HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Groupe SUR de l'OSSIR

13 janvier 2004

Services réseaux Windows

Jean-Baptiste Marchand
<Jean-Baptiste.Marchand@hsc.fr>

Plan

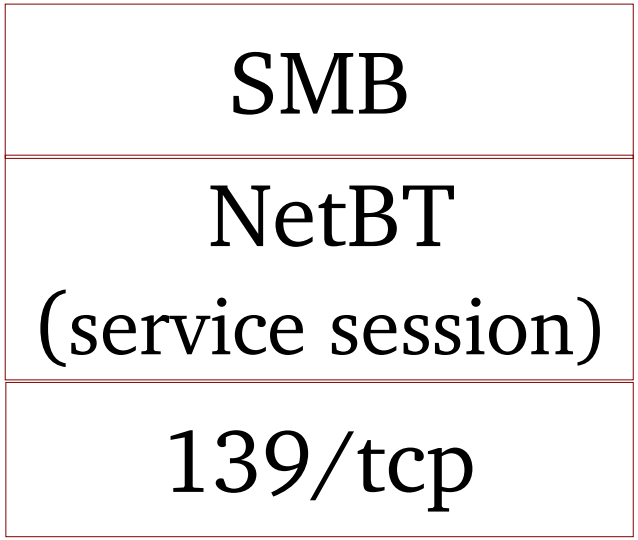
- Introduction
- NetBIOS et NetBT
- SMB
- MSRPC
  - Introduction
  - DCE RPC sur SMB
  - DCE RPC sur TCP/IP
  - DCOM
- Conclusion

Introduction

- Services réseaux Windows
  - Reposent sur des protocoles de communication spécifiques
  - Un protocole, au coeur des réseaux Windows : SMB/CIFS
    - SMB = Server Message Block
    - CIFS = Common Internet FileSystem
      - Nouveau nom donné par Microsoft à SMB autour de 1997
  - Un autre protocole, historiquement étroitement lié à SMB : NetBIOS
    - Stricto sensu, NetBIOS n'est pas un protocole mais une API (interface de programmation) : NETwork Basic Input Output System
    - Mise en oeuvre de cette API dans le monde TCP/IP : NetBT (NetBIOS over TCP/IP)
      - Normalisé à l'IETF (RFC 1001 et 1002, en 1987)
    - NetBT est souvent confondu avec SMB !
      - NetBT est utilisé pour le transport de SMB avant Windows 2000

SMB et NetBT

Windows NT 4.0 et < :



Windows 2000 et > :

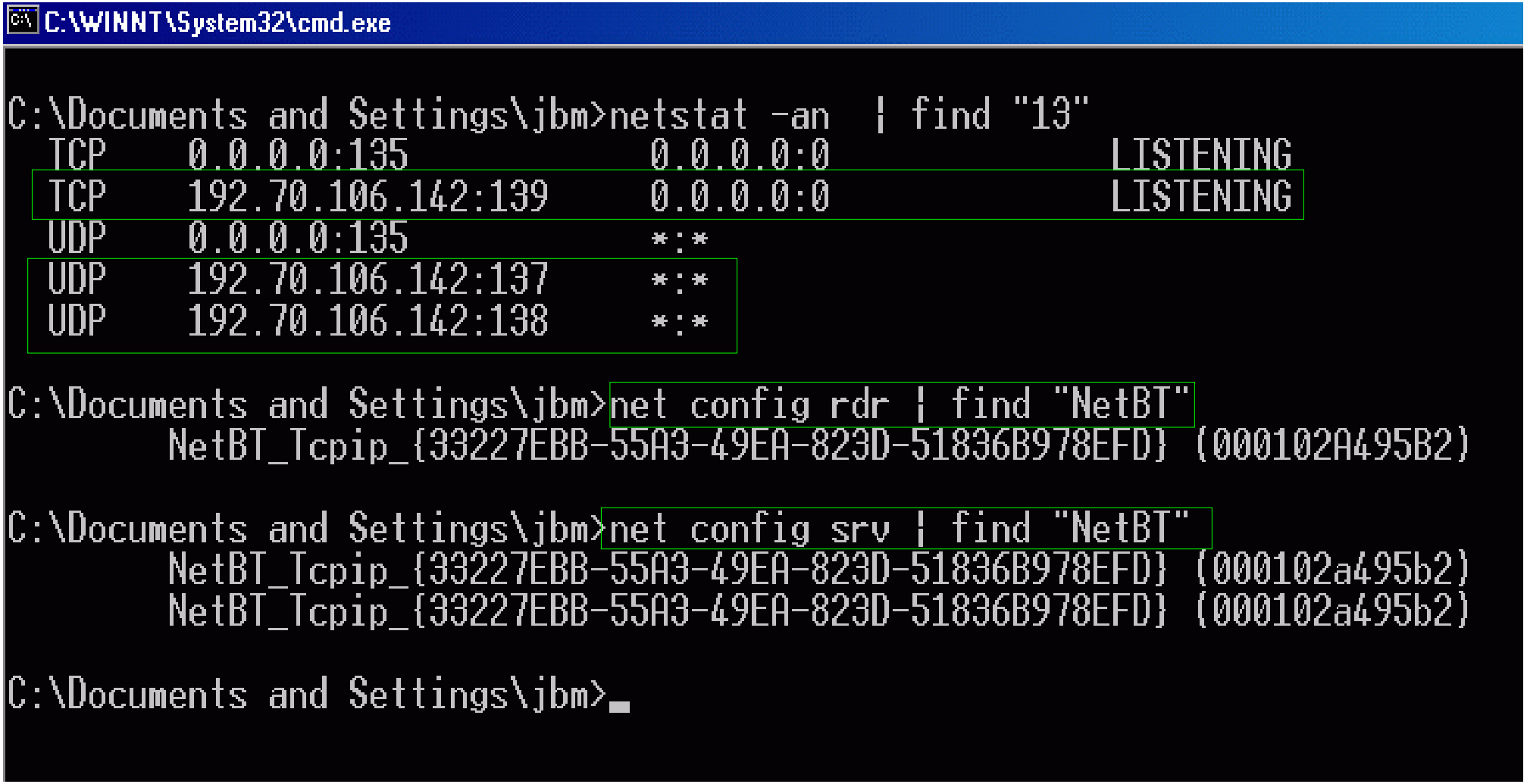
NetBIOS et NetBT : concepts

- L'API NetBIOS identifie les services avec des noms
  - Équivalent des ports TCP ou UDP dans le modèle TCP/IP
  - Nom NetBIOS : 16 caractères
    - 15 caractères + 1 caractère suffixe, identifiant la nature du service
      - http://support.microsoft.com/?id=163409
- NetBT : services disponibles
  - Service de gestion de noms (nbns) : enregistrement et résolution de noms
    - 137/udp, résolution des noms NetBIOS en adresses IP, enregistrement des noms
    - En diffusion ou via WINS (équivalent du DNS pour NetBIOS)
  - Service datagramme : 138/udp (nbdgm)
    - Annonce des services disponibles sur un LAN
  - Service session : 139/tcp (nbss)
    - Utilisé pour le transport de SMB

NetBT : en pratique

- Sous Windows, NetBIOS sur TCP/IP est configuré au niveau de chaque interface réseau
  - Ports 137/udp, 138/udp et 139/tcp en écoute sur des adresses IPv4 spécifiques
  - Voir la sortie de la commande netstat sur le transparent suivant
- Outils de gestion liés à NetBT
  - nbtstat (Windows)
    - Gestion des noms NetBIOS, locaux et distants
    - Options -a et -A à distance, option -n pour les noms locaux
  - nmblookup (Samba)
    - Mêmes fonctionnalités que nbtstat

Configuration NetBT sous Windows



nbtstat : exemple

```
C:\Documents and Settings\jbm>nbtstat -A 192.70.106.80

eth0:
Node IpAddress: [192.70.106.142] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    PLUTUS          <00>  UNIQUE      Registered
    WORKGROUP       <00>  GROUP       Registered
    PLUTUS          <03>  UNIQUE      Registered
    PLUTUS          <20>  UNIQUE      Registered
    WORKGROUP       <1E>  GROUP       Registered

    MAC Address = 00-00-39-FE-08-3B

C:\Documents and Settings\jbm>nbtstat -n

eth0:
Node IpAddress: [192.70.106.142] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    FENETRE         <00>  UNIQUE      Registered
    FENETRE         <20>  UNIQUE      Registered
    STAGIAIRES      <00>  GROUP       Registered
```

NetBT et transport de SMB

- SMB typiquement transporté dans NetBT avant Windows 2000
  - Service session (nbss), 139/tcp
  - Établissement d'une **session NetBIOS**
    - Nom NetBIOS source, de suffixe `<00>`
      - `<00>` identifie le service workstation = partie cliente SMB
    - Nom NetBIOS destination, de suffixe `<20>`
      - `<20>` identifie le service server = partie serveur SMB
      - Nom générique, supporté à partir de Windows NT 4 : `*SMBSERVER<20>`
- À partir de Windows 2000, transport de SMB directement dans TCP (445/tcp)
  - Plus d'établissement de session NetBIOS
  - Pseudo en-tête NetBIOS maintenu pour compatibilité ascendante

Transport de SMB dans NetBT (139/tcp)

No.	Time	Source	Destination	Protocol	Info
23	1.771828	192.168.1.3	192.168.1.1	TCP	29089 > 139 [SYN] Seq=2919563613 Ack=0 Win=16384 Len=0 MSS=1460 WS=0 TSV=1203306877 TSER=0
24	1.771913	192.168.1.1	192.168.1.3	TCP	139 > 29089 [SYN, ACK] Seq=3706349405 Ack=2919563614 Win=17520 Len=0 MSS=1460 WS=0 TSV=0 TSE
25	1.772957	192.168.1.3	192.168.1.1	TCP	29089 > 139 [ACK] Seq=2919563614 Ack=3706349406 Win=17376 Len=0 TSV=1203306877 TSER=0
26	2.026255	192.168.1.3	192.168.1.1	NBSS	Session request, to *SMBSERVER<20> from GARBAREK<00>
27	2.026428	192.168.1.1	192.168.1.3	NBSS	Positive session response
28	2.027880	192.168.1.3	192.168.1.1	SMB	Negotiate Protocol Request

```
⊞ Frame 28 (234 bytes on wire, 234 bytes captured)
⊞ Ethernet II, Src: 00:60:08:b3:07:05, Dst: 52:54:05:fd:c5:f9
⊞ Internet Protocol, Src Addr: 192.168.1.3 (192.168.1.3), Dst Addr: 192.168.1.1 (192.168.1.1)
⊞ Transmission Control Protocol, Src Port: 29089 (29089), Dst Port: 139 (139), Seq: 2919563690, Ack: 3706349410, Len: 168
⊟ NetBIOS Session Service
    Message Type: Session message
  ⊞ Flags: 0x00
    Length: 164
⊞ SMB (Server Message Block Protocol)
```

Transport de SMB sur 445/tcp

No.	Time	Source	Destination	Protocol	Info
1	0,0000	192,168,1,1	192,168,1,42	TCP	1153 > 445 [SYN] Seq=1415221918 Ack=0 Win=16384 Len=0 MSS=1460
3	0,0400	192,168,1,42	192,168,1,1	TCP	445 > 1153 [SYN, ACK] Seq=1912760860 Ack=1415221919 Win=17520 Len=0 MSS=1460
4	0,0402	192,168,1,1	192,168,1,42	TCP	1153 > 445 [ACK] Seq=1415221919 Ack=1912760861 Win=17520 Len=0
5	0,0432	192,168,1,1	192,168,1,42	SMB	Negotiate Protocol Request
7	0,0954	192,168,1,42	192,168,1,1	SMB	Negotiate Protocol Response

```
⊞ Frame 5 (191 bytes on wire, 191 bytes captured)
⊞ Ethernet II, Src: 52:54:05:fd:c5:f9, Dst: 00:50:56:40:40:5e
⊞ Internet Protocol, Src Addr: 192.168.1.1 (192.168.1.1), Dst Addr: 192.168.1.42 (192.168.1.42)
⊞ Transmission Control Protocol, Src Port: 1153 (1153), Dst Port: 445 (445), Seq: 1415221919, Ack: 1912760861, Len: 137
⊟ NetBIOS Session Service
      Message Type: Session message
      Length: 133
⊞ SMB (Server Message Block Protocol)
```

NetBIOS et sécurité

- NetBIOS et sécurité :
  - Fuite d'informations avec les noms NetBIOS ?
    - Enumération de noms NetBIOS pas fondamentalement différent d'un scan de ports
- Protocole NetBT
  - Protocole nuisible avant tout
  - Très verbeux sur un réseau local, notamment en l'absence de serveurs WINS
  - Complexe à mettre en oeuvre
    - Voir les nombreux détails sur le protocole NetBT dans le chapitre 1 de l'ouvrage *Implementing CIFS* (Christopher R. Hertel)
- Vulnérabilités récentes dans la mise en oeuvre NetBT de Windows
  - MS00-047 : possibilité de voler des noms NetBIOS déjà enregistrés sur un LAN
  - MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure

Conclusion sur NetBT

- NetBT est "juste" un protocole de transport pour SMB
- Son importance décroît depuis Windows 2000
  - Réseaux Windows reposent désormais sur des standards du monde TCP/IP : DNS, LDAP, Kerberos V
  - NetBT tend à disparaître
    - SMB peut être transporté directement dans TCP
    - Enregistrements SRV dans le DNS remplacent les noms NetBIOS pour la localisation des ressources
    - DNS dynamique remplace la fonctionnalité d'enregistrement dynamique de WINS
- NetBT n'est pas le protocole le plus important !
  - **Ne dites plus "partages NetBIOS" mais "partages SMB" !**

SMB : introduction

- SMB est le protocole réseau majeur des environnements Windows
  - Assure les fonctionnalités de partage de ressources (fichiers et imprimantes)
    - Systèmes de fichiers distribués
    - À rapprocher du standard NFS du monde Unix
  - Également utilisé comme protocole de transport pour les RPC
    - D'administration distante
    - De fonctionnement des domaines NT4
    - Pas d'analogie dans le monde Unix, Microsoft a ajouté un transport SMB au standard DCE RPC
  - Ces deux utilisations en font le protocole réseau au coeur des systèmes Windows

SMB : concepts

- Concepts
  - Protocole client-serveur
    - Partie cliente : accès à des ressources partagées
    - Partie serveur : mise à disposition de ressources partagées
  - Partage : groupe de ressources partagées
    - Partage de fichiers
    - Partage d'imprimantes
    - Partage spécial : IPC$
  - Session SMB
    - Protocole SMB est orienté session
    - Une session SMB débute toujours par une phase d'authentification
    - Utilisation d'un protocole d'authentification réseau
      - (NT)LM ou Kerberos V

Sessions SMB : exemples

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
28	2.027880	192.168.1.3	192.168.1.1	SMB	Negotiate Protocol Request
29	2.028025	192.168.1.1	192.168.1.3	SMB	Negotiate Protocol Response
31	4.132695	192.168.1.3	192.168.1.1	SMB	Session Setup AndX Request, User: MYGROUP\JBM
32	4.135542	192.168.1.1	192.168.1.3	SMB	Session Setup AndX Response
33	4.137370	192.168.1.3	192.168.1.1	SMB	Tree Connect AndX Request, Path: \\192.168.1.1\CAPS
34	4.137857	192.168.1.1	192.168.1.3	SMB	Tree Connect AndX Response
35	4.150064	192.168.1.3	192.168.1.1	SMB	Check Directory Request, Directory: \
36	4.150319	192.168.1.1	192.168.1.3	SMB	Check Directory Response
38	6.824912	192.168.1.3	192.168.1.1	SMB	Open AndX Request, Path: \cifs.txt
39	6.825423	192.168.1.1	192.168.1.3	SMB	Open AndX Response, FID: 0x4000

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
6	0.004250	192.70.106.149	192.70.106.143	SMB	Negotiate Protocol Request
7	0.007689	192.70.106.143	192.70.106.149	SMB	Negotiate Protocol Response
8	0.011336	192.70.106.149	192.70.106.143	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
9	0.014343	192.70.106.143	192.70.106.149	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10	0.017035	192.70.106.149	192.70.106.143	SMB	Session Setup AndX Request, NTLMSSP_AUTH
11	0.022452	192.70.106.143	192.70.106.149	SMB	Session Setup AndX Response
12	0.024078	192.70.106.149	192.70.106.143	SMB	Tree Connect AndX Request, Path: \\192.70.106.143\IPC$
13	0.025221	192.70.106.143	192.70.106.149	SMB	Tree Connect AndX Response
15	21.231530	192.70.106.149	192.70.106.143	SMB	NT Create AndX Request, Path: \lsarpc
16	21.250662	192.70.106.143	192.70.106.149	SMB	NT Create AndX Response, FID: 0x4000

SMB : en pratique sous Windows

- Client SMB
  - Commande `net use` : établissement d'une session SMB
- Serveur SMB
  - Commande `net share` : gestion des partages
    - Énumération des partages actifs, ajout, suppression
  - Commande `net sessions` : gestion des sessions SMB
    - Énumération, suppression
  - Commande `net files` : gestion des ressources partagées
    - Énumération, suppression

SMB : côté client

```
C:\>net use * \\192.70.106.131\D$ /u:jbm *
Type the password for \\192.70.106.131\D$:
Drive J: is now connected to \\192.70.106.131\D$.

The command completed successfully.


C:\>net use \\192.70.106.131\IPC$ /u: *
Type the password for \\192.70.106.131\IPC$:
The command completed successfully.


C:\>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           J:        \\192.70.106.131\D$       Microsoft Windows Network
OK                     \\192.70.106.131\IPC$     Microsoft Windows Network
The command completed successfully.
```

SMB : côté serveur

```
C:\>net sessions
Computer                User name           Client Type        Opens Idle time
-------------------------------------------------------------------------------
\\HSC                   JBM                 Unix                   1 00:00:05
The command completed successfully.

C:\>net share IPC$
Share name                                  IPC$
Path
Remark                                      Remote IPC
Maximum users                               No limit
Users                                       JBM
The command completed successfully.

C:\>net files
ID          Path                                 User name            # Locks
-------------------------------------------------------------------------------
3           \PIPE\eventlog                       JBM                       0
The command completed successfully.

C:\>net files 3 /close
The command completed successfully.

C:\>net sessions \\HSC /delete
The command completed successfully.
```

Mises en oeuvre SMB sous Unix

- Projet Samba
  - Mise en oeuvre de NetBT et SMB/CIFS sous Unix
  - Porté sur de nombreux Unix, libres ou propriétaires
  - Composants principaux
    - Démon `nmbd` : gère NetBT
    - Démon `smbd` : gère SMB/CIFS
    - Démon `winbind` : gère l'authentification dans un domaine NT4 ou ActiveDirectory
    - Fichier de configuration unique `smb.conf`, entretenant la confusion entre la configuration de NetBT et de SMB/CIFS...
  - Outils en ligne de commande :
    - `smbclient` : interface ftp-like pour manipuler des fichiers via SMB/CIFS
    - `rpcclient` et `net` (Samba 3) : commandes d'administration distante

Smbclient

```
jbm@garbarek ~> smbclient -I 192.70.106.142 '\\192.70.106.142\H$' -U 'jbm'
Password:
smb: \> ls
  RECYCLER                            DHS        0  Wed Feb 12 11:42:01 2003
  System Volume Information           DHS        0  Fri Jan 12 17:25:26 2001

                32882 blocks of size 32768. 32518 blocks available
smb: \> help
?               altname         archive         blocksize       cancel
cd              chmod           chown           del             dir
du              exit            get             help            history
lcd             link            lowercase       ls              mask
md              mget            mkdir           more            mput
newer           open            print           printmode       prompt
put             pwd             q               queue           quit
rd              recurse         reget           rename          reput
rm              rmdir           setmode         symlink         tar
tarmode         translate       !
smb: \>
```

Mises en oeuvre clientes de SMB sous Unix : systèmes de fichiers

- Approche systèmes de fichiers : clients SMB
  - Approche différente de Samba
    - Samba : implémentation SMB/CIFS en espace **utilisateur**
    - Systèmes de fichiers : pilote de périphérique, donc en mode **noyau**
  - Intérêts de cette approche
    - Intégration transparente au système, accès à un partage SMB via un point de montage dans une arborescence Unix
  - Mises en oeuvres disponibles
    - Linux : smbfs (implémentation historique, 1995), cifs-vfs (implémentation moderne, écrite par Steve French (IBM), intégrée dans les noyaux 2.6.x)
    - FreeBSD : smbfs (Boris Popov, repris dans NetBSD)
    - Mac OS X : basée sur smbfs de Boris Popov, divergences depuis (Conrad Minshall)
      - http://lists.samba.org/archive/samba-technical/2003-October/032271.html
      - http://cvs.opendarwin.org/index.cgi/src/smb/

Cifs-vfs (Linux) et smbfs (FreeBSD)

```
dull# cat /proc/filesystems | grep cifs
nodev   cifs
dull# ls /proc/fs/cifs
DebugData               LookupCacheEnabled  OplockEnabled         SimultaneousOps  traceSMB
ExtendedSecurity        MultiuserMount      PacketSigningEnabled  Stats
LinuxExtensionsEnabled  NTLMV2Enabled       QuotaEnabled          cifsFYI
dull# ./mount.cifs //192.70.106.142/H\$ /mnt -o user=jbm
Password:
dull# mount | grep cifs
//192.70.106.142/H$ on /mnt type cifs (0)
dull# ls /mnt
RECYCLER  System Volume Information
dull# umount /mnt
dull#
```

```
jbm@garbarek ~> sudo mount_smbfs -I 192.70.106.142 '//jbm@*SMBSERVER/H$' /mnt
Password:
jbm@garbarek ~> mount | grep smbfs                                    14:54:35
//JBM@*SMBSERVER/H$ on /mnt (smbfs)
jbm@garbarek ~> ls /mnt                                               14:54:50
RECYCLER                        System Volume Information
jbm@garbarek ~> sudo umount /mnt                                      14:54:52
jbm@garbarek ~>                                                       14:54:56
```

SMB et sécurité

- Protocole SMB
  - Protocole très complexe
    - Nombreux dialectes, nombreuses commandes, plusieurs façons de faire la même chose
    - Complexe à mettre en oeuvre, sujet à des erreurs
  - Problème de sécurité le plus connu :
    - Sessions SMB nulles : possibilité de récupérer des informations de façon anonyme
  - Vulnérabilités récentes dans la mise en oeuvre SMB des systèmes Windows
    - MS02-045: Unchecked Buffer in Network Share Provider Can Lead to Denial of Service
    - MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified
    - MS03-049 - Buffer Overrun in the Workstation Service Could Allow Code Execution

SMB comme protocole de transport

- SMB comme protocole de transport
  - Partage IPC$ est un partage spécial
  - Donne accès, à travers le réseau, à des points de communications appelés **tubes nommés**
  - Des données sont envoyées et reçues via ces **tubes nommés** en utilisant le protocole SMB
  - Les données en question sont des PDU (Protocol Data Unit) DCE RPC
    - SMB devient un protocole de transport pour DCE RPC
    - Ajouté par Microsoft pour plusieurs raisons
      - Notamment parce que SMB peut être lui-même transporté dans plusieurs protocoles, via l'API NetBIOS
      - Authentification réalisée au niveau SMB héritée au niveau DCE RPC
        - Il n'y a pas réauthentification au niveau DCE RPC

MSRPC : introduction

- MSRPC
  - Mise en oeuvre du standard DCE RPC par Microsoft
  - DCE RPC prévu pour être indépendant du protocole de transport utilisé
    - TCP/IP, IPX/SPX, NetBEUI, ...
    - Microsoft a ajouté un transport utilisant SMB
- Analogie
  - DCE RPC sur TCP/IP utilise des ports TCP/IP pour communiquer
  - DCE RPC sur SMB utilise des tubes nommés
- DCE RPC sur TCP/IP est utilisé pour transporter DCOM
  - Voir les vulnérabilités récentes sur DCOM, exploitables via TCP/IP (port 135)

DCE RPC sur SMB

- DCE RPC sur SMB
  - Utilisés par la plupart des outils Windows d'administration distante
  - Noms des tubes nommés identifient les services accessibles via DCE RPC
  - Exemple : `eventlog` pour la consultation des journaux à distance, `winreg` pour l'accès distant à la base de registres, `svcctl` pour la gestion des services Windows à distance, etc...
- En pratique
  - Authentification réalisée de façon transparente au niveau SMB
    - Pas d'authentification au niveau DCE RPC
  - Possibilité d'utiliser une **session SMB nulle** (login et mot de passe vides lors de l'authentification au niveau SMB)
  - Façon de récupérer des informations de façon anonyme...
    - Concerne principalement les tubes nommés `lsarpc` (LSA Windows), `samr` (SAM), `wkssvc` (service workstation), `srvsvc` (service serveur)

DCE RPC sur SMB : en pratique

- DCE RPC sur SMB : en pratique
  - Utilisation d'un outil d'administration Windows en spécifiant un nom de serveur distant déclenche l'utilisation de DCE RPC sur SMB
  - Exemple : consultation à distance des journaux d'un système Windows
    - Ouverture d'une session SMB (typiquement authentifiée avec des accréditations administrateur)
    - Connexion au partage `IPC$`
    - Ouverture du tube nommé `eventlog`
    - Écriture et lecture de données via le descripteur de fichier ouvert sur le tube `eventlog`, correspondant à des appels de procédures distantes permettant la consultation des journaux du système distant
  - Ethereal décode un certain nombre d'interfaces MSRPC, outil privilégié pour observer *sur le fil* DCE RPC sur SMB

Consultation distante des journaux

No.	Time	Source	Destination	Protocol	Info
11	0.264201	192.70.106.76	192.70.106.142	SMB	Tree Connect AndX Request, Path: \\192.70.106.142\IPC$
12	0.264369	192.70.106.142	192.70.106.76	SMB	Tree Connect AndX Response
14	3.782651	192.70.106.76	192.70.106.142	SMB	NT Create AndX Request, Path: \EVENTLOG
15	3.783149	192.70.106.142	192.70.106.76	SMB	NT Create AndX Response, FID: 0x4000
17	3.789518	192.70.106.76	192.70.106.142	DCERPC	Bind: call_id: 1 UUID: EVENTLOG
18	3.789664	192.70.106.142	192.70.106.76	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 4280 max_recv: 4280
19	3.791691	192.70.106.76	192.70.106.142	EVENTLOG	ElfrOpenELW request
20	3.792145	192.70.106.142	192.70.106.76	EVENTLOG	ElfrOpenELW reply[Long frame (20 bytes)]
21	3.794115	192.70.106.76	192.70.106.142	EVENTLOG	ElfrNumberOfRecords request
22	3.794277	192.70.106.142	192.70.106.76	EVENTLOG	ElfrNumberOfRecords reply
23	3.796683	192.70.106.76	192.70.106.142	EVENTLOG	ElfrReadELW request
24	3.796810	192.70.106.142	192.70.106.76	EVENTLOG	ElfrReadELW reply
25	3.798288	192.70.106.76	192.70.106.142	EVENTLOG	ElfrReadELW request
26	3.798412	192.70.106.142	192.70.106.76	EVENTLOG	ElfrReadELW reply
27	3.803304	192.70.106.76	192.70.106.142	EVENTLOG	ElfrReadELW request
28	3.803646	192.70.106.142	192.70.106.76	EVENTLOG	ElfrReadELW reply

```
⊞ Frame 19 (226 bytes on wire, 226 bytes captured)
⊞ Ethernet II, Src: 00:00:e8:d6:e0:52, Dst: 00:01:02:a4:95:b2
⊞ Internet Protocol, Src Addr: 192.70.106.76 (192.70.106.76), Dst Addr: 192.70.106.142 (192.70.106.142)
⊞ Transmission Control Protocol, Src Port: 1043 (1043), Dst Port: 139 (139), Seq: 1300032575, Ack: 2096328376, Len: 160
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB Pipe Protocol
⊞ DCE RPC
⊞ Microsoft Eventlog Service
```

DCE RPC sur SMB depuis Unix

- RPC d'administration Microsoft
  - Mis en oeuvre par le projet Samba, entièrement par *reverse-engineering*
  - Certains de ces RPC étaient en effet indispensables pour émuler un contrôleur de domaine Windows NT4
  - Outils développés par Samba
    - Permettent de tester et d'utiliser la mise en oeuvre des RPC réalisées par le projet Samba
    - Commande `rpcclient` (version Samba et Samba-TNG)
      - http://www.hsc.fr/tips/remote_windows_rpcclient.html
    - Commande `net`, dans Samba 3
    - Ces commandes permettent d'administrer à distance des systèmes Windows depuis Unix
      - En ligne de commande, possibilité de scripter des tâches d'administration

rpcclient : Samba-TNG

```
marchand@dull:~/tng/usr/bin$ ./rpcclient -U jbm -S 192.70.106.142
Enter Password:
Server: \\192.70.106.142:       User:   jbm     Domain:
Connection:     session setup ok
Domain=[STAGIAIRES] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
OK
[jbm@192.70.106.142]$
!               dfsenum         lsaenumsids     samuserset
?               dfsremove       lsaquery        samuserset2
abortshutdown   dispinfo        lsashowsd       service
addaliasmem     dominfo         ntlogin         set
addgroupmem     domlist         ntpass          setsecret
at              domtrust        privinfo        share
brsinfo         enumaliases     querysecret     shutdown
brsstats        enumdomains     registry        spool
createalias     enumgroups      samalias        srvconnections
creategroup     enumprivs       samaliasmem     srvfiles
createsecret    enumusers       samgroup        srvinfo
createuser      eventlog        samgroupmem     srvsessions
delalias        exit            samlookupnames  srvtransports
delaliasmem     help            samlookuprids   time
delgroup        lookupdomain    samquerysec     trustinfo
delgroupmem     lookupnames     samsync         use
deluser         lookupsids      samtest         who
dfsadd          lsaenumdomains  samuser         wksinfo
[jbm@192.70.106.142]$
```

rpcclient : Samba 3.0

```
jbm@garbarek ~> rpcclient -U jbm -I 192.70.106.142 192.70.106.142
Password:
rpcclient $> help
---------------         ----------------------
            ECHO
      echoaddone        Add one to a number
        echodata        Echo data
        sinkdata        Sink data
      sourcedata        Source data
---------------         ----------------------
             REG
       shutdown         Remote Shutdown
   abortshutdown        Abort Shutdown
---------------         ----------------------
             DFS
       dfsexist         Query DFS support
         dfsadd         Add a DFS share
      dfsremove         Remove a DFS share
     dfsgetinfo         Query DFS share info
        dfsenum         Enumerate dfs shares
---------------         ----------------------
          SRVSVC
        srvinfo         Server query info
    netshareenum        Enumerate shares
     netfileenum        Enumerate open files
    netremotetod        Fetch remote time of day
---------------         ----------------------
        NETLOGON
     logonctrl2         Logon Control 2
      logonctrl         Logon Control
```

net : Samba 3.0

```
jbm@garbarek *> net rpc

Usage:
  net rpc info                  show basic info about a domain
  net rpc join                  to join a domain
  net rpc oldjoin                       to join a domain created in server manager


  net rpc testjoin              tests that a join is valid
  net rpc user                  to add, delete and list users
  net rpc group                 to list groups
  net rpc share                 to add, delete, and list shares
  net rpc file                  to list open files
  net rpc changetrustpw         to change the trust account password
  net rpc getsid                fetch the domain sid into the local secrets.tdb
  net rpc vampire               syncronise an NT PDC's users and groups into the local
  net rpc samdump               diplay an NT PDC's users, groups and other data
  net rpc trustdom              to create trusting domain's account
                                        or establish trust
  net rpc abortshutdown         to abort the shutdown of a remote server
  net rpc shutdown              to shutdown a remote server

'net rpc shutdown' also accepts the following miscellaneous options:
        -r or --reboot  request remote server reboot on shutdown
        -f or --force   request the remote server force its shutdown
        -t or --timeout=<timeout>       number of seconds before shutdown
        -c or --comment=<message>       text message to display on impending shutdown
```

DCE RPC sur TCP/IP

- Services RPC sur TCP/IP
  - Utilisés plus fréquemment dans des domaines ActiveDirectory
    - Ex : Réplication des annuaires Active Directory
  - Autre protocole basé sur des RPC sur TCP/IP : MAPI (Exchange)
  - Autre grande utilisation de DCE RPC sur TCP/IP : transport de DCOM
    - Via le port 135/tcp, activation d'objets COM à distance
    - Certaines interfaces RPC accessibles via 135/tcp ont des opérations accessibles en anonyme
    - Vers Blaster (été 2003), exploitant une vulnérabilité dans une opération d'une interface RPC nécessaire au fonctionnement de DCOM
  - Service associé : portmapper, donnant la correspondance entre un identifiant d'interface RPC et un port (TCP ou UDP) sur lequel ce service est accessible
    - Port 135, équivalent du portmapper des ONC RPC (port 111)

DCOM sur DCE RPC sur TCP/IP

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.70.106.76	192.70.106.142	TCP	49163 > 135 [SYN] Seq=3113638230 Ack=0 Win=65535 Len=0 MSS
2	0.000812	192.70.106.142	192.70.106.76	TCP	135 > 49163 [SYN, ACK] Seq=3228813016 Ack=3113638231 Win=1
3	0.000903	192.70.106.76	192.70.106.142	TCP	49163 > 135 [ACK] Seq=3113638231 Ack=3228813017 Win=33304
4	0.000976	192.70.106.76	192.70.106.142	DCERPC	Bind: call_id: 9 UUID: REMACT
5	0.002227	192.70.106.142	192.70.106.76	DCERPC	Bind_ack: call_id: 9 accept max_xmit: 5840 max_recv: 5840
6	0.002335	192.70.106.76	192.70.106.142	REMACT	RemoteActivation request
7	0.003838	192.70.106.142	192.70.106.76	REMACT	RemoteActivation reply
8	0.003903	192.70.106.76	192.70.106.142	TCP	49163 > 135 [FIN, ACK] Seq=3113638429 Ack=3228813169 Win=3
9	0.003987	192.70.106.76	192.70.106.142	TCP	49164 > 135 [SYN] Seq=2727600172 Ack=0 Win=65535 Len=0 MSS

```
⊞ Frame 6 (192 bytes on wire, 192 bytes captured)
⊞ Ethernet II, Src: 00:00:39:d1:d0:2e, Dst: 00:40:05:67:04:72
⊞ Internet Protocol, Src Addr: 192.70.106.76 (192.70.106.76), Dst Addr: 192.70.106.142 (192.70.106.142)
⊞ Transmission Control Protocol, Src Port: 49163 (49163), Dst Port: 135 (135), Seq: 3113638303, Ack: 3228813077, Len: 126
⊞ DCE RPC
⊟ DCOM Remote Activation
    Operation: RemoteActivation (0)
    Stub data (102 bytes)
```

MSRPC et sécurité

- MSRPC est une implémentation apparemment fragile
  - Certaines interfaces RPC peuvent être accessibles sans authentification
    - Via une session nulle pour des services DCE RPC sur SMB
    - Via TCP/IP (typiquement port 135), pour des services RPC ne nécessitant pas une authentification
      - Va probablement changer avec le SP2 de Windows XP
  - Service rpcss est un processus système (identité SYSTEM)
    - Vulnérabilité dans une interface RPC de ce service permet, si l'exploitation est possible, d'exécuter du code sous l'identité SYSTEM
  - Bien penser à filtrer tous les protocoles de communication permettant l'utilisation des RPC
    - SMB (port 139 et 445), TCP/IP (port 135 et ports dynamiques, à restreindre dans une plage de ports spécifiques), HTTP (593/tcp, pas activé par défaut)

Conclusion

- Protocoles réseaux Windows
  - NetBIOS sur TCP/IP est juste un protocole de transport pour SMB
  - SMB/CIFS est le protocole coeur
    - Partage de ressources (fichiers et imprimantes)
    - Protocole de transport des RPC d'administration distantes
  - MSRPC est également au coeur des systèmes Windows
    - Les composants Windows utilisent une version locale des RPC pour communiquer entre eux
    - Attire depuis longtemps l'attention de la communauté sécurité
      - Nombreuses vulnérabilités découvertes ces dernières années
      - MSRPC est apparemment une implémentation fragile
  - Les fonctionnalités et risques de ces protocoles doivent être connus pour sécuriser les accès réseaux des systèmes Windows

Références

- *Implementing CIFS*. Christopher R. Hertel. Prentice Hall
  - http://www.ubiqx.org/cifs/
- *DCE/RPC over SMB: Samba and Windows NT Domain Internals*. Luke Kenneth Casson Leighton. MTP
- Samba et Samba-TNG
  - http://www.samba.org, http://www.samba-tng.org
- Ethereal
  - http://www.ethereal.com
  - Analyseur réseau disponible en logiciel libre (Unix et Windows)
  - Support de nombreux protocoles, dont les protocoles évoqués ici
  - Outil le plus approprié pour comprendre le fonctionnement des protocoles réseaux en environnement Windows

Références : autres publications

- Autres publications
  - Brève : Administration distante de systèmes Windows avec rpcclient (version Samba-TNG)
    - http://www.hsc.fr/tips/remote_windows_rpcclient.html
  - Brève : Minimisation des services réseaux Windows
    - http://www.hsc.fr/tips/min_srv_res_win.html
  - Présentation : Windows network services for Samba folks (SambaXP 2003)
    - http://www.hsc.fr/ressources/presentations/sambaxp2003/
  - Présentation : Windows network services internals (HiverCon 03)
    - http://www.hsc.fr/ressources/presentations/hivercon03/
  - Article : Windows network services internals
    - http://www.hsc.fr/ressources/articles/win_net_srv/

Questions ?

jbm@hsc.fr