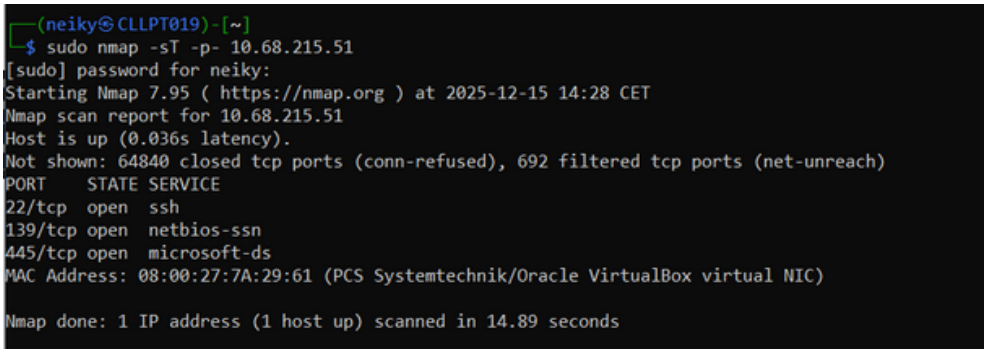
WRITE-UP : CHALLENGE SUPERSHUTTLE

1. RECONNAISSANCE

L'objectif est d'attaquer la machine située à l'adresse IP 10.68.215.51.

J'ai commencé par une phase de découverte de ports via nmap. Les scans classiques (-sS) ne passant pas (probablement à cause des raw sockets), nous avons opté pour un scan de type TCP Connect (-sT) sur l'ensemble des ports.

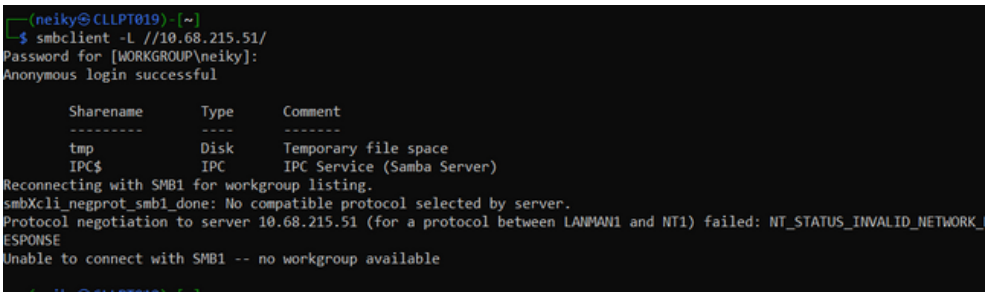
Commande utilisée :
sudo nmap -sT -p- 10.68.215.51



Résultat :
Le scan révèle que le service SMB est ouvert.

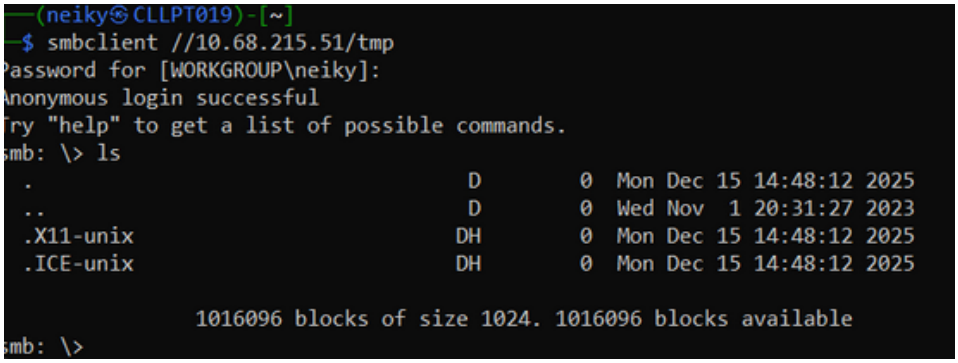
2. ÉNUMÉRATION DU SERVICE SMB

J'ai tenté une connexion sur le service SMB pour lister les partages disponibles.



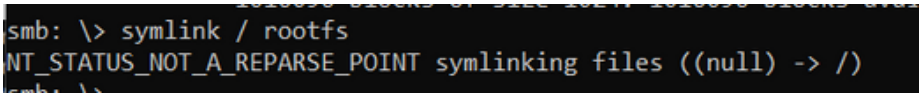
- Authentification : Succès. L'authentification anonyme est activée sur le serveur.
- Partages découverts : Deux partages sont visibles, IPC$ et tmp.

Analyse du partage "tmp"
Je me suis connecté au partage tmp. L'accès est autorisé en lecture et en écriture.
La présence de dossiers caractéristiques comme .X11-unix indique que ce partage pointe directement vers le répertoire système /tmp du serveur.



Tests de vulnérabilités (Non concluants) :

- Exécution : Tentative d'exécution de fichiers directement via SMB, ce qui a échoué car SMB ne le permet pas nativement.
- Symlink Traversal : J'ai tenté une attaque par lien symbolique pour accéder à la racine du système de fichiers (rootfs).

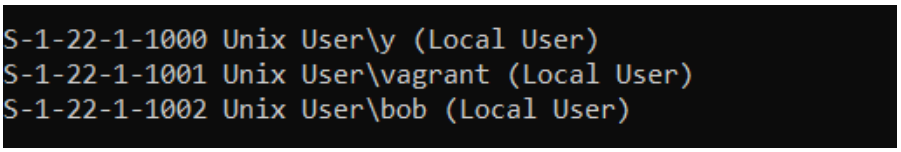


Résultat : NT_STATUS_NOT_A_REPARSE_POINT. Le serveur est sécurisé contre les liens symboliques insécurisés.

Analyse du partage "IPC$"

Le partage IPC$ est un canal de communication permettant d'interagir avec les processus internes du serveur. Cela nous a permis d'effectuer une énumération plus poussée des utilisateurs via l'outil enum4linux.

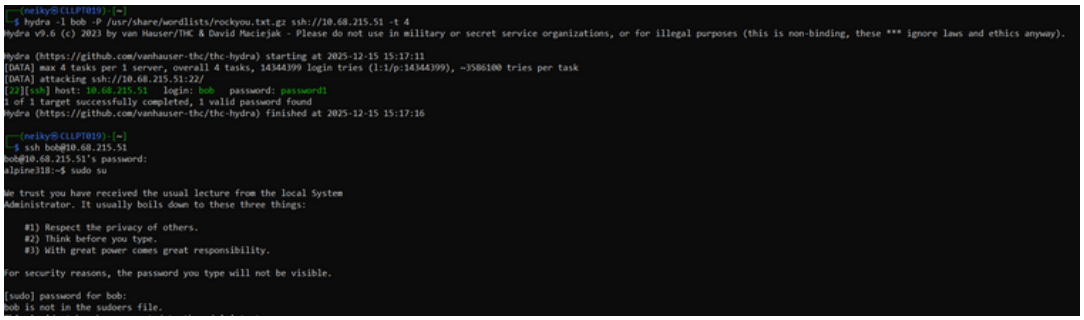
Commande utilisée :
enum4linux -a 10.68.215.51



Résultat :
L'outil a permis d'identifier plusieurs utilisateurs potentiels, notamment bob et vagrant.

3. EXPLOITATION ET ACCÈS INITIAL

Tentative sur l'utilisateur "bob" (Fausse piste)
j'ai d'abord tenté une attaque par force brute sur l'utilisateur bob à l'aide de l'outil Hydra. Bien que nous ayons réussi à nous connecter, l'utilisateur bob ne possédait pas les droits suffisants : la commande sudo su a échoué (impossible d'accéder au /root pour trouver le flag).



Vecteur d'attaque : "Vagrant Box"
L'identification de l'utilisateur vagrant ainsi que le nom de la machine suggèrent qu'il s'agit d'une "Vagrant Box" (une machine virtuelle pré-configurée pour le développement). Ces machines possèdent souvent des identifiants par défaut connus.

Exploitation SSH :
J'ai testé les identifiants par défaut :
- User : vagrant
- Password : vagrant

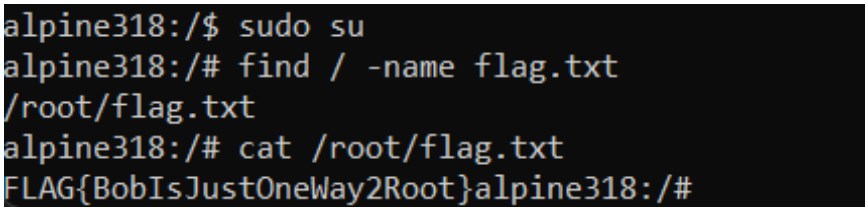
Commande de connexion :
ssh vagrant@10.68.215.51
L'authentification a réussi.

4. ÉLÉVATION DE PRIVILÈGES (ROOT)

Une fois connecté en tant que vagrant, j'ai tenté d'élever nos privilèges via sudo su. Sur les box Vagrant, cet utilisateur a généralement les droits d'administration par défaut.

Commande :
sudo su

j'ai pu obtenir un accès root et trouver le flag.



FLAG{BobIsJustOneWay2Root}