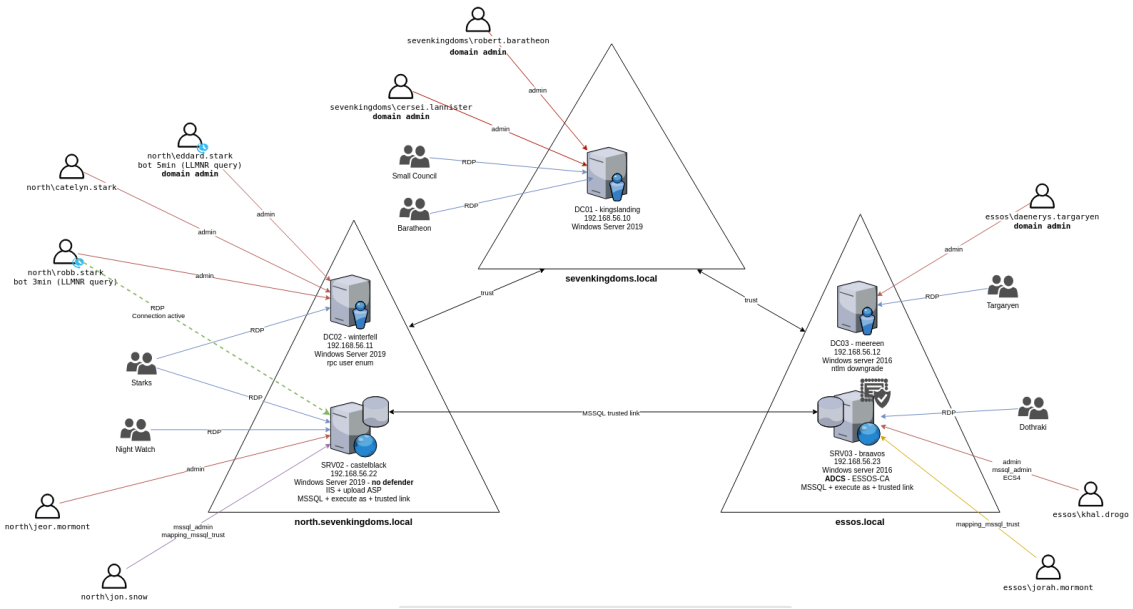
GOAD

GOAD is the first and main lab of this project. It contains 3 domains and 2 forest.



Servers

This lab is actually composed of five virtual machines:

domain sevenkingdoms.local

- **kingslanding** : DC01 running on Windows Server 2019 (with windefender enabled by default)

domain north.sevenkingdoms.local

- **winterfell** : DC02 running on Windows Server 2019 (with windefender enabled by default)
- **castelblack** : SRV02 running on Windows Server 2019 (with windefender **disabled** by default)

domain essos.local

- **meereen** : DC03 running on Windows Server 2016 (with windefender enabled by default)
- **braavos** : SRV03 running on Windows Server 2016 (with windefender enabled by default)

WRITEUP

- All the writeups of the Game Of Active Directory lab are available on mayfly's blog : https://mayfly277.github.io/categories/goad/

Computers Users and group permissions

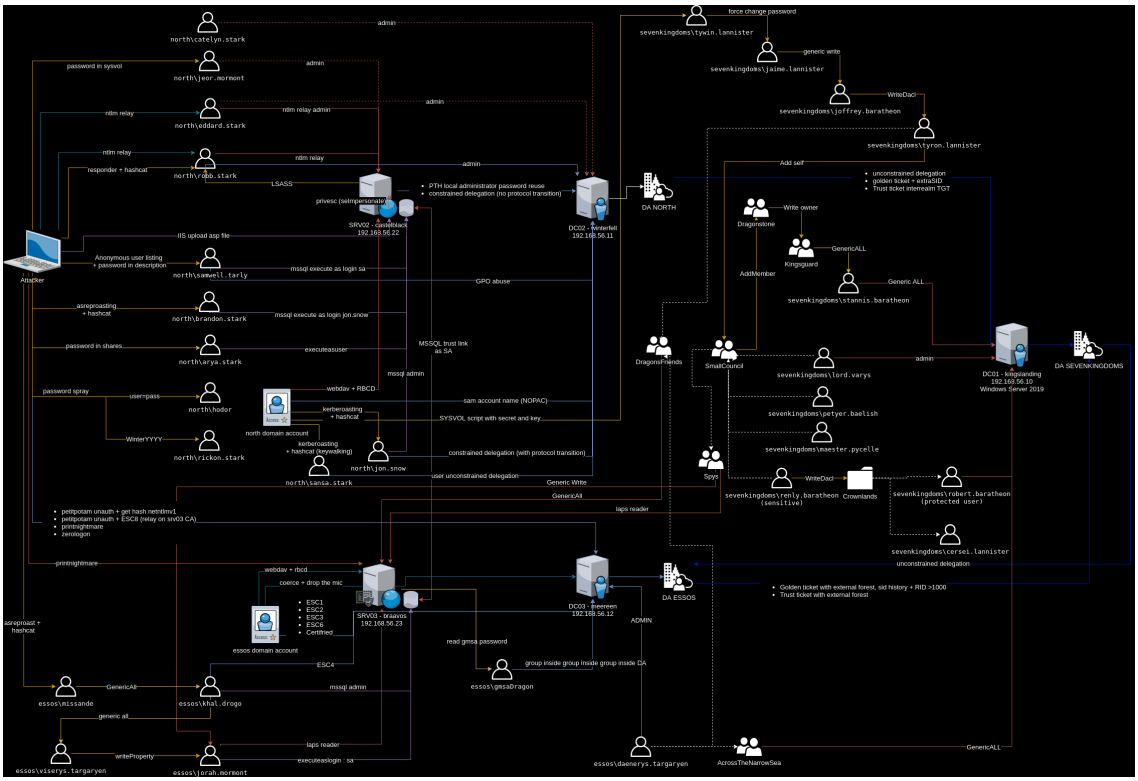
- **SEVENKINGDOMS / sevenkingdoms.local**
  - DC01 : kingslanding.sevenkingdoms.local (Windows Server 2019) (SEVENKINGDOMS DC)
    - Admins : robert.baratheon (U), cersei.lannister (U)
    - RDP: Small Council (G)
- **NORTH / north.sevenkingdoms.local**
  - DC02 : winterfell.north.sevenkingdoms.local (Windows Server 2019) (NORTH DC)
    - Admins : eddard.stark (U), catelyn.stark (U), robb.stark (U)
    - RDP: Stark(G)
  - SRV02 : castelblack.essos.local (Windows Server 2019) (IIS, MSSQL, SMB share)
    - Admins: jeor.mormont (U)
    - RDP: Night Watch (G), Mormont (G), Stark (G)
    - IIS : allow asp upload, run as NT Authority/network
    - MSSQL:
      - admin : jon.snow
      - impersonate :

        - execute as login : samwel.tarlly -> sa
        - execute as user : arya.stark -> dbo
      - link :
        - to braavos : jon.snow -> sa

- **ESSOS / essos.local**
  - DC03 : meereen.essos.local (Windows Server 2016) (ESSOS DC)
    - Admins: daenerys.targaryen (U)
    - RDP: Targaryen (G)
  - SRV03 : braavos.essos.local (Windows Server 2016) (MSSQL, SMB share)
    - Admins: khal.drogo (U)
    - RDP: Dothraki (G)
    - MSSQL :
      - admin : khal.drogo
      - impersonate :
        - execute as login : jorah.mormont -> sa
      - link:
        - to castelblack: jorah.mormont -> sa

Users/Groups and associated scenarios

- Graph of some scenarios is available here :



NORTH.SEVENKINGDOMS.LOCAL

- STARKS: RDP on WINTERFELL AND CASTELBLACK
  - arya.stark: Execute as user on mssql, pass on all share
  - eddard.stark: DOMAIN ADMIN NORTH/ (bot 5min) LLMRN request to do NTLM relay with responder
  - catelyn.stark:
  - robb.stark: bot (3min) RESPONDER LLMR / lsass present user
  - sansa.stark: keywalking password / unconstrained delegation
  - brandon.stark: ASREP_ROASTING
  - rickon.stark: pass spray WinterYYYY
  - jon.snow: mssql admin / KERBEROASTING / mssql trusted link
  - hodor: PASSWORD SPRAY (user=password)
- NIGHT WATCH: RDP on CASTELBLACK
  - samwell.tarly: Password in ldap description / mssql execute as login GPO abuse (Edit Settings on "STARKWALLPAPER" GPO)

    - jon.snow: (see starks)
    - jeor.mormont: (see mormont)
- MORMONT: RDP on CASTELBLACK
    - jeor.mormont: Admin castelblack, pass in sysvol script
- AcrossTheSea : cross forest group

SEVENKINGDOMS.LOCAL

- LANISTERS
    - tywin.lannister: ACE forcechangepassword on jaime.lanister, password on sysvol cyphered
    - jaime.lannister: ACE genericwrite-on-user joffrey.baratheon
    - tyron.lannister: ACE self membership on small council
    - cersei.lannister: DOMAIN ADMIN SEVENKINGDOMS
- BARATHEON: RDP on KINGSLANDING
    - robert.baratheon: DOMAIN ADMIN SEVENKINGDOMS, protected user
    - joffrey.baratheon: ACE Write DACL on tyron.lannister
    - renly.baratheon: WriteDACL on container, sensitive user
    - stannis.baratheon: ACE genericall-on-computer kingslanding
- SMALL COUNCIL : ACE add Member to group dragon stone / RDP on KINGSLANDING
    - petyer.baelish:
    - lord.varys: ACE genericall-on-group Domain Admins and sdholder
    - maester.pycelle:
- DRAGONSTONE : ACE Write Owner on group KINGSGUARD
- KINGSGUARD : ACE generic all on user stannis.baratheon
- AccorsTheNarrowSea: cross forest group

ESSOS.LOCAL

- TARGERYEN
    - missande : ASREP roasting, generic all on khal
    - daenerys.targaryen: DOMAIN ADMIN ESSOS

    - viserys.targaryen: ACE write property on jorah.mormont
    - jorah.mormont: mssql execute as login / mssql trusted link / Read LAPS Password
- DOTHRAKI
    - khal.drogo: mssql admin / GenericAll on viserys (shadow credentials) / GenericAll on ECS4
- DragonsFriends: cross forest group
- Spys: cross forest group / Read LAPS password / ACL generic all jorah.mormont