Les risques liés à l'attribut dSHeuristics

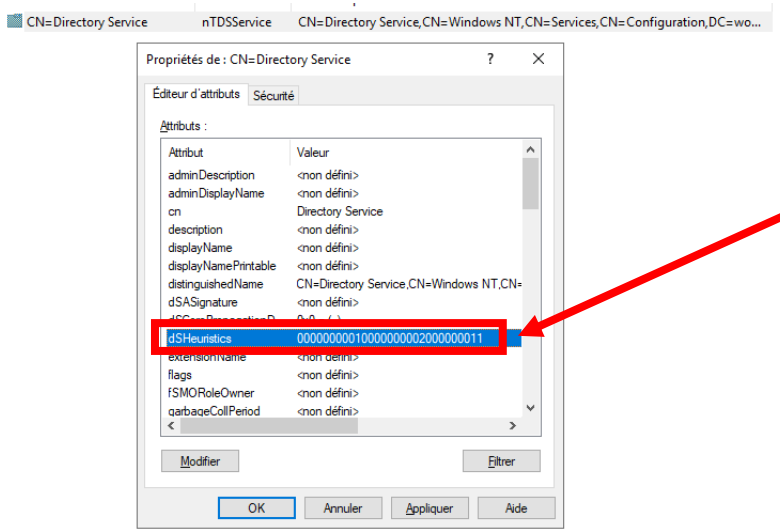
(environnement Active Directory)

Version 1.0 - 2025

L'attribut dSHeuristics : c'est quoi ?

Un garde-fou « désactivable » contre plusieurs problèmes de configuration impactant la sécurité de l'AD :

- Un attribut de l'objet NTDS-Service, qui contient les informations sur la configuration de la forêt du service d'annuaire



Configuration optimale (niveau 5 ADS) Apparaît comme <non défini> nativement (niveau 4 ADS)

- Disposant de 29 caractères, dont **27 paramètres** (le 10ème caractère vaut 1 et le 20ème vaut 2)

Les paramètres dangereux identifiés par l'ANSSI

Dans le cadre de l'audit ADS, l'ANSSI contrôle 6 paramètres sur les 27 possibles :

Paramètres dSHeuristics dangereux

vuln_dsheuristics_bad EN

Des paramètres dangereux sont configurés dans l'attribut `dSHeuristics`. Cette vulnérabilité peut apparaître aux niveaux 1 et 2 selon le problème rencontré :

- 1 si `fAllowAnonNSPI` est différent de 0 ;
- 1 si `dwAdminSDExMask` est différent de 0 ;
- 2 si `fLDAPBlockAnonOps` est égal à 2 ;
- 2 si `DoNotVerifyUPNAndOrSPNUniqueness` est différent de 0 (KB5008382) ;
- 2 si `AttributeAuthorizationOnLDAPAdd` est égal à 2 (KB5008383) ;
- 2 si `BlockOwnerImplicitRights` est égal à 2 (KB5008383) ;
- 4 si `AttributeAuthorizationOnLDAPAdd` est différent de 1 (KB5008383) ;
- 4 si `BlockOwnerImplicitRights` est différent de 1 (KB5008383).

Le tableau ci-dessous liste les valeurs explicitement définies dans l'attribut `dSHeuristics`. Les valeurs vides signifient qu'aucune valeur n'a été définie, et que la valeur par défaut s'applique. La valeur `0000000001000000000200000011` permet par exemple d'atteindre le niveau 5 : elle met tous les champs à leur valeur par défaut, sauf `BlockOwnerImplicitRights` et `AttributeAuthorizationOnLDAPAdd` qui sont mis à 1.

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « fAllowAnonNSPI » :

0000000**0**01000000002000000011

- 8ème caractère / 29
- Si défini à 1, autorise les connexions NSPI (utilisation par Outlook et Exchange) anonyme à l'Active Directory
- À l'aide du script exchanger.py de la suite Impacket par exemple, il serait donc possible d'extraire la liste de tous les utilisateurs de l'AD via l'interface OWA exposée sur Internet
- Afin d'interdire les connexions anonymes, maintenir ce paramètre à 0

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « dwAdminSDExMask » :

- 16ème caractère / 29
- Si la valeur est différente de 0, certains groupes protégés nativement par le processus SDProp et l'objet AdminSDHolder ont été exclus de ce mécanisme

- Rappel : SDProp réapplique automatiquement (toutes les heures par défaut) les autorisations définies sur l'objet AdminSDHolder pour les comptes et groupes protégés

- Afin d'interdire les modifications de privilèges sur les compte protégés, maintenir ce paramètre à 0

0000000001000000002000000011

Les groupes peuvent êtres exclus en implémentant le paramètre ainsi :

- Opérateurs de compte : **1** (0001 en binaire)
- Opérateurs de serveur : **2** (0010 en binaire)
- Opérateurs d'impression : **4** (0100 en binaire)
- Opérateurs de sauvegarde : **8** (1000 en binaire)
- Les 4 groupes : **f** (1111 en binaire)

Les groupes protégés par défaut :

Windows Server 2003 R2 RTM	Windows Server 2003 SP1	Windows Server 2012, Windows Server 2008 R2 Windows Server 2008	Windows Server 2016
Opérateurs de compte	Opérateurs de compte	Opérateurs de compte	Opérateurs de compte
Administrateur	Administrateur	Administrateur	Administrateur
Administrateurs	Administrateurs	Administrateurs	Administrateurs
Opérateurs de sauvegarde	Opérateurs de sauvegarde	Opérateurs de sauvegarde	Opérateurs de sauvegarde
Éditeurs de certificats			
Administrateurs du domaine	Administrateurs du domaine	Administrateurs du domaine	Administrateurs du domaine
Contrôleurs de domaine	Contrôleurs de domaine	Contrôleurs de domaine	Contrôleurs de domaine
Administrateurs de l'entreprise	Administrateurs de l'entreprise	Administrateurs de l'entreprise	Administrateurs de l'entreprise
Krbtgt	Krbtgt	Krbtgt	Krbtgt
Opérateurs d'impression	Opérateurs d'impression	Opérateurs d'impression	Opérateurs d'impression
		Contrôleurs de domaine en lecture seule	Contrôleurs de domaine en lecture seule
Duplicateur	Duplicateur	Duplicateur	Duplicateur
Administrateurs du schéma	Administrateurs du schéma	Administrateurs du schéma	Administrateurs du schéma
Opérateurs de serveur	Opérateurs de serveur	Opérateurs de serveur	Opérateurs de serveur

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « fLDAPBlockAnonOps» :

000000**0**0010000000002000000011

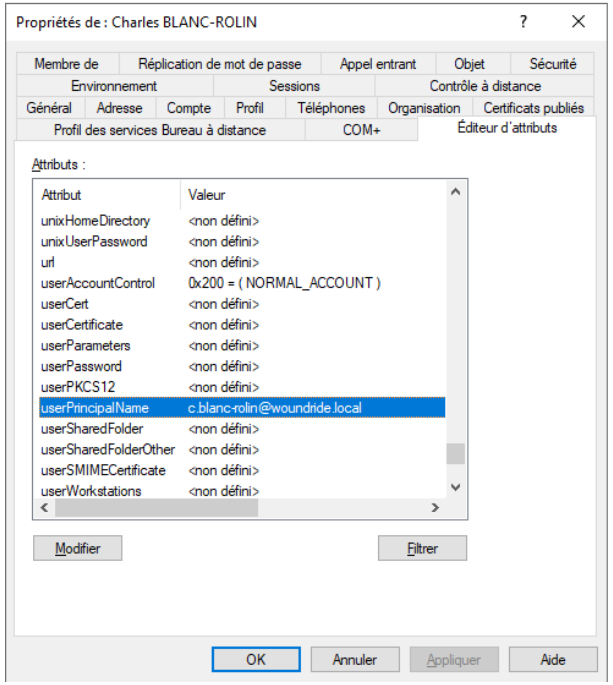
- 7ème caractère / 29
- Si défini à 2, désactive le mécanisme empêchant les connexions LDAP anonymes, implémenté depuis Windows 2003 Server
- Associé à des autorisations anonymes sur l'annuaire, il peut permettre de requêter l'annuaire à distance
- Afin d'interdire les connexions anonymes, maintenir ce paramètre à 0

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « DoNotVerifyUPNAndOrSPNUniqueness » :

00000000010000000002**0**00000011

- 21ème caractère / 29
- Si défini à 1, désactivation du mécanisme permettant de vérifier qu'il n'y a pas de doublons sur l'attribut UPN d'un compte
- Usurpation de compte possible

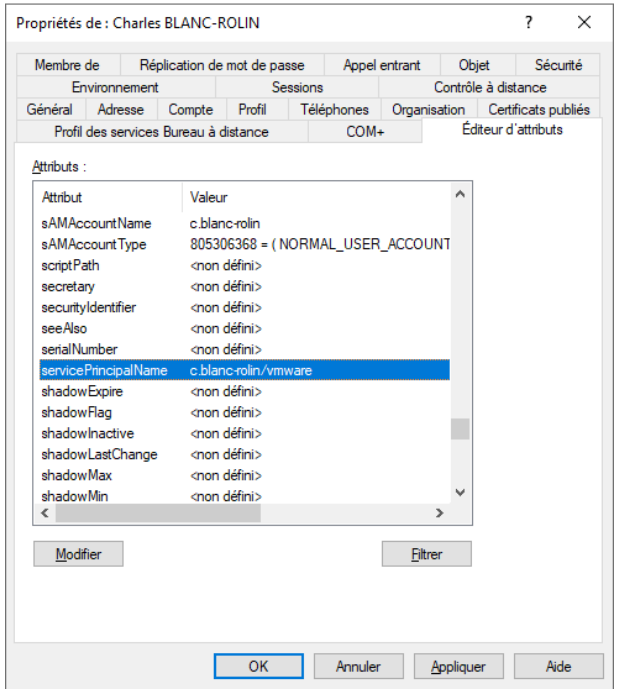


Les paramètres dangereux identifiés par l'ANSSI

Paramètre « DoNotVerifyUPNAndOrSPNUniqueness » :

00000000010000000002**0**00000011

- 21ème caractère / 29
- Si défini à 2, désactivation du mécanisme permettant de vérifier qu'il n'y a pas de doublons sur l'attribut SPN d'un compte
- Pourrait par exemple permettre à un utilisateur de modifier l'attribut SPN d'un compte d'ordinateur / utilisateur, lui attribuer un SPN déjà utilisé par un autre compte et s'authentifier sur un service à sa place via le protocole Kerberos



Les paramètres dangereux identifiés par l'ANSSI

Paramètre « DoNotVerifyUPNAndOrSPNUniqueness » :

00000000010000000002**0**00000011

- 21ème caractère / 29
- Si défini à 3, désactivation des 2 mécanismes vus précédemment
- Pour éviter des usurpations de compte, maintenir ce paramètre à 0

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « AttributeAuthorizationOnLDAPAdd » :

00000000010000000020000000**1**1

- 28ème caractère / 29
- Si valeur à 0 = non défini (niveau 4 ADS)
- Si défini à 2, désactive le mécanisme interdisant l'écriture via LDAP « externe », il est donc possible d'écrire sur l'AD de manière « illégitime »
- Pour éviter des écritures illégitimes dans l'annuaire (création, modification, suppression de comptes…), maintenir ce paramètre à 1

Les paramètres dangereux identifiés par l'ANSSI

Paramètre « BlockOwnerImplicitRights » :

000000000100000000020000000011

- 29ème caractère / 29
- Si valeur à 0 = non défini (niveau 4 ADS)
- Si défini à 2, désactive le mécanisme interdisant l'écriture sur des objets de l'AD à des comptes non privilégiés
- Pour éviter des écritures illégitimes dans l'annuaire (création, modification, suppression de comptes…), maintenir ce paramètre à 1

Exploitation via LDAP d'un paramétrage dangereux de l'attribut dSHeuristics

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -H ldap://192.168.46.2:389 -LLL -b "DC=woundride,DC=local" -x "objectClass=computer" operatingsystem operatingsystemversion
dn: CN=W2019-DC01,OU=T0_DC,OU=T0,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows Server 2019 Standard
operatingSystemVersion: 10.0 (17763)

dn: CN=PC01,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Professionnel
operatingSystemVersion: 10.0 (19044)

dn: CN=PC03,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 7 Professionnel
operatingSystemVersion: 6.1 (7601)

dn: CN=PC02,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Professionnel
operatingSystemVersion: 10.0 (17134)

dn: CN=PC04,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Enterprise
operatingSystemVersion: 10.0 (18362)
```

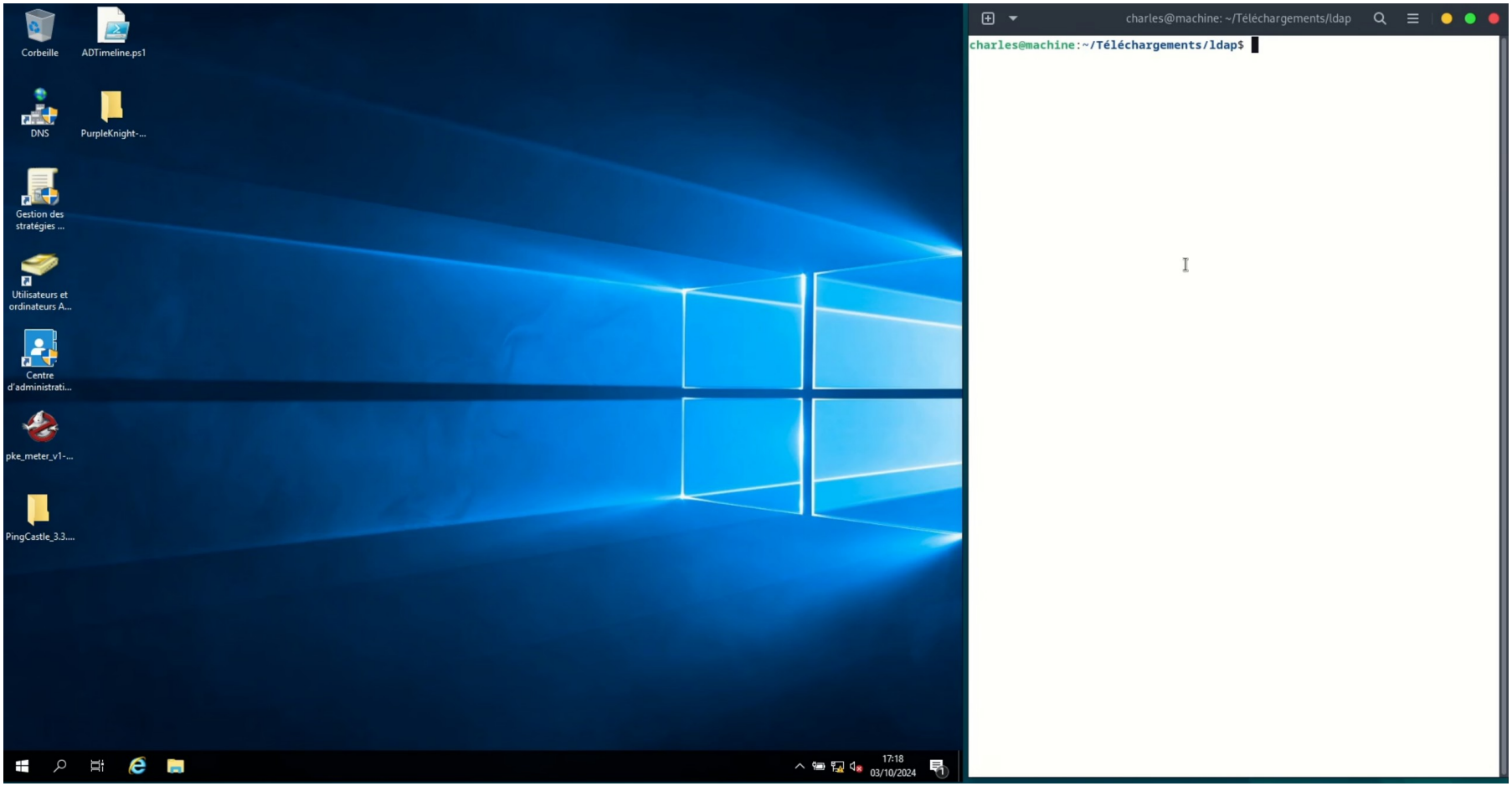
kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -H ldap://192.168.46.2:389 -x -LLL -b "DC=woundride,DC=local" "(&(objectClass=user)(!(objectClass=computer)))
" samaccountname memberof
dn:: Q049SW52aXTDqSxDTj1Vc2VycyxEQz13b3VuZHJpZGUsREM9bG9jYWw=
memberOf:: Q049SW52aXTDqXMsQ049QnVpbHRpbixEQz13b3VuZHJpZGUsREM9bG9jYWw=
sAMAccountName:: SW52aXTDqQ==

dn: CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisate
 urs,DC=woundride,DC=local
memberOf: CN=Service 1,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,
 DC=woundride,DC=local
memberOf: CN=Utilisateurs T2,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woun
 dride,DC=local
sAMAccountName: c.blanc-rolin

dn: CN=[Admin T1] Charles BLANC-ROLIN,OU=T1_Administrateurs,OU=T1,OU=_Utilisat
 eurs,DC=woundride,DC=local
memberOf: CN=Admins T1,OU=T1_Administrateurs,OU=T1,OU=_Utilisateurs,DC=woundri
 de,DC=local
sAMAccountName: admin_t1_cbr

dn: CN=[Admin T2] Charles BLANC-ROLIN,OU=T2_Administrateurs,OU=T2,OU=_Utilisat
 eurs,DC=woundride,DC=local
memberOf: CN=Admins T2,OU=T2_Administrateurs,OU=T2,OU=_Utilisateurs,DC=woundri
 de,DC=local
sAMAccountName: admin_t2_cbr

dn: CN=Louis Pouzin,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=
 woundride,DC=local
memberOf: CN=Service 1,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,
 DC=woundride,DC=local
memberOf: CN=Utilisateurs T2,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woun
 dride,DC=local
sAMAccountName: l.pouzin
```

Exploitation via LDAP d'un paramétrage dangereux de l'attribut dSHeuristics

En particulier ici fLDAPBlockAnonOps, AttributeAuthorizationOnLDAPAdd et BlockOwnerImplicitRights



Les paramètres contrôlés par Purple Knight

Seuls les 2 paramètres de niveau 1 ADS (ANSSI) sont contrôlés :

SECURITY INDICATOR

Anonymous NSPI access to AD enabled

IOE Found

C+ 88 %

SEVERITY: Warning

WEIGHT: 6

Security Frameworks

MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_dsheuristics_bad

Description

Anonymous name service provider interface (NSPI) access on AD is a feature that allows anonymous RPC-based binds to AD. This indicator detects when NSPI access is enabled.

Likelihood of Compromise

NSPI access is rarely ever enabled so if you find it enabled, this should be a cause for concern.

Result

Found risky configuration in the forest that enables anonymous access to NSPI RPC operations.

LastChanged	DistinguishedName	DSHeuristics	Ignored
02/10/2024 17:36:56	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=woundride,DC=local	000000210100000f0002100000022	False

Showing 1 of 1

SECURITY INDICATOR

Operator groups no longer protected by AdminSDHolder and SDProp

IOE Found

B- 91 %

SEVERITY: Warning

WEIGHT: 5

Security Frameworks

MITRE ATT&CK

- Defense Evasion

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_dsheuristics_bad

Description

This indicator checks if dwAdminSDExMask mask on dsHeuristics has been set, which indicates a change to the SDProp behavior that could compromise security. Certain groups can be removed from SDProp protection with this setting.

Likelihood of Compromise

Normally the default behavior for AdminSDHolder SDProp should be left intact. If its behavior is modified, this could indicate an attempt at defense evasion.

Result

Found non-default configuration on the forest for SDProp's protected groups.

LastChanged	DistinguishedName	DSHeuristics	GroupsExcluded	Ignored
20241002153656.0Z	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=woundride,DC=local	000000210100000f0002100000022	Backup Operators, Print Operators, Server Operators, Account Operators	False

Showing 1 of 1

Les paramètres contrôlés par PingCastle

Seul le paramètre relatif à SDProp n'est pas contrôlé :

Check for access without any account to the Name Service Provider Interface (NSPI) protocol

Rule ID:
A-DsHeuristicsAllowAnonNSPI

Description:
The purpose is to identify domains having the NSPI protocol exposed without any required account

Technical explanation:
The way an Active Directory behaves can be controlled via the attribute *DsHeuristics* of *CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration*. A parameter stored in its attribute and whose value is *fAllowAnonNSPI* can be set to allow access to the NSPI protocol without any account.
The NSPI protocol is used internally by Exchange to resolve addresses, and thus can be used to dump all the users of the forest. It can be exposed to the internet via RPC over HTTP.

Advised solution:
The easiest and fastest way to correct this issue is to **replace the eighth (8th) character of the DsHeuristics attribute**. If it is not a 0, replace by 0 to fix the issue.

Points:
5 points if present

Documentation:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/e5899be4-862e-496f-9a38-33950617d2c5
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nspi/6dd0a3ea-b4d4-4a73-a857-add03a89a543
[US]STIG V-8555 - Anonymous Access to AD forest data above the rootDSE level must be disabled.
[FR]ANSSI - Dangerous dsHeuristics settings (vuln1_dsheuristics_bad) 1
[MITRE]T1110.003 Brute Force: Password Spraying

Check for access without any account via a forest wide setting

Rule ID:
A-DsHeuristicsAnonymous

Description:
The purpose is to identify domains having a forest setting which allows access to the domain without any account

Technical explanation:
The way an Active Directory behaves can be controlled via the attribute *DsHeuristics* of *CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration*. A parameter stored in its attribute and whose value is *fLDAPBlockAnonOps* can be set to allow access without any account on the **whole forest level**.
It is possible to verify the results provided by the PingCastle solution by using a Kali Linux distribution. You should run *rpcclient -U " target_ip_address* and press enter at the password prompt to finally type *enumdomusers*.

Advised solution:
The easiest and fastest way to correct this issue is to **replace the seventh (7th) character of the DsHeuristics attribute**. If it is a 2, replace by 0 to fix the issue.

Points:
5 points if present

Documentation:
https://msdn.microsoft.com/en-us/library/cc223560.aspx
https://support.microsoft.com/en-us/help/326690/anonymous-ldap-operations-to-active-directory-are-disabled-on-windows
[US]STIG V-8555 - Anonymous Access to AD forest data above the rootDSE level must be disabled.
[FR]ANSSI - Dangerous dsHeuristics settings (vuln2_dsheuristics_bad) 2
[MITRE]T1110.003 Brute Force: Password Spraying

Check if the UPN and SPN uniqueness check has been disabled

Rule ID:
A-DsHeuristicsDoNotVerifyUniqueness

Description:
The purpose is to identify domains having the SPN and UPN uniqueness check disabled

Technical explanation:
The way an Active Directory behaves can be controlled via the attribute *DsHeuristics* of *CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration*. A parameter stored in its attribute and whose value is *DoNotVerifyUPNAndOrSPNUniqueness* can be set to disable the UPN or SPN check.
This setting has been introduced to overwrite the mitigation of the vulnerability CVE-2021-42282 fixed by the KB5008382.

Advised solution:
The easiest and fastest way to correct this issue is to **replace the 21th character of the DsHeuristics attribute**. If it is not a 0, replace by 0 to fix the issue.

Points:
5 points if present

Documentation:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/e5899be4-862e-496f-9a38-33950617d2c5
https://support.microsoft.com/en-us/topic/kb5008382-verification-of-uniqueness-for-user-principal-name-service-principal-name-and-the-service-principal-name-alias-cve-2021-42282-4651b175-290c-4e59-8fcb-e4e5cd0cdb29
[FR]ANSSI - Dangerous dsHeuristics settings (vuln2_dsheuristics_bad) 2
[MITRE]T1187 Forced Authentication

Les paramètres contrôlés par PingCastle

Les 2 derniers paramètres sont contrôlés dans une règle unique :

Check if the mitigation for CVE-2021-42291 has been enabled

Rule ID:
A-DsHeuristicsLDAPSecurity

Description:
The purpose is to identify domains having mitigation for CVE-2021-42291 not set to enabled

Technical explanation:
The way an Active Directory behaves can be controlled via the attribute *DsHeuristics* of *CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration*.
A parameter stored in its attribute and whose value is *LDAPAddAutZVerifications* and *LDAPOwnerModify* can be set to modify the mitigatation of CVE-2021-42291.
The KB5008383 has introduced changes to default security descriptor of Computer containers to add audit and limit computer creation without being admin.
Indeed, it is recommended to not let anyone create computer accounts as they can be used to abuse Kerberos or to perform relay attacks.

Mitigations in CVE-2021-42291 consist of 3 choices to be set on 2 settings.
They are named LDAPAddAutZVerifications and LDAPOwnerModify and are respectively the 28th and 29th character of this string.
For the expected values:
- With the value 0 (the default), it enables an additional audit mechanism
- With the value 1 (recommended), it enforces new security permissions, especially to require an action of the domain admin when unusual actions are performed
- With the value 2 (not recommended), it disables the audit mechanism that has been added by default and do not enable the new security permissions

Advised solution:
The easiest and fastest way to correct this issue is to **replace the 28th and 29th character of the DsHeuristics attribute**.
The value of LDAPAddAutZVerifications and LDAPOwnerModify should be set to 1.

Open the procedure embedded into the KB5008383 to apply this mitigation and change the DsHeuristics value.

Note: You have to pay attention that there are control characters at the 10th and 20th position to avoid undesired changes of the DsHeuristics attribute.
Typically if the DsHeuristics is empty, the expected new value is 0000000001000000002000000011

Points:
Informative rule (0 point)

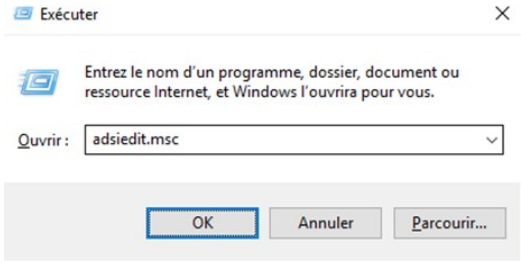
Documentation:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/e5899be4-862e-496f-9a38-33950617d2c5
https://support.microsoft.com/en-au/topic/kb5008383-active-directory-permissions-updates-cve-2021-42291-536d5555-ffba-4248-a60e-d6cbc849cde1
[FR]ANSSI - Dangerous dsHeuristics settings (vuln3_dsheuristics_bad) 3
[MITRE]T1187 Forced Authentication

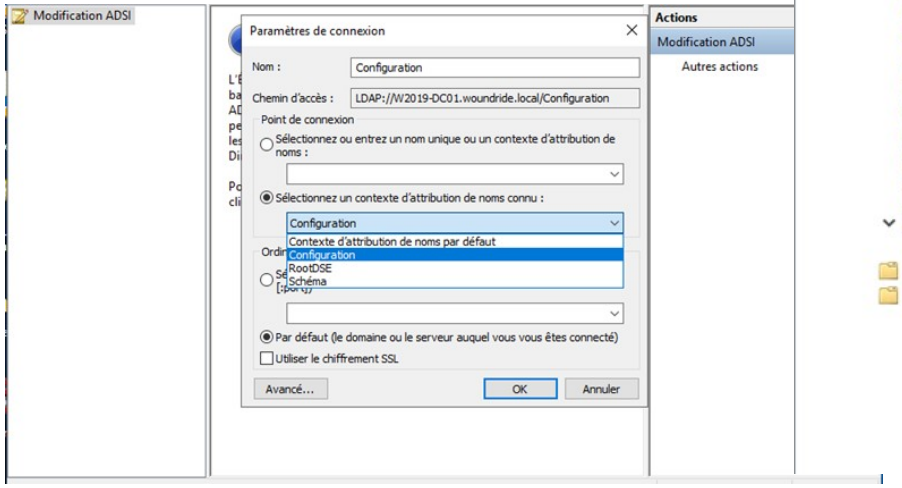
Details:

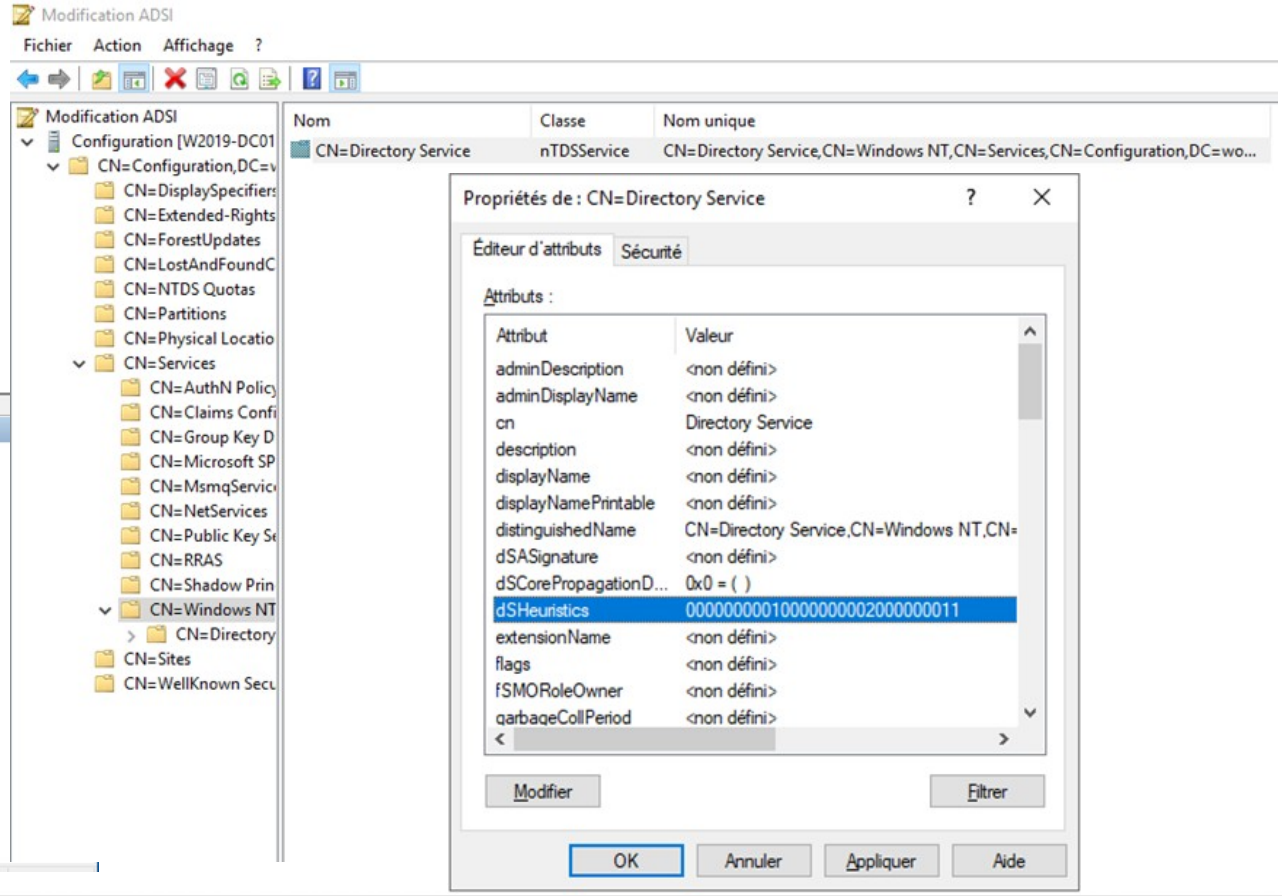
Setting	Position	Value
LDAPAddAuthZVerifications	28th	2
LDAPOwnerModify	29th	2

Reconfigurer les paramètres de l'attribut dSHeuristics

Via la console adsiedit.msc :







Ressources et outils utilisés

- dSHeuristics (Microsoft) :
  https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/e5899be4-862e-496f-9a38-33950617d2c5

- Vulnérabilités dSHeuristics (ANSSI) :
  https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_dsheuristics_bad

- AdminSDHolder (Petri) :
  https://petri.com/active-directory-security-understanding-adminsdholder-object/

- PingCastle (Vicent LE TOUX) :
  https://www.pingcastle.com/

- Purple Knight (Semperis) :
  https://semperis.com/downloads/tools/pk/PurpleKnight-Community.zip