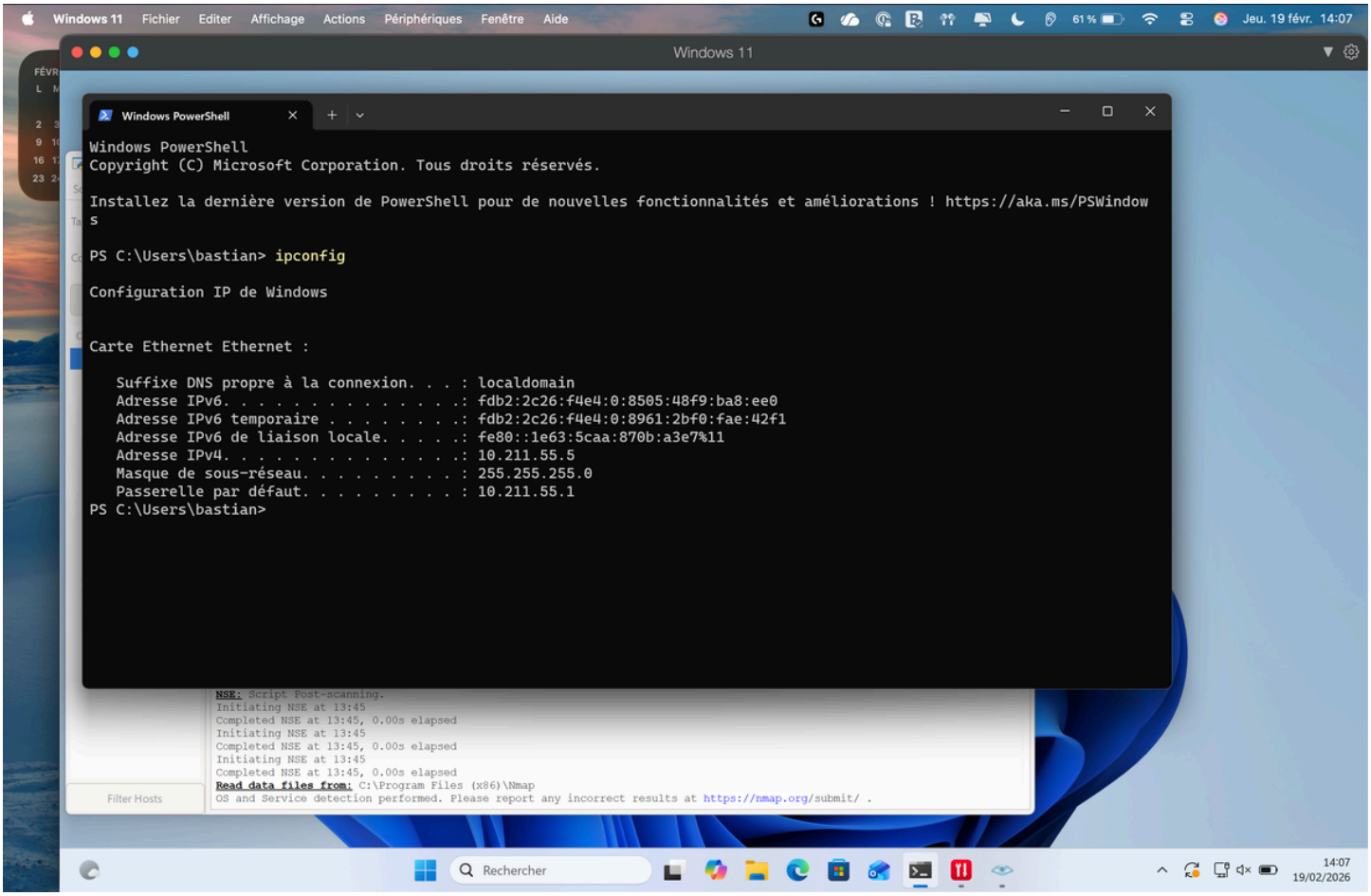
AUDIT RÉSEAU D'UNE MACHINE WINDOWS VIRTUELLE AVEC NMAP

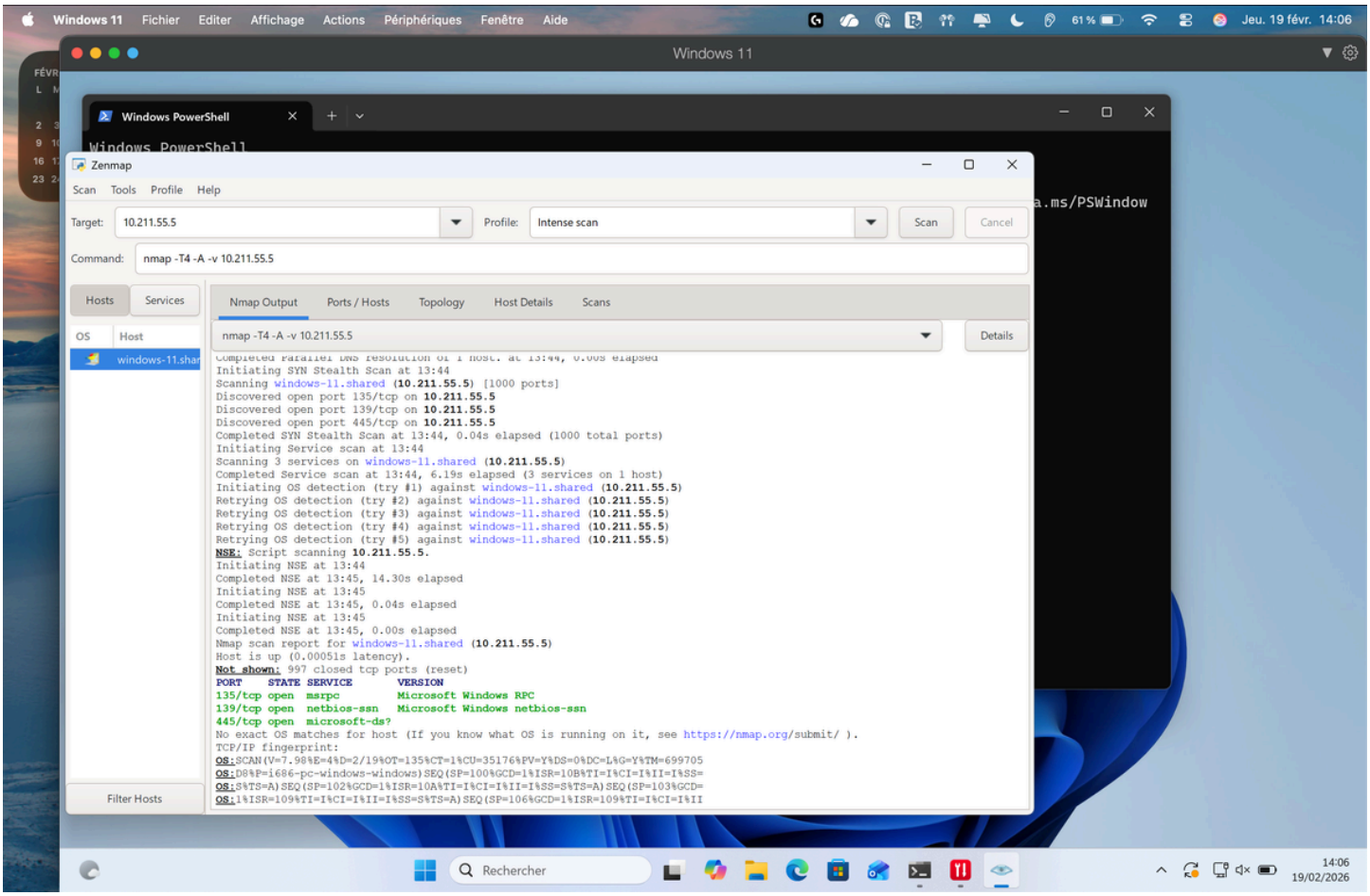
Projet — Analyse des ports et services d'une machine Windows 11 virtuelle

CAPTURE 1 : IDENTIFICATION DE L'ADRESSE IP LOCALE SUR WINDOWS



La commande ipconfig a été utilisée pour identifier l'adresse IPv4 de la machine cible. Ceci est nécessaire pour scanner correctement le réseau avec Nmap, (Profile : Intense scan).

CAPTURE 2 : RÉSULTAT DU SCAN NMAP – PORTS OUVERTS ET FERMÉS



Cette capture montre les ports détectés sur la machine Windows 11 virtuelle.

Les ports ouverts sont :

- 135/tcp → Microsoft RPC

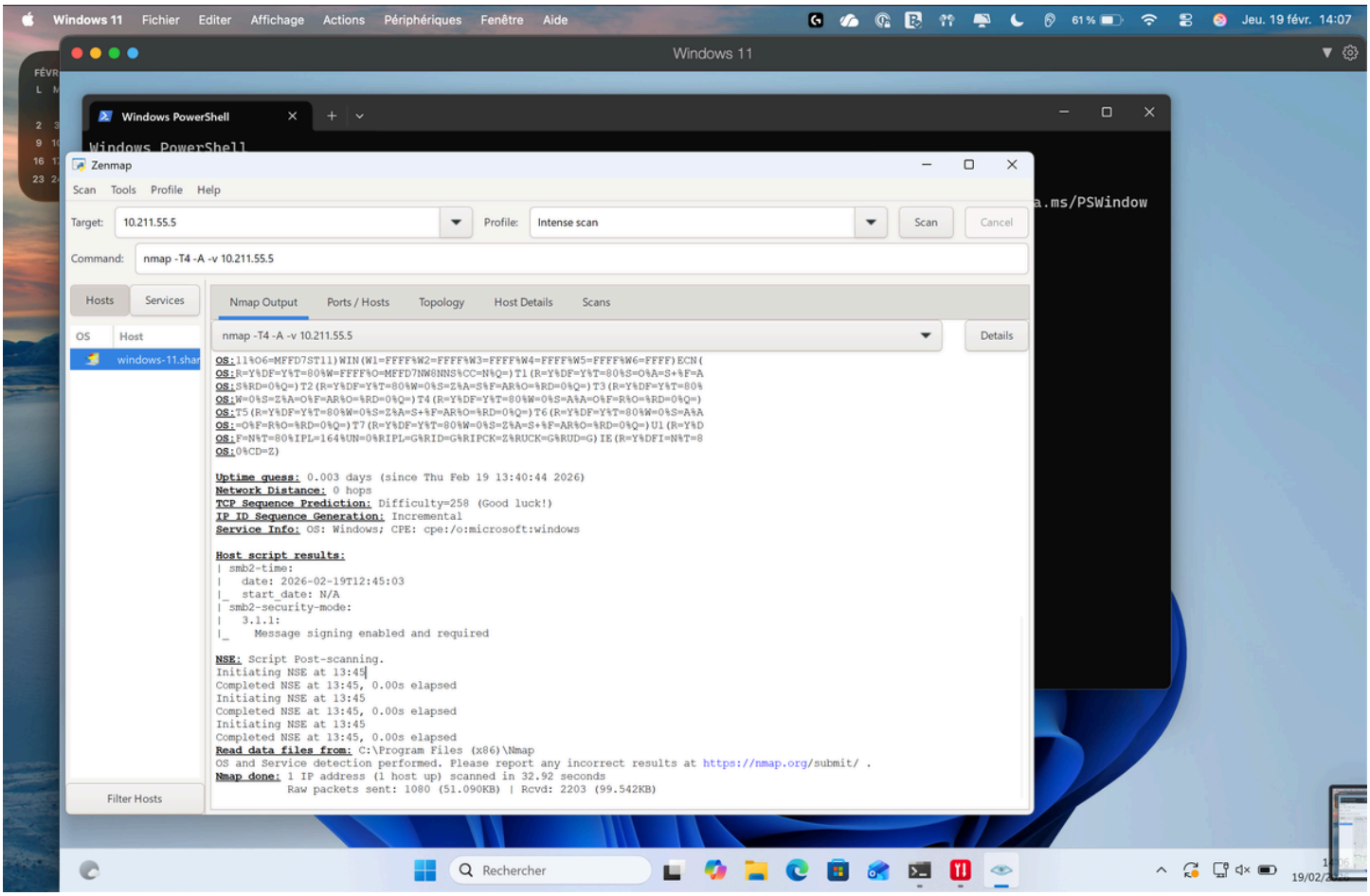
- 139/tcp → NetBIOS

- 445/tcp → SMB

Les autres ports (997) sont fermés (Not shown), ce qui signifie qu'ils ne sont pas accessibles et réduisent la surface d'attaque du système.

Analyse : Les ports ouverts correspondent à des services standards de Windows et sont normaux pour le fonctionnement réseau. Ils représentent néanmoins la surface d'attaque potentielle de la machine.

CAPTURE 3 : ANALYSE DÉTAILLÉE NMAP – OS, SCRIPTS ET SÉCURITÉ



Cette capture montre plusieurs informations avancées fournies par Nmap :

- Uptime guess : 0.003 days → la machine vient de démarrer.

- Network Distance : 0 hops → la machine est sur le réseau local.

- TCP Sequence Prediction : difficulté 258 → sécurité correcte contre prédiction TCP.

- Service Info : Windows, cpe:/o:microsoft:windows → type de système détecté.

- Host script results : SMB2 signature activée → communication sécurisée et protégée contre attaques man-in-the-middle.

- Nmap done : scan terminé avec succès, aucune erreur critique.

Analyse : La machine est correctement configurée pour un environnement Windows standard. Le service SMB est sécurisé, et la machine présente une surface d'attaque minimale.

CONCLUSION:

Ce projet a permis de réaliser un audit réseau d'une machine Windows 11 virtuelle avec Nmap. Trois ports ouverts ont été identifiés (135, 139, 445), correspondant à des services standards (RPC, NetBIOS, SMB). Le service SMB est sécurisé avec le message signing activé. L'analyse montre que la machine est correctement configurée et que la surface d'attaque est limitée. Pour

renforcer la sécurité, il est recommandé de maintenir le système à jour et de désactiver les services inutiles. Ce projet m’a permis de comprendre la configuration réseau, l’analyse des services exposés et les bonnes pratiques en cybersécurité.