SCANNER LES VULNERABILITES D'UN SYSTEME ET EXPLOITEZ-LES

1. Installer Nessus sur Windows ou Kali selon votre préférence
2. Effectuer prioritairement un scan basique de votre réseau et de préférence relancer le scan de la machine qui comporte des failles critiques
3. Exporter le fichier Nessus contenant le rapport de vulnérabilités
4. Lancer votre console Metasploit *(msfconsole)* en mode root
5. Rechercher un exploit qui vous permettra d'exploiter votre vulnérabilité *(Search_nom de la faille).* Vous avez le nom de l'exploit et le taux de réussite d'exploitation de cette faille)
6. Exploiter cette faille *(Use_nom de l'exploit…)*
    a. *Show options*
    b. Cibler votre machine (*Set RHOST adresse IP de la machine)*
    c. Choisir un payload *(show payload)*
    d. *Utiliser le payload (use payload_nom du payload)* – de préférence un payload avec un Rank élevé
    e. Exécuter *(Run)*
    f. Observer toutes les fonctions que vous pouvez exécuter *(help)*
    g. Effectuer 2 ou 3 actions de votre choix puis éteignez la machine distante