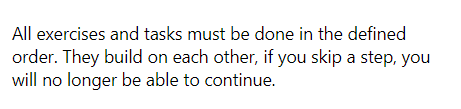
**🧑‍🎓 Student name:** TEJEDA David, PEUGNET Thomas

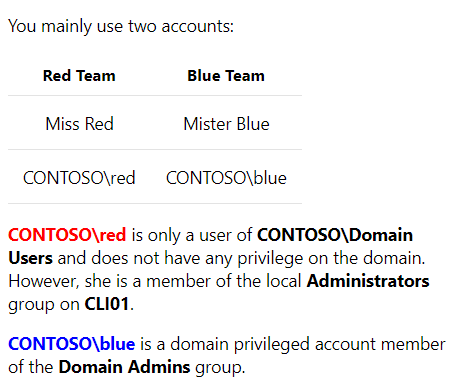
**🏛️ Student class:** EFREI RS3 2025

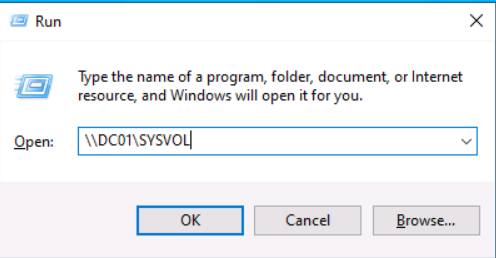
**📅 Date:** 25/01/2024

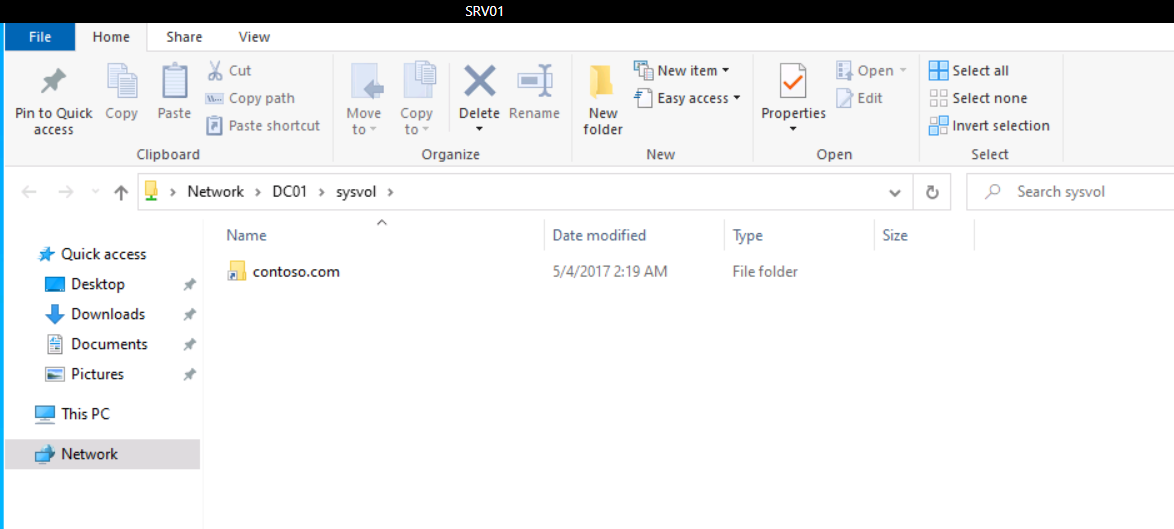
# Threats targeting the hybrid & cloud identity platform

Reconnaissance



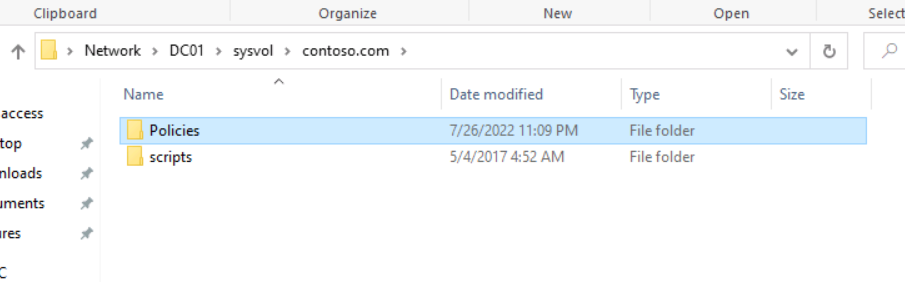




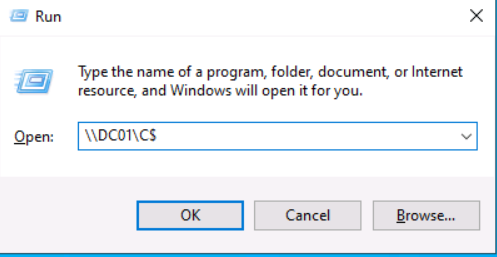


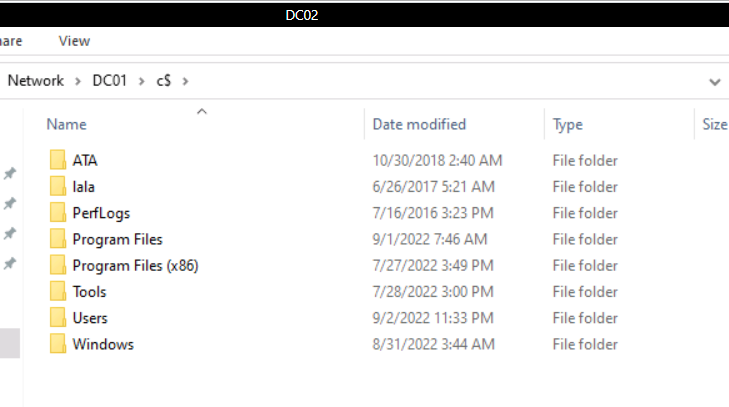
### Exercise 1 - Prepare the environment

📝 What types of files can we find in this folder?

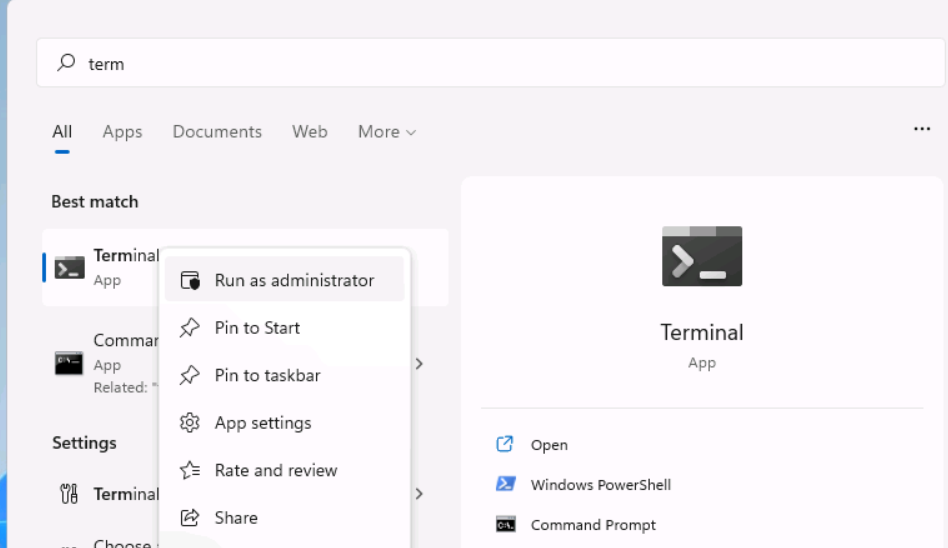


**SYSVOL et Politiques de Groupe**: Le dossier SYSVOL sur un contrôleur de domaine Windows inclut des fichiers de politique de groupe (GPO), qui sont utilisés pour centraliser la gestion des paramètres de configuration des ordinateurs et utilisateurs du domaine. Ces fichiers comprennent des modèles administratifs, des paramètres de sécurité, des scripts, et des fichiers de préférences. En plus, SYSVOL contient des scripts de connexion et de déconnexion qui sont exécutés lorsque les utilisateurs se connectent ou se déconnectent d'un ordinateur du domaine.





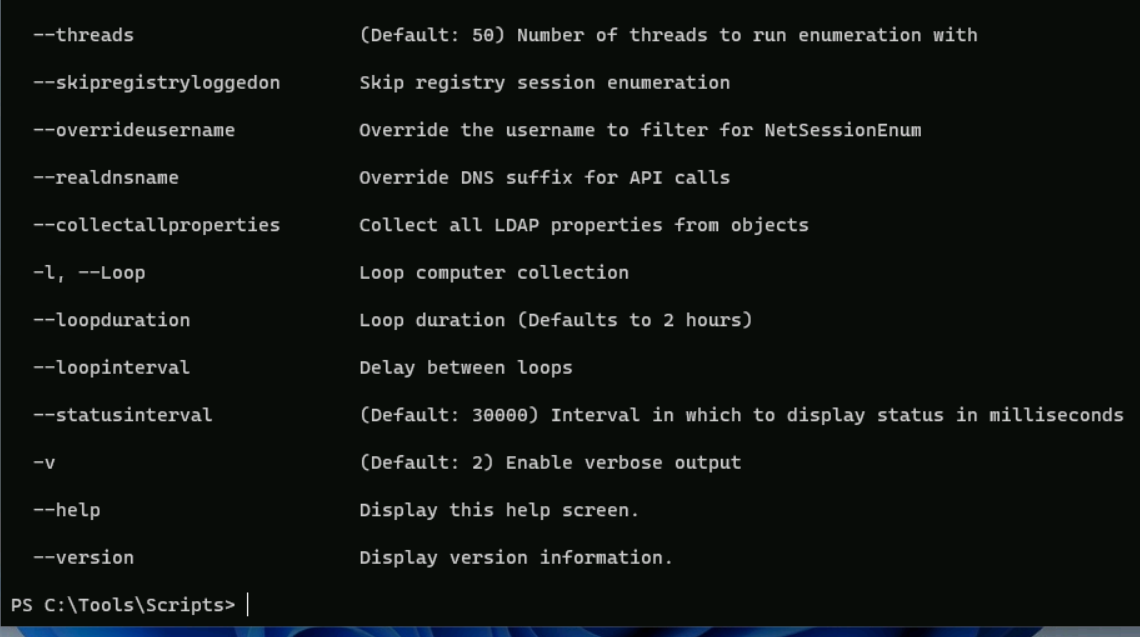


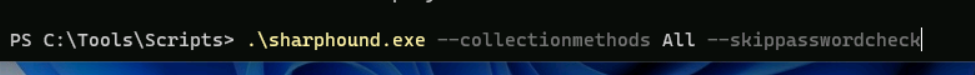


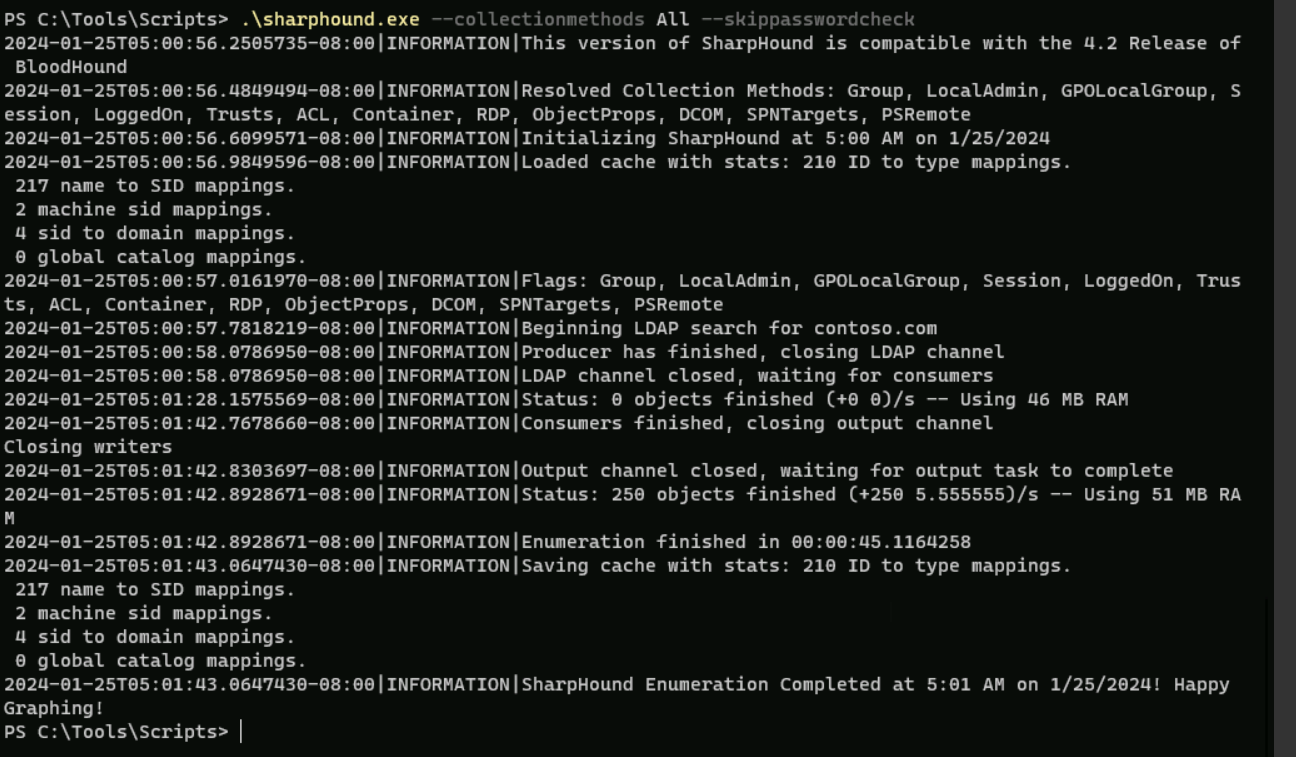
### Exercise 2 - Use BloodHound for recon

📝 ls is an alias for what PowerShell command?

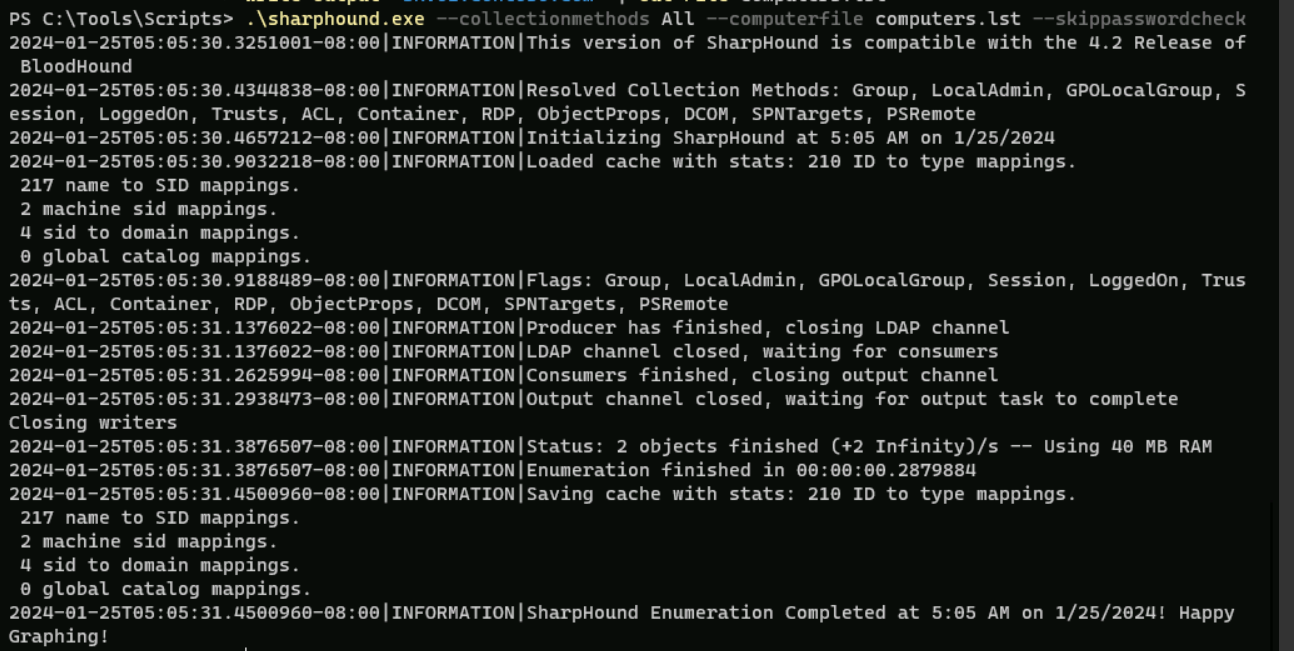
* C’est un alias pour la commande dir.



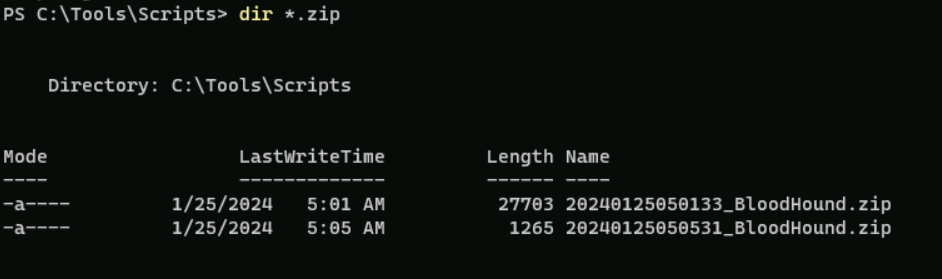


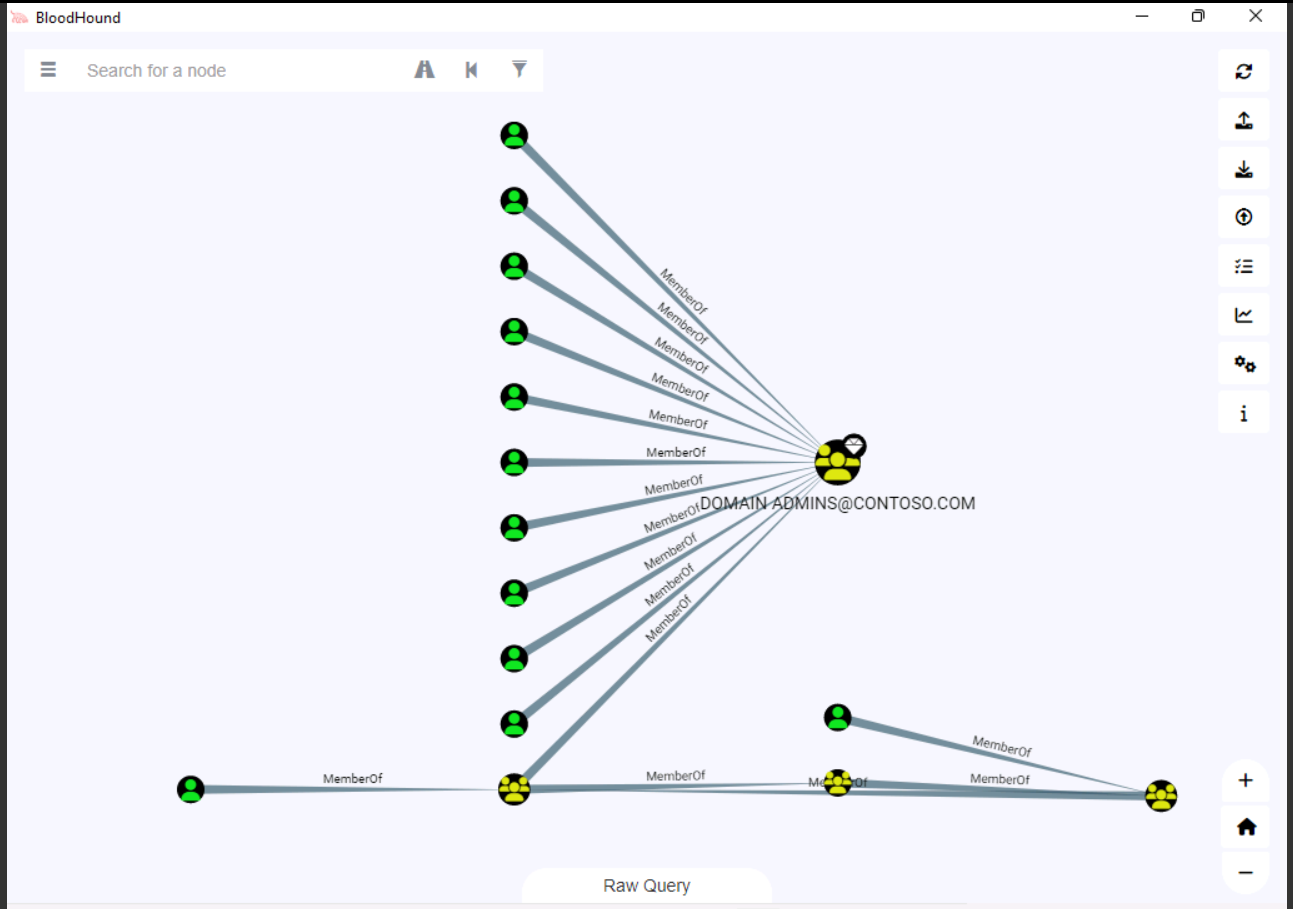


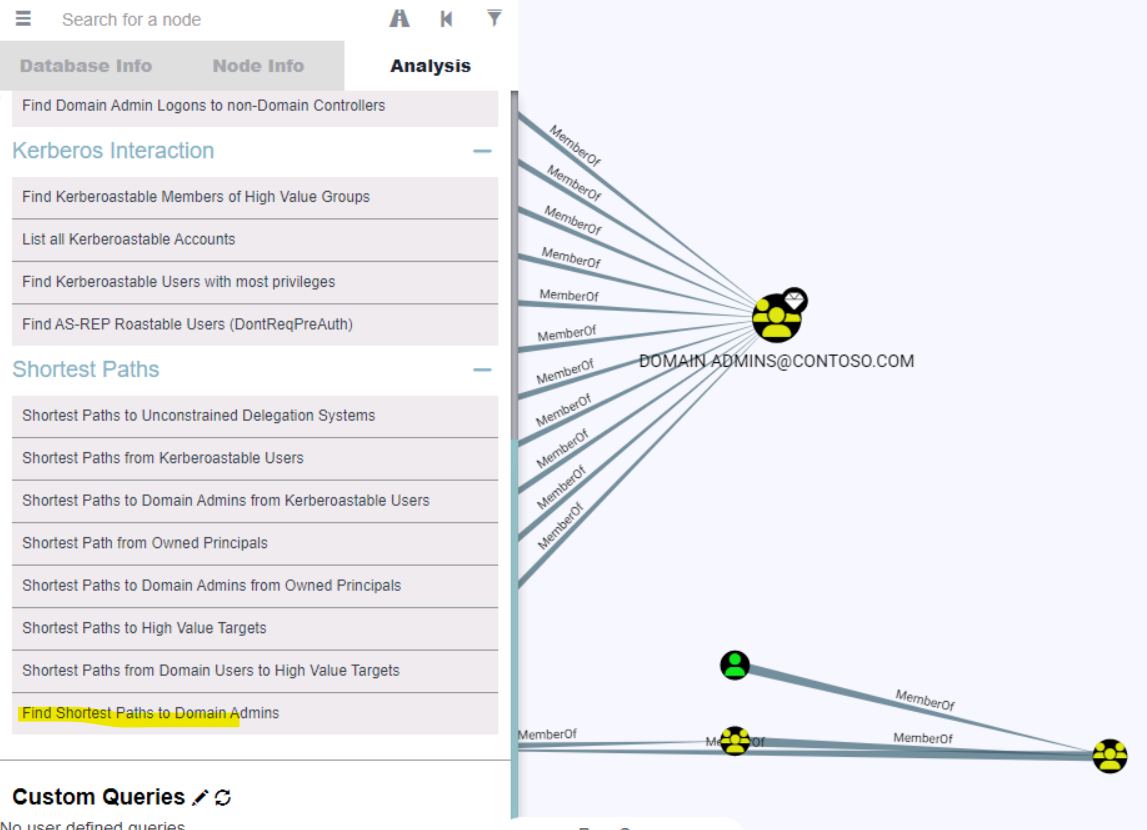


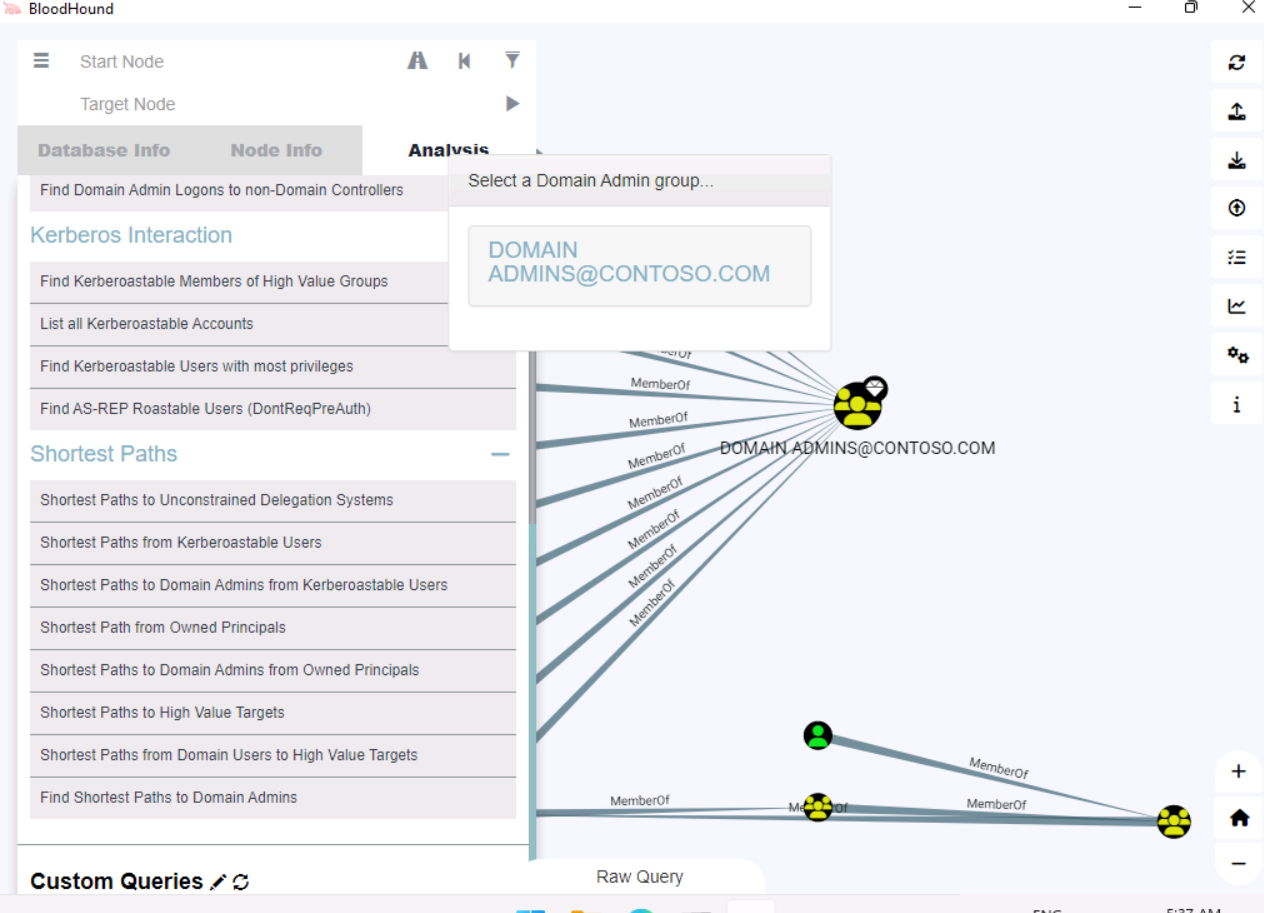


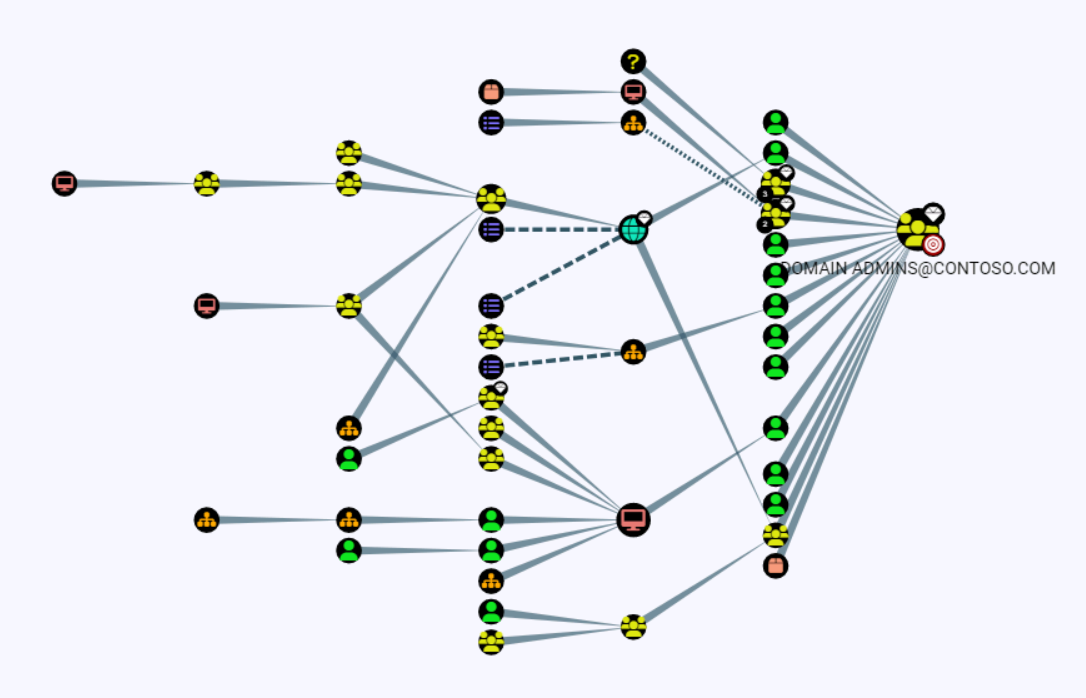
📝 How many zip files do you see?



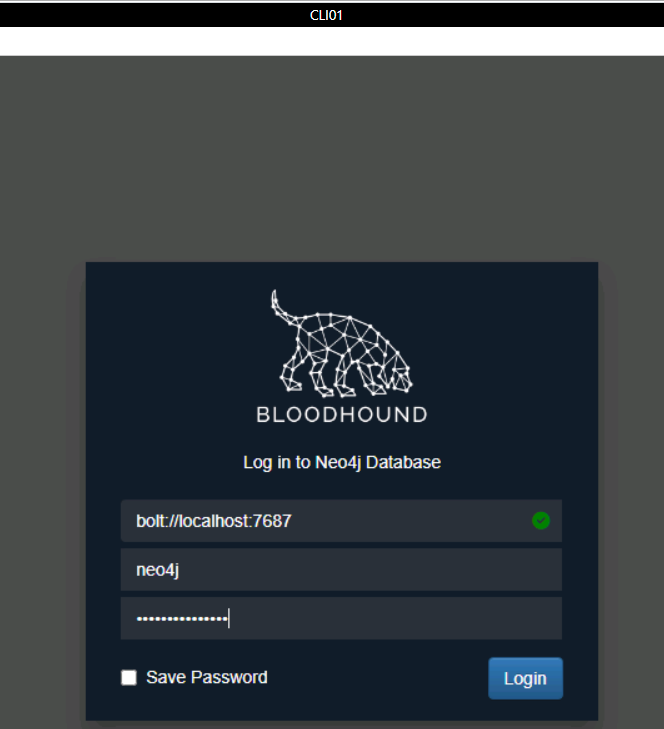


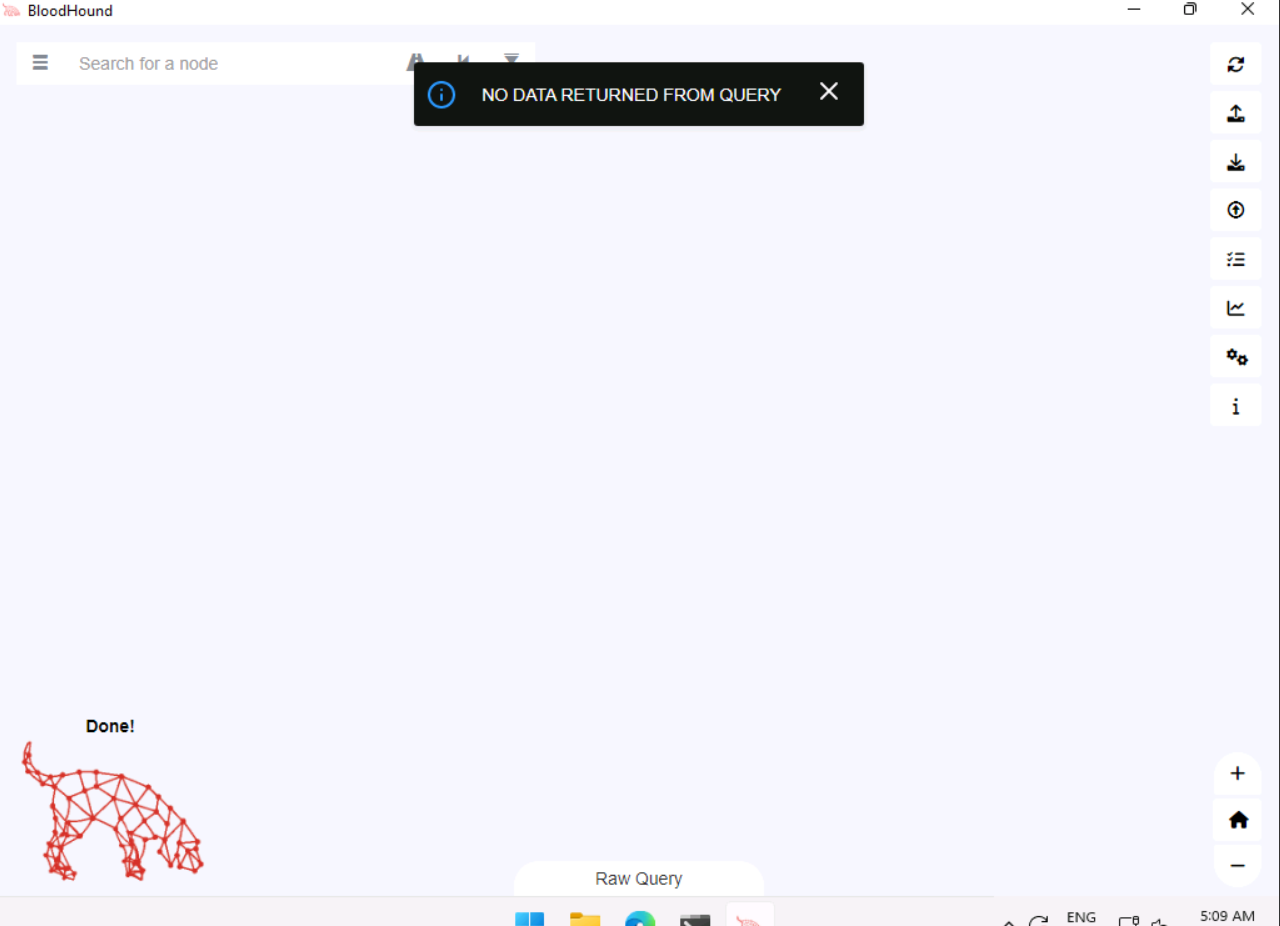


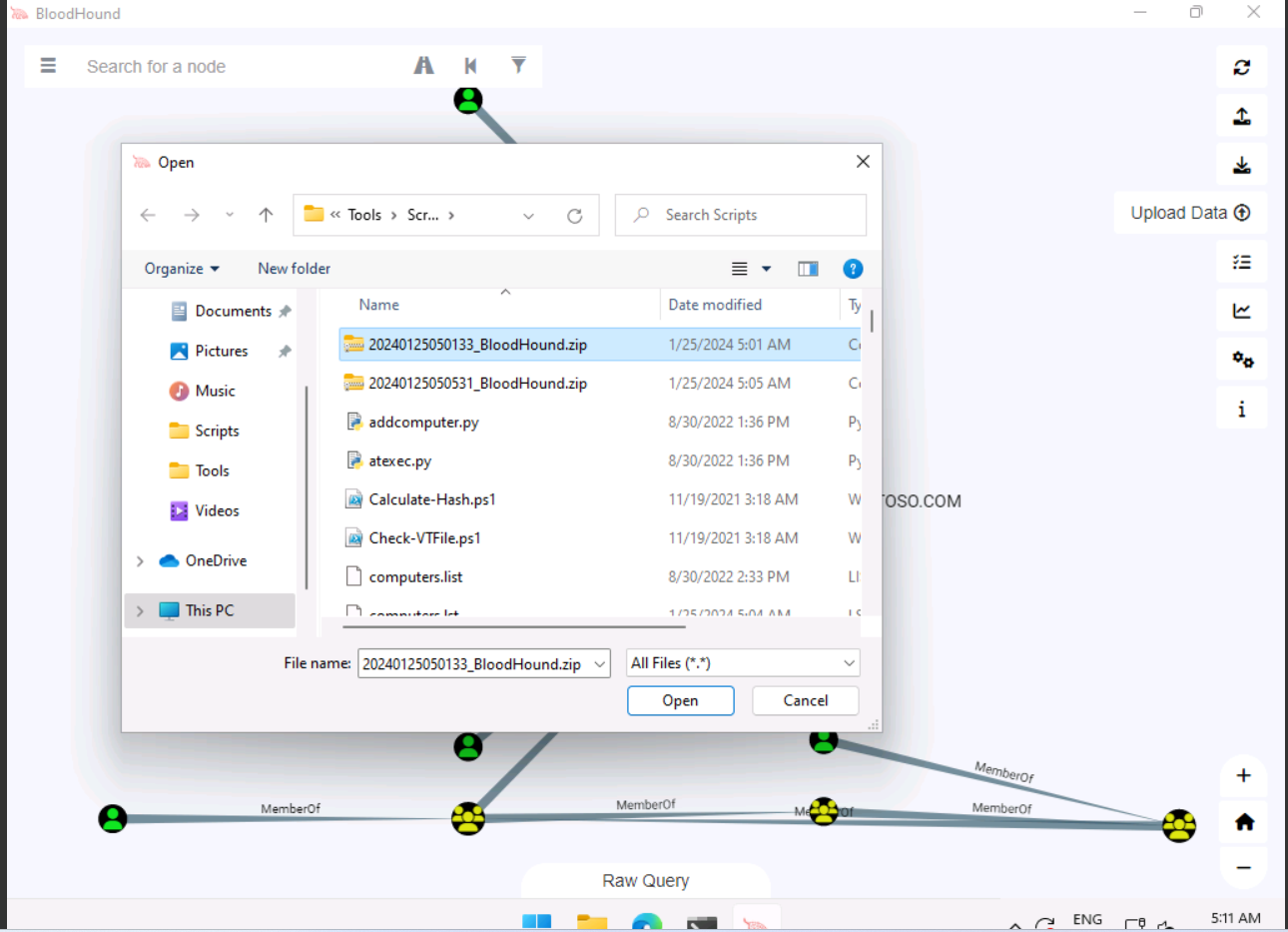


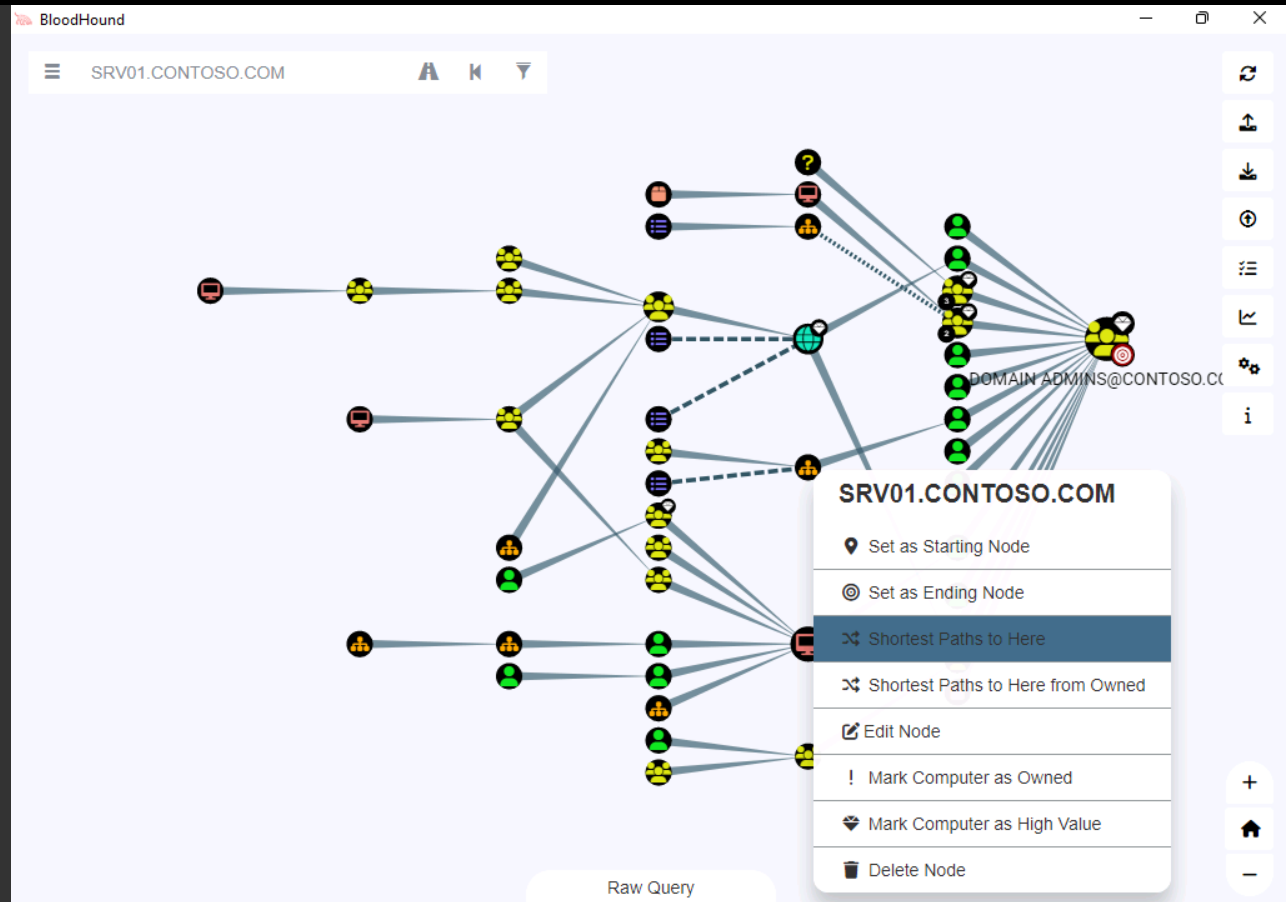


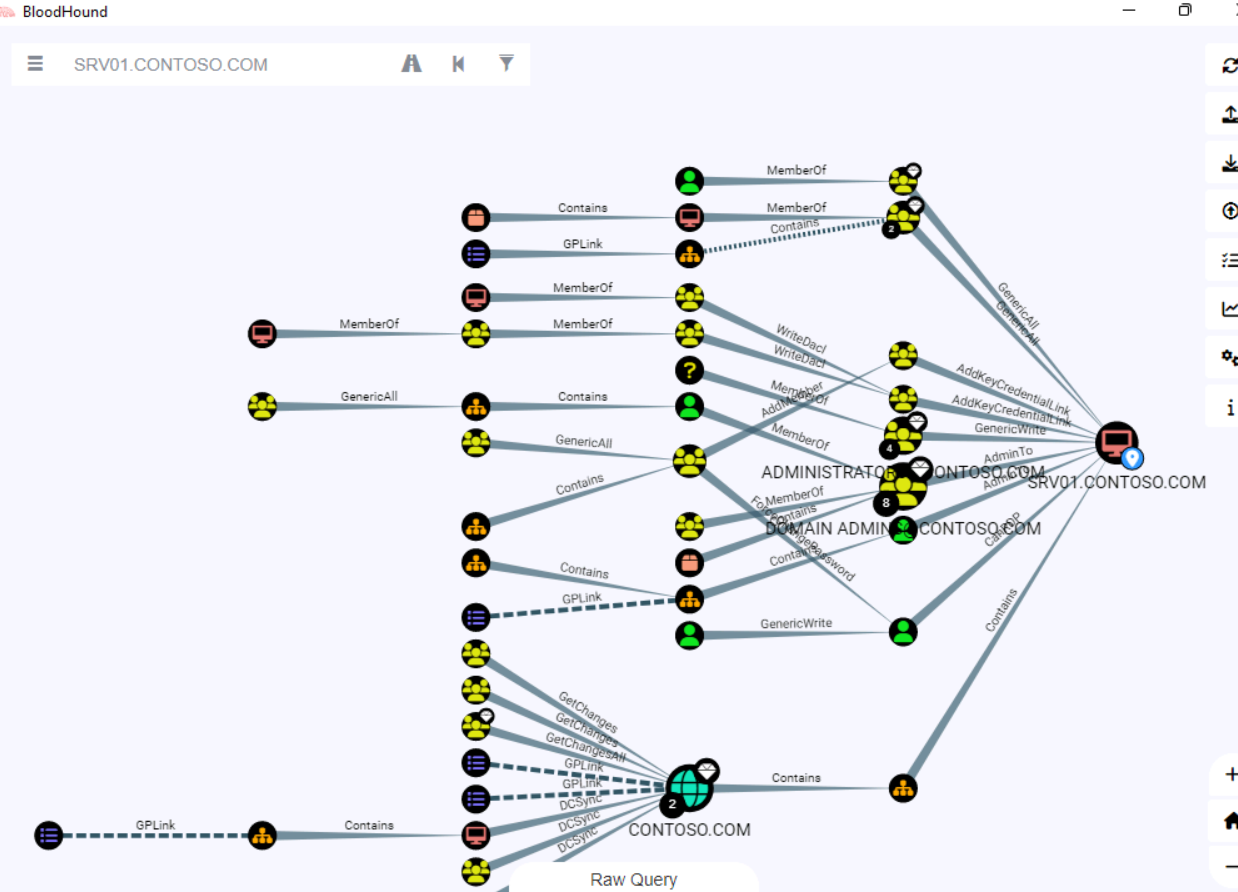
📝 Can you see who has a session and from where?







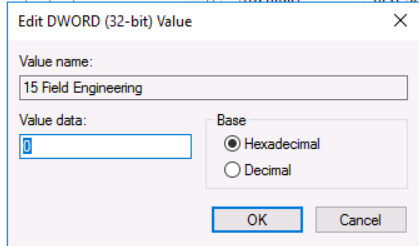


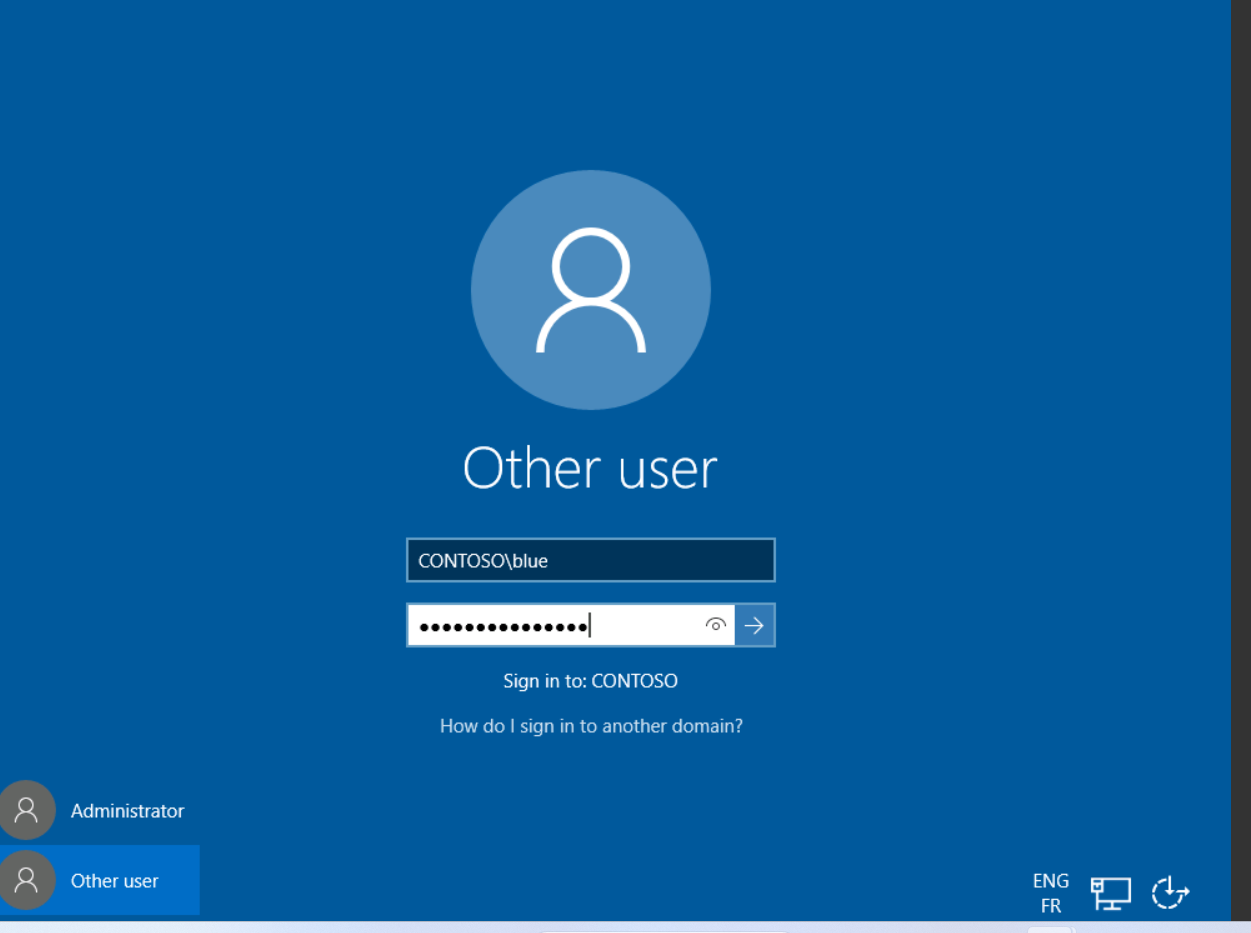


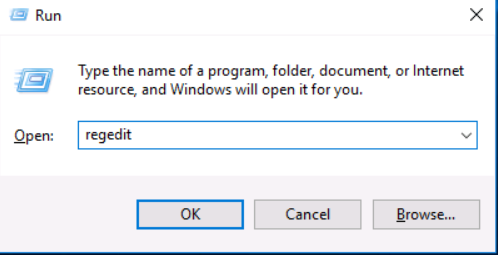
### Exercise 3 - Enable LDAP logging

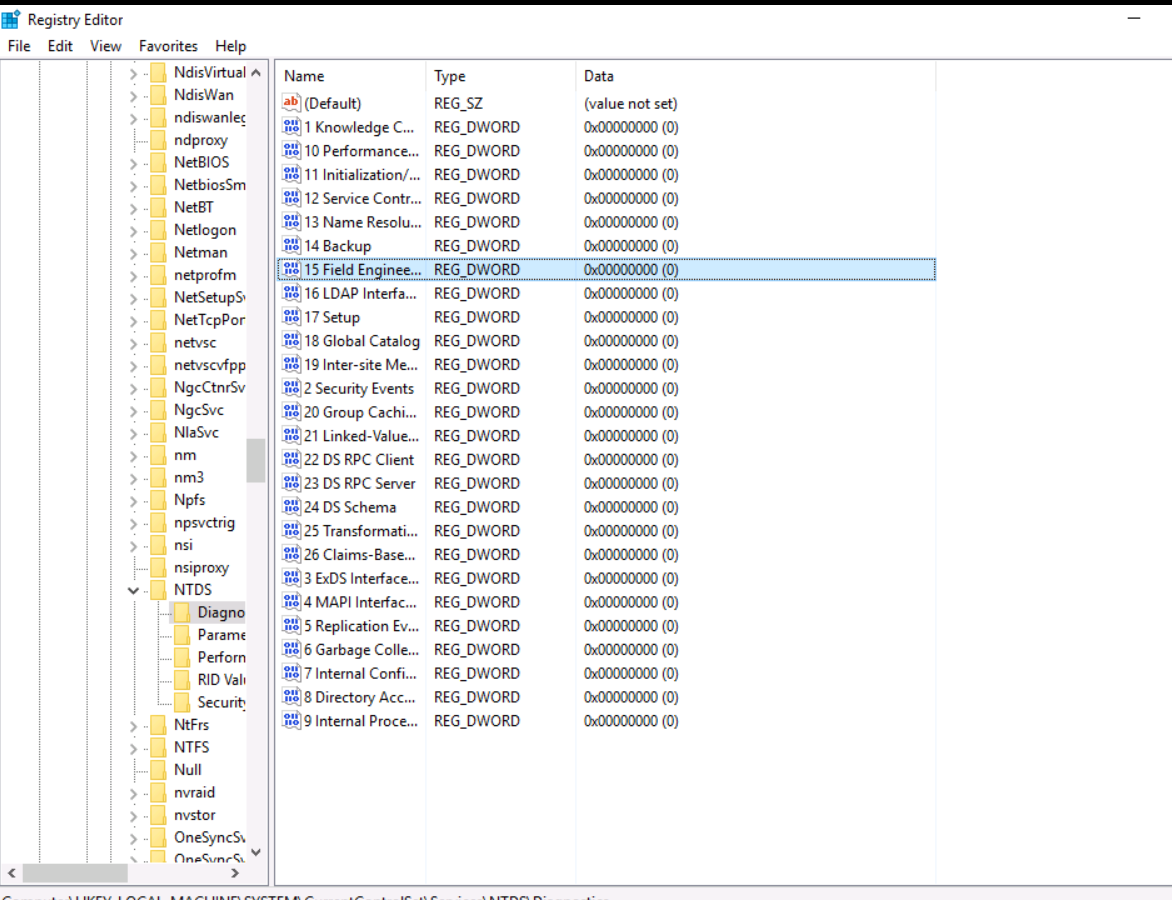
📝 What is the default value of all diagnostics configurations?

* Réponse sur la capture ci-dessous.

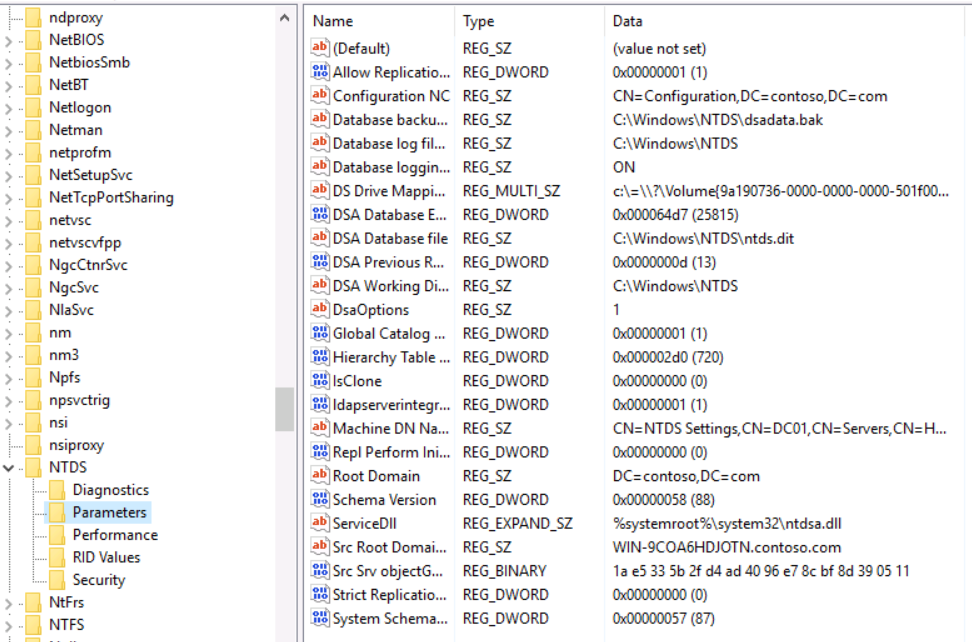


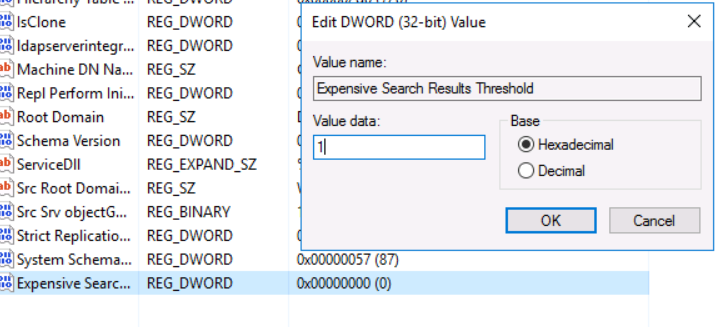


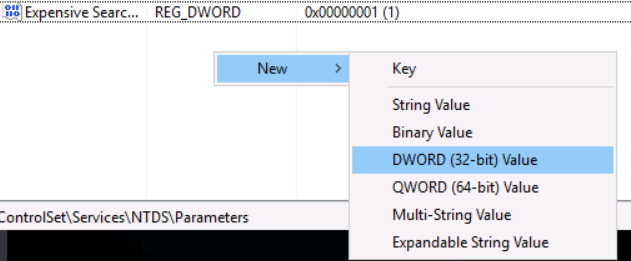


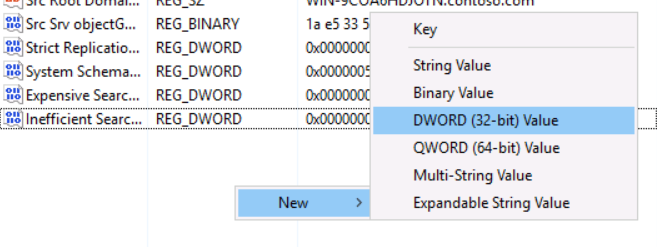


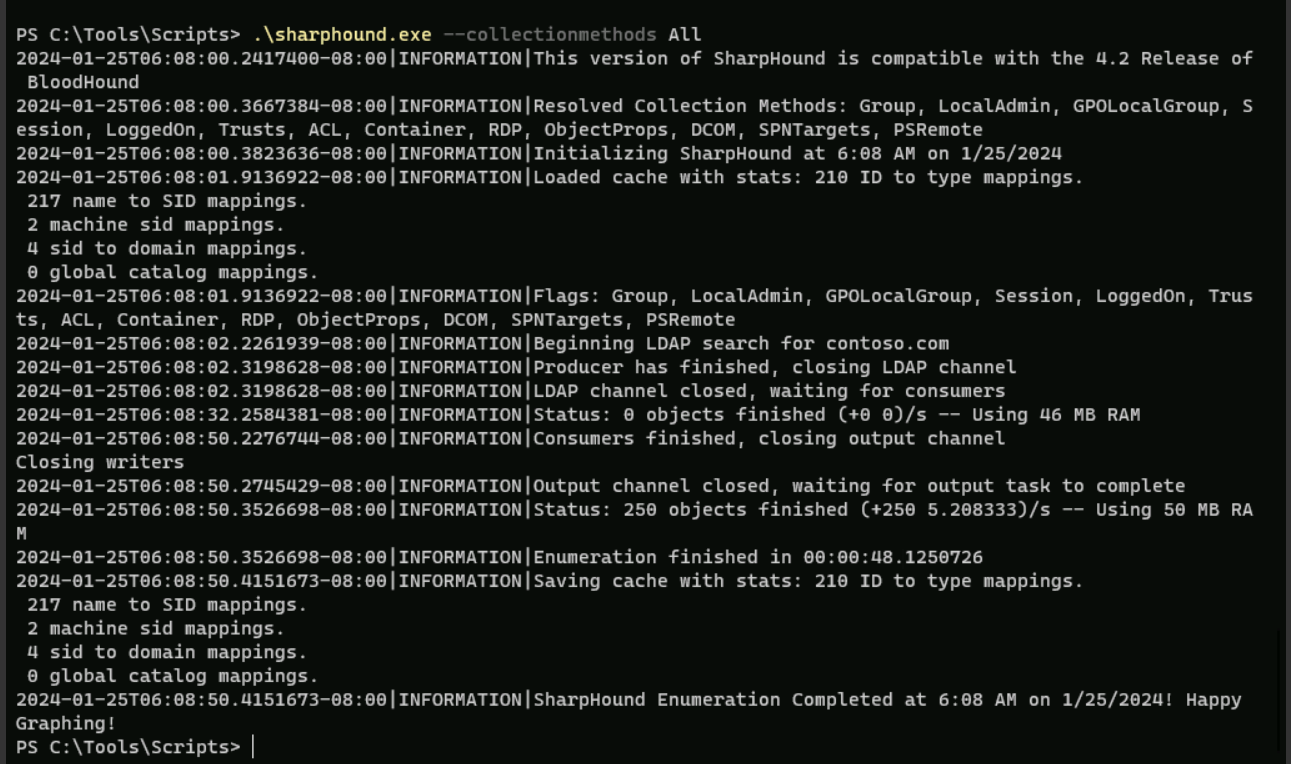


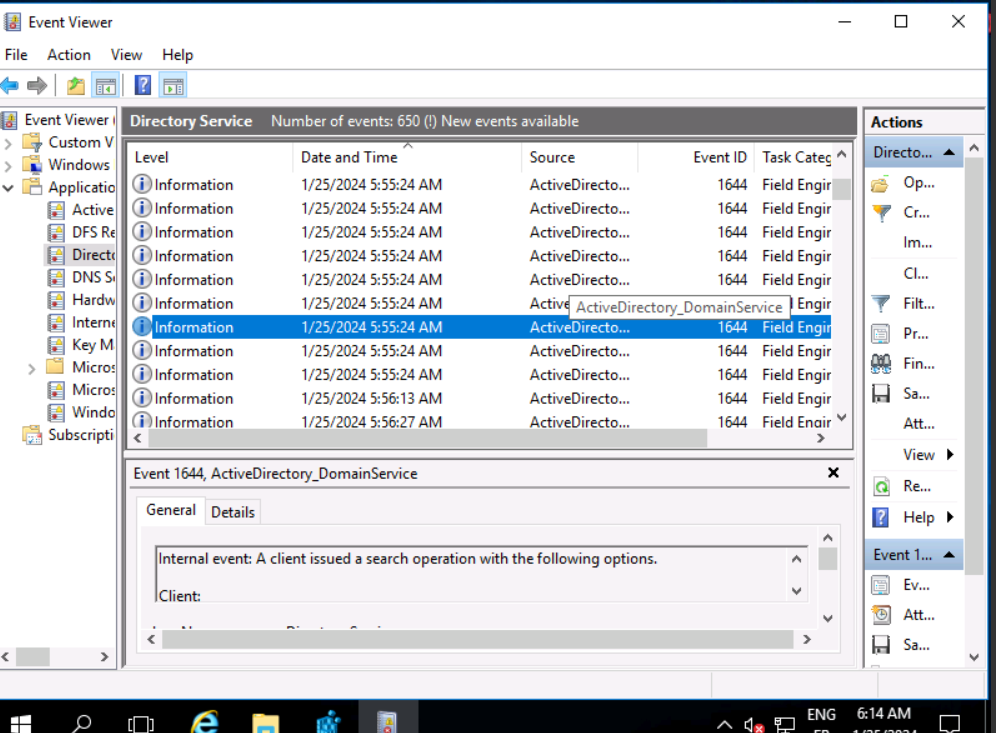


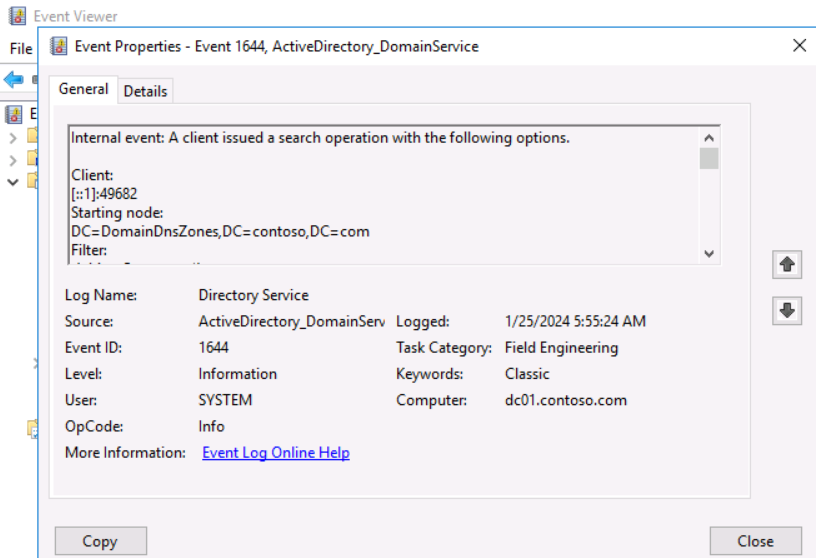






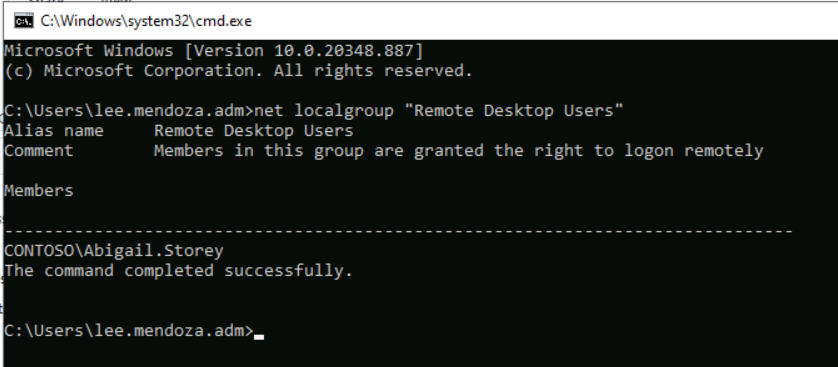


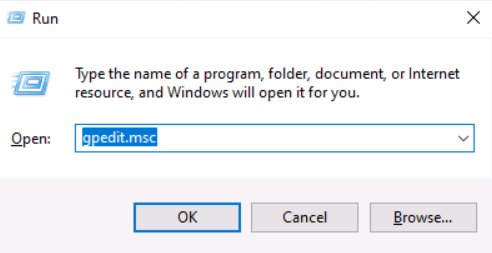


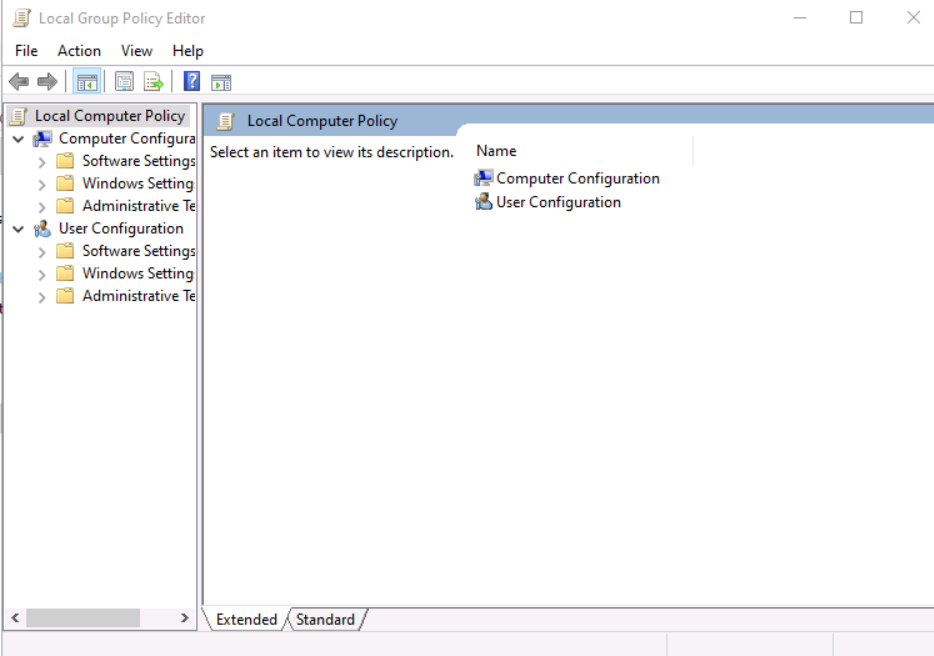


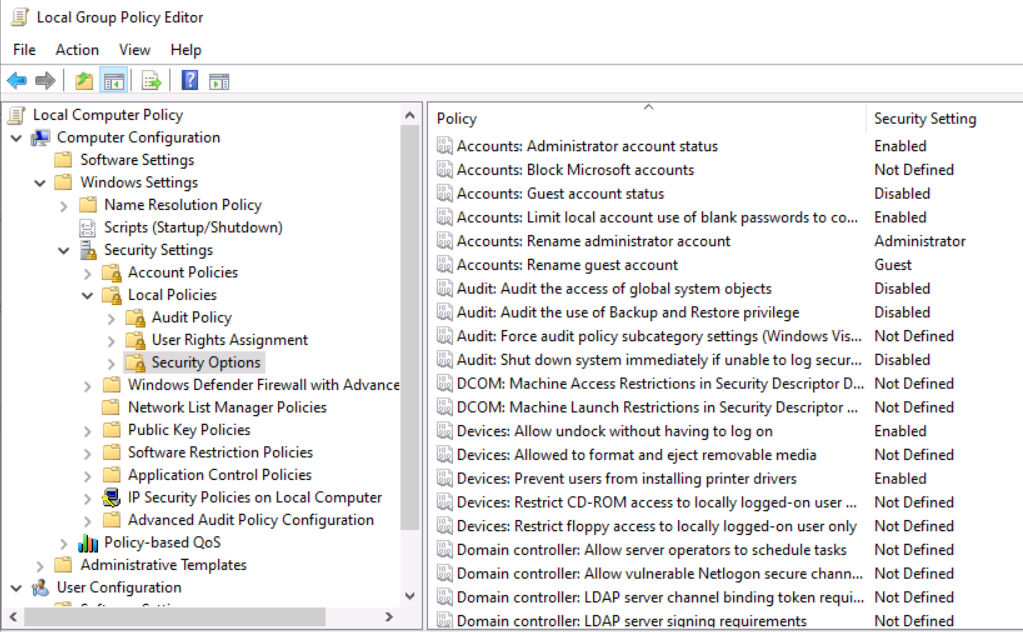
### Exercise 4 - Restrict SAM-R enumeration on a member server

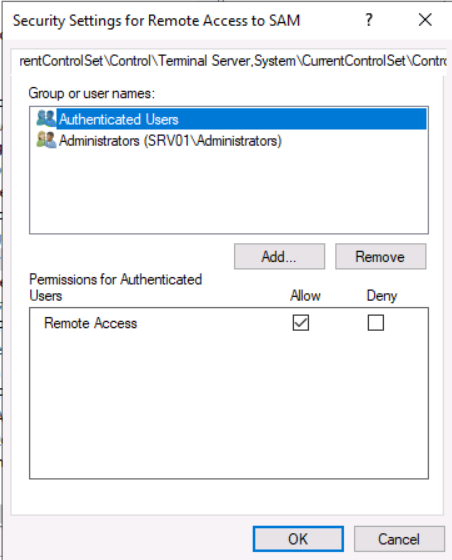
📝 Who is a member of the group?

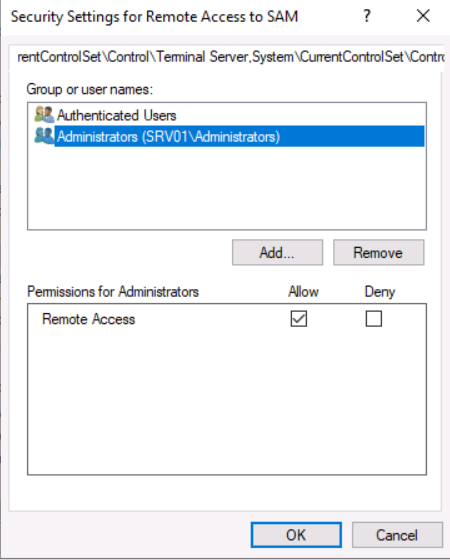










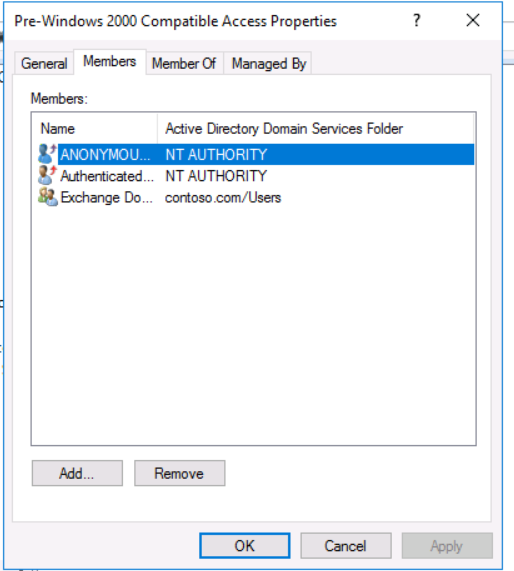


📝 Why is using a group policy recommended to use a group policy for these settings?

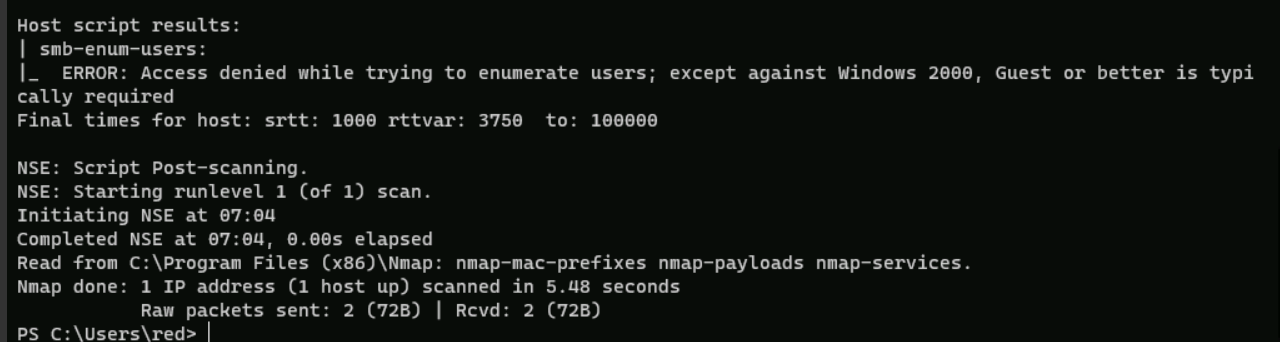
L’utilisation d’une stratégie de groupe est recommandée pour ces paramètres car elle permet une configuration centralisée et cohérente des politiques des ordinateurs et des utilisateurs à travers un réseau, améliorant ainsi la sécurité et la gestion.

### Exercise 5 - Enumerate domain users and group anonymously

📝 Who else is a member of this group in the lab?



📝 What is the error message?





### Exercise 6 - Restrict SMB enumeration [optional]

📝 Try to run the previous command without the "| Out-GridView -Title "SMB permissions". What is the difference?

📝 Do you still see connections?

