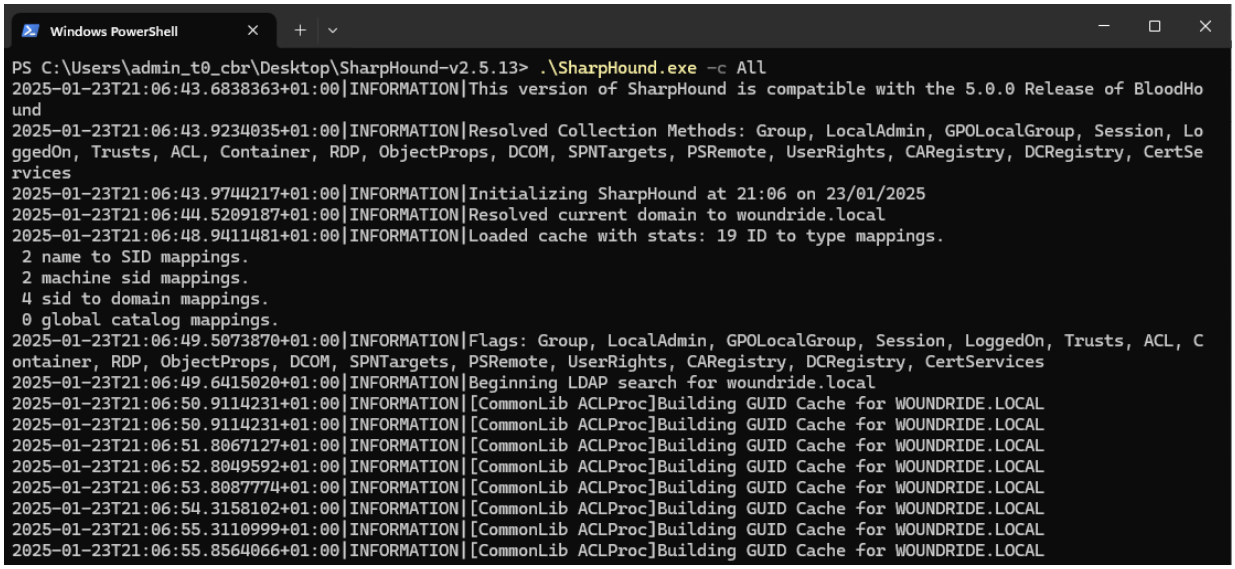
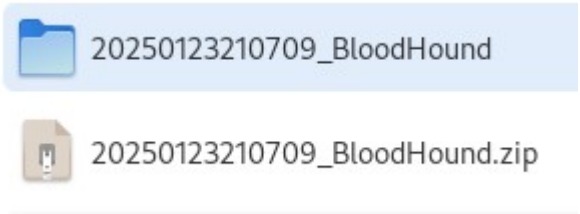
SharpHound / BloodHound

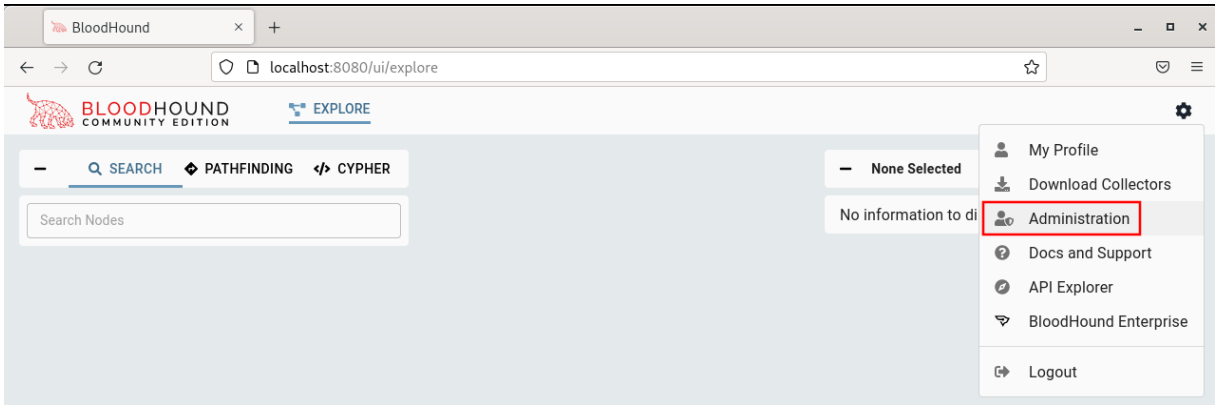
Collecte des infos avec SharpHound :

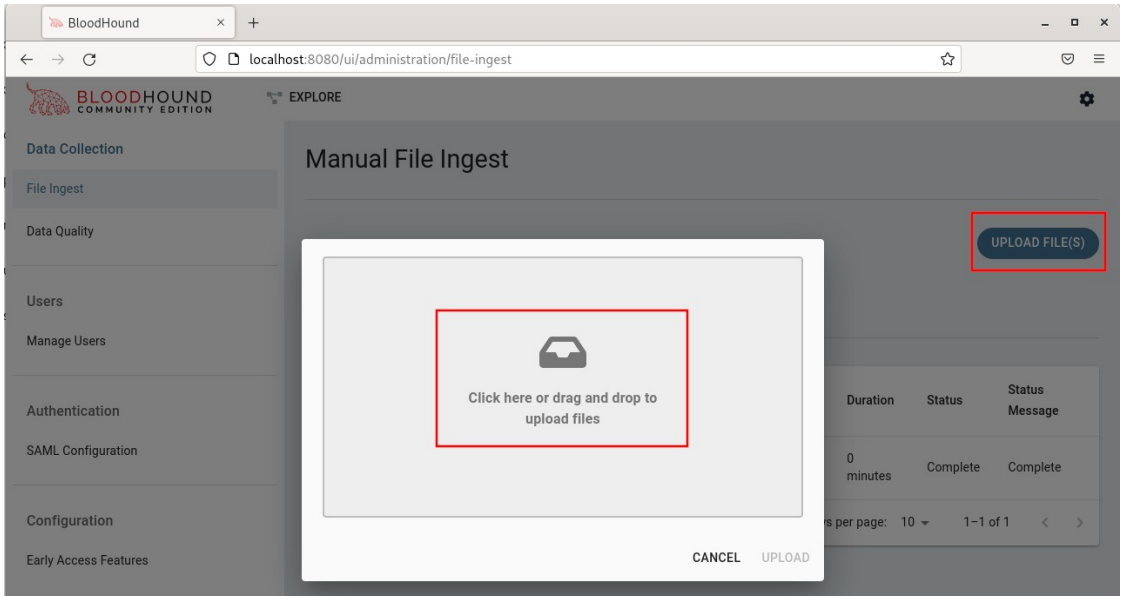


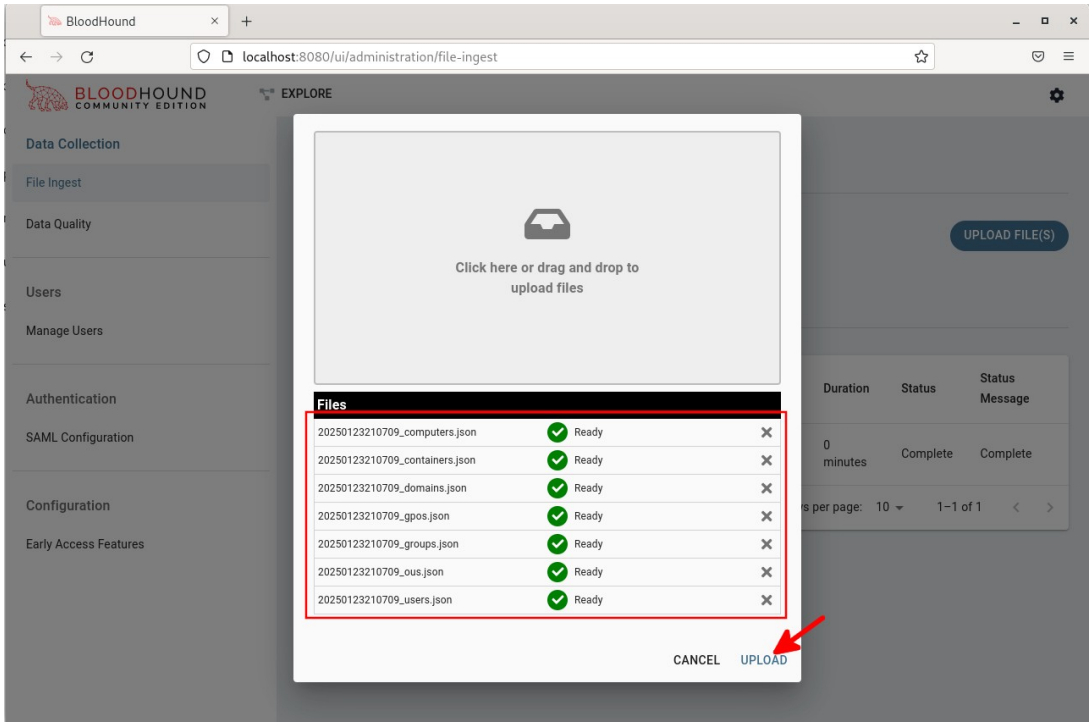
Extraction des infos du Zip :



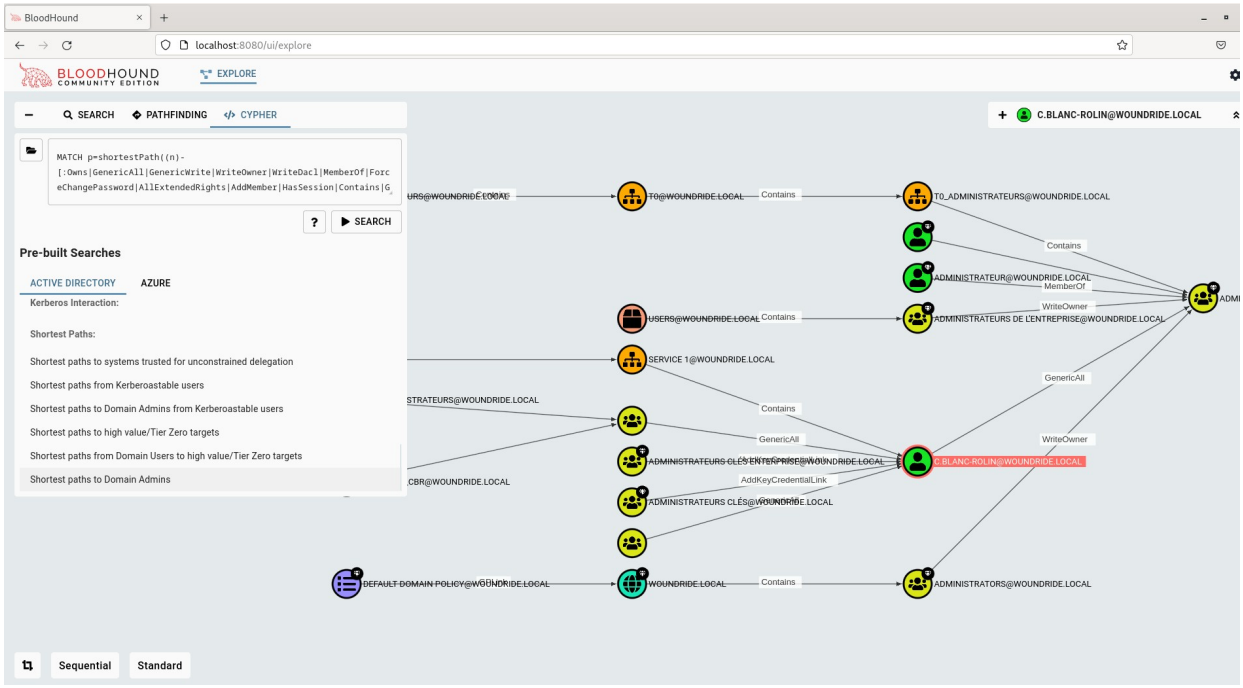
Import dans BloodHound :







On retrouve ici les chemins les plus rapides pour devenir admin de domaine :


BloodHound
localhost:8080/ui/explore
BLOODHOUND
COMMUNITY EDITION
EXPLORE
SEARCH
PATHFINDING
CYPHER
C.BLANC-ROLIN@WOUNDRIDE.LOCAL
MATCH p=shortestPath((n)-
[:Owns|GenericAll|GenericWrite|WriteOwner|WriteDacl|MemberOf|Forc
eChangePassword|AllExtendedRights|AddMember|HasSession|Contains|G
?
SEARCH
Pre-built Searches
ACTIVE DIRECTORY
AZURE
Kerberos Interaction:
Shortest Paths:
Shortest paths to systems trusted for unconstrained delegation
Shortest paths from Kerberoastable users
Shortest paths to Domain Admins from Kerberoastable users
Shortest paths to high value/Tier Zero targets
Shortest paths from Domain Users to high value/Tier Zero targets
Shortest paths to Domain Admins
T0@WOUNDRIDE.LOCAL
Contains
T0_ADMINISTRATEURS@WOUNDRIDE.LOCAL
ADMINISTRATEUR@WOUNDRIDE.LOCAL
MemberOf
USERS@WOUNDRIDE.LOCAL
ADMINISTRATEURS DE L'ENTREPRISE@WOUNDRIDE.LOCAL
WriteOwner
SERVICE 1@WOUNDRIDE.LOCAL
GenericAll
ADMINISTRATEURS CLÉS@WOUNDRIDE.LOCAL
AddKeyCredentialLink
DEFAULT DOMAIN POLICY@WOUNDRIDE.LOCAL
WOUNDRIDE.LOCAL
ADMINISTRATORS@WOUNDRIDE.LOCAL
Sequential
Standard