Authentification Windows 2000

1 Objectifs

Windows 2000 (Win2k) implémente plusieurs protocoles d'authentification réseau. Le protocole utilisé par défaut est Kerberos v5. Mais pour des raisons de compatibilité avec les versions précédentes de Windows, Win2k support les protocoles issus de LanManager (LM, NTLM, NTLMv2).

Les buts de ce document sont de :

- Montrer où et comment sont stockés les *passwords.*
- Illustrer les différents mécanismes d'authentification réseau (Netlogon).
- Comprendre les vulnérabilités et mettre en œuvre des attaques permettant d'obtenir des *passwords*.
- Appliquer les mesures pour limiter les chances de réussite de ces attaques.

2 Stockage des mots de passe sur Win2k

2.1 SAM

Sur les machines W2k Pro et Serveur, la SAM (Security Accounts Manager) est l'élément qui contient les noms des utilisateurs et les *hashs* des *passwords* de tous les utilisateurs d'un système local (comptes locaux). Ces informations sont stockées dans le fichier %systemroot%\system32\config\SAM (<100ko). Ce fichier représente l'entrepôt de stockage physique des données spécifiées dans la base de registre HKEY_LOCAL_MACHINE\SAM. Il est verrouillé par le système d'exploitation, donc n'est pas lisible ni par les utilisateurs et ni par l'administrateur. Il est toutefois récupérable en *bootant* le machine à l'aide d'un autre OS compatible avec le système de fichier (Disquette Dos + NTFSDOS).

Il y a 2 types de *hash* de mots de passes stockés dans la SAM :

- Lan Manager compatible
- NTLM compatible

2.2 Active Directory (AD)

Le contrôleur de domaine (DC) d'un domaine Win2k, contient tous les noms des utilisateurs et les *hashs* des *passwords* de tous les utilisateurs du domaine (compte de domaine). Ces éléments ne sont pas stockés dans la SAM, mais dans Active Directory (AD).

AD ce trouve dans le fichier %windir%\NTDS\ntds.dit (~10Mo). Comme pour la SAM, ce fichier est verrouillé par le système d'exploitation, donc n'est pas lisible par les utilisateurs. De plus, sa grande taille le rend difficilement récupérable en utilisant une simple disquette de boot Dos.

Le DC possède aussi une SAM, mais celle-ci n'est pas utilisée par le système. Lorsqu'un serveur devient DC, les comptes utilisateurs qui existaient dans la SAM sont copiés dans AD. La SAM du DC est remplacée par une SAM basique (SAM d'origine) contenant les comptes *Administrator* et *Guest*. Ces comptes ne sont pas utilisés par le système et n'ont rien à voir avec les comptes *Administrator* et *Guest* se trouvant dans AD.

2.3 SYSKEY

SYSKEY ajoute un niveau supplémentaire d'encryptions aux *hashs* des *passwords* stockés dans la SAM ou dans AD. Par défaut, cette fonction est activée sur Win2k.

Ainsi, des programmes comme **L0phtCrack** ou **pwdump** ne sont pas capables de récupérer les *hashs* des *passwords* dans une SAM extraite d'une machine. Par contre, **pwdump2** est capable de contourner SYSKEY (Voir § 5.4).

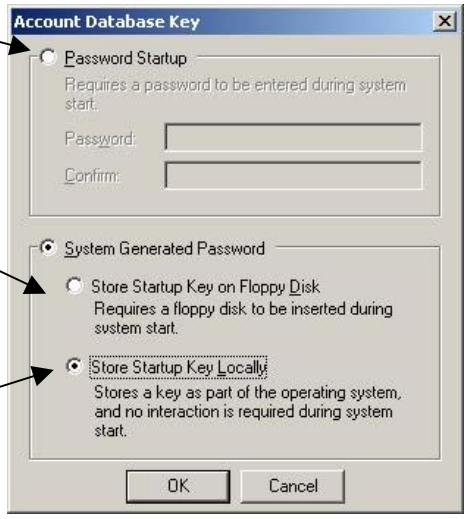
SYSKEY établit une clé de cryptage de 128 bits. Par défaut, cette clé est stockée localement par le système. Si le système requière un haut niveau de sécurité, il est possible de stocker la clé sur une disquette ou de la remplacer par un *password*. Cette disquette ou ce *password* est nécessaire pour *booter* la machine.

Pour modifier l'emplacement de la clé : ***Start – Run… - syskey - Update***

Si cette option est sélectionnée, la clé utilisée par SYSKEY est issue à partir d'un *password*. Ce *password* est demandé lors de chaque *boot* de la machine.

Si cette option est sélectionnée, la clé utilisée par SYSKEY est stockée sur une disquette. Cette disquette est demander lors de chaque *boot* de la machine.

Si cette option est sélectionnée, la clé utilisée par SYSKEY est stockée sur le système (défaut).

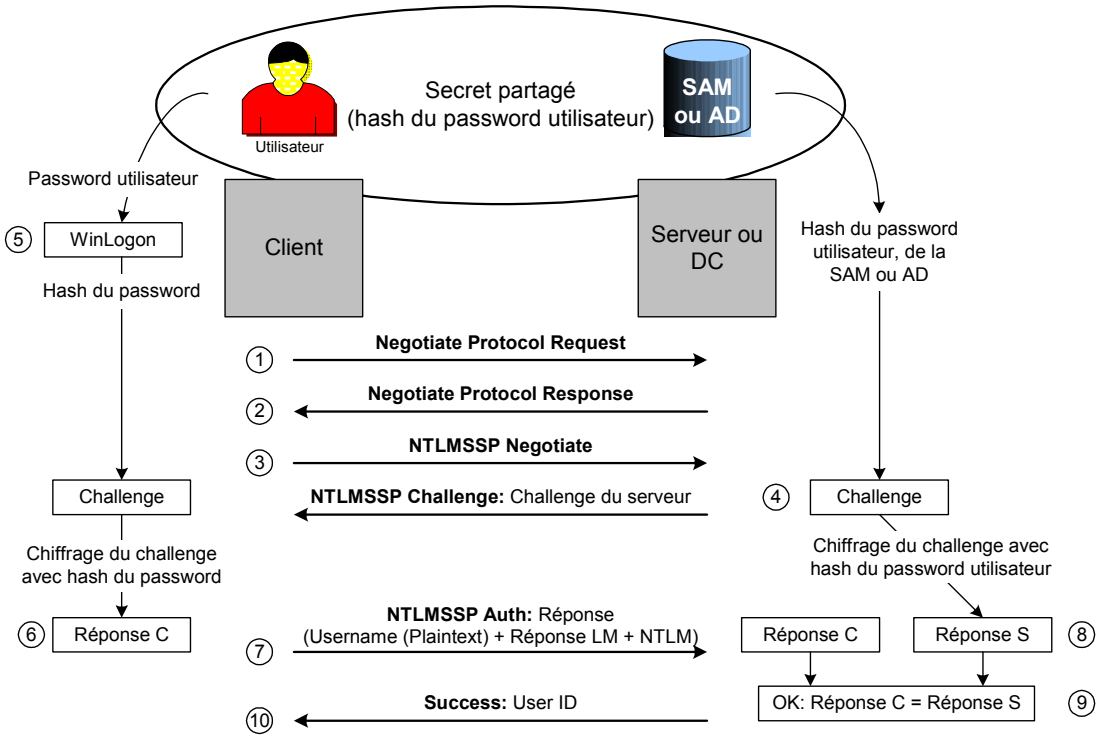


3 Authentification réseau (Netlogon)

3.1 LM, NTLM et NTLMv2

Win2k a hérité de plusieurs protocoles d'authentification réseaux, pour des raisons de compatibilité avec les versions précédentes de Windows. Le plus ancien est LanManager (LM) développé par IBM et utilisé dans les versions précédant Windows NT. Windows NT a introduit NTLM qui supprime certaines vulnérabilités de LM. La dernière évolution, NTLMv2, est apparue avec Windows NT SP4. Comme nous le verrons plus bas, les principales différances entre ces trois modes d'authentifications sont les algorithmes utiliser pour le calcul des *hashs*.

Entre deux postes Win2k, ces trois modes d'authentifications fonctionnent selon le principe du « *challenge/response* » illustré ci-dessous :



Remarque : La capture de cet échange se trouve dans l'*annexe 1*.

1. Envoi d'un « *SMB Negotiate Protocol* » contenant la liste des dialectes supportés. Le flag « *Extanded Security Negotiation* » est à 1. Cela signifie l'utilisation de NTLMSSP.

2. Réponse avec indice du dialecte à utiliser. Avec des postes Win2k, la valeur de l'indice est de 5.

3. Demande de session et négociation des options NTLMSSP.

4. Un *challenge* (nombre aléatoire de 8 bytes) est générer par le serveur et envoyé au client.

5. L'utilisateur entre son *Username* et son *password*. Le *hash* du *password* est généré.

6. Le challenge est chiffré à avec le *hash* du password. Pour des raisons de compatibilité avec les versions précédentes de Windows, cette opération est effectuée deux fois avec LM et NTLM.

7. La réponse contient les deux challenges chiffrés et le *Username* en clair.

7. Grâce à ce *Username*, le serveur récupère, dans la SAM, le *hash* du *password* lui correspondant. Le serveur chiffre à son tour le challenge à l'aide de ce *hash*.

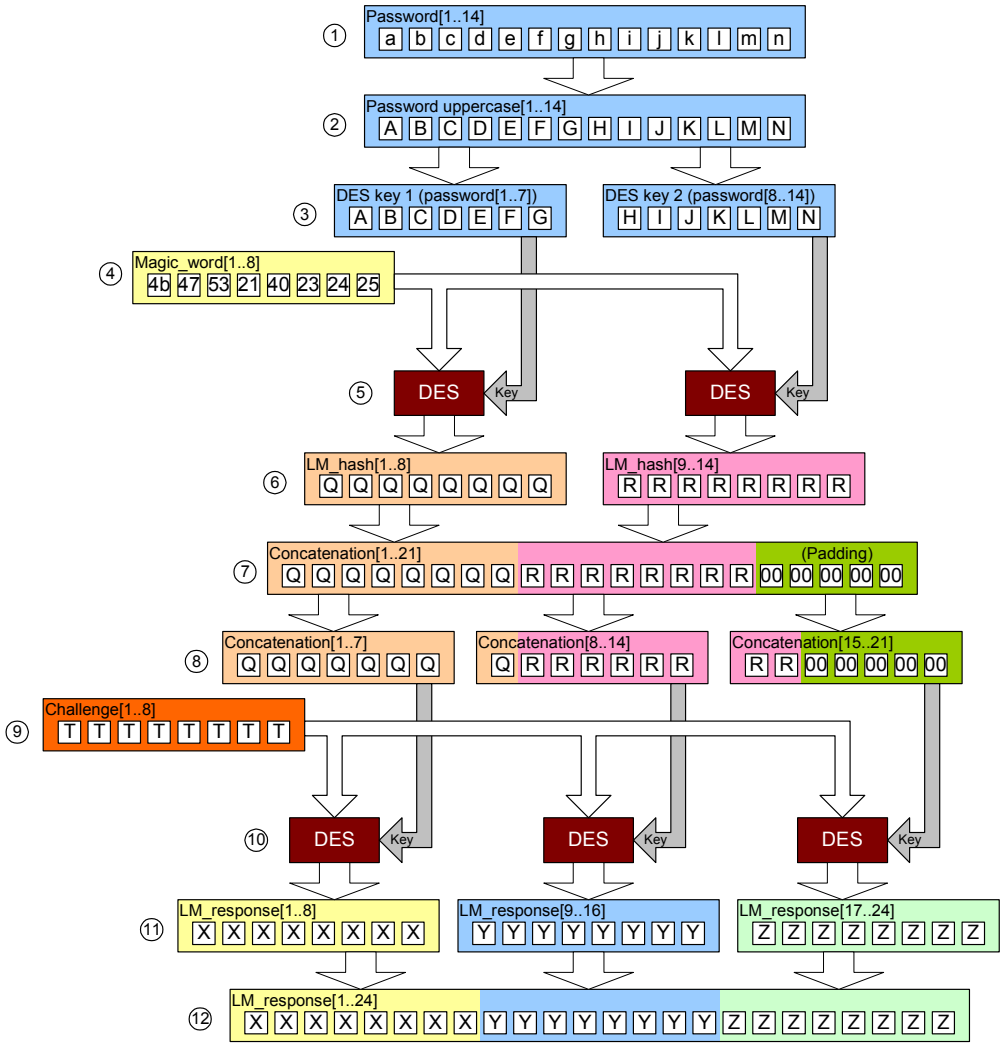
9. Le serveur compare le résultat obtenu à celui reçu du client. S'ils sont identiques, le client est authentifié.

10. Le serveur envoie un *User ID* nécessaire pour permettre l'accès aux données.

Remarque : NTLMSSP (*NTLM Security Support Provider*) est utilisé uniquement entre des postes Win2k ou supérieur. Si l'authentification est faite avec un poste plus ancien, le *challenge* est envoyer dans le paquet « *Negotiate Protocol Response* ». Il n'y a donc que 4 échanges au lieu de 6.

3.1.1 LanManager (LM)

La figure ci-dessous illustre le fonctionnement de LM :



1. Le *password* de l'utilisateur peux être au maximum de 14 caractères. S'il fait moins de 14 caractères, des « 0 » sont ajoutés (*padding*).

2. Le *password* est mis en majuscule (non case-sensitive).

3. Il est divisé en deux parties de 7 bytes qui serviront de clé.

4. LM utilise une constante de 8 bytes (0x4b 0x47 0x53 0x21 0x40 0x23 0x24 0x25).

5 & 6. La constante est chiffrée avec l'algorithme DES (ECB mode) à l'aide de la clé issue du *password*. Cette opération est effectuée pour les deux clés.

7. Les deux résultats du chiffrement sont concaténés. 5 bytes de « 0 » y sont ajouter (padding) pour obtenir un total de 21 bytes.

8. Cette concaténation est divisée en trois parties de 7 bytes.

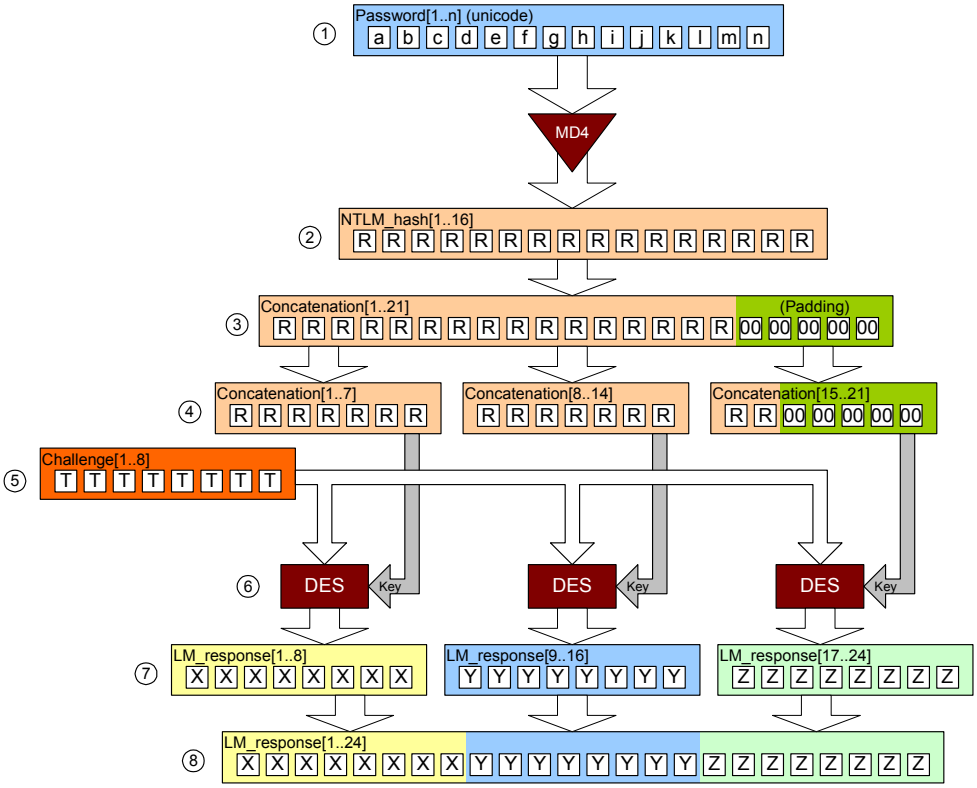
9. *Challenge* envoyé par le serveur (8 bytes).

10 & 11. Le *challenge* est chiffré avec l'algorithme DES (ECB mode) à l'aide des clés issues de la concaténation. Cette opération est effectuée pour les trois clés.

12. Les trois résultats du chiffrement sont concaténé pour créer la réponse de 24 bytes qui est retourné au serveur.

3.1.2 NTLM

La figure ci-dessous illustre le fonctionnement de NTLM :



1. Le *password* de l'utilisateur est codé en Unicode (*case-sensitive*). Il peut avoir jusqu'à 127 caractères, mais au-delà de 14, il n'est plus compatible avec les versions de Windows 9x.

2. Le *hash* NTLM de 128 bits est obtenu avec l'algorithme MD4.

3. 5 bytes de « 0 » sont ajouter au *hash* (padding) pour obtenir un total de 21 bytes.

4. Cette concaténation est divisée en trois parties de 7 bytes.

5. *Challenge* envoyé par le serveur (8 bytes).

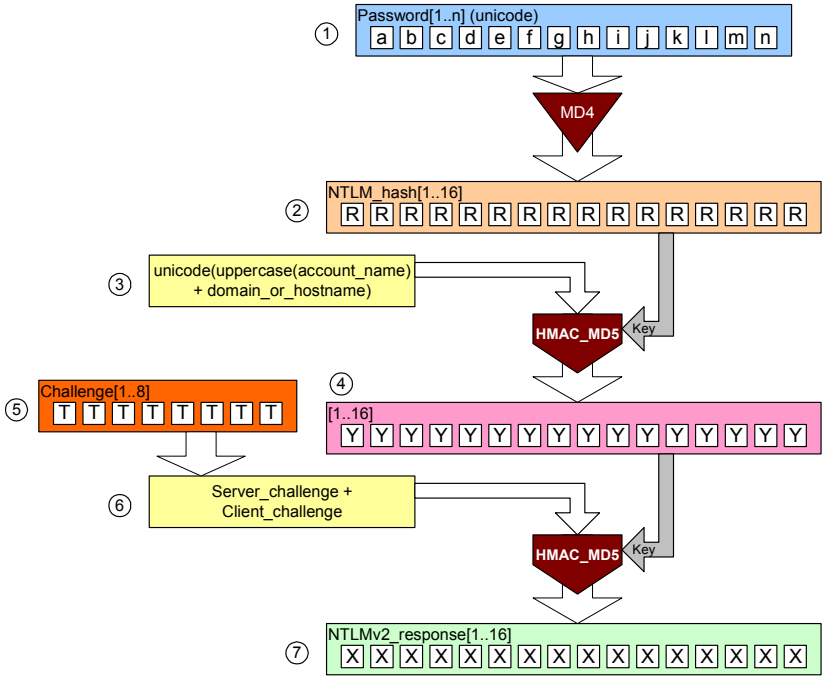
6 & 7. Le *challenge* est chiffré avec l'algorithme DES (ECB mode) à l'aide des clés issues de la concaténation. Cette opération est effectuée pour les trois clés.

8. Les trois résultats du chiffrement sont concaténé pour créer la réponse de 24 bytes qui est retourné au serveur.

Remarque : Aucune explication claire sur le fonctionnement de l'algorithme NTLM n'a été trouvée. La figure ci-dessus est donc une hypothèse faite à partir du tableau décrit sur le *slide* 15 du document « *Cracking NTLMv2 Authentication* » [CrNtlmPpt] .

3.1.3 NTLMv2

La figure ci-dessous illustre le fonctionnement de NTLMv2 :



1. Le *password* de l'utilisateur est codé en Unicode (*case-sensitive*). Il peut avoir jusqu'à 127 caractères, mais au-delà de 14, il n'est plus compatible avec les versions de Windows 9x.

2. Le *hash* NTLM de 128 bits est obtenu avec l'algorithme MD4.

3 & 4. Une clé de 128 bits est créée en effectuant un HMAC sur la concaténation du *username* et du nom du domaine (ou du *hostname*) en utilisant le *hash* NTLM comme clé.

5. *Challenge* envoyé par le serveur (8 bytes).

6 & 7. Le *challenge* du serveur et un *challenge* du client sont *hashé* avec la fonction HMAC en utilisant la clé de 128 bits générés précédemment. Le *hash* obtenu est retourné au serveur comme réponse.

Remarques : Le *challenge* du client n'a pas été identifié lors de l'analyse des échanges entre client et serveur.

Lors de l'analyses des captures (*annexes 3 - 5*) on constate que la longueur de la réponse n'est pas de 16 bytes (128 bits) mais de 92 bytes. La zone grisée ci dessous représente la réponse NTLMv2 (`NTLM Response: 48C25F6F31D2C1757CA336B73A089E2E...`). On constate que le nom du serveur (v24) est ajouter à la suite du *hash*.

```
00e0  5e c9 da 32 f3 a2 ef 0f 7b 48 c2 5f 6f 31 d2 c1   ^..2....{H._o1..
00f0  75 7c a3 36 b7 3a 08 9e 2e 01 01 00 00 00 00 00   u|.6.:..........
0100  00 50 2a 92 5f 33 de c2 01 c9 da 32 f3 a2 ef 0f   .P*._3.....2....
0110  7b 00 00 00 00 02 00 06 00 56 00 32 00 34 00 01   {........V.2.4..
0120  00 06 00 56 00 32 00 34 00 04 00 06 00 76 00 32   ...V.2.4.....v.2
0130  00 34 00 03 00 06 00 76 00 32 00 34 00 00 00 00   .4.....v.2.4....
0140  00 00 00 00 00 3e 93 3e be 4b e9 8a 2b a1 66 bf   .....>.>.K..+.f.
```

3.1.4 Tableau récapitulatif

Le tableau ci-dessous réunit les principales caractéristiques des trois modes d'authentification.

	LM	NTLM	NTLMv2
Password max length	2x7 char	127 char *	127 char *
Password case sensitive	non	oui	oui
Hash key length	56bit + 56bit	-	-
Password hash alogorithm	DES (ECB mode)	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit
C/R key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
C/R length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit

Remarque : * Si le *password* est plus grand que 14 caractères, il n'est pas compatible avec les versions de Windows 9x.

3.2 Kerberos

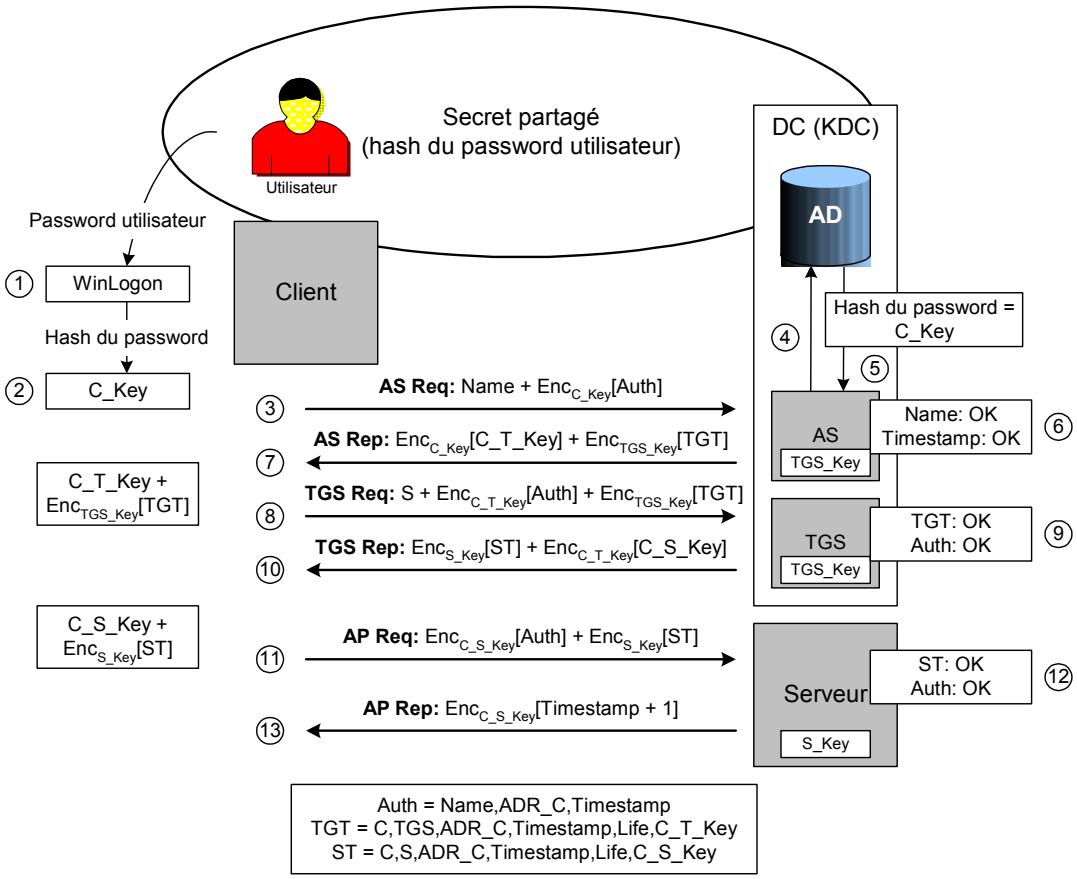
Kerberos (*RFC 1510*) est le protocole d'authentification par défaut utiliser entre des systèmes Win2k faisant parti d'un même domaine. Les avantages de ce protocole sont :

- Aucun *password* (ou *hash*) chiffré ne circule sur le réseau
- Protocole permettant l'authentification mutuelle d'entités
- Architecture *Single Sign On*

Kerberos repose sur l'utilisation de clés symétriques (*symmetrical key*) ainsi que sur des clés de session (*session key*) qui permettent au client et au serveur Kerberos de dialoguer avec des messages cryptés. Kerberos utilise le cryptage DES (*Data Encryption Standard*).

Le cœur du system est le serveur Kerberos. Le serveur Kerberos aussi appelé KDC (*Key Distribution Center*) est le centre de distribution de clé qui accepte les requêtes de tickets émanant des clients. Il comprend le service d'authentification (AS) ainsi que le service de délivrance des tickets (TGS). Le KDC possède une base de donnée pour établir la correspondance entre un client et sa clé. Pour Win2k, cette base de donnée est AD. La clé d'un utilisateur, qui est le secret partagé, est obtenue à partir d'une fonction de hachage MD5 sur son mot de passe.

La figure ci dessous illustre le processus d'authentification d'un client désirant accéder à un serveur :



1. L'utilisateur entre son *username*, son *password* et le nom de domaine.

2. La clé du client est générée par fonction de *hashage* MD5 du *password*.

3. Envoi d'un « *Authentication Service Request* » (*AS Req*) contenant le *username* et un authentifieur chiffré avec la clé du client.

4 & 5. L'AS (*Authentication Service*) utilise le *username* pour rechercher la clé du client dans AD.

6. Avec cette clé, le client déchiffre l'authentifieur qui contient le nom du client, son adresse et l'heure (*timestamp*). Le *timestamp* est une mesure empêchant à un intrus de rejouer des requêtes. Si le nom et le *timestamp* sont valides, le client est authentifié.

7. Envoi d'un « *Authentication Service Response* » (*AS Rep*) contenant un ticket (TGT) et une clé de session. La clé de session est chiffrée avec la clé du client. Cette clé de session est utilisée pour chiffrer les échanges entre le client et le TGS (*Ticket Granting Service*). Le TGT (*Ticket Granting Ticket*) est chiffré avec la clé du TGS et ne peut pas être déchiffré par le client.

Une fois en possession du TGT, le client n'a plus besoin de s'authentifier pour accéder aux différant services du domaine (*Single Sign On*). La clé du client (*hash* du *password*) n'est pas conservée plus longtemps sur le post client. Pour se connecter aux autres services, le client présente sont TGT au TGS.

8. Envoi d'un *TGS Req* contenant le service (ou serveur) désiré, le TGT et un authentifieur chiffré avec la clé de session client-TGS. Le TGS utilise sa clé pour déchiffrer le TGT qui contient le nom du client et du TGS, l'adresse du client, un *timestamp*, la durée de validité du ticket et la clé de session client-TGS. Le TGS utilise cette dernière clé pour déchiffrer l'authentifieur.

9. Le TGS vérifie la validité des données contenues dans le TGT et l'authentifieur.

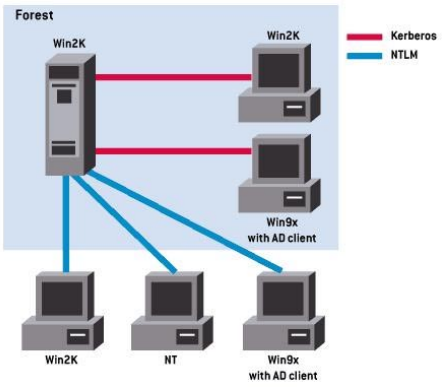
10. Envoi du *TGS Rep* contenant un ticket pour le service (ou serveur) désiré (ST) et une clé de session client-serveur. La clé de session est chiffrée avec la clé de session client-TGS. Le ticket est chiffré avec la clé du serveur et ne peut pas être déchiffré par le client.

11. Envoi d'un « *Application Request* » (*AP Req*) contenant le ticket du serveur et un authentifieur chiffré avec la clé de session client-serveur. Le serveur utilise sa clé pour déchiffrer le ticket qui contient le nom du client et du serveur, l'adresse du client, un *timestamp*, la durée de validité du ticket et la clé de session client-serveur. Le serveur utilise cette dernière clé pour déchiffrer l'authentifieur.

12. Le serveur vérifie la validité des données contenues dans le ticket et l'authentifieur.

13. Envoi d'un « *Application Response* » (*AP Rep*) contenant le *timestamp* du client incrémenté de 1. Cela permet au client d'authentifier le serveur (authentification mutuelle), car seul le serveur possédant la bonne clé est capable de déchiffrer le ticket.

3.3 NTLM ou Kerberos ?

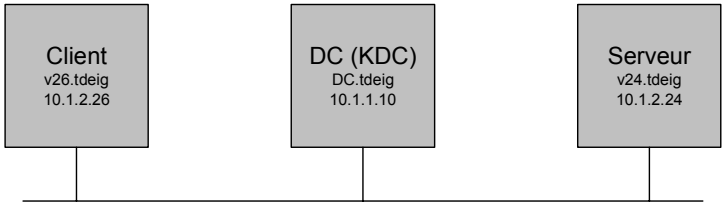


Win2k utilise Kerberos à la place d'NTLM seulement quand l'authentification dois se faire sur une autre machine Win2k ou XP (ou Win9x avec un client AD) qui se trouve dans le même domaine ou dans un domaine *trusté*. Dans tous les autres cas, Win2k utilise NTLM (Source : [InW2kS] p.304).

Par exemple, si un client Win2k se connecte sur un serveur Win2k n'étant pas membre du domaine, Win2k utilisera NTLM pour l'authentification.

Deux postes Win2k dans Workgroup utilisent NTLM

Kerberos utilise les noms DNS pour identifier les machines. Si l'accès à un partage (dans le même domaine) se fait en utilisant l'adresse IP (ex : \\10.1.2.24\partege), Kerberos ne fonctionne pas et NTLM est utilisé.



Dans les captures ci-dessous, on voit le client (10.1.2.26) qui s'authentifie auprès du KDC (10.1.1.10) afin d'obtenir un ticket pour accéder au serveur (10.1.2.24).

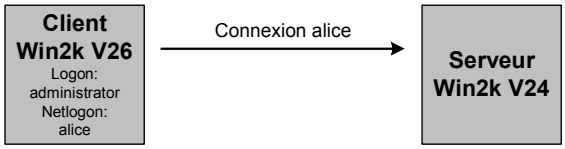
No.	Time	Source	Destination	Protocol	Info
170	26.939096	10.1.2.26	10.1.1.10	KRB5	AS-REQ
171	26.941284	10.1.1.10	10.1.2.26	KRB5	AS-REP
172	26.942126	10.1.2.26	10.1.1.10	KRB5	TGS-REQ
173	26.943171	10.1.1.10	10.1.2.26	KRB5	KRB-ERROR
174	26.943958	10.1.2.26	10.1.1.10	KRB5	TGS-REQ
175	26.944936	10.1.1.10	10.1.2.26	KRB5	KRB-ERROR
176	26.945711	10.1.2.26	10.1.1.10	KRB5	TGS-REQ
177	26.946686	10.1.1.10	10.1.2.26	KRB5	KRB-ERROR
178	26.947136	10.1.2.26	10.1.2.24	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
179	26.947629	10.1.2.24	10.1.2.26	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE
180	26.947999	10.1.2.26	10.1.2.24	SMB	Session Setup AndX Request, NTLMSSP_AUTH

Comme on le voit dans l'*annexe 6*, l'*AS-Request* et l'*AS-Response* se passent normalement. Mais lors du *TGS-Request*, le client passe l'adresse IP du serveur comme nom de serveur. Le KDC ne connaissant que le nom des machines (ex. v24.tdeig), il retourne l'erreur « **KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN ».**

Après plusieurs tentatives infructueuses, le client se connecte directement au serveur en utilisant NTLM.

Une série de tests à permis d'illustrer des différences dans le mode d'authentification du client en fonction de la méthode utilisée pour accéder au serveur.

Les tests sont effectués de la manière suivante :



- Le client ouvre sa session local avec le compte « administrator » et se connecte au serveur en utilisant le compte « alice ».
- Si le serveur est *standalone*, le compte « alice » est local au serveur.
- Si le serveur est dans le domaine, le compte « alice » est un compte de domaine (AD), sauf pour les testes avec « ** » (voir tableau ci-dessous).

Les méthodes d'accès au serveur testées sont :

- Par le bureau : ***My Network Places – Computers Near Me – V24***
- Avec le nom du serveur : ***Start – Run… -* *V24***
- Avec l'IP du serveur : ***Start – Run… -* *10.1.2.24***
- Avec l'FQDN du serveur : ***Start – Run… -* *V24.tdeig***

Les testes sont effectuer avec est sans NetBIOS sur TCP/IP.

Le tableau si dessous illustre les résultats :

Modes d'accès					
		Avec NetBIOS		Sans NetBIOS	
Méthode d'accès	Typ. Username	Typ. Prot.	port	Typ. Prot.	port
Client Standalone --> Serveur Standalone					
Computer Near Me - V24	alice	NTLM	139	-	-
	alice@tdeig	-	-	-	-
Run… - \\V24	alice	NTLM	139	-	-
	alice@tdeig	-	-	-	-
Run… - \\10.1.2.24	alice	NTLM	445	NTLM	445
	alice@tdeig	-	-	-	-
Run… - \\V24.tdeig	alice	NTLM *	445 *	NTLM *	445 *
	alice@tdeig	-	-	-	-
Client Standalone --> Serveur Domaine * **					
Computer Near Me - V24	alice	NTLM **	445 **	-	-
	alice@tdeig	Krb5	88	-	-
Run… - \\V24	alice	NTLM **	445 **	-	-
	alice@tdeig	Krb5	88	-	-
Run… - \\10.1.2.24	alice	NTLM **	445 **	NTLM **	445 **
	alice@tdeig	NTLM	445	NTLM	445
Run… - \\V24.tdeig	alice	NTLM **	445 **	NTLM **	445 **
	alice@tdeig	Krb5	88	Krb5	88
Client Domaine --> Serveur Domaine					
Computer Near Me - V24	alice	Krb5	88	-	-
	alice@tdeig	Krb5	88	-	-
Run… - \\V24	alice	Krb5	88	Krb5	88
	alice@tdeig	Krb5	88	Krb5	88
Run… - \\10.1.2.24	alice	NTLM	445	NTLM	445
	alice@tdeig	NTLM	445	NTLM	445
Run… - \\V24.tdeig	alice	Krb5	88	Krb5	88
	alice@tdeig	Krb5	88	Krb5	88
Client Domaine --> Serveur Standalone * **					
Computer Near Me - V24	alice	NTLM	139 (445 *)	-	-
	alice@tdeig	-	-	-	-
Run… - \\V24	alice	NTLM	139 (445 *)	NTLM *	445 *
	alice@tdeig	-	-	-	-
Run… - \\10.1.2.24	alice	NTLM	445	NTLM	445
	alice@tdeig	-	-	-	-
Run… - \\V24.tdeig	alice	NTLM *	445 *	NTLM *	445 *
	alice@tdeig	-	-	-	-

* Seulement si le serveur est présent dans le DNS (cela est fait dynamiquement pour le serveur dans le domaine)
** Le compte doit être local au serveur
***Le client appartient au même workgroup que le serveur

Selon la documentation [WM15892], Win2k utilise le port 445, pour communiquer avec d'autres postes Win2k, ou le port 139, pour communiquer avec les versions précédentes de Windows.

Comme on le voit dans le tableau, si le serveur est *standalone* et que l'on utilise le nom de la machine « \\V24 » (nom NetBIOS) pour la résolution d'adresse, le port SMB utilisé est le 139, même entre deux postes Win2k.
Mais si le client fait partie du domaine « tdeig », le suffix DNS « tdeig » est automatiquement ajouter à « \\V24 », donc la connections se fait bien par le port 445.

On constat aussi qu'il est possible d'accéder à un serveur dans un domaine en utilisant un compte de domaine depuis un poste client *standalone*. Pour cela, il faut utiliser l'*Universal Principal Name* (UPN → user@domain) pour forcer l'exécution de Kerberos.

Remarque : Il est possible que des authentifications devant normalement se faire avec Kerberos ne le soient pas. En effet, si le DC ne répond pas à la requête Kerberos du client (*flooding* du DC), le client passe en NTLM.

4 Mesure pour augmenter la sécurité des *password*

4.1 Désactivé LM et NTLM

Win2k possède une clé de registre permettant de choisir quel type de réponse le client peut envoyer au serveur lors du *logon* et quel type de réponse le serveur peux accepter. Cette clé est « LMCompatibilityLevel » du type « REG_DWORD » et peut avoir la valeur de 0 à 5. Cette clé se trouve dans ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA***.

- **Level 0 (Send LM and NTLM response) :** Le *Level 0* est le niveau par défaut. Il envoie les deux types de réponses, LM et NTLM (*annexe 1*). Ce niveau est compatible avec toutes versions de Windows, mais est le plus vulnérable.

- **Level 1 (Send LM and NTLM - Use NTLM 2 session if negotiated) :** Le *Level 1* négocie le plus haut niveau d'authentification possible, c'est à dire NTLMv2. Mais le *Level 1* revient à l'authentification LM en cas de besoin et n'améliore pas la sécurité.

- **Level 2 (Send NTLM response only) :** Le *Level 2* envoie uniquement des réponses du type NTLM. Selon l'article « *Inside SP4 NTLMv2 Security Enhancements* » [WM7072], les champs *LM-Response* et *NTLM-Response* sont remplies avec la réponse NTLM pour des raisons de compatibilité. Mais dans l'*annexe 2*, on constate que le *hash* LM est différant du *hash* NTLM.

- **Level 3 (Send NTLMv2 response only) :** Le *Level 3* envoie uniquement des réponses du type NTLMv2. Toujours selon l'article « *Inside SP4 NTLMv2 Security Enhancements* » [WM7072], Microsoft voulait remplir les champs *LM-Response* et *NTLM-Response* avec la réponse NTLMv2, pour des raisons de compatibilité, comme pour le *Level 2*. Malheureusement, le champ *LM-Response* ne peut pas dépasser 24 bytes et la réponse NTLMv2 est plus grande que 24 bytes. Microsoft a donc créé une réponse de 24 bytes appelé LMv2 (aucune documentation sur cet algorithme n'a été trouvé).

  En forçant l'utilisation de NTLMv2, le client doit ouvrir sa session Windows en utilisant un compte existant sur le serveur :
  - Compte de domaine : Pas de problèmes
  - Compte local : Le compte doit exister sur le client et le serveur.

  Si le compte du client est différant du compte du serveur, il faut donner le *username* de la forme suivante : « server_name/server_account » (ex : v24/alice). En effet, si on tape uniquement « alice » comme *username*, cela correspond à « client_name/alice » qui n'est pas connu par le serveur, donc cela ne fonctionne pas. Dans l'*annexe 3*, on voit que le client retourne le nom du serveur (v24) dans le champ *Domain Name*.

- **Level 4 (Send NTLMv2 response only \ refuse LM) :** Pour le poste client, le *Level 4* est identique au *Level 3*. Le *Level 4* spécifie que le serveur refuse la connexion d'un client, ne supportant pas NTLM ou NTLMv2, utilisant un compte local du serveur. Le DC refuse toutes connexions d'un client ne supportant pas NTLM ou NTLMv2.

- **Level 5 (Send NTLMv2 response only \ refuse LM & NTLM) :** Le *Level 5* est identique au *Level 4* à la différance que seul le client supportant NTLMv2 peut se connecter au serveur.

Win2k à implémenté le choix de ces différents niveaux d'authentifications dans les GPO (*Group Policy Object*) : ***Security Settings – Local Policies – Security Options – Lan Manager Authentication Level***

Comme on peut le constater, il n'y a pas de moyen de désactiver complètement ces trois types d'authentification afin de n'utiliser que Kerberos. Par contre, dans un environnement purement Win2k, il est déjà possible de limiter les risque en forçant l'utilisation d'NTLMv2.

Les *annexes 1* à *5* sont des captures d'authentifications pour chacun de ces niveaux (sauf le *Level1*). On constate que ces échanges sont identiques. On ne voit pas de différance lors de la négociation du protocole. La seule différance est la longueur du *NTLM-Response* qui est de 92 bytes pour NTLMv2 et de 24 bytes pour NTLM.

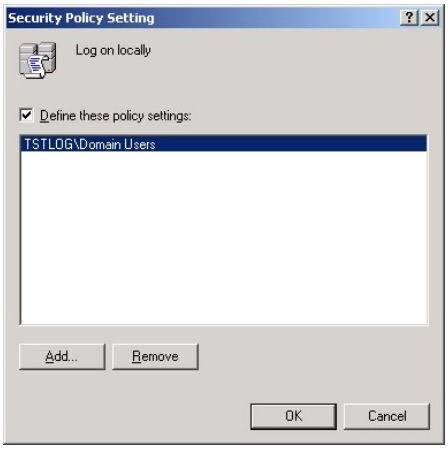
Sources : [Q147706] [Q239869] [WM7072]

4.2 Forcer l'utilisation de Kerberos

Comme nous l'avons vu au § 3.3, Win2k utilise l'authentification Kerberos pour des machines se trouvant dans le même domaine ou dans un domaine *trusté*. Donc, ce protocole ne peut pas être utilisé entre des postes *standalones*, car un KDC est nécessaire. Par contre, si un client *standalones* désire se connecter à un serveur se trouvant dans un domaine, il est possible de forcer l'utilisation de Kerberos en utilisant un *Universal Principal Name* (UPN → user@domain) lors de l'authentification. De cette manière, le client se connecte au serveur en utilisant un compte de domaine. Pour que cela fonctionne, il faut que le serveur DNS par défaut du client connaisse le DC et le serveur.

Pour dire les choses de manière différente, Kerberos fonctionne que si l'on utilise des comptes de domaine et non des comptes locaux. Donc si on désire limiter les risques d'utiliser un protocole issu de LM, il est nécessaire d'empêcher l'utilisation de ces comptes locaux. Cela peut être fait au niveau d'AD en plaçant les postes clients et les serveurs dans un OU. Il faut ensuite créer et éditer le GPO suivant pour cet OU :
Computer Configuration – Windows Settings – Security Settings – Local Policies – User Right Assignment

Ouvrer la *Policy* « *Log on locally* » puis ajouter (***Add…***) *Domain Users* à la liste. Ainsi, seul les utilisateurs faisant parti du domaine (compte de domaine) peuvent ouvrir une session localement.



Il faut effectuer la même opération sur la *Policy* « *Access this computer from the network* » afin d'empêcher la connexion d'un client sur le poste en utilisant un compte local.

Pour se connecter à un serveur, il est important d'utiliser son FQDN et non pas sont adresse IP, sinon Kerberos ne fonctionnera pas (§ 3.3).

Remarque : Les Filtres IPSec de Win2k permettraient de forcer l'authentification Kerberos.

4.3 Suppression de la SAM de secours

Un fichier SAM de secours est contenu dans %systemroot%\repair. Il contient tous les utilisateurs configurés sur un système lors de son installation. Ce fichier est créé par l'utilitaire de réparation de disque (*Create Emergency Repair Disk*) intégré à l'application Microsoft Backup v.5 (ntbackup.exe). Ce fichier n'est pas verrouillé par le système d'exploitation, donc vérifier les droits d'accès sur le fichier.

Après la création d'un « *Emergency Repair Disk* », il est conseiller de supprimer le fichier SAM du répertoire %systemroot%\repair et de mettre la disquette dans un lieu sur (elle contient la SAM).

Les risque d'attaque sur ce fichier sont atténuée, car les mécanismes de décryptage d'un fichier crypté avec SYSKEY (à l'inverse de l'application **pwdump2** à un fichier SAM actif) n'ont pas été diffusés dans le grand public (p.269 [HalHac]).

4.4 Suppression des *hash* LM dans la SAM et AD

Comme nous l'avons vu plus haut, deux types de *hash* (LM & NTLM) sont stockés dans la SAM (ou dans AD) pour des raisons de compatibilité descendante. Comme nous le verrons dans le § 5, le *hash* LM est beaucoup plus vulnérable aux attaques que le *hash* NTLM.
Depuis Win2k SP2, il est possible d'empêcher la création du *hash* LM dans la SAM et AD grâce à une nouvelle clé de registre [Q299656]. Pour cela :

- Avec ***Regedit*** aller dans ***HKLM\SYSTEM\CurrentControlSet\Control\Lsa***
- Dans le menu ***Edit – New – Key*** taper « NoLMHash »
- Fermer ***Regedit*** et rebooter la machine

Attention : Une fois la clé de registre ajoutée, les *hash* LM des comptes utilisateurs déjà existant ne sont pas supprimés tant que les utilisateurs ne changent pas leur *password*.

5 Attaques

5.1 Interception des paquets *challenges – responses*

Le but de cette attaque est de s'emparer du *password* des utilisateurs se connectant à un serveur. En *sniffant* le réseau, il est possible d'intercepter les paquets *challenges – responses* entre le client et le serveur. Ensuit, en utilisant différentes méthodes (dictionnaire, hybride ou *brute force* (voir § 5.5)), des *passwords* sont générés pour *hasher* le *challenge*. Dès que le résultat obtenu est identique au message *response* du client, le *password* généré correspond au *password* de l'utilisateur.

5.1.1 L0phtCrack 4 (LC4)

L0phtCrack 4 (LC4) est un outil de détection ou de récupération de mots de passes développer par **@stake** (http://www.atstake.com/research/lc/). Il permet de retrouver des *passwords* soit en extrayant les hashes des *passwords* à partir de la SAM (voir § 5.5) ou directement en capturant les paquets *challenges – responses* sur le réseau.

Malheureusement, lors des testes, on a constaté que LC4 n'arrive pas à intercepter les paquets d'authentification si le client et le serveur sont des postes Win2k. Cela peut avoir deux raisons :

- La première : Si le client et le serveur Win2k sont membre du même domaine ou d'un domaine *trusté*, l'authentification se fait par Kerberos. LC4 n'est pas capable d'intercepter et de *cracker* Kerberos. Il fonctionne uniquement pour les échanges *challenges – response* de type LM ou NTLM (aucune indication n'est donnée sur NTLMv2). Mais même en faisant des testes entre deux postes Win2k *standalone* qui utilisent NTLM, LC4 n'a pas été capable d'intercepter l'échange.

- La deuxième : Selon l'article « Win2K Password Protection » [WM15892], LC4 est capable de capturer les échanges entre un post Win2k et NT qui utilise le port 139 (NTLM et SMB), mais pas entre deux post Win2k qui utilise le port 445 (CIFS (Common Internet File System)). Mais comme nous l'avons vu dans le tableau au § 3.3, il est possible de s'authentifier entre deux postes Win2k en utilisant le port 139. Malgré cela, LC4 n'a pas été capable d'intercepter l'échange.

Comme nous l'avons remarqué au § 3.1, Win2k utilise NTLMSSP (*NTLM Security Support Provider*) lors de l'authentification avec un autre poste Win2k. Cela n'est pas le cas pour des postes plus anciens (NT, 9x). La meilleure hypothèse à retenir est que le *sniffer* de LC4 n'est pas capable de capturer les échanges NTLMSSP.

Dans se version actuelle, la fonction *sniff* de LC4 n'est donc pas utilisable entre deux postes Win2k. Par contre cet outil reste très précieux pour retrouver les *passwords* à partir des *hashs* extrait de la SAM (§ 5.5)

5.1.2 ScoopLM et BeatLM

ScoopLM et BeatLM sont des outils de capture et de recherche de *passwords* LM, NTLM et NTLMv2 développé par **SecurityFriday** (http://www.securityfriday.com/).

ScoopLM est le *sniffeur* permettant de récupérer les paquets *challenges – response*. Il permet de sauvegarder les captures dans un fichier afin de les utiliser avec BeatLM.
BeatLM et l'application qui recherche les *passwords* en utilisant les méthodes par dictionnaire, hybride ou *brute force*.

Grâce à ces programmes, il est possible de capturer les échanges entre deux postes Win2k, mais malheureusement, la recherche des *passwords* ne fonctionne pas. Aucune information n'a été trouvée à ce sujet.

5.2 Attaque des échanges Kerberos

Actuellement, aucun outil disponible ne permet de retrouver le *password* d'un utilisateur en capturant les échanges Kerberos sur le réseau. Cela ne veut pas dire que ce n'est pas possible. L'article « *Feasibility of attacking Windows 2000 Kerberos Passwords* **»** [AttKrbPa] décrit la manière qui permettrai de réaliser cette attaque.

Le principe est simple. Il suffit de capturer l'authentifieur chiffré envoyé lors de l'*AS Req*. L'authentifieur contient un *timestamp* dont le format est YYYYMMDDHHMMSSZ (ex : 20030319163425Z) et un *cryptographic checksum*. Des *passwords* peuvent être générés (à la manière de LC4) pour déchiffrer l'authentifieur et rechercher un *string* correspondant au format du *timestamp*. Si le résultat ressemble à ce format, le *password* est presque certainement correct. Pour vérifier la validité du *password*, il suffit de recalculer le *cryptographic checksum* est de le comparer avec celui contenu dans l'authentifieur.

5.3 Accès à la SAM

L'accès à la SAM n'est pas possible tant qu'une session Windows est ouverte.

La solution est de booter la machine avec une disquette DOS et de monter les partitions NTFS en utilisant le logiciel NTFSDOS (http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml). Ensuite la SAM peut être copier sur la disquette.

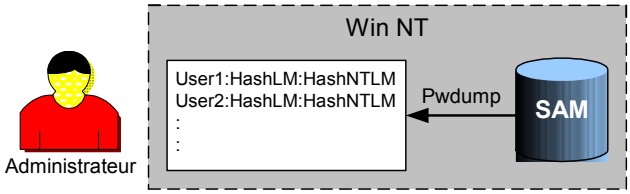
Remarque : La version demo de NTFSDOS permet uniquement la lecture des fichiers NTFS.

Une autre solution est de s'emparer du fichier SAM de secours, contenu dans %systemroot%\repair, s'il n'a pas été supprimé. Ce fichier n'est pas verrouillé par le système d'exploitation et peut donc être copié

Remarque : Si aucun « *Emergency Repair Disk* » n'a été créé sur le poste, la SAM de secours contient uniquement les comptes *Administrator* et *Guest* créé lors de l'installation de Win2k

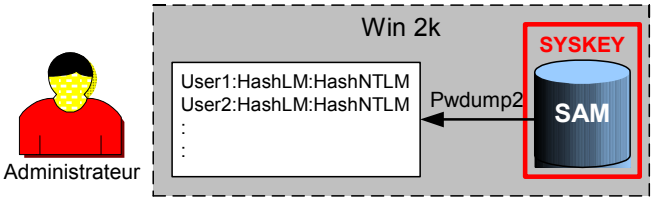
5.4 Extraction des informations du fichier SAM

Pwdump est un programme qui permet d'extraire les *username* et les *hash* des *passwords* de la base de données SAM d'un system NT.



Sur les systemes Win2k, le contenu de la SAM est protégé par SYSKEY. SYSKEY ajoute un niveau supplémentaire d'encryptions aux *hashs* des *passwords* stockés dans la SAM (§ 2.3). Actuellement, il n'existe pas encore de moyen de déchiffrer la SAM sans posséder la bonne clé. Il n'est donc pas possible d'extraire ces informations du fichier SAM.

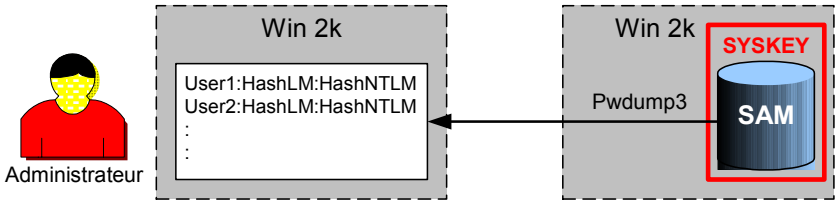
Une version plus agressive de Pwdump, appelée Pwdump2, permet de surmonter SYSKEY (p.195 [HalHac]). Pwdump2 peut être téléchargé sur http://razor.bindview.com/tools/desc/pwdump2_readme.html.



Pwdump2 exploite l'injection de DLL pour charger son propre code dans l'espace de traitement d'un processus doté de droits d'accès élevés. Le processus visé est lsass.exe, c'est à dire le sous-système local de sécurité. Une fois chargé dans le processus, le code pirate peut effectuer un appel API interne accédant aux *hashs* des *passwords* cryptés par SYSKEY, sans avoir à les décrypter.

Pwdump2 doit être lancé dans l'espace de traitement du système cible (localement). Des droits d'accès Administrateur sont nécessaires.

Pwdump3 (http://www.polivec.com/pwdump3.html) est une amélioration de Pwdump2. Il peut être exécuté à travers le réseau même si SYSKEY est activé. Pwdump3 ne représente pas un nouvel exploit puisque des privilèges administratifs sont encore exigés sur le système distant, comme les versions précédentes de Pwdump. Une des grandes améliorations avec Pwdump3 est qu'il n'est plus obligatoire d'exécuter le programme directement sur chaque machine.



5.5 Décryptage des *hashs* des mots de passe

Le décryptage des *hashs* des *passwords* consiste en réalité à :

- Générer un *password*
- Calculer son *hash*
- Comparer le résultat au *hash* extrait de la SAM

S'ils sont identiques, le *password* généré correspond au *password* de l'utilisateur.

La génération du *password* peut se faire de différentes méthodes :

- Dictionnaire : Liste de *passwords* (ex : monpass)
- Hybride : Ajout de un ou plusieurs caractères aux *passwords* du dictionnaire (ex : monpass21)
- *Brute force* : Génération de toutes les combinaisons possible de *password* (ex : Ad4$hr4)

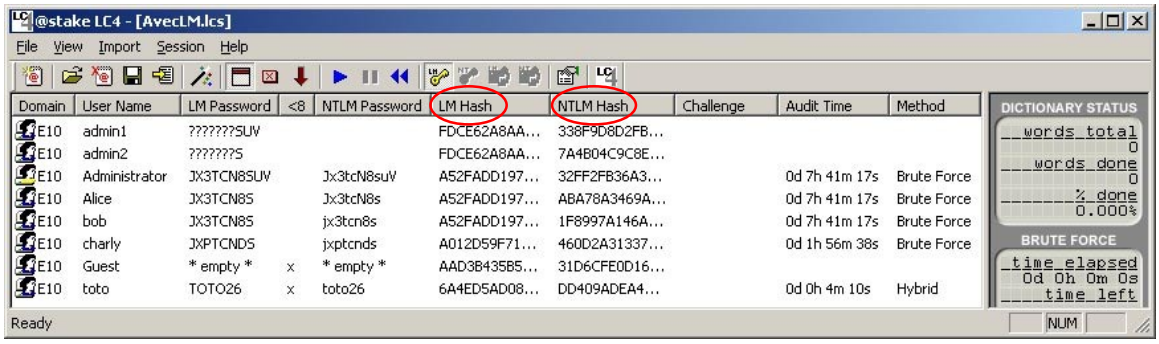
Dans l'exemple ci-dessous, nous utilisons LC4 (L0phtcrack 4, voir § 5.1.1) pour tester la « dureté » des différents *passwords* contre ce type d'attaque.

LC4 intègre Pwdump2. Il est directement capable d'extraire les informations de la SAM du system sur lequel il est installé puis de rechercher les *passwords*. Pour cette raison, les essais sont faits localement sur un poste de test.

Le tableau ci-dessous représente les compte créés sur le système testé et les *passwords* de complexité diverse :

Username	Password	caractéristiques
Admin2	Jx3?cN8s	8 car. , minuscules, majuscules, chiffres, car. spéciaux
Admin1	Jx3?cN8suV	10 car. , minuscules, majuscules, chiffres, car. spéciaux
Administrator	Jx3tcN8suV	10 car. , minuscules, majuscules, chiffres
Alice	Jx3tcN8s	8 car. , minuscules, majuscules, chiffres
Bob	jx3tcn8s	8 car. , minuscules, chiffres
Charly	jxptcnds	8 car. , minuscules
Toto	toto26	*password* simple

En lançant LC4 (***Import – Import from local machine***), on voit qu'il récupère les *hashs* LM et les *hashs* NTLM dans le fichier SAM locale.



Voici ce qui se passe quand on lance le « décryptage » :

- LC4 utilise les mots contenus dans un dictionnaire pour générer les *hashs* LM et compare le résultat avec les *hashs* extraient de la SAM.

- Si les *passwords* ne sont pas découverts, LC4 commence la recherche hybride. Pour cela, un ou plusieurs caractères (2 car. par défaut) sont ajoutés aux mots du dictionnaire. Ce test montre l'exemple du *password* « TOTO26 ». Le mot « TOTO » est contenu dans le dictionnaire. En ajoutant différents caractères, le *password* est découvert en quelques minutes (4m10s).

- Si tous les *passwords* ne sont toujours pas découverts, LC4 lance l'attaque *brute force*. Comme nous l'avons vu au §3.1.1, la *hash* LM est calculé en découpant le *password* en deux parties de 7 caractères. Donc LC4 ne doit s'attaquer qu'à un passwords non *case-sensitive* (majuscule) de 7 caractères. Cela donne 36^7 combinaisons **alphanumériques**. Comme on le voit sur les 2 premières lignes de la capture ci-dessus, la deuxième partie des *passwords*, ne contenant que peut de caractères, sont trouvés presque instantanément.

- Lorsque le *password* LM est retrouvé, LC4 teste toutes les combinaisons majuscules et minuscules pour retrouver le *password* NTLM.

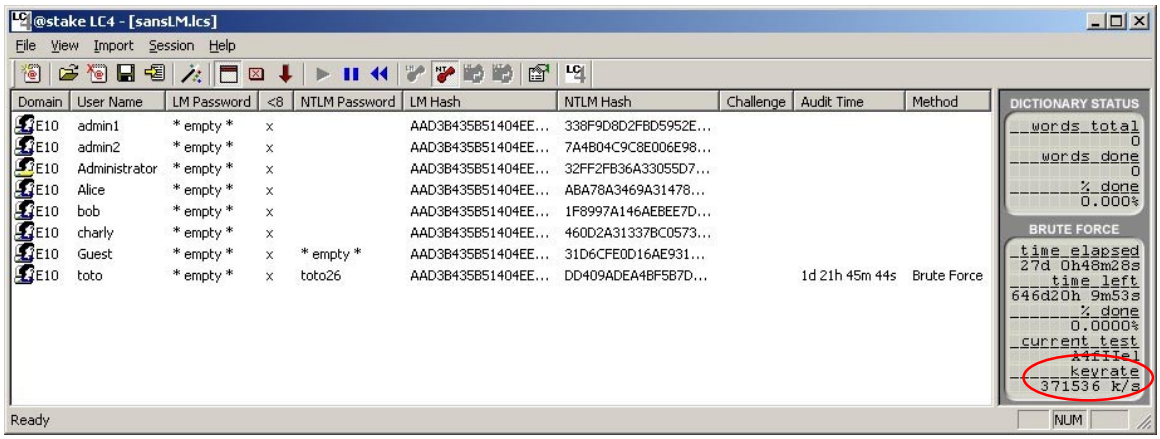
Remarques : Sur la capture ci-dessus, on constate que les *passwords* des comptes *Administrator*, *Alice* et *bob* ont été trouvé en même temps (7h41m17s). Cela est dû au fait que les 7 premiers caractères de ces 3 *passwords* en majuscule sont identiques et que la résolution de la deuxième partie des *passwords* est finit bien avant la première.

Les *passwords* des comptes *admin1* et *admin2* n'ont pas été résolus car ils contiennent des caractères spéciaux. Il est possible de configurer LC4 pour effectuer une attaque *brute force* utilisant ce type de caractères mais cela aurai pris plusieurs semaines.

Ce premier test montre bien que la longueur des *passwords* ne change pas beaucoup le temps de recherche si le *hash* LM est présent (7 car.). Par contre, on voit bien que les *passwords* simples sont « cassés » en quelques minutes, alors que des *passwords* employant des caractères spéciaux nécessite plusieurs semaines.

Pour le deuxième test, les *hash* LM sont supprimés de la SAM (voir § 4.4). En lançant LC4 (***Import – Import from local machine***), on constate que des *hashs* LM sont tout de même récupérés. En réalité, la valeur afficher correspond au résultat par défaut du *hash* LM s'il n'y a pas de *password*.

Le *hash* LM n'étant pas présent, LC4 doit s'attaquer au *hash* NTLM. Comme le *password* est *case-sensitive* et peut avoir 14 caractères, cela représante 62^{14} combinaisons **alphanumériques**.



Lors du lancement du test, on constate immédiatement que la génération des *hashs* NTLM est beaucoup plus lente (calcul sur 14 car.) que celle des *hashs* LM. En effet, l'attaque par dictionnaire à durée 55 minutes alors qu'il n'a fallu que 13 secondes pour les *hash* LM. Pour l'attaque *Brute Force*, LC4 calcule 380'000 *hash* NTLM par seconde contre 3'500'000 *hash* LM. L'attaque hybride étant estimée à plusieurs semaines, ce test n'est pas activé afin de passer directement au *Brute Force*.

On constate que le *password* de 6 caractères « toto26 » est retrouvé en 1 jour et 22 heure. Après 27 jours de test, aucun *password* de 8 caractères n'est découvert. Le temps estimé pour le calcule de toutes les combinaisons alphanumériques oscille entre 500 et 800 jours.

Remarque : Ces testes sont fait à l'aide d'un Pentium 4 (1,8G).

Ce test montre bien qu'il est plus difficile de retrouver un *password* à partir d'un *hash* NTLM. En plus de la complexité de l'algorithme (temps de calcule), d'un nombre de combinaisons plus important (62^{14} alphanumériques), la durée de l'attaque est, cette fois, directement dépendante de la longueur du *password*.

5.6 Suppression du *password* administrateur

Le *password* Administrateur peut être supprimé en effaçant le fichier SAM (p.272 [HalHac]). En faisant cela, tous les comptes locaux sont perdus. Par contre, lors du boot, Windows constate l'absence de la SAM et recrée une SAM d'origine contenant les comptes *Administrator* et *Guest*. Malheureusement, ces comptes ne sont pas protéger par un *password* et permette l'ouverture de session en tant qu'administrateur.

Pour effectuer cette attaque, il suffit de *bootter* la machine à l'aide d'une disquette DOS, de monter les partitions NTFS avec le logiciel NTFSDOS Pro (http://www.winternals.com) puis d'effacer la SAM dans le répertoire %systemroot%\system32\config\ .

Remarque : Cette opération n'est pas réalisable avec la version demo de NTFSDOS. En effet, l'effacement d'un fichier est considéré comme une écriture.

6 Conclusion

Kerberos est certainement le protocole offrant la meilleure sécurité sur des systèmes Win2k. Malheureusement, il n'existe encore aucun moyen pour désactiver tous les protocoles issus de *Lan Manager* et ainsi garantir l'utilisation de Kerberos. De plus, il est possible qu'un outil simple (comme LC4), permettant d'attaquer Kerberos, voit le jour dans un futur proche.

Les différents tests montrent l'importance de la « dureté » des *passwords*. Des *passwords* mal choisis peuvent être retrouver rapidement quel que soit le protocole utilisé.

Une solution à ces problèmes existe. Il s'agit de la mise en place de l'extension Kerberos PKINI utilisant une infrastructure PKI (clé asymétrique, certificat, CA, …) à la place du *username* et du *password*. Les avantages sont :

- Utilisation d'authentification forte (*token* + PIN)
- Attaques de type *brut force* irréalisable dans une durée acceptable
- Possibilité de forcer l'authentification par *token* dans un domaine Win2k (garanti la non-utilisation des protocoles issus de *Lan Manager*)

En permettant l'accès physique à une machine, il est difficile de garantir sa sécurité. C'est pour cela qu'il est important d'empêcher l'accès à une machine sensible (serveur) en la plaçant dans un local fermé à clé.

Pour des postes client, il est préférable de supprimer le *floppy* et le CDRom de la séquence de *boot*, de verrouillé le BIOS par un mot de passe, et de fermer le boîtier à l'aide d'un cadenas.

7 Sources

- **Halte aux Hacker (deuxième edition)** [HalHac]
  Scambray, McClure, Kurtz
  Editions OEM, ISBN 2-7464-0292-0

- **Hacking Windows 2000 Exposed** [Hac2kEx]
  Scambray, McClure
  Osborne / McGraw, ISBN 0-07-219262-3

- **Inside Windows 2000 Server** [InW2kS]
  William Boswell
  New Riders Publishing 2000, ISBN 1-56205-929-7

- **Cracking NTLMv2 Authentication** [CrNtlmPpt]
  http://www.blackhat.com/presentations/win-usa-02/urity-winsec02.ppt

- **Inside SP4 NTLMv2 Security Enhancements** [WM7072]
  http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7072

- **How to Disable LM Authentication on Windows NT** [Q147706]
  http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B147706

- **How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT** [Q239869]
  http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B239869

- **Remove LM Hashes from Active Directory and Security Account Manager** [Q299656]
  http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B299656

- **Win2K Password Protection** [WM15892]
  http://www.winnetmag.com/Articles/Index.cfm?ArticleID=15892

- **Feasibility of attacking Windows 2000 Kerberos Passwords** [AttKrbPa]
  http://www.brd.ie/papers/w2kkrb/feasibility_of_w2k_kerberos_attack.htm

Annexe 1

Netlogon entre 2 postes Win2k Level 0

```
Frame 19 (191 bytes on wire, 191 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: 10.1.2.24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1029 (1029), Dst Port: 139 (139), Seq: 179180367, Ack: 695332516, Len: 137
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response in: 20
      SMB Command: Negotiate Protocol (0x72)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x18
         0... .... = Request/Response: Message is a request to the server
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc853
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .1.. .... = Long Names Used: Path names in request are long file names
         .... .... .... .0.. = Security Signatures: Security signatures are not supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 0
      Multiplex ID: 0
   Negotiate Protocol Request (0x72)
      Word Count (WCT): 0
      Byte Count (BCC): 98
      Requested Dialects
         Dialect: PC NETWORK PROGRAM 1.0
         Dialect: LANMAN1.0
         Dialect: Windows for Workgroups 3.1a
         Dialect: LM1.2X002
         Dialect: LANMAN2.1
         Dialect: NT LM 0.12
```

```
Frame 20 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: 10.1.2.24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1029 (1029), Seq: 695332516, Ack: 179180504, Len: 89
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response to: 19
      Time from request: 0.000371000 seconds
      SMB Command: Negotiate Protocol (0x72)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x98
         1... .... = Request/Response: Message is a response to the client/redirector
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc853
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .1.. .... = Long Names Used: Path names in request are long file names
         .... .... .... .0.. = Security Signatures: Security signatures are not supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 0
      Multiplex ID: 0
   Negotiate Protocol Response (0x72)
      Word Count (WCT): 17
      Dialect Index: 5, greater than LANMAN2.1
      Security Mode: 0x03
         .... ...1 = Mode: USER security mode
         .... ..1. = Password: ENCRYPTED password. Use challenge/response
         .... .0.. = Signatures: Security signatures NOT enabled
         .... 0... = Sig Req: Security signatures NOT required
      Max Mpx Count: 50
      Max VCs: 1
      Max Buffer Size: 16644
      Max Raw Buffer: 65536
      Session Key: 0x00000000
      Capabilities: 0x8000f3fd
         .... .... .... .... .... .... .... ...1 = Raw Mode: Read Raw and Write Raw are supported
         .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
         .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
         .... .... .... .... .... .... .... 1... = Large Files: Large files are supported
         .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
         .... .... .... .... .... .... ..1. .... = RPC Remote APIs: RPC remote APIs are supported
         .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
         .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
         .... .... .... .... .... ...1 .... .... = Lock and Read: Lock and Read is supported
         .... .... .... .... .... ..1. .... .... = NT Find: NT Find is supported
         .... .... .... .... ...1 .... .... .... = Dfs: Dfs is supported
         .... .... .... .... ..1. .... .... .... = Infolevel Passthru: NT information level request passthrough is supported
         .... .... .... .... .1.. .... .... .... = Large ReadX: Large Read andX is supported
         .... .... .... .... 1... .... .... .... = Large WriteX: Large Write andX is supported
         .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
         .... ..0. .... .... .... .... .... .... = Reserved: Reserved
         ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
         .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
         1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
      System Time: Feb 25, 2003 11:42:04.287811279
      Server Time Zone: -60 min from UTC
      Key Length: 0
      Byte Count (BCC): 16
      Server GUID: 1F7724E6872BAA41A689B64C36457245
      Security Blob: <MISSING>
```

```
Frame 45 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: 10.1.2.24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1029 (1029), Dst Port: 139 (139), Seq: 179182200, Ack: 695333910, Len: 168
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response in: 46
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x18
         0... .... = Request/Response: Message is a request to the server
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
```

```
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 0
    Multiplex ID: 705
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 164
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 32
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ..0. .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 105
    Security Blob: 4E544C4D535350000100000097820 8E0...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        Flags: 0xe0088297
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
          .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
          .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
          .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
          .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
          .... .... .... .... 0... .... .... .... = Negotiate 0x00000800: Not set
          .... .... .... .... .0.. .... .... .... = Negotiate 0x00000400: Not set
          .... .... .... .... ..1. .... .... .... = Negotiate NTLM key: Set
          .... .... .... .... ...0 .... .... .... = Negotiate Netware: Not set
          .... .... .... .... .... 1... .... .... = Negotiate Lan Manager Key: Set
          .... .... .... .... .... .0.. .... .... = Negotiate Datagram Style: Not set
          .... .... .... .... .... ..0. .... .... = Negotiate Seal: Not set
          .... .... .... .... .... ...1 .... .... = Negotiate Sign: Set
          .... .... .... .... .... .... 0... .... = Request 0x00000008: Not set
          .... .... .... .... .... .... .1.. .... = Request Target: Set
          .... .... .... .... .... .... ..1. .... = Negotiate OEM: Set
          .... .... .... .... .... .... ...1 .... = Negotiate UNICODE: Set
        Calling workstation domain: NULL
        Calling workstation name: NULL
    Native OS: Windows 2000 2195
    Native LAN Manager: Windows 2000 5.0
    Primary Domain:
```

```
Frame 46 (273 bytes on wire, 273 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: 10.1.2.24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1029 (1029), Seq: 695333910, Ack: 179182368, Len: 219
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response to: 45
    Time from request: 0.000358000 seconds
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 8195
    Multiplex ID: 705
  Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 215
    Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Security Blob Length: 98
    Byte Count (BCC): 172
    Security Blob: 4E544C4D535350000200000006000600...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        Domain: V24
          Length: 6
          Maxlen: 6
          Offset: 48
        Flags: 0xe08a8215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
```

```
        ..1. .... .... .... .... .... .... = Negotiate 128: Set
        ...0 .... .... .... .... .... .... = Negotiate 0x10000000: Not set
        .... 0... .... .... .... .... .... = Negotiate 0x08000000: Not set
        .... .0.. .... .... .... .... .... = Negotiate 0x04000000: Not set
        .... ..0. .... .... .... .... .... = Negotiate 0x02000000: Not set
        .... ...0 .... .... .... .... .... = Negotiate 0x01000000: Not set
        .... .... 1... .... .... .... .... = Negotiate Target Info: Set
        .... .... .0.. .... .... .... .... = Negotiate 0x00400000: Not set
        .... .... ..0. .... .... .... .... = Negotiate 0x00200000: Not set
        .... .... ...0 .... .... .... .... = Negotiate 0x00100000: Not set
        .... .... .... 1... .... .... .... = Negotiate NTLM2 key: Set
        .... .... .... .0.. .... .... .... = Negotiate Challenge Non NT Session Key: Not set
        .... .... .... ..1. .... .... .... = Negotiate Challenge Accept Response: Set
        .... .... .... ...0 .... .... .... = Negotiate Challenge Init Response: Not set
        .... .... .... .... 1... .... .... = Negotiate Always Sign: Set
        .... .... .... .... .0.. .... .... = Negotiate This is Local Call: Not set
        .... .... .... .... ..0. .... .... = Negotiate Workstation Supplied: Not set
        .... .... .... .... ...0 .... .... = Negotiate Domain Supplied: Not set
        .... .... .... .... .... 0... .... = Negotiate 0x00000800: Not set
        .... .... .... .... .... .0.. .... = Negotiate 0x00000400: Not set
        .... .... .... .... .... ..1. .... = Negotiate NTLM key: Set
        .... .... .... .... .... ...0 .... = Negotiate Netware: Not set
        .... .... .... .... .... .... 0... = Negotiate Lan Manager Key: Not set
        .... .... .... .... .... .... .0.. = Negotiate Datagram Style: 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
        .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
    NTLM Challenge: 8998332BC906CE06
    Reserved: 0000000000000000
    Address List
      Length: 44
      Maxlen: 44
      Offset: 54
      Domain NetBIOS Name: V24
      Server NetBIOS Name: V24
      Domain DNS Name: v24
      Server DNS Name: v24
  Native OS: Windows 5.0
  Native LAN Manager: Windows 2000 LAN Manager
```

```
Frame 47 (352 bytes on wire, 352 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: 10.1.2.24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1029 (1029), Dst Port: 139 (139), Seq: 179182368, Ack: 695334129, Len: 298
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response in: 48
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_SUCCESS (0x00000000)
    Flags: 0x18
      0... .... = Request/Response: Message is a request to the server
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 8195
    Multiplex ID: 769
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 294
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 162
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ..0. .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 235
    Security Blob: 4E544C4D535350000300000018001800...
    NTLMSSP
      NTLMSSP identifier: NTLMSSP
      NTLM Message Type: NTLMSSP_AUTH (0x00000003)
      Lan Manager Response: 8C684487A3F9D25F0000000000000000...
        Length: 24
        Maxlen: 24
        Offset: 98
      NTLM Response: B55DE25D38CD931F2BC2E508EEFDA365...
        Length: 24
        Maxlen: 24
        Offset: 122
      Domain name: V26PRO
        Length: 12
        Maxlen: 12
        Offset: 64
      User name: alice
        Length: 10
        Maxlen: 10
        Offset: 76
      Host name: V26PRO
        Length: 12
        Maxlen: 12
        Offset: 86
      Session Key: D38A784A84EF19F8F9A17B391BD850EE
        Length: 16
        Maxlen: 16
        Offset: 146
      Flags: 0xe0888215
        1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
        .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
        ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
        ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
        .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
        .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
        .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
        .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
        .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
```

```
            .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
            .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
            .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
            .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
            .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
            .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
            .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
        Native OS: Windows 2000 2195
        Native LAN Manager: Windows 2000 5.0
        Primary Domain:
```

```
Frame 48 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: 10.1.2.24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1029 (1029), Seq: 695334129, Ack: 179182666, Len: 121
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 47
        Time from request: 0.000730000 seconds
        SMB Command: Session Setup AndX (0x73)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x98
            1... .... = Request/Response: Message is a response to the client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .0.. .... = Long Names Used: Path names in request are not long file names
            .... .... .... .1.. = Security Signatures: Security signatures are supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 8195
        Multiplex ID: 769
    Session Setup AndX Response (0x73)
        Word Count (WCT): 4
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 117
        Action: 0x0000
            .... .... .... ...0 = Guest: Not logged in as GUEST
        Security Blob Length: 0
        Byte Count (BCC): 74
        Security Blob: <MISSING>
        Native OS: Windows 5.0
        Native LAN Manager: Windows 2000 LAN Manager
```

Annexe 2

Netlogon entre 2 postes Win2k Level 2

```
Frame 17 (191 bytes on wire, 191 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 247180332, Ack: 317719029, Len: 137
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 18
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Request (0x72)
        Word Count (WCT): 0
        Byte Count (BCC): 98
        Requested Dialects
            Dialect: PC NETWORK PROGRAM 1.0
            Dialect: LANMAN1.0
            Dialect: Windows for Workgroups 3.1a
            Dialect: LM1.2X002
            Dialect: LANMAN2.1
            Dialect: NT LM 0.12
```

```
Frame 18 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 317719029, Ack: 247180469, Len: 89
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 17
        Time from request: 0.000359000 seconds
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x98
            1... .... = Request/Response: Message is a response to the client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Response (0x72)
        Word Count (WCT): 17
        Dialect Index: 5, greater than LANMAN2.1
        Security Mode: 0x03
        Max Mpx Count: 50
        Max VCs: 1
        Max Buffer Size: 16644
        Max Raw Buffer: 65536
        Session Key: 0x00000000
        Capabilities: 0x8000f3fd
            .... .... .... .... .... .... .... ...1 = Raw Mode: Read Raw and Write Raw are supported
            .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
            .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
            .... .... .... .... .... .... .... 1... = Large Files: Large files are supported
            .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
            .... .... .... .... .... .... ..1. .... = RPC Remote APIs: RPC remote APIs are supported
            .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
            .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
            .... .... .... .... .... ...1 .... .... = Lock and Read: Lock and Read is supported
            .... .... .... .... .... ..1. .... .... = NT Find: NT Find is supported
            .... .... .... .... ...1 .... .... .... = Dfs: Dfs is supported
            .... .... .... .... ..1. .... .... .... = Infolevel Passthru: NT information level request passthrough is supported
            .... .... .... .... .1.. .... .... .... = Large ReadX: Large Read andX is supported
            .... .... .... .... 1... .... .... .... = Large WriteX: Large Write andX is supported
            .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
            .... ..0. .... .... .... .... .... .... = Reserved: Reserved
            ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
            .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
            1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
        System Time: Feb 27, 2003 09:41:44.640859603
        Server Time Zone: -60 min from UTC
        Key Length: 0
        Byte Count (BCC): 16
        Server GUID: 1F7724E6872BAA41A689B64C36457245
        Security Blob: <MISSING>
```

```
Frame 41 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 247182165, Ack: 317720423, Len: 168
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 42
        SMB Command: Session Setup AndX (0x73)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
```

```
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 0
    Multiplex ID: 705
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 164
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 32
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ...0 .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 105
    Security Blob: 4E544C4D53535000010000000978208E0...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        Flags: 0xe0088297
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
          .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
          .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
          .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
          .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
          .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
          .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
          .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
          .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
          .... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
          .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: Not set
          .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
          .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
          .... .... .... .... .... .... 0... .... = Request 0x00000008: Not set
          .... .... .... .... .... .... .1.. .... = Request Target: Set
          .... .... .... .... .... .... ..1. .... = Negotiate OEM: Set
          .... .... .... .... .... .... ...1 .... = Negotiate UNICODE: Set
        Calling workstation domain: NULL
        Calling workstation name: NULL
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 42 (273 bytes on wire, 273 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 317720423, Ack: 247182333, Len: 219
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response to: 41
    Time from request: 0.000327000 seconds
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 2051
    Multiplex ID: 705
  Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 215
    Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Security Blob Length: 98
    Byte Count (BCC): 172
    Security Blob: 4E544C4D535350000200000006000600...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        Domain: V24
          Length: 6
          Maxlen: 6
          Offset: 48
        Flags: 0xe08a8215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
```

```
            .... ...0 .... .... .... .... .... = Negotiate 0x01000000: Not set
            .... .... 1... .... .... .... .... = Negotiate Target Info: Set
            .... .... .0.. .... .... .... .... = Negotiate 0x00400000: Not set
            .... .... ..0. .... .... .... .... = Negotiate 0x00200000: Not set
            .... .... ...0 .... .... .... .... = Negotiate 0x00100000: Not set
            .... .... .... 1... .... .... .... = Negotiate NTLM2 key: Set
            .... .... .... .0.. .... .... .... = Negotiate Challenge Non NT Session Key: Not set
            .... .... .... ..1. .... .... .... = Negotiate Challenge Accept Response: Set
            .... .... .... ...0 .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
        NTLM Challenge: 4C8EF9297CD3822B
        Reserved: 0000000000000000
        Address List
          Length: 44
          Maxlen: 44
          Offset: 54
          Domain NetBIOS Name: V24
          Server NetBIOS Name: V24
          Domain DNS Name: v24
          Server DNS Name: v24
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

```
Frame 43 (352 bytes on wire, 352 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 247182333, Ack: 317720642, Len: 298
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response in: 44
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_SUCCESS (0x00000000)
    Flags: 0x18
      0... .... = Request/Response: Message is a request to the server
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 2051
    Multiplex ID: 769
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 294
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 162
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... .... ..0. = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .... .1.. = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... .... 1... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... .... .... ...0 = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... .... ..0. .... = NT Find: NT Find is not supported
      .... .... .... .... .... .... ...0 .... = Dfs: Dfs is not supported
      .... .... .... .... .... .... ..0. .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .... .... .0.. .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... .... .... 0... .... = Large WriteX: Large Write andX is not supported
      .... .... .... .... .... .... .... 0... = UNIX: UNIX extensions are not supported
      .... .... .... .... .... .... ..0. .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 235
    Security Blob: 4E544C4D535350000300000018001800...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_AUTH (0x00000003)
        Lan Manager Response: 3A44D620AB27440700000000000000000...
          Length: 24
          Maxlen: 24
          Offset: 98
        NTLM Response: 603D546E7DA8FC46DBFD7923945818A7...
          Length: 24
          Maxlen: 24
          Offset: 122
        Domain name: V26PRO
          Length: 12
          Maxlen: 12
          Offset: 64
        User name: alice
          Length: 10
          Maxlen: 10
          Offset: 76
        Host name: V26PRO
          Length: 12
          Maxlen: 12
          Offset: 86
        Session Key: FFF876B9676AA2B8D78CB5ED389DD038
          Length: 16
          Maxlen: 16
          Offset: 146
        Flags: 0xe0888215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
```

```
            .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
            .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 44 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 317720642, Ack: 247182631, Len: 121
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response to: 43
      Time from request: 0.000698000 seconds
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x98
         1... .... = Request/Response: Message is a response to the client/redirector
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc807
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .0.. .... = Long Names Used: Path names in request are not long file names
         .... .... .... .1.. = Security Signatures: Security signatures are supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 2051
      Multiplex ID: 769
   Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 117
      Action: 0x0000
         .... .... .... ...0 = Guest: Not logged in as GUEST
      Security Blob Length: 0
      Byte Count (BCC): 74
      Security Blob: <MISSING>
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

Annexe 3

Netlogon entre 2 postes Win2k Level 3

```
Frame 10 (191 bytes on wire, 191 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 1013313418, Ack: 2462554430, Len: 137
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 11
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Request (0x72)
        Word Count (WCT): 0
        Byte Count (BCC): 98
        Requested Dialects
            Dialect: PC NETWORK PROGRAM 1.0
            Dialect: LANMAN1.0
            Dialect: Windows for Workgroups 3.1a
            Dialect: LM1.2X002
            Dialect: LANMAN2.1
            Dialect: NT LM 0.12

Frame 11 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2462554430, Ack: 1013313555, Len: 89
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 10
        Time from request: 0.000362000 seconds
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x98
            1... .... = Request/Response: Message is a response to the client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Response (0x72)
        Word Count (WCT): 17
        Dialect Index: 5, greater than LANMAN2.1
        Security Mode: 0x03
        Max Mpx Count: 50
        Max VCs: 1
        Max Buffer Size: 16644
        Max Raw Buffer: 65536
        Session Key: 0x00000000
        Capabilities: 0x8000f3fd
            .... .... .... .... .... .... .... ...1 = Raw Mode: Read Raw and Write Raw are supported
            .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
            .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
            .... .... .... .... .... .... .... 1... = Large Files: Large files are supported
            .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
            .... .... .... .... .... .... ..1. .... = RPC Remote APIs: RPC remote APIs are supported
            .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
            .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
            .... .... .... .... .... ...1 .... .... = Lock and Read: Lock and Read is supported
            .... .... .... .... .... ..1. .... .... = NT Find: NT Find is supported
            .... .... .... .... .... ..1 .... .... = Dfs: Dfs is supported
            .... .... .... .... .... .1.. .... .... = Infolevel Passthru: NT information level request passthrough is supported
            .... .... .... .... .... 1... .... .... = Large ReadX: Large Read andX is supported
            .... .... .... .... ...1 .... .... .... = Large WriteX: Large Write andX is supported
            .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
            .... ..0. .... .... .... .... .... .... = Reserved: Reserved
            ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
            .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
            1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
        System Time: Feb 27, 2003 08:39:08.265157699
        Server Time Zone: -60 min from UTC
        Key Length: 0
        Byte Count (BCC): 16
        Server GUID: 1F7724E6872BAA41A689B64C36457245
        Security Blob: <MISSING>
```

```
Frame 63 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 1013315964, Ack: 2462556121, Len: 168
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 64
        SMB Command: Session Setup AndX (0x73)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
        .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
        .... .... .0.. .... = Long Names Used: Path names in request are not long file names
        .... .... .... .1.. = Security Signatures: Security signatures are supported
        .... .... .... ..1. = Extended Attributes: Extended attributes are supported
        .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 0
    Multiplex ID: 897
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 164
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 32
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ..0. .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 105
    Security Blob: 4E544C4D535350000100000097820 8E0...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        Flags: 0xe0088297
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
          .... .... .... 1... .... .... .... .... = Negotiate Always Sign: Set
          .... .... .... .0.. .... .... .... .... = Negotiate This is Local Call: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Workstation Supplied: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Domain Supplied: Not set
          .... .... .... .... 0... .... .... .... = Negotiate 0x00000800: Not set
          .... .... .... .... .0.. .... .... .... = Negotiate 0x00000400: Not set
          .... .... .... .... ..1. .... .... .... = Negotiate NTLM key: Set
          .... .... .... .... ...0 .... .... .... = Negotiate Netware: Not set
          .... .... .... .... .... 1... .... .... = Negotiate Lan Manager Key: Set
          .... .... .... .... .... .0.. .... .... = Negotiate Datagram Style: Not set
          .... .... .... .... .... ..0. .... .... = Negotiate Seal: Not set
          .... .... .... .... .... ...1 .... .... = Negotiate Sign: Set
          .... .... .... .... .... .... 0... .... = Request 0x00000008: Not set
          .... .... .... .... .... .... .1.. .... = Request Target: Set
          .... .... .... .... .... .... ..1. .... = Negotiate OEM: Set
          .... .... .... .... .... .... ...1 .... = Negotiate UNICODE: Set
        Calling workstation domain: NULL
        Calling workstation name: NULL
    Native OS: Windows 2000 2195
    Native LAN Manager: Windows 2000 5.0
    Primary Domain:
```

```
Frame 64 (273 bytes on wire, 273 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2462556121, Ack: 1013316132, Len: 219
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response to: 63
    Time from request: 0.000345000 seconds
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 4097
    Multiplex ID: 897
  Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 215
    Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Security Blob Length: 98
    Byte Count (BCC): 172
    Security Blob: 4E544C4D535350000200000006000600...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        Domain: V24
          Length: 6
          Maxlen: 6
          Offset: 48
        Flags: 0xe08a8215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
```

```
            .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
            .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
            .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
            .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
            .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
            .... .... .... ..1. .... .... .... .... = Negotiate Challenge Accept Response: Set
            .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
          NTLM Challenge: 8D13AA0C3F057704
          Reserved: 0000000000000000
          Address List
            Length: 44
            Maxlen: 44
            Offset: 54
            Domain NetBIOS Name: V24
            Server NetBIOS Name: V24
            Domain DNS Name: v24
            Server DNS Name: v24
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

```
Frame 65 (414 bytes on wire, 414 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 1013316132, Ack: 2462556340, Len: 360
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response in: 66
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_SUCCESS (0x00000000)
    Flags: 0x18
      0... .... = Request/Response: Message is a request to the server
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 4097
    Multiplex ID: 961
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 356
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 224
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ..0. .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 297
    Security Blob: 4E544C4D535350000300000001800...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_AUTH (0x00000003)
        Lan Manager Response: A1DCC4822B1D6AD9F9B141DABA36085E...
          Length: 24
          Maxlen: 24
          Offset: 92
        NTLM Response: 48C25F6F31D2C1757CA336B73A089E2E...
          Length: 92
          Maxlen: 92
          Offset: 116
        Domain name: v24
          Length: 6
          Maxlen: 6
          Offset: 64
        User name: alice
          Length: 10
          Maxlen: 10
          Offset: 70
        Host name: V26PRO
          Length: 12
          Maxlen: 12
          Offset: 80
        Session Key: 3E933EBE4BE98A2BA166BFCF0DF2A65F
          Length: 16
          Maxlen: 16
          Offset: 208
        Flags: 0xe0888215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
```

```
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 66 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2462556340, Ack: 1013316492, Len: 121
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response to: 65
      Time from request: 0.000780000 seconds
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x98
         1... .... = Request/Response: Message is a response to the client/redirector
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc807
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .0.. .... = Long Names Used: Path names in request are not long file names
         .... .... .... .1.. = Security Signatures: Security signatures are supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 4097
      Multiplex ID: 961
   Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 117
      Action: 0x0000
         .... .... .... ...0 = Guest: Not logged in as GUEST
      Security Blob Length: 0
      Byte Count (BCC): 74
      Security Blob: <MISSING>
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

Annexe 4

Netlogon entre 2 postes Win2k Level 4

```
Frame 10 (191 bytes on wire, 191 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1032 (1032), Dst Port: 139 (139), Seq: 3228751112, Ack: 1102346586, Len: 137
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 11
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Request (0x72)
        Word Count (WCT): 0
        Byte Count (BCC): 98
        Requested Dialects
            Dialect: PC NETWORK PROGRAM 1.0
            Dialect: LANMAN1.0
            Dialect: Windows for Workgroups 3.1a
            Dialect: LM1.2X002
            Dialect: LANMAN2.1
            Dialect: NT LM 0.12
```

```
Frame 11 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1032 (1032), Seq: 1102346586, Ack: 3228751249, Len: 89
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 10
        Time from request: 0.000350000 seconds
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x98
            1... .... = Request/Response: Message is a response to the client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Response (0x72)
        Word Count (WCT): 17
        Dialect Index: 5, greater than LANMAN2.1
        Security Mode: 0x03
        Max Mpx Count: 50
        Max VCs: 1
        Max Buffer Size: 16644
        Max Raw Buffer: 65536
        Session Key: 0x00000000
        Capabilities: 0x8000f3fd
            .... .... .... .... .... .... .... ...1 = Raw Mode: Read Raw and Write Raw are supported
            .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
            .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
            .... .... .... .... .... .... .... 1... = Large Files: Large files are supported
            .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
            .... .... .... .... .... .... ..1. .... = RPC Remote APIs: RPC remote APIs are supported
            .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
            .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
            .... .... .... .... .... ...1 .... .... = Lock and Read: Lock and Read is supported
            .... .... .... .... .... ..1. .... .... = NT Find: NT Find is supported
            .... .... .... .... ...1 .... .... .... = Dfs: Dfs is supported
            .... .... .... .... ..1. .... .... .... = Infolevel Passthru: NT information level request passthrough is supported
            .... .... .... .... .1.. .... .... .... = Large ReadX: Large Read andX is supported
            .... .... .... .... 1... .... .... .... = Large WriteX: Large Write andX is supported
            .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
            .... ..0. .... .... .... .... .... .... = Reserved: Reserved
            ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
            .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
            1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
        System Time: Feb 27, 2003 09:00:52.492683410
        Server Time Zone: -60 min from UTC
        Key Length: 0
        Byte Count (BCC): 16
        Server GUID: 1F7724E6872BAA41A689B64C36457245
        Security Blob: <MISSING>
```

```
Frame 78 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1032 (1032), Dst Port: 139 (139), Seq: 3228753658, Ack: 1102348277, Len: 168
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 79
        SMB Command: Session Setup AndX (0x73)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
```

```
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 0
    Multiplex ID: 897
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 164
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 32
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ...0 .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 105
    Security Blob: 4E544C4D53535000010000000978208E0...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        Flags: 0xe0088297
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
          .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
          .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
          .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
          .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
          .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
          .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
          .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
          .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
          .... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
          .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: Not set
          .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
          .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
          .... .... .... .... .... .... 0... .... = Request 0x00000008: Not set
          .... .... .... .... .... .... .1.. .... = Request Target: Set
          .... .... .... .... .... .... ..1. .... = Negotiate OEM: Set
          .... .... .... .... .... .... ...1 .... = Negotiate UNICODE: Set
        Calling workstation domain: NULL
        Calling workstation name: NULL
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 79 (273 bytes on wire, 273 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1032 (1032), Seq: 1102348277, Ack: 3228753826, Len: 219
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response to: 78
    Time from request: 0.000347000 seconds
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 4097
    Multiplex ID: 897
  Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 215
    Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Security Blob Length: 98
    Byte Count (BCC): 172
    Security Blob: 4E544C4D535350000200000006000600...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        Domain: V24
          Length: 6
          Maxlen: 6
          Offset: 48
        Flags: 0xe08a8215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
```

```
            .... ...0 .... .... .... .... .... = Negotiate 0x01000000: Not set
            .... .... 1... .... .... .... .... = Negotiate Target Info: Set
            .... .... .0.. .... .... .... .... = Negotiate 0x00400000: Not set
            .... .... ..0. .... .... .... .... = Negotiate 0x00200000: Not set
            .... .... ...0 .... .... .... .... = Negotiate 0x00100000: Not set
            .... .... .... 1... .... .... .... = Negotiate NTLM2 key: Set
            .... .... .... .0.. .... .... .... = Negotiate Challenge Non NT Session Key: Not set
            .... .... .... ..1. .... .... .... = Negotiate Challenge Accept Response: Set
            .... .... .... ...0 .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
         NTLM Challenge: DEA85EE45068435A
         Reserved: 0000000000000000
         Address List
            Length: 44
            Maxlen: 44
            Offset: 54
            Domain NetBIOS Name: V24
            Server NetBIOS Name: V24
            Domain DNS Name: v24
            Server DNS Name: v24
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

```
Frame 80 (414 bytes on wire, 414 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1032 (1032), Dst Port: 139 (139), Seq: 3228753826, Ack: 1102348496, Len: 360
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response in: 81
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x18
         0... .... = Request/Response: Message is a request to the server
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc807
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .0.. .... = Long Names Used: Path names in request are not long file names
         .... .... .... .1.. = Security Signatures: Security signatures are supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 4097
      Multiplex ID: 961
   Session Setup AndX Request (0x73)
      Word Count (WCT): 12
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 356
      Max Buffer: 16644
      Max Mpx Count: 50
      VC Number: 1
      Session Key: 0x00000000
      Security Blob Length: 224
      Reserved: 00000000
      Capabilities: 0x800000d4
         .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
         .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
         .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
         .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
         .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
         .... .... .... .... .... .... .... ..0. = RPC Remote APIs: RPC remote APIs are not supported
         .... .... .... .... .... .... .... .1.. = NT Status Codes: NT status codes are supported
         .... .... .... .... .... .... .... 1... = Level 2 Oplocks: Level 2 oplocks are supported
         .... .... .... .... .... .... .... ...0 = Lock and Read: Lock and Read is not supported
         .... .... .... .... .... .... .... ..0. = NT Find: NT Find is not supported
         .... .... .... .... .... .... .... ...0 = Dfs: Dfs is not supported
         .... .... .... .... .... .... ...0 .... = Infolevel Passthru: NT information level request passthrough is not supported
         .... .... .... .... .... .... .0.. .... = Large ReadX: Large Read andX is not supported
         .... .... .... .... .... .... 0... .... = Large WriteX: Large Write andX is not supported
         .... .... .... .... .... .... 0... .... = UNIX: UNIX extensions are not supported
         .... .... .... .... .... .... ..0. .... = Reserved: Reserved
         .... .... .... .... .... .... .0.. .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
         .... .... .... .... .... .... 0... .... = Compressed Data: Compressed data transfer is not supported
         .... .... .... .... .... .... 1... .... = Extended Security: Extended security exchanges are supported
      Byte Count (BCC): 297
      Security Blob: 4E544C4D535350000300000018001800...
         NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_AUTH (0x00000003)
            Lan Manager Response: 9F23454864EEE4197031507D7F1FFA0D...
               Length: 24
               Maxlen: 24
               Offset: 92
            NTLM Response: 2A616B1590830B968C2188D3C55271E8...
               Length: 92
               Maxlen: 92
               Offset: 116
            Domain name: v24
               Length: 6
               Maxlen: 6
               Offset: 64
            User name: alice
               Length: 10
               Maxlen: 10
               Offset: 70
            Host name: V26PRO
               Length: 12
               Maxlen: 12
               Offset: 80
            Session Key: 10BD045382A15A2415CEFFA5BFDDA146
               Length: 16
               Maxlen: 16
               Offset: 208
            Flags: 0xe0888215
               1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
               .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
               ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
               ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
               .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
               .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
               .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
               .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
               .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
               .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
               .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
               .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
               .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
               .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
```

```
            .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
            .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 81 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1032 (1032), Seq: 1102348496, Ack: 3228754186, Len: 121
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response to: 80
      Time from request: 0.000779000 seconds
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x98
         1... .... = Request/Response: Message is a response to the client/redirector
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc807
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .0.. .... = Long Names Used: Path names in request are not long file names
         .... .... .... .1.. = Security Signatures: Security signatures are supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 4097
      Multiplex ID: 961
   Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 117
      Action: 0x0000
         .... .... .... ...0 = Guest: Not logged in as GUEST
      Security Blob Length: 0
      Byte Count (BCC): 74
      Security Blob: <MISSING>
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

Annexe 5

Netlogon entre 2 postes Win2k Level 5

```
Frame 13 (191 bytes on wire, 191 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 2597631364, Ack: 2340843329, Len: 137
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 14
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Request (0x72)
        Word Count (WCT): 0
        Byte Count (BCC): 98
        Requested Dialects
            Dialect: PC NETWORK PROGRAM 1.0
            Dialect: LANMAN1.0
            Dialect: Windows for Workgroups 3.1a
            Dialect: LM1.2X002
            Dialect: LANMAN2.1
            Dialect: NT LM 0.12
```

```
Frame 14 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2340843329, Ack: 2597631501, Len: 89
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 13
        Time from request: 0.000373000 seconds
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x98
            1... .... = Request/Response: Message is a response to the client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 00000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Response (0x72)
        Word Count (WCT): 17
        Dialect Index: 5, greater than LANMAN2.1
        Security Mode: 0x03
        Max Mpx Count: 50
        Max VCs: 1
        Max Buffer Size: 16644
        Max Raw Buffer: 65536
        Session Key: 0x00000000
        Capabilities: 0x8000f3fd
            .... .... .... .... .... .... .... ...1 = Raw Mode: Read Raw and Write Raw are supported
            .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
            .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
            .... .... .... .... .... .... .... 1... = Large Files: Large files are supported
            .... .... .... .... .... .... ...1 .... = NT SMBs: NT SMBs are supported
            .... .... .... .... .... .... ..1. .... = RPC Remote APIs: RPC remote APIs are supported
            .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
            .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
            .... .... .... .... .... ...1 .... .... = Lock and Read: Lock and Read is supported
            .... .... .... .... .... ..1. .... .... = NT Find: NT Find is supported
            .... .... .... .... ...1 .... .... .... = Dfs: Dfs is supported
            .... .... .... .... ..1. .... .... .... = Infolevel Passthru: NT information level request passthrough is supported
            .... .... .... .... .1.. .... .... .... = Large ReadX: Large Read andX is supported
            .... .... .... .... 1... .... .... .... = Large WriteX: Large Write andX is supported
            .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
            .... ..0. .... .... .... .... .... .... = Reserved: Reserved
            ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
            .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
            1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
        System Time: Feb 27, 2003 09:09:01.134315490
        Server Time Zone: -60 min from UTC
        Key Length: 0
        Byte Count (BCC): 16
        Server GUID: 1F7724E6872BAA41A689B64C36457245
        Security Blob: <MISSING>
```

```
Frame 60 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 2597633910, Ack: 2340845020, Len: 168
NetBIOS Session Service
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 61
        SMB Command: Session Setup AndX (0x73)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
```

```
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 0
    Multiplex ID: 897
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 164
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 32
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... ...0 .... = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .1.. .... = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... 1... .... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... ...0 .... .... = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... ..0. .... .... = NT Find: NT Find is not supported
      .... .... .... .... ...0 .... .... .... = Dfs: Dfs is not supported
      .... .... .... .... ..0. .... .... .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .0.. .... .... .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... 0... .... .... .... = Large WriteX: Large Write andX is not supported
      .... .... 0... .... .... .... .... .... = UNIX: UNIX extensions are not supported
      .... ..0. .... .... .... .... .... .... = Reserved: Reserved
      ..0. .... .... .... .... .... .... .... = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .0.. .... .... .... .... .... .... .... = Compressed Data: Compressed data transfer is not supported
      1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 105
    Security Blob: 4E544C4D53535000010000000978208E0...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        Flags: 0xe0088297
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
          .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
          .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
          .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
          .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
          .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
          .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
          .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
          .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
          .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
          .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
          .... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
          .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: Not set
          .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
          .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
          .... .... .... .... .... .... 0... .... = Request 0x00000008: Not set
          .... .... .... .... .... .... .1.. .... = Request Target: Set
          .... .... .... .... .... .... ..1. .... = Negotiate OEM: Set
          .... .... .... .... .... .... ...1 .... = Negotiate UNICODE: Set
        Calling workstation domain: NULL
        Calling workstation name: NULL
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 61 (273 bytes on wire, 273 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2340845020, Ack: 2597634078, Len: 219
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response to: 60
    Time from request: 0.000354000 seconds
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 4097
    Multiplex ID: 897
  Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 215
    Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Security Blob Length: 98
    Byte Count (BCC): 172
    Security Blob: 4E544C4D535350000200000006000600...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        Domain: V24
          Length: 6
          Maxlen: 6
          Offset: 48
        Flags: 0xe08a8215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
```

```
            .... ...0 .... .... .... .... .... = Negotiate 0x01000000: Not set
            .... .... 1... .... .... .... .... = Negotiate Target Info: Set
            .... .... .0.. .... .... .... .... = Negotiate 0x00400000: Not set
            .... .... ..0. .... .... .... .... = Negotiate 0x00200000: Not set
            .... .... ...0 .... .... .... .... = Negotiate 0x00100000: Not set
            .... .... .... 1... .... .... .... = Negotiate NTLM2 key: Set
            .... .... .... .0.. .... .... .... = Negotiate Challenge Non NT Session Key: Not set
            .... .... .... ..1. .... .... .... = Negotiate Challenge Accept Response: Set
            .... .... .... ...0 .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
        NTLM Challenge: 54E633D6ADA9BC31
        Reserved: 0000000000000000
        Address List
          Length: 44
          Maxlen: 44
          Offset: 54
          Domain NetBIOS Name: V24
          Server NetBIOS Name: V24
          Domain DNS Name: v24
          Server DNS Name: v24
    Native OS: Windows 5.0
    Native LAN Manager: Windows 2000 LAN Manager
```

```
Frame 62 (414 bytes on wire, 414 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9b:3b:98
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: V24 (10.1.2.24)
Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: 139 (139), Seq: 2597634078, Ack: 2340845239, Len: 360
NetBIOS Session Service
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    Response in: 63
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_SUCCESS (0x00000000)
    Flags: 0x18
      0... .... = Request/Response: Message is a request to the server
      .0.. .... = Notify: Notify client only on open
      ..0. .... = Oplocks: OpLock not requested/granted
      ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
      .... 1... = Case Sensitivity: Path names are caseless
      .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
      .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
    Flags2: 0xc807
      1... .... .... .... = Unicode Strings: Strings are Unicode
      .1.. .... .... .... = Error Code Type: Error codes are NT error codes
      ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
      ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
      .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
      .... .... .0.. .... = Long Names Used: Path names in request are not long file names
      .... .... .... .1.. = Security Signatures: Security signatures are supported
      .... .... .... ..1. = Extended Attributes: Extended attributes are supported
      .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
    Reserved: 00000000000000000000000000
    Tree ID: 0
    Process ID: 65279
    User ID: 4097
    Multiplex ID: 961
  Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 356
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 224
    Reserved: 00000000
    Capabilities: 0x800000d4
      .... .... .... .... .... .... .... ...0 = Raw Mode: Read Raw and Write Raw are not supported
      .... .... .... .... .... .... .... ..0. = MPX Mode: Read Mpx and Write Mpx are not supported
      .... .... .... .... .... .... .... .1.. = Unicode: Unicode strings are supported
      .... .... .... .... .... .... .... 0... = Large Files: Large files are not supported
      .... .... .... .... .... .... .... ...1 = NT SMBs: NT SMBs are supported
      .... .... .... .... .... .... .... ..0. = RPC Remote APIs: RPC remote APIs are not supported
      .... .... .... .... .... .... .... .1.. = NT Status Codes: NT status codes are supported
      .... .... .... .... .... .... .... 1... = Level 2 Oplocks: Level 2 oplocks are supported
      .... .... .... .... .... .... .... ...0 = Lock and Read: Lock and Read is not supported
      .... .... .... .... .... .... .... ..0. = NT Find: NT Find is not supported
      .... .... .... .... .... .... .... ...0 = Dfs: Dfs is not supported
      .... .... .... .... .... .... ...0. .... = Infolevel Passthru: NT information level request passthrough is not supported
      .... .... .... .... .... .... .0.. .... = Large ReadX: Large Read andX is not supported
      .... .... .... .... .... .... 0... .... = Large WriteX: Large Write andX is not supported
      .... .... .... .... .... .... .... 0... = UNIX: UNIX extensions are not supported
      .... .... .... .... .... .... .... ..0. = Reserved: Reserved
      .... .... .... .... .... .... .... .0.. = Bulk Transfer: Bulk Read and Bulk Write are not supported
      .... .... .... .... .... .... .... 0... = Compressed Data: Compressed data transfer is not supported
      .... .... .... .... .... .... .... 1... = Extended Security: Extended security exchanges are supported
    Byte Count (BCC): 297
    Security Blob: 4E544C4D535350000300000018001800...
      NTLMSSP
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_AUTH (0x00000003)
        Lan Manager Response: 610C7B39C6FD74E0ECEA76D2C2C767CF...
          Length: 24
          Maxlen: 24
          Offset: 92
        NTLM Response: C9D067C70E7C463134B95F0758E5E7E5...
          Length: 92
          Maxlen: 92
          Offset: 116
        Domain name: v24
          Length: 6
          Maxlen: 6
          Offset: 64
        User name: alice
          Length: 10
          Maxlen: 10
          Offset: 70
        Host name: V26PRO
          Length: 12
          Maxlen: 12
          Offset: 80
        Session Key: 48FA5ABF4C710953D38E8BAA46393704
          Length: 16
          Maxlen: 16
          Offset: 208
        Flags: 0xe0888215
          1... .... .... .... .... .... .... .... = Negotiate 0x80000000: Set
          .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
          ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
          ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
          .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
          .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
          .... ..0. .... .... .... .... .... .... = Negotiate 0x02000000: Not set
          .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
          .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
          .... .... .0.. .... .... .... .... .... = Negotiate 0x00400000: Not set
          .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
          .... .... ...0 .... .... .... .... .... = Negotiate 0x00100000: Not set
          .... .... .... 1... .... .... .... .... = Negotiate NTLM2 key: Set
          .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
```

```
            .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
            .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
            .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
            .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
            .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
            .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
            .... .... .... .... .... 0... .... .... = Negotiate 0x00000800: Not set
            .... .... .... .... .... .0.. .... .... = Negotiate 0x00000400: Not set
            .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
            .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
            .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
            .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: 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
            .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

```
Frame 63 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: 00:04:76:9b:3b:98, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: V24 (10.1.2.24), Dst Addr: 10.1.2.26 (10.1.2.26)
Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1030 (1030), Seq: 2340845239, Ack: 2597634438, Len: 121
NetBIOS Session Service
SMB (Server Message Block Protocol)
   SMB Header
      Server Component: SMB
      Response to: 62
      Time from request: 0.000810000 seconds
      SMB Command: Session Setup AndX (0x73)
      NT Status: STATUS_SUCCESS (0x00000000)
      Flags: 0x98
         1... .... = Request/Response: Message is a response to the client/redirector
         .0.. .... = Notify: Notify client only on open
         ..0. .... = Oplocks: OpLock not requested/granted
         ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
         .... 1... = Case Sensitivity: Path names are caseless
         .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
         .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
      Flags2: 0xc807
         1... .... .... .... = Unicode Strings: Strings are Unicode
         .1.. .... .... .... = Error Code Type: Error codes are NT error codes
         ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
         ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
         .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
         .... .... .0.. .... = Long Names Used: Path names in request are not long file names
         .... .... .... .1.. = Security Signatures: Security signatures are supported
         .... .... .... ..1. = Extended Attributes: Extended attributes are supported
         .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
      Reserved: 00000000000000000000000000
      Tree ID: 0
      Process ID: 65279
      User ID: 4097
      Multiplex ID: 961
   Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 117
      Action: 0x0000
         .... .... .... ...0 = Guest: Not logged in as GUEST
      Security Blob Length: 0
      Byte Count (BCC): 74
      Security Blob: <MISSING>
      Native OS: Windows 5.0
      Native LAN Manager: Windows 2000 LAN Manager
```

Annexe 6
Echec authentification Kerberos avec IP

Frame 170 (339 bytes on wire, 339 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9c:7c:76
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: 10.1.1.10 (10.1.1.10)
User Datagram Protocol, Src Port: 1341 (1341), Dst Port: 88 (88)
Kerberos
  Version: 5
  MSG Type: AS-REQ
  Pre-Authentication
    Type: PA-ENC-TIMESTAMP
    Value: 303DA003020117A2360434381D9F99DA...
    Type: PA-PAC-REQUEST
    Value: 3005A0030101FF
  Request
    Options: 0040810010
    Client Name: alice@tdeig
      Type: Unknown name type 0xa
      Name: alice@tdeig
    Realm: TDEIG
    Server Name: krbtgt
      Type: Service and Instance
      Name: krbtgt
      Name: TDEIG
    End Time: 2037-09-13 02:48:05 (Z)
    Renewable Until: 2037-09-13 02:48:05 (Z)
    Random Number: 278202509
    Encryption Types
  Addresses
    Type: NETBIOS
    Value: V26<20> (Server service)

Frame 171 (1290 bytes on wire, 1290 bytes captured)
Ethernet II, Src: 00:04:76:9c:7c:76, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: 10.1.1.10 (10.1.1.10), Dst Addr: 10.1.2.26 (10.1.2.26)
User Datagram Protocol, Src Port: 88 (88), Dst Port: 1341 (1341)
Kerberos
  Version: 5
  MSG Type: AS-REP
  Realm: TDEIG
  Client Name: alice
    Type: Principal
    Name: alice
  Ticket
    Version: 5
    Realm: TDEIG
    Service Name: krbtgt
      Type: Service and Instance
      Name: krbtgt
      Name: TDEIG
    Encrypted Data: Ticket data
      Type: rc4-hmac
      CipherText: 71DE0797DC475A87780570A8282A34A5...
  Encrypted Data: Encrypted Payload
    Type: rc4-hmac
    KVNO: 1
    CipherText: CF417DE367C4DE30B1FE25442EB586A0...

Frame 172 (1264 bytes on wire, 1264 bytes captured)
Ethernet II, Src: 00:04:76:9b:7a:ab, Dst: 00:04:76:9c:7c:76
Internet Protocol, Src Addr: 10.1.2.26 (10.1.2.26), Dst Addr: 10.1.1.10 (10.1.1.10)
User Datagram Protocol, Src Port: 1342 (1342), Dst Port: 88 (88)
Kerberos
  Version: 5
  MSG Type: TGS-REQ
  Pre-Authentication
    Type: PA-TGS-REQ
    Value: 6E82042D30820429A003020105A10302...
  Request
    Options: 0040810010
    Realm: TDEIG
    Server Name: HOST
      Type: Service and Instance
      Name: HOST
      Name: 10.1.2.24
    End Time: 2037-09-13 02:48:05 (Z)
    Random Number: 279199905
    Encryption Types

Frame 173 (124 bytes on wire, 124 bytes captured)
Ethernet II, Src: 00:04:76:9c:7c:76, Dst: 00:04:76:9b:7a:ab
Internet Protocol, Src Addr: 10.1.1.10 (10.1.1.10), Dst Addr: 10.1.2.26 (10.1.2.26)
User Datagram Protocol, Src Port: 88 (88), Dst Port: 1342 (1342)
Kerberos
  Version: 5
  MSG Type: KRB-ERROR
  stime: 2003-03-03 13:19:49 (Z)
  susec: 938664
  Error Code: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
  realm: TDEIG
  sname: krbtgt
    Type: Service and Instance
    Name: krbtgt
    Name: TDEIG