BLUE

Objectif: Découvrir des bases de l'exploitation de windows

Résolution du ctf:
Faire un scan avec nmap et trouver un backdoor , un exploit puis démarrer metasploit avec:
> msfconsole
puis rechercher l'exploit avec:
> search
- soit c'est un cve => search CVE date
- soit un exploit directement ou OS search [exploit]

> use chemin_exploit/id pour l'utiliser
> show options pour connaitre les options.
et les set avec:
> set OPTION Valeur

checker le bon payload(le code qui sera executé sur la machine cible) avec:
> show payloads et set le PAYLOAD avec
set PAYLOAD ...
> puis faire exploit ou run -j pour etre en background et de facon plus douce

important de mettre en background si pas encore fait: avec ctrl+Z et un id sera attribué à cette session

Prochaine étape: convertir le shell en meterpreter, un shell mieux organisé.
juste faire un search shell_to_meterpreter et utiliser le module
puis set l'option session à celui de la machine qui avait été exploité et qui est bakcgroundet faire run .
ne pas oublier de l'utiliser en faisant sessions num_sessions_de_la_transition.

BLUE

schema commun : faire
ps pour voir les processus et faire
migrate id_processus pour y migrer sinon rien ne marchera, ca permet de se mettre correctement sur la machine

Puis enfin pour couronner le tout:
hashump pour voir les user et leur mdp