Kenobi

=> **Samba** est juste le systeme de partage de fichiers pour windows,

et ce dernier utilise le protocole smb

on peut notamment trouver sur google un script utilisable par nmap avec l'option –script pour voir quels sont les partages actuelles et les users qui les font.

puis vu que linux a un smbclient préintégré, suffit de faire

smbclient //IP/user

pour télécharger des trucs disponible sur le smb suffit de faire:

smbget -R smb://IP/user

Petit secret : Pour trouver des exploits en ligne de commande au lieu d'aller sur exploit db, faire searchsploit...

parlons de proftpd , un serveur ftp

nc peut par exemple par exemple permettre de se connecter, voilà.
en faisant:
nc IP port

attention, les clés id_rsa ne peuvent avoir que les permissions 600 pour etre utilisé.
Dans ce contexte, je me suis connecté avec netcat sur le serveur, j'ai copié la clé id_rsa dans le rep /tmp, puis j'ai monter tout le var/ du serveur vers un repertoire que j'ai créé. Enfin j'utilisé la clé id_rsa pour me connecter.

ssh -i id_rsa user@serveur

Escalade :
Rechercher tous les fichiers avec un suid et voir ce qui est intriguant .

find / -type f -perm -u=s 2>/dev/null

Kenobi

Une méthode serait de regarder, contourner, faire ce qui est possible , qui à changer une commande en quelque chose qu'il n'est pas censé faire..
en fait /bin/sh est un interpreteur universel, du coup le lancer permet d'obtenir l'acces root haha si exécuté grade à un binaire avec un suid

Si un programme SUID root exécute `/bin/sh`, alors **le shell obtenu tourne avec les droits root !**