Doku: AECID-WIN-Testbed

1. Schwachstellen

Folgende Konfigurationen wurden durchgeführt:

- SPN – wsadmin (atb-ansible-primarydc)
- PrivEsc via vulnerable Task –
    - Rolle: atb-ansible-winvulnserver
    - PreReq: SeBatchLogonRight (Wird via GPO in primarydc vergeben)
    - Task läuft als wsadmin und führt ein PS-Skript (WriteLog.ps1) aus.
        - ACL für das Skript wurde angepasst auf DomainUsers
    - SSDL für den Task angepasst damit es enumeriert werden kann via „schtasks“
- Grundsätzlich haben alle User RDP Rechte (GPO).
- Für das Angriffsszenario wurde Alice auch als Remotemanagementuser hinzugefügt.

2. Post-Exploit

- Evil-WinRM mit den Credentials von Alice (non-priv)
- schtasks um den vulnerablen Task zu finden
    - schtasks /query /TN
    - schtasks /query /fo LIST /v /TN "\WriteLog"
- Skript modifizieren → Add-LocalGroupMember
- Schtasks um den vulnerablen Task auszuführen
    - schtasks /run /tn WriteLog
- Neue WinRM Session für den privilegierten Token

3. Ansible-Rollen

Bis auf den PrimaryDC, ist die Unterteilung der Rollen in Server und Service. Daher Server enthält die Basiskonfiguration + DomainJoin und Service ist dann z.B. der Webserver. Folgende Reihenfolge ergibt sich pro Host.

1. PrimaryDC
2. msclient – SecondaryDC
3. Kafka (Ubuntu)
4. msclient - WEC
5. msclient – Webserver – vulnserver (Bei Bedarf wo anders)
6. ghostsserver (Ubuntu)
7. msclient – ghostsagent

Grafik mit den Abhängigkeiten werden noch überarbeitet! (MemberServer + Client = msclient)

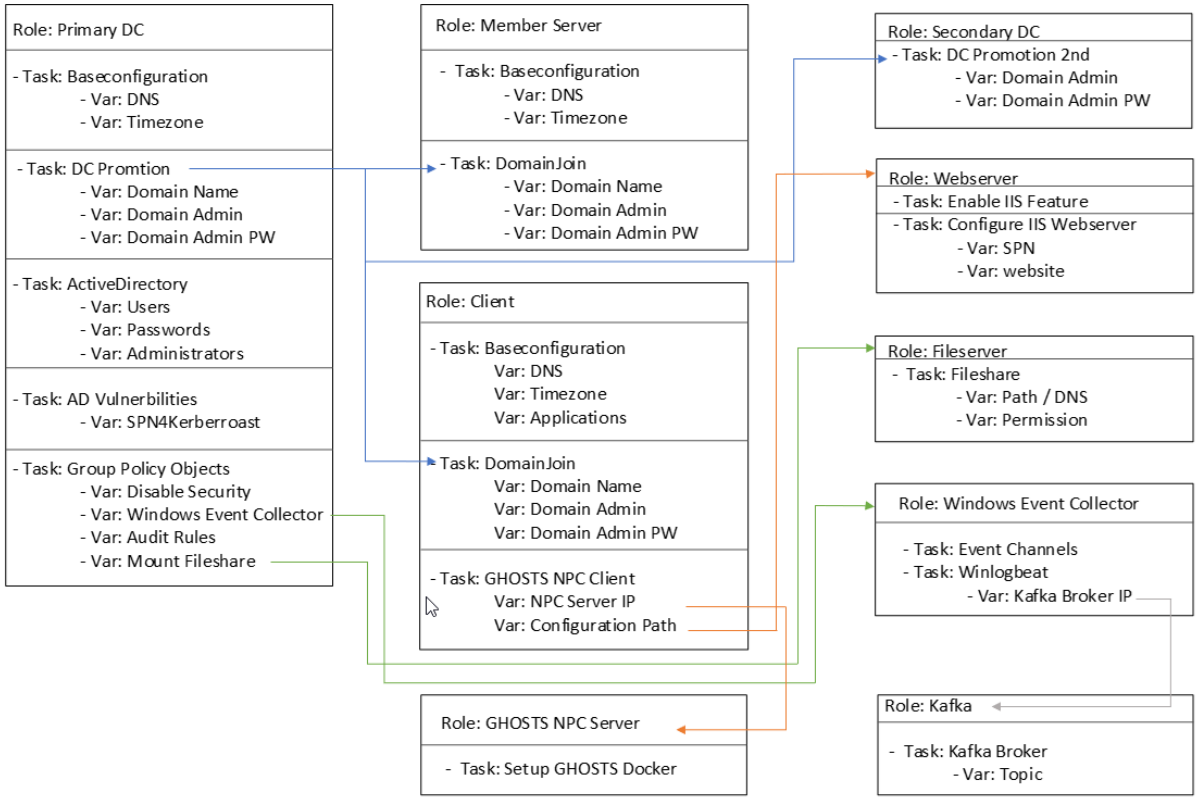

Figure 0-1 Dependency

4. Attackmate

Prod_Killchain.yml