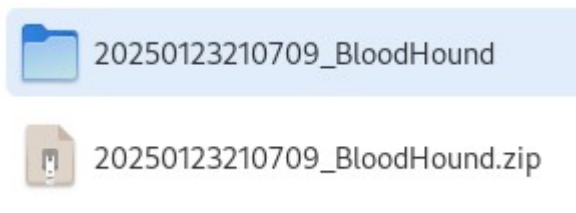


## SharpHound / BloodHound

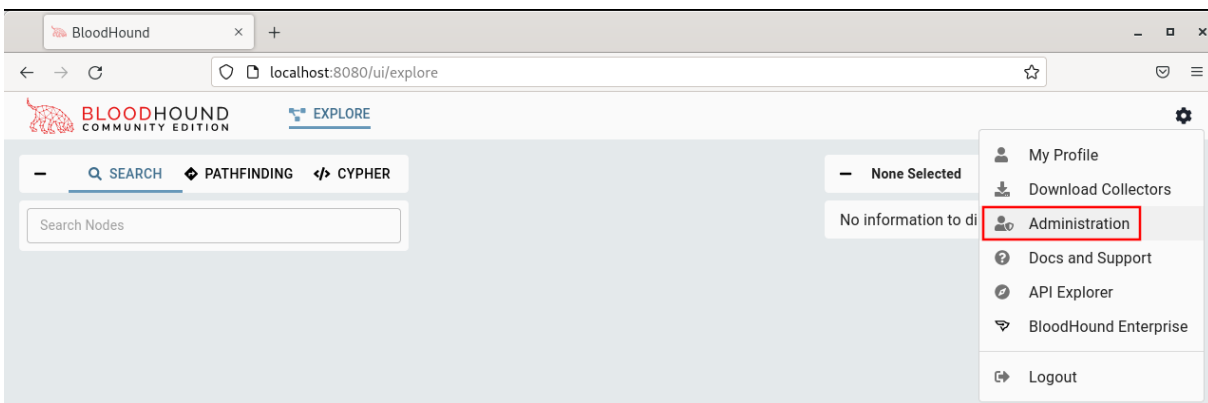
Collecte des infos avec SharpHound :

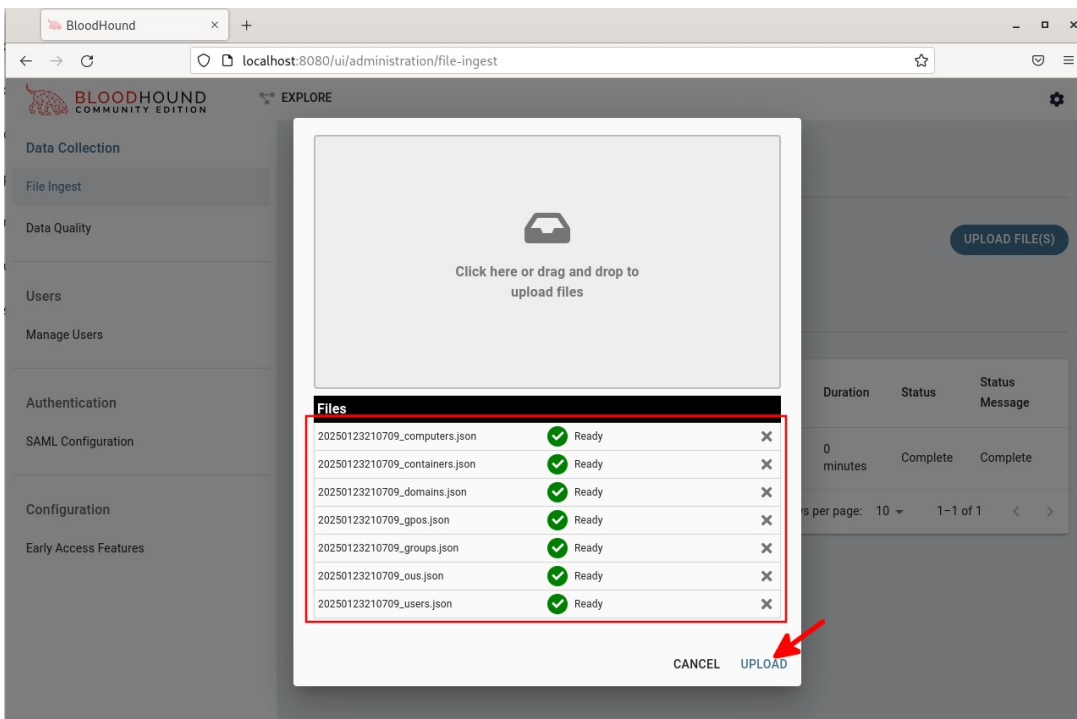
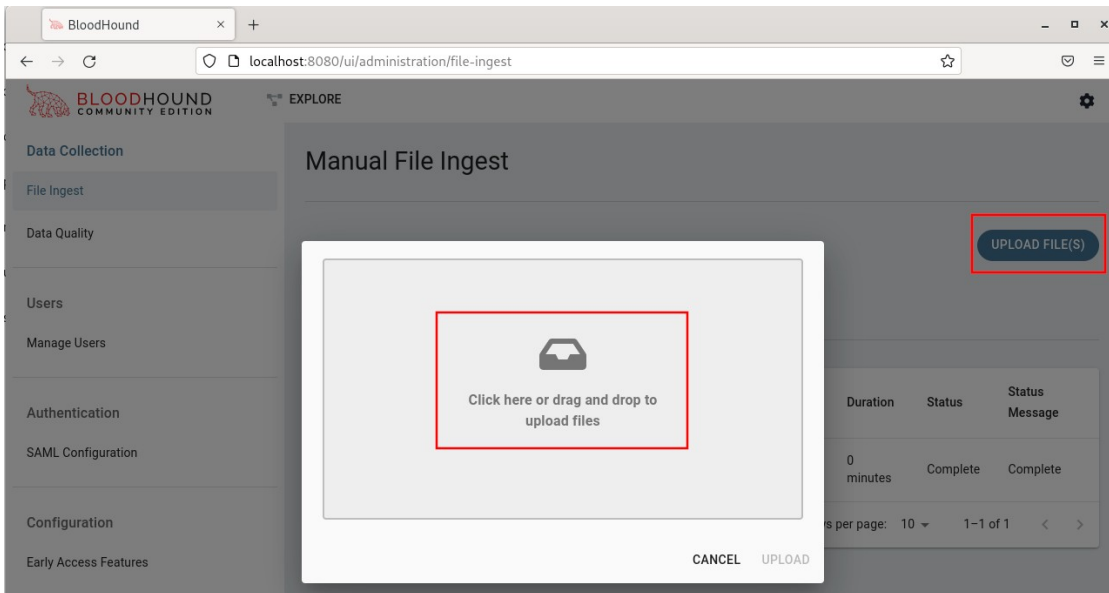
```
Windows PowerShell
PS C:\Users\admin_t0_cbr\Desktop\SharpHound-v2.5.13> .\SharpHound.exe -c All
2025-01-23T21:06:43.6838363+01:00|INFORMATION|This version of SharpHound is compatible with the 5.0.0 Release of BloodHound
2025-01-23T21:06:43.9234035+01:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, UserRights, CARegistry, DCRegistry, CertServices
2025-01-23T21:06:43.9744217+01:00|INFORMATION|Initializing SharpHound at 21:06 on 23/01/2025
2025-01-23T21:06:44.5209187+01:00|INFORMATION|Resolved current domain to woundride.local
2025-01-23T21:06:48.9411481+01:00|INFORMATION|Loaded cache with stats: 19 ID to type mappings.
  2 name to SID mappings.
  2 machine sid mappings.
  4 sid to domain mappings.
  0 global catalog mappings.
2025-01-23T21:06:49.5073870+01:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, UserRights, CARegistry, DCRegistry, CertServices
2025-01-23T21:06:49.6415020+01:00|INFORMATION|Beginning LDAP search for woundride.local
2025-01-23T21:06:50.9114231+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:50.9114231+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:51.8067127+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:52.8049592+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:53.8087774+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:54.3158102+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:55.3110999+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
2025-01-23T21:06:55.8564066+01:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for WOUNDRIDE.LOCAL
```

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

MATCH p=shortestPath{(n)-[:Owns|GenericAll|GenericWrite|WriteOwner|WriteDacl|MemberOf|ForceChangePassword|AllExtendedRights|AddMember|HasSession|Contains]G

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

UR@WOUNDRIDE.LOCAL

FTO@WOUNDRIDE.LOCAL

TO\_ADMINISTRATEURS@WOUNDRIDE.LOCAL

ADMINISTRATEUR@WOUNDRIDE.LOCAL

ADMINISTRATEURS DE L'ENTREPRISE@WOUNDRIDE.LOCAL

ADM

USERS@WOUNDRIDE.LOCAL

Contains

WriteOwner

MemberOf

GenericAll

Service 1@WOUNDRIDE.LOCAL

STRATEURS@WOUNDRIDE.LOCAL

Contains

GenericAll

WriteOwner

CBR@WOUNDRIDE.LOCAL

ADMINISTRATEURS GLE@WOUNDRIDE.LOCAL

ADMINISTRATEURS GLE@WOUNDRIDE.LOCAL

ADMINISTRATEURS CLES@WOUNDRIDE.LOCAL

ADMINISTRATEURS CLES@WOUNDRIDE.LOCAL

ADDKEYCREDENTIALLINK

C.BLANC-ROLIN@WOUNDRIDE.LOCAL

WriteOwner

DEFAULT DOMAIN POLICY@WOUNDRIDE.LOCAL

WOUNDRIDE.LOCAL

Contains

ADMINISTRATORS@WOUNDRIDE.LOCAL

Sequential Standard