Lien vers le drawio : https://drive.google.com/file/d/1\_vR\_ENe-VM03ji44uiLKJ2tZPcJpntGg/view?usp=sharing

On utilise Active Directory

Bruteforce

Phishing

Site Web

Crontab (clean utilisateurs inactifs)

Reverse shell

Site Web → accès site web via bruteforce de mdp → injection sql récupération adresse mail → phishing → accès plus haut niveau = nouvelle interface → injection de commande pour modifier fichier crontab → créé nouvel utilisateur/reverse shell

Bloodhound