



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

**Groupe sécurité Windows de l'OSSIR**

**13 septembre 2004**

**Protocoles et trafic réseau en  
environnements Active Directory**

**Jean-Baptiste Marchand**

**<[Jean-Baptiste.Marchand@hsc.fr](mailto:Jean-Baptiste.Marchand@hsc.fr)>**

- x Introduction aux protocoles réseaux d'Active Directory
- x Méthodologie d'analyse du trafic réseau avec ethereal
- x Typologie du trafic observé pour chaque protocole
- x Scénarios typiques
- x Limites et approches complémentaires
- x Conclusion
- x Références

- × Active Directory repose sur des protocoles réseaux (protocoles applicatifs)
  - × Normalisés : DNS, LDAP, Kerberos V, SNTTP
  - × Propriétaires : SMB/CIFS, MSRPC
- × Utilisation de protocoles de l'Internet, avec des spécificités propres à Microsoft

- × DNS
  - × Spécifications : nombreuses RFCs
    - × <http://www.dns.net/dnsrd/rfc/>
  - × Service de résolution de noms (remplace la résolution de noms NetBIOS des domaines NT)
    - × Mises à jour dynamiques des entrées DNS
    - × GSS-TSIG (RFC 3645)
  - × Localisation des services d'un domaine
    - × Enregistrements DNS de type SRV

- × LDAP
  - × Spécifications : voir RFC 3377
  - × Active Directory est un annuaire qui peut être interrogé via LDAP
    - × Ports 389 (TCP et UDP), 636 (LDAPS), 3268 et 3269 (Global Catalog AD)
  - × Mécanisme SASL utilisé spécifique : GSS-SPNEGO
  - × Systèmes Windows accèdent également à Active Directory via MSRPC
    - × Interfaces RPC [samr](#) et [drsuapi](#)
  - × Informations sensibles transitent chiffrées
    - × Sessions LDAP sur le port 389, chiffrées via GSS-SPNEGO
    - × Opérations MSRPC chiffrées (*packet privacy*)
  - × Dans LDAP, pas de normalisation de la répllication des annuaires
    - × Active Directory se réplique via MSRPC ou SMTP

- × Kerberos V
  - × Protocole d'authentification réseau
  - × Protocole défini au MIT puis normalisation IETF, largement déployé en environnements Unix
  - × Mis en œuvre par Microsoft, avec des ajouts à la norme
    - × Chiffrement RC4-HMAC, transport sur TCP, PAC (Privilege Access Certificate), PKINIT, ...
    - × Interfaces standards implémentées pour compatibilité mais non utilisées par les clients Windows natifs
      - × Exemple du service kpasswd (pour le changement des mots de passe)
  - × Kerberos V intégré aux services Windows via la couche SSPI
    - × SPNEGO pour la négociation entre différents *packages* de sécurité (NTLM, Kerberos V, Schannel, ...)

- × SNTP
  - × Simple Network Time Protocol, version 3 (RFC 1769)
  - × Version simplifiée du protocole NTP (RFC 1305)
    - × même format de paquets, port 123 UDP
    - × précision moindre que NTP (mais suffisante pour Kerberos V)
  - × Signature des synchronisations
    - × normalement ignorée dans SNTP
    - × permet d'authentifier les synchronisations

- × SMB/CIFS
  - × Protocole de partage de ressources des domaines Windows
    - × Souvent confondu avec NetBIOS sur TCP/IP
  - × Utilisé pour le partage de fichiers / imprimantes
  - × Egalement un des transports possibles pour MSRPC
    - × Transport via tubes nommés (`ncacn_np`)
    - × Nettement moins utilisé que dans NT 4.0, au profit du transport sur TCP/IP
      - × Encore utilisé lors de l'ajout d'une machine dans un domaine...
  - × Déploiement Group Policy : partage `sysvol`
    - × Fichiers `gpt.ini`, `registry.pol`, `*.adm`, `GptTmpl.inf`
  - × Scripts de connexion : partage `netlogon`



- × MSRPC
  - × Mise en œuvre MS du standard DCE RPC
  - × Domaines Active Directory reposent sur des interfaces RPC clés :
    - × `lsarpc` : accès à la LSA (Local Security Authority)
    - × `netlogon` : service d'authentification réseau
    - × `samr` : accès à la base SAM (compatibilité arrière avec NT 4.0, fonctionne avec l'annuaire AD)
    - × `drsuapi` : accès à l'annuaire Active Directory
  - × Active Directory utilise le transport TCP pour ces services RPC
    - × Portmapper sur le port 135/TCP
    - × Intervalles de ports par défaut des services RPC sur TCP
      - × 1025-5000, intervalle par défaut, à modifier avec `rpccfg`
    - × Rappel : NT 4.0 reposait sur des services RPC transportés sur SMB, lui-même dans NetBIOS sur TCP/IP (port 139 TCP)

- × Kerberos V est le protocole d'authentification réseau dans AD
  - × Remplace avantageusement NTLM
  - × Authentification mutuelle
  - × Protocoles réseaux mentionnés ont été modifiés pour supporter Kerberos
    - × Authentification des sessions SMB/CIFS
    - × Authentification des sessions LDAP
    - × Authentification des appels MSRPC
    - × Authentification des mises à jour dynamiques du DNS
  - × Support de Kerberos V via un protocole de négociation, SPNEGO (Simple Protected Negotiation Mechanism, RFC 2478)
    - × Plusieurs erreurs dans l'implémentation de SPNEGO par Microsoft, rendant l'interopérabilité difficile...

- × Buts possibles de l'analyse du trafic réseau
  - × Comprendre Active Directory
  - × Valider le bon fonctionnement des mécanismes clés d'Active Directory
    - × Ex 1 : renouvellement des tickets Kerberos
    - × Ex 2 : application régulière de la Group Policy
  - × Tracer des dysfonctionnements

- × Avoir accès au trafic réseau des contrôleurs de domaines
  - × Pour pouvoir le capturer
- × Utiliser un analyseur réseau supportant les protocoles sus-cités
  - × Analyseur réseau de choix : ethereal
  - × Logiciel libre fonctionnant sous Unix et Windows
  - × Support de nombreux protocoles, dont les protocoles spécifiques Windows (SMB/CIFS et MSRPC)
  - × Supporte le déchiffrement du trafic Kerberos
    - × Sous Unix avec Heimdal (<http://www.pdc.kth.se/heimdal/>)
  - × <http://www.ethereal.com/>

- × Aperçu de la typologie du trafic
  - × Examiner les protocoles observés
    - × fonction `Protocol Hierarchy` d'ethereal
  - × Examiner la typologie du trafic
    - × fonction `Conversations` d'ethereal
    - × `IPv4 conversations` : systèmes ayant généré du trafic
    - × `TCP, UDP conversation` : couples adresses IP, ports (sources et destinations)

# Fonction *Protocol Hierarchy*

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
[-] Frame	100.00%	278	73952	0.003	0	0	0.000
[-] Ethernet	100.00%	278	73952	0.003	0	0	0.000
Address Resolution Protocol	2.88%	8	462	0.000	8	462	0.000
[-] Internet Protocol	97.12%	270	73490	0.003	0	0	0.000
[-] User Datagram Protocol	12.95%	36	20158	0.001	0	0	0.000
Domain Name Service	5.04%	14	2123	0.000	14	2123	0.000
[-] Lightweight Directory Access Protocol	2.16%	6	1315	0.000	3	664	0.000
Lightweight Directory Access Protocol	1.08%	3	651	0.000	3	651	0.000
Kerberos	5.04%	14	16500	0.001	14	16500	0.001
Network Time Protocol	0.72%	2	220	0.000	2	220	0.000
[-] Transmission Control Protocol	82.73%	230	53082	0.002	114	12540	0.001
[-] DCE RPC	12.95%	36	9223	0.000	12	2823	0.000
DCE/RPC Endpoint Mapper	2.16%	6	1160	0.000	6	1160	0.000
Microsoft Network Logon	3.60%	10	3376	0.000	10	3376	0.000
Microsoft Directory Replication Service	2.88%	8	1864	0.000	8	1864	0.000
[-] NetBIOS Session Service	11.51%	32	6669	0.000	0	0	0.000
SMB (Server Message Block Protocol)	11.51%	32	6669	0.000	32	6669	0.000
[-] Lightweight Directory Access Protocol	15.83%	44	23807	0.001	42	22481	0.001
Lightweight Directory Access Protocol	0.72%	2	1326	0.000	2	1326	0.000
Hypertext Transfer Protocol	1.44%	4	843	0.000	4	843	0.000
Internet Control Message Protocol	1.44%	4	250	0.000	4	250	0.000



Ethernet: 3 | Fibre Channel | FDDI | IPv4: 2 | IPX | **TCP: 13** | Token Ring | UDP: 17

## TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
192.70.106.144	1046	192.70.106.151	80	11	1249	5	625	6	624
192.70.106.144	1029	192.70.106.151	135	15	1604	9	908	6	696
192.70.106.144	1052	192.70.106.151	135	12	1040	7	638	5	402
192.70.106.144	1056	192.70.106.151	389	23	7166	13	3157	10	4009
192.70.106.144	1043	192.70.106.151	389	20	7815	12	3096	8	4719
192.70.106.144	1045	192.70.106.151	389	15	3103	9	2240	6	863
192.70.106.144	1057	192.70.106.151	389	12	3891	7	2019	5	1872
192.70.106.144	1058	192.70.106.151	389	12	3823	7	1974	5	1849
192.70.106.144	1059	192.70.106.151	389	12	3869	7	2019	5	1850
192.70.106.144	1035	192.70.106.151	445	44	8835	25	5700	19	3135
192.70.106.144	1039	192.70.106.151	1025	22	5685	12	4078	10	1607
192.70.106.144	1031	192.70.106.151	1025	18	3702	11	2324	7	1378
192.70.106.144	1030	192.70.106.151	1025	14	1300	8	828	6	472

Ethernet: 3   Fibre Channel   FDDI   IPv4: 2   IPX   TCP: 13   Token Ring   **UDP: 17**

## UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
192.70.106.144	1026	192.70.106.151	53	4	758	2	244	2	514
192.70.106.144	1047	192.70.106.151	53	2	252	1	83	1	169
192.70.106.144	1048	192.70.106.151	53	2	252	1	126	1	126
192.70.106.144	1049	192.70.106.151	53	2	251	1	87	1	164
192.70.106.144	1050	192.70.106.49	53	2	231	1	171	1	60
192.70.106.144	1053	192.70.106.151	53	2	379	1	122	1	257
192.70.106.144	1036	192.70.106.151	88	2	1728	1	361	1	1367
192.70.106.144	1037	192.70.106.151	88	2	2666	1	1346	1	1320
192.70.106.144	1038	192.70.106.151	88	2	2645	1	1339	1	1306
192.70.106.144	1040	192.70.106.151	88	2	2666	1	1346	1	1320
192.70.106.144	1041	192.70.106.151	88	2	2600	1	1324	1	1276
192.70.106.144	1044	192.70.106.151	88	2	2720	1	1364	1	1356
192.70.106.144	1051	192.70.106.151	88	2	1475	1	1335	1	140
192.70.106.144	123	192.70.106.151	123	2	220	1	110	1	110
192.70.106.144	1028	192.70.106.151	389	2	467	1	250	1	217
192.70.106.144	1034	192.70.106.151	389	2	424	1	207	1	217
192.70.106.144	1054	192.70.106.151	389	2	424	1	207	1	217



- × Filtrage du trafic réseau
  - × Ethereal supporte des filtres d'affichage (*display filters*)
  - × La plupart des dissecteurs ethereal rendent accessibles les différents champs du protocole décodé
  - × Filtrage des trames affichées peut se faire sur la valeur de n'importe quel champ décodé
  - × Fonctions `Apply as filter` et `Prepare a filter`

- x Filtres d'affichage des différents protocoles
  - x `smb` : sessions SMB
  - x `ldap && udp` : trafic CLDAP
  - x `ldap && tcp` : trafic LDAP
  - x `dcerpc` : trafic MSRPC
  - x `kerberos && udp` : messages Kerberos (port 88 UDP)
  - x `kerberos.msg.type == 10` : affiche les messages Kerberos AS-REQ
  - x `smb && kerberos, ldap && kerberos, dcerpc && kerberos` : trames d'authentification des différents protocoles (messages AP-REQ et AP-REP)
    - x Ici, équivalent à : `kerberos && tcp`

# Authentication Kerberos : SMB, MSRPC, LDAP

No.	Time	Source .	Destination	Protocol	Info
55	2004-07-15 11:18:56.957848	192.70.106.144	192.70.106.151	SMB	Session Setup AndX Request
57	2004-07-15 11:18:57.016509	192.70.106.151	192.70.106.144	SMB	Session Setup AndX Response
75	2004-07-15 11:18:57.927875	192.70.106.144	192.70.106.151	DCERPC	Bind; call_id: 1 UUID: DRSUAPI
77	2004-07-15 11:18:57.958316	192.70.106.151	192.70.106.144	DCERPC	Bind_ack; call_id: 1 accept max_
78	2004-07-15 11:18:57.960004	192.70.106.144	192.70.106.151	DCERPC	Alter_context; call_id: 1 UUID: I
104	2004-07-15 11:18:58.521506	192.70.106.144	192.70.106.151	LDAP	MsgId=3 Bind Request, DN=(null)
105	2004-07-15 11:18:58.599533	192.70.106.151	192.70.106.144	LDAP	MsgId=3 Bind Result
112	2004-07-15 11:18:58.667594	192.70.106.144	192.70.106.151	LDAP	MsgId=7 Bind Request, DN=(null)
113	2004-07-15 11:18:58.749381	192.70.106.151	192.70.106.144	LDAP	MsgId=7 Bind Result
217	2004-07-15 11:20:00.033894	192.70.106.144	192.70.106.151	LDAP	MsgId=3 Bind Request, DN=(null)
218	2004-07-15 11:20:00.116670	192.70.106.151	192.70.106.144	LDAP	MsgId=3 Bind Result
230	2004-07-15 11:20:00.238930	192.70.106.144	192.70.106.151	LDAP	MsgId=10 Bind Request, DN=(null)
231	2004-07-15 11:20:00.324893	192.70.106.151	192.70.106.144	LDAP	MsgId=10 Bind Result
243	2004-07-15 11:20:00.381976	192.70.106.144	192.70.106.151	LDAP	MsgId=15 Bind Request, DN=(null)
244	2004-07-15 11:20:00.474899	192.70.106.151	192.70.106.144	LDAP	MsgId=15 Bind Result
255	2004-07-15 11:20:00.504705	192.70.106.144	192.70.106.151	LDAP	MsgId=20 Bind Request, DN=(null)
256	2004-07-15 11:20:00.574816	192.70.106.151	192.70.106.144	LDAP	MsgId=20 Bind Result

- x Scénarios typiques
  - x Ajout d'une machine dans le domaine
  - x Démarrage d'une station membre du domaine ou un contrôleur de domaine
  - x Changement du mot de passe des comptes machines
    - x Tous les 30 jours par défaut
  - x Authentification d'un utilisateur sur le domaine
  - x Répliquions entre contrôleurs de domaine
  - x Applications de la Group Policy
  - x ...

- × Trafic DNS
  - × Résolution d'enregistrements SRV
    - × `_service._protocol.DnsDomainName`
    - × Ex: `_ldap._tcp.sitename._sites.dc._msdcs.domainname` pour localiser un contrôleur de domaine
- × Trafic CLDAP
  - × Obtenir le contrôleur de domaine le plus proche (en terme de sites)
  - × API `DsGetDcName()`, implémentée par un pseudo-appel RPC à Active Directory
    - × Nom du site est mis en cache (valeur `DynamicSiteName`)
  - × Filtre etheréal : `ldap && udp`
  - × Documenté dans la section *Locating Active Directory Servers* du Resource Kit de Windows 2000

- × Mise à jour dynamique
  - × réalisée par le service dhcp (même en adressage statique)
    - × `Register this connection's addresses in DNS` (activé par défaut)
    - × au démarrage de la machine en adressage statique (A et PTR)
    - × a chaque changement d'adresse en adressage dynamique (DHCP)
      - × En fonction du paramétrage du serveur DHCP (par défaut, uniquement le A)
    - × toutes les 24 heures par défaut
      - × Valeur `DefaultRegistrationRefreshInterval`
      - × TTL de 20 minutes par défaut pour les enregistrements {A, PTR} mis à jour (valeur `DefaultRegistrationTtl`)
  - × exécutable manuellement : `ipconfig /registerdns`



```

⊞ Ethernet II, Src: 00:0c:29:1f:da:98, Dst: 00:10:dc:ca:f3:53
⊞ Internet Protocol, Src Addr: 192.70.106.146 (192.70.106.146), Dst Addr: 192.70.106.151 (192.70.106.151)
⊞ Transmission Control Protocol, Src Port: 1053 (1053), Dst Port: 53 (53), Seq: 1461, Ack: 1, Len: 1181
⊞ Domain Name System (query)
  Length: 2639
  Transaction ID: 0x7ae7
  ⊞ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ⊞ Queries
  ⊞ Additional records
    ⊞ 972-ms-7.1-15435.139f420e-fa8e-11d8-9694-000c291fda98: type TKEY, class any
      Name: 972-ms-7.1-15435.139f420e-fa8e-11d8-9694-000c291fda98
      Type: Transaction Key
      Class: any
      Time to live: 0 time
      Data length: 2503
      Algorithm name: gss-tsig
      Signature inception: Aug 30, 2004 16:08:33.000000000
      Signature expiration: Aug 31, 2004 16:08:33.000000000
      Mode: GSSAPI
      Error: No error
      Key Size: 2477
    ⊞ Key Data
      ⊞ GSS-API
        OID: 1.3.6.1.5.5.2 (SNMPv2-SMI::security.5.2) (SPNEGO - Simple Protected Negotiation)
      ⊞ SPNEGO
        ⊞ negTokenInit
          ⊞ mechType
          ⊞ mechToken
            ⊞ krb5_blob: 6082096706092A864886F71201020201...
              OID: 1.2.840.113554.1.2.2 (iso.2.840.113554.1.2.2) (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REQ (0x0001)
            ⊞ Kerberos AP-REQ
  
```

- x Trafic LDAP
  - x typiquement authentifié via le mécanisme SASL GSS-SPNEGO
    - x Le dn (*distinguished name*) au niveau du *bind* LDAP est vide
  - x débute par une requête pour obtenir certains attributs du rootDSE
    - x `SupportedSASLMechanisms`
    - x `LdapServiceName`
  - x trafic LDAP peut être chiffré
  - x Lorsque le trafic est en clair, examiner les paramètres de la recherche :
    - x DN de base, portée (*scope*), filtre, attributs, ...
  - x erreurs dans une requête LDAP
    - x Filtre `ldap.result.errormsg`
  - x



- × Trafic MSRPC
  - × Localisation des services RPC sur TCP/IP
    - × endpoint mapper, port TCP 135 ([epm](#))
    - × Retourne le port TCP sur lequel écoute un service RPC donné
    - × Opération [map](#), non authentifiée
  - × Accès à la Local Security Authority ([lsa](#))
    - × Authentification Kerberos
    - × Port TCP (typiquement 1025, à fixer cf MSKB #224196)
    - × Ex: opérations [LsarQueryInformationPolicy\(2\)](#)
  - × Accès à Active Directory via interface RPC de la SAM ([samr](#))
    - × Authentification Kerberos, sur le même port TCP
    - × Exemple : création d'un compte machine sur un DC pour un nouveau serveur membre est réalisé via [samr](#) (opération [SamrCreateUser2InDomain](#))

- × Trafic MSRPC (suite)
  - × Authentification sur le domaine, service netlogon (`rpc_netlogon`)
    - × Toujours le même port TCP
    - × Opérations `NetrServerReqChallenge` et `NetrServerAuthenticate3`
  - × Accès à Active Directory via RPC (plutôt que LDAP)
    - × Interface `drsuapi`, toujours sur le même port TCP
    - × Typiquement, opération `DRSCrackNames` (opérations `DrsBind` et `DrsUnbind`), qui implémente l'API `DsCrackNames( )`
    - × Trafic chiffré donc typiquement pas visible en analyse réseau

- × Trafic Kerberos
  - × Obtention de TGT
    - × Démarrage d'une machine sur le domaine
    - × Authentification utilisateur
    - × Messages AS-REQ (10) et AS-REP (11)
  - × Obtention de tickets de services
    - × Messages TGS-REQ (12) et TGS-REP (13)
    - × Noms de services typiques : host, ldap, cifs, dns, ...
  - × Utilisation des tickets de services
    - × Messages AP-REQ (14) et AP-REP (15)
    - × Typiquement encapsulés dans SPNEGO

- × *Service Principal Names*

- × Authentification par Kerberos auprès des services réseaux AD se fait en obtenant un ticket pour un service donné
- × Le service est désigné via un SPN (Service Principal Name)
- × Attribut `servicePrincipalName` (*case-insensitive*) de la classe User
- × Egalement, attribut `sPNMappings` (SPNs équivalents au SPN Host)

- × *Sur le fil*

- × SPN apparaît au niveau des messages TGS-REQ, TGS-REP et AS-REQ
- × Message TGS-REP peut contenir un SPN différent de celui envoyé
  - × Option de mise sous forme canonique sous Windows 2000
  - × SPN retourné est de la forme SERVER\$
  - × Mise sous forme canonique désactivée dans Windows Server 2003

```
C:\WINDOWS\system32\cmd.exe
```

```
C:\>setspn -L SERVEUR
```

```
Registered ServicePrincipalNames for CN=SERVEUR,OU=Domain Controllers,DC=DomaineBlah,DC=com:
```

```
NtFrs-88f5d2bd-b646-11d2-a6d3-00c04fc9b232/serveur.DomaineBlah.com
```

```
DNS/serveur.DomaineBlah.com
```

```
ldap/serveur.DomaineBlah.com/TAPI3Directory.DomaineBlah.com
```

```
ldap/serveur.DomaineBlah.com/ForestDnsZones.DomaineBlah.com
```

```
GC/serveur.DomaineBlah.com/DomaineBlah.com
```

```
HOST/serveur.DomaineBlah.com/DOMAINEBLAH
```

```
HOST/SERVEUR
```

```
HOST/serveur.DomaineBlah.com
```

```
HOST/serveur.DomaineBlah.com/DomaineBlah.com
```

```
E3514235-4B06-11D1-AB04-00C04FC2DCD2/276d4866-4940-49e4-91ec-991746baf84a/DomaineBlah.com
```

```
ldap/276d4866-4940-49e4-91ec-991746baf84a._msdcs.DomaineBlah.com
```

```
ldap/serveur.DomaineBlah.com/DOMAINEBLAH
```

```
ldap/SERVEUR
```

```
ldap/serveur.DomaineBlah.com
```

```
ldap/serveur.DomaineBlah.com/DomainDnsZones.DomaineBlah.com
```

```
ldap/serveur.DomaineBlah.com/DomaineBlah.com
```

# Kerberos : tickets d'un utilisateur connecté à un domaine (Windows 2000)

```
C:\>klist tickets
```

```
Cached Tickets: (5)
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 8/27/2004 0:51:47  
Renew Time: 9/2/2004 14:51:47
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 8/27/2004 0:51:47  
Renew Time: 9/2/2004 14:51:47
```

```
Server: HOST/serveur.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 8/27/2004 0:51:47  
Renew Time: 9/2/2004 14:51:47
```

```
Server: ldap/serveur.DomaineBlah.com/DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 8/27/2004 0:51:47  
Renew Time: 9/2/2004 14:51:47
```

```
Server: LDAP/serveur.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 8/27/2004 0:51:47  
Renew Time: 9/2/2004 14:51:47
```



# Kerberos : tickets d'un utilisateur connecté à un domaine (Windows XP)

```
C:\>klist tickets
```

```
Cached Tickets: (6)
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
Server: ldap/serveur.DomaineBlah.com/DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
Server: cifs/serveur.domaineblah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
Server: LDAP/serveur.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
Server: host/wxpdfilt.domaineblah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC<NT>  
End Time: 7/30/2004 5:56:27  
Renew Time: 8/5/2004 19:56:27
```

```
C:\>klist tickets
```

```
Cached Tickets: (9)
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: krbtgt/DOMAINEBLAH.COM@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: W2KKDC$@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: SERVEUR$@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```



```
Server: ldap/w2kdc.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: ldap/w2kdc.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: HOST/serveur.DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
Server: E3514235-4B06-11D1-AB04-00C04FC2DCD2/276d4866-4940-49e4-91ec-991746ba  
f84a@DomaineBlah.com@DOMAINEBLAH.COM  
Kerberos Ticket Encryption Type: RSADSI RC4-HMAC(NT)  
End Time: 9/7/2004 20:32:06  
Renew Time: 9/14/2004 10:32:06
```

```
C:\>
```

- × Trafic Kerberos : erreurs communes
  - × Message KRB-ERROR (30) (`kerberos.msg.type == 30`)
    - × KRB5KRB\_AP\_ERR\_SKEW
      - × Problème de synchronisation horaire
    - × KRB5KDC\_ERR\_PREAUTH\_FAILED
      - × Typiquement, mauvais mot de passe
    - × KRB5KRB\_AP\_ERR\_TKT\_EXPIRED
      - × Ticket expiré, à renouveler
      - × La LSA cache le mot de passe des utilisateurs donc peut obtenir un nouveau TGT, dans la limite de 7 jours (*Max. Lifetime for user ticket renewal*)
    - × KRB5KDC\_ERR\_S\_PRINCIPAL\_UNKNOWN
      - × Principal non reconnu par le KDC
      - × Absence de SPN (attribut `servicePrincipalName`) sur un compte dans AD ?
      - × Ex : utilisation d'une adresse IP dans un nom UNC
        - × Fallback sur l'authentification NTLM

```

Client realm: DOMAINEBLAH.COM
☒ Client Name (Principal): vtsoin$
☒ Ticket
  Tkt-vno: 5
  Realm: DOMAINEBLAH.COM
  ☒ Server Name (Service and Instance): LDAP/serveur.DomaineBlah.com
    Name-type: Service and Instance (2)
    Name: LDAP
    Name: serveur.DomaineBlah.com
  ☒ enc-part rc4-hmac
    Encryption type: rc4-hmac (23)
    Kvno: 21
    ☒ enc-part: A9ADC3F96D13DD9C26E763D3DC902B8F...
      [Decrypted using: keytab principal serveur@$DOMAINEBLAH.COM]
    ☒ EncTicketPart
      Padding: 0
      ☒ Ticket Flags (Forwardable, Renewable, Pre-Auth, Ok As Delegate)
      ☒ key rc4-hmac
        Client Realm: DOMAINEBLAH.COM
        ☒ Client Name (Principal): vtsoin$
        ☒ TransitedEncoding DOMAIN-X500-COMPRESS
        Authtime: 2004-08-27 13:32:15 (Z)
        Start time: 2004-08-27 13:32:15 (Z)
        End time: 2004-08-27 23:32:15 (Z)
        Renew-till: 2004-09-03 13:32:15 (Z)
      ☒ AuthorizationData AD-IF-RELEVANT
        Type: AD-IF-RELEVANT (1)
        ☒ Data: 308202623082025EA00402020080A182...
          ☒ IF_RELEVANT AD-Win2k-PAC
            Type: AD-Win2k-PAC (128)
            ☒ Data: 04000000000000001000000C0010000...
              Num Entries: 4
              Version: 0
              ☒ Type: Logon Info (1)
              ☒ Type: Client Info Type (10)
              ☒ Type: Server Checksum (6)
              ☒ Type: Privsvr Checksum (7)
        ☒ enc-part rc4-hmac
          Encryption type: rc4-hmac (23)
          ☒ enc-part: 71CAA300948E49193D8A4AFC32FD1DA7...
            [Decrypted using: key learnt from frame 79]
  
```

- × Réplication d'Active Directory
  - × Interface MSRPC `drsuapi` (1 port TCP)
  - × Fixer le port TCP des services RPC `netlogon` et `drsuapi` (MSKB #224196)
  - × Entre contrôleurs de domaine
    - × Opération `DRSReplicaSync` (`drsuapi`)
      - × Prévenir un partenaire qu'il y a des données à répliquer
    - × Opération `DRSGetNCChanges` (`drsuapi`)
      - × Obtenir les changements pour un NC (*Naming Context*) donné
    - × Connexions RPC au service `drsuapi` sont authentifiées avec un ticket Kerberos obtenu pour le nom de principal suivant :
      - × `e3514235-4b06-11d1-ab04-00c04fc2dcd2` (UUID de l'interface `drsuapi`)
      - × GUID du contrôleur de domaine cible
      - × Nom DNS du domaine

- × Réplication FRS
  - × Interface MSRPC `frsrpc` (1 port TCP)
  - × Fixer le port TCP du service RPC du service FRS (MSKB #319553)
  - × Entre contrôleurs de domaine
    - × Opération `FrsRpcStartPromotionParent` au démarrage d'un DC
    - × Opération `FrsRpcSendCommPkt` pour la réplication régulière

- × Trafic NTP
  - × Service w32time, démarré sur les serveurs membres d' un domaine
  - × Mode NT5DS (par défaut), qui utilise la hiérarchie AD pour la synchronisation horaire
  - × Synchronisation NTP au démarrage, avec un contrôleur de domaine
    - × Identifié via CLDAP au démarrage
    - × Puis toutes les 45 minutes (3 fois de suite) puis toutes les 8 heures
  - × Mécanisme de synchronisation
    - × Client envoie le RID (compte machine) dans la requête (champ *KeyID*)
      - × Ce RID est obtenu en retour de l'opération `NetrServerAuthenticate3`
    - × Temps retourné est signé (champ *Message authentication code*)



- × Limites de l'analyse réseau
  - × Trafic chiffré : typiquement LDAP et certaines opérations MSRPC
  - × Trafic non décodé par un analyseur réseau
    - × Typiquement avec MSRPC, où les opérations RPC ne contiennent pas de référence à l'interface DCE RPC utilisée  
→ **Utiliser la fonction Decode As DCE-RPC d'ethereal**
- × Approches complémentaires
  - × Corrélation des traces réseaux avec les événements journalisés
    - × Journaux Sécurité et Système des systèmes Windows
  - × Outils de diagnostic sur les serveurs
    - × Ex : statistiques accessibles via l'outil *System Monitor* (perfmon.msc), avec l'objet NTDS
    - × Ex : outils pour visualiser le cache des tickets Kerberos

- × Une bonne compréhension des protocoles présentés ici est nécessaire pour exploiter au mieux Active Directory
- × L'analyse réseau est une des manières possibles d'acquérir une telle compréhension
  - × Voir les protocoles sur le fil, dans un environnement réel, est un bon complément à la lecture des *whitepapers* techniques
- × L'analyse réseau permet également de diagnostiquer des dysfonctionnements
  - × Lorsque les outils de diagnostic ou les journaux ne sont pas suffisants...
- × ethereal est l'outil de choix pour analyser des traces collectées en environnements Active Directory



- × Trafic réseau en environnement Windows
  - × Windows 2000 Startup and Logon Traffic Analysis
    - × <http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/w2kstart.mspx>
  - × Network Ports Used by Key Microsoft Server Products
    - × [http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref\\_net\\_ports\\_ms\\_prod.mspx](http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref_net_ports_ms_prod.mspx)
- × Using Windows { XP SP1, 2000 SP4, Server 2003} in a Managed Environment
  - × <http://go.microsoft.com/fwlink/?LinkId={22607, 22608, 22609}>

- × Implémentation du DNS dans Active Directory
  - × Windows 2000 DNS White Paper
    - × <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp>
  - × RFC 3645 : Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)

- × Protocole

- × [draft-ietf-krb-wg-kerberos-clarifications-08.txt](#)

- × Mise à jour de la RFC 1510 (spécification originale de Kerberos V)

- × <http://kerberos.info/>

- × Documents

- × Troubleshooting Kerberos Errors (Microsoft)

- × <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx>

- × Outils

- × klist, kerbtray (Microsoft)

- × tktview : <http://msdn.microsoft.com/msdnmag/issues/0500/security/>

- × leash32 : <http://web.mit.edu/kerberos/>

- × LDAP et CLDAP
  - × Active Directory Domain Controller Location Service (Anthony Liguori, Samba team)
    - × Description de CLDAP (Connectionless LDAP)
    - × <http://oss.software.ibm.com/linux/presentations/samba/cifs2003/Liguorifinal.pdf>
  - × Active Directory LDAP compliance (Microsoft)
    - × <http://www.microsoft.com/windowsserver2003/techinfo/overview/ldapcomp.msp>
  - × Schéma LDAP Active Directory (Windows 2000, Windows Server 2003 et ADAM)
    - × [http://msdn.microsoft.com/library/en-us/adschema/adschema/active\\_directory\\_schema.asp](http://msdn.microsoft.com/library/en-us/adschema/adschema/active_directory_schema.asp)

- × Ouvrage de référence sur SMB/CIFS
  - × Livre en ligne Implementing CIFS
    - × <http://www.ubiqx.org/cifs/>
- × MSRPC
  - × Windows network services internals
    - × [http://www.hsc.fr/ressources/articles/win\\_net\\_srv/](http://www.hsc.fr/ressources/articles/win_net_srv/)
  - × Testing MSRPC (Andrew Tridgell, Samba Team)
    - × [http://samba.org/ftp/samba/slides/tridge\\_cifs04.pdf](http://samba.org/ftp/samba/slides/tridge_cifs04.pdf)
  - × MSRPC architecture & security problems related
    - × [http://www.xfocus.net/projects/Xcon/2003/Xcon2003\\_kkqq.pdf](http://www.xfocus.net/projects/Xcon/2003/Xcon2003_kkqq.pdf)
  - × Microsoft Windows RPC Security Vulnerabilities
    - × <http://conference.hackinthebox.org/materials/lsd/>

- × Références Microsoft
  - × The Windows Time Service
    - × <http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/operate/wintime.mspx>
  - × Basic Operation of the Windows Time Service (MSKB #224799)
  - × Windows Time Service Tools and Settings (Windows Server 2003 Technical Reference)
  - × Using Windows XP Professional with Service Pack 1 in a Managed Environment (Windows Time Service)
    - × [http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/27\\_xpwts.mspx](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/27_xpwts.mspx)
  - × Security aspects of time synchronization infrastructure
    - × <http://www.security.nnov.ru/advisories/timesync.asp>



- × Emmanuel Le Chevoir et Fabien Dupont
- × Communauté de développeurs ethereal