
| --- |
| TryHackMe  Capture the Flag  Room : Agent Sudo (easy) |
| TryHackMe | Cyber Security TrainingUne image contenant oiseau, Graphique, conception  Description générée automatiquement |
| Réalisé par : CHARPEIL Romain |

## Scanning

Pour ce CTF là, j’ai recherché comment effectuer un scan disons ‘réaliste’ :

Nmap -sS -p- -sV –version-light -O –osscan-limit @ip

-sS : SYN scan (demi-connexion, plus discret qu'un TCP connect -sT)

-p- : Scanne tous les ports (1-65535) au lieu des 1000 par défaut

-sV --version-light : Détecte les versions des services mais en mode léger

-O --osscan-limit : Essaie d’identifier l’OS mais uniquement si les conditions sont bonnes

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

## Enumération

Dans un premier temps, je me suis concentré au niveau du port FTP, j’ai regardé une documentation, sur comment énumérer un port FTP.

Il était noté que pour la connexion il suffit de ‘FTP @IP’

Et qu’il existe un user ‘anonymous’ qui ne nécessite pas de mot de passe.

J’ai tenté la connexion avec celui-ci :

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

L’user anonymous n’était pas configuré.

J’ai vu qu’on pouvait essayer de brute force le login et mot de passe avec Hydra, je vais essayer, même si quand on n’a ni user ni password le brute force s’avère plus compliqué :

Une image contenant texte, capture d’écran, Police, information

Le contenu généré par l’IA peut être incorrect.

On peut également regarder si la version du Protocol est obsolète :

Une image contenant texte, Police, nombre, ligne

Le contenu généré par l’IA peut être incorrect.

Il y en une ‘Remote Denial of Service’ mais ce n’est pas ce que l’on souhaite, ceci sert simplement à bloquer le serveur.

On va s’appuyer du côté http maintenant, port 80 :

On peut directement lancer un gobuster en même temps de visiter le site web :

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Quand on se dirige sur l’URL :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

« Utilisez votre propre nom de code en tant qu’user agent pour accéder au site »

A première vue, cela me fais penser à l’utilisation de BurpSuit.

On peut regarder le résultat de notre gobuster :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Pas vraiment de choses intéressantes, index.php on peut le dirsearch peut être :

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Non plus. Il reste alors l’utilisation de Burp Suite, par rapport à l’user agent, comme indiqué sur le site, ou peut-être qu’il existe du brut force d’user agent je vais regarder :

## Exploitation

J’ai trouvé une liste et un script sur Github, qui permettrait d’effectuer du brute force

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

On va essayer :

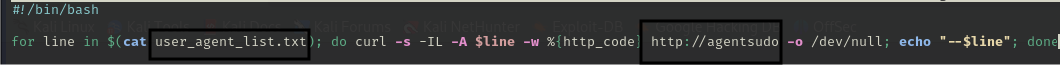
Une image contenant texte, capture d’écran, Police, information

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Pour chaque ligne du user\_agent\_list.txt, il va faire un curl, a nous de modifier l’URL :



On peut tester maintenant pour voir ce que ça donne

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Cela n’a pas vraiment fonctionné, tout les user-agent étaient acceptés .

J’ai eu une autre idée, en fait le prénommé ‘Agent R’ indique d’utiliser les ‘codename’.

R -> codename

J’ai lancé cette commande :

« curl -A -L <user-agent> » :

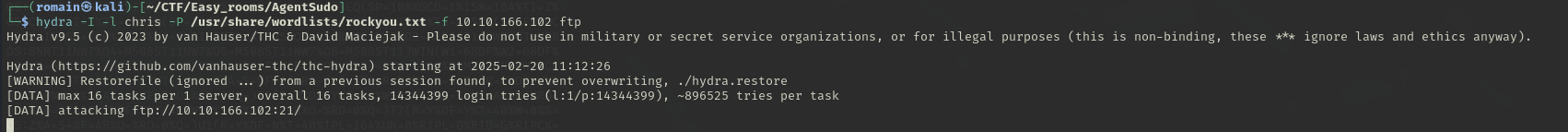
Une image contenant texte, capture d’écran

Le contenu généré par l’IA peut être incorrect.

On sait que l’utilisateur se nomme chris et qu’il a un faible password (bruteforce)

On va utiliser hydra pour brute force son password afin d’accèer au service FTP :

Hydra -I -l chris -P /usr/share/wordlist/rockyou.txt 10.10.166.102 ftp



Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

On a le password ‘crystal’

On peut maintenant essayer de ce connecter au port ftp :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Connexion réussie

Une image contenant texte, Police, capture d’écran

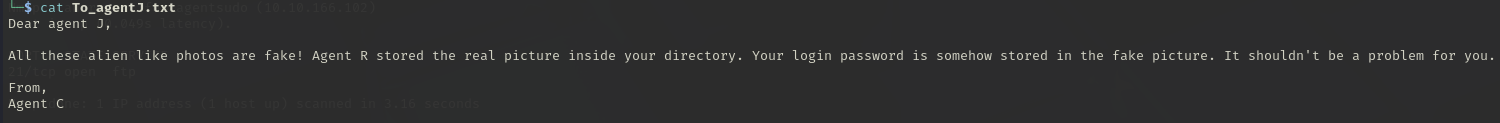
Le contenu généré par l’IA peut être incorrect.

On récupère tout le contenu

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Ensuite, quand on cat le To\_agentJ.txt



Il est indiqué que dans une photo, il y a de stocké le mot de passe de l’agentJ afin d’accéder aux vraies photos.

J’ai d’abord essayé avec l’outil StegHide pour extraire des données cachés dans une image, en l’occurrence ‘cute\_alien.jpg’. Cela demandait une passphrase que je n’avais pas, j’ai installé l’outil stegcracker qui brute force ces systèmes :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Il nous a sorti un fichier cute\_alien.jpeg.out

Quand je le cat :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Mais en fait je me suis trop avancé dans le CTF, j’ai sauté des étapes :

Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

Donc on retourne en arrière, il faut trouver un ZIP, je vais plutôt me diriger vers l’autre image, un png et utilisé l’outil ‘binwalk’ :



Cela nous a créé un dossier extract :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Si on essaye de dezip le zip :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Il est encrypté, on va donc utiliser ‘John’ :

Zip2john 8702.zip > zip.hash

&&

John zip.hash

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Le mot de passe est alien

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

On dirait qu’on a du texte encodé, on va utiliser CyberChed pour remédier cela :

Une image contenant texte, capture d’écran, affichage, logiciel

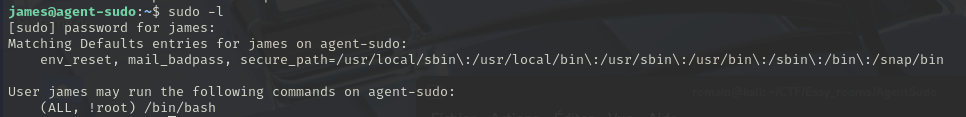
Le contenu généré par l’IA peut être incorrect.

Le password est Area51 comme au début quand j’ai utilisé stegcracker.

On se connecte en ssh à james :



Maintenant, si on tape sudo -l :



L’utilisateur peut exécuter la commande /bin/bash en tant que n’importe quel utilisateur sauf root.

TryHackMe nous aident un peu en disant qu’il faut chercher un CVE, ce que nous allons faire :

## Elévation de privilèges

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, logiciel, Police, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Que fait cette CVE :

Une image contenant texte, capture d’écran, document, Police

Le contenu généré par l’IA peut être incorrect.

CVE-2019-14287 permet de contourner les restrictions de sudo en exploitant une faille dans la gestion des ID d'utilisateur, permettant ainsi d'obtenir des privilèges root de manière non autorisée.

sudo ne vérifie pas correctement l'existence de l'ID d'utilisateur spécifié avec l'option -u. En utilisant -u#-1, sudo interprète # -1 comme l'UID -1, qui est équivalent à 0 (l'UID de root)



On est bien devenu root, on peut se rendre dans son dossier pour récupérer le flag :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Terminé

J’ai tout compris, sauf au niveau de chiffrement avec John, comment savoir qu’il était chiffré ? Le reste, à port pour passer root, comprendre la CVE, ça va.