Windows network services for Samba folks

Jean-Baptiste Marchand
<jbm@hsc.fr>
Hervé Schauer Consultants

Agenda

- SMB/CIFS implementation
- MSRPC implementation
- Network authentication
- Interesting tools
- References

SMB/CIFS architecture

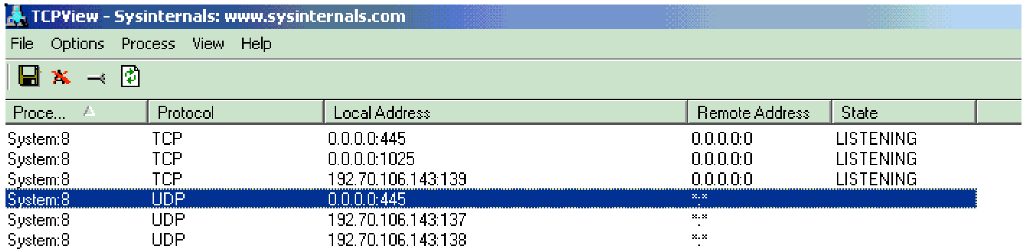
- kernel-mode components
  - Client-side: redirector
    - rdr.sys (NT), mrxsmb.sys (W2K and >)
  - Server-side: server (srv.sys)
- User-mode services
  - lanmanserver and lanmanworkstation
  - configuration of kernel-mode components

SMB/CIFS transport

- Typical SMB/CIFS transports
  - NetBT (TCP port 139) or raw (TCP port 445)
  - NetBios over TCP/IP driver (netbt.sys)
    - Ports: UDP 137 and 138 , TCP 139 and 445 (kernel mode)
    - NetBT: one device per network adapter (NetBT_Tcpip_)
    - raw SMB: unique device (NetbiosSmb)
      - MSKB #204279 (http://support.microsoft.com/?id=204279)
      - SmbDeviceEnabled registry value (NetBT\Parameters\)

TCPView

- TCPView (sysinternals)
    - displays processes that owns a TCP or UDP endpoint
    - System process: endpoints opened by a driver

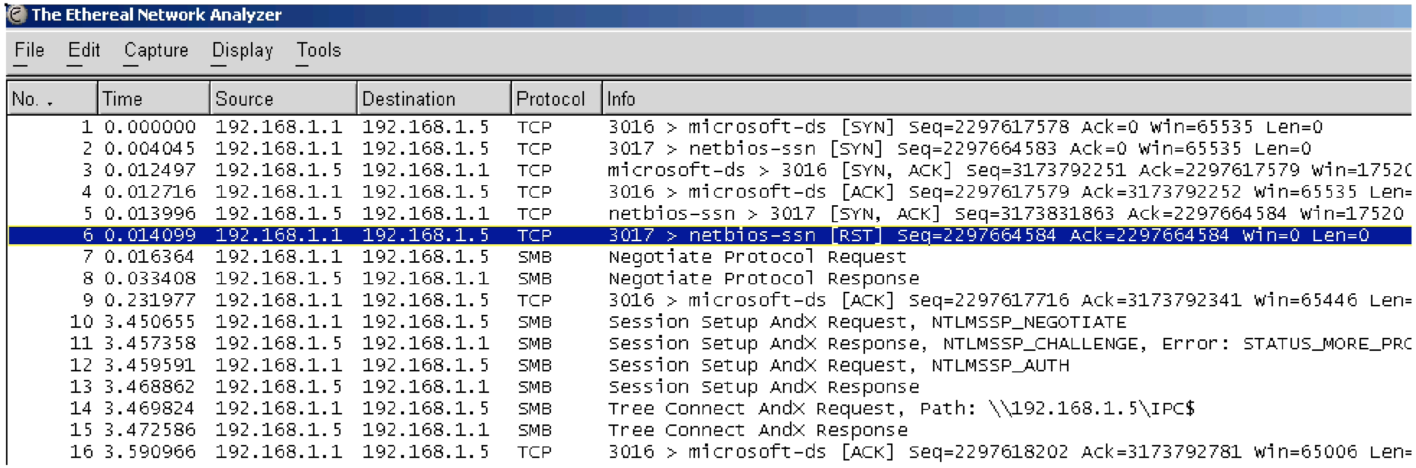


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Proce...	Protocol	Local Address	Remote Address	State
System:8	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
System:8	TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
System:8	TCP	192.70.106.143:139	0.0.0.0:0	LISTENING
System:8	UDP	0.0.0.0:445	*:*	
System:8	UDP	192.70.106.143:137	*:*	
System:8	UDP	192.70.106.143:138	*:*	

NetBT and raw SMB transport

- raw SMB preferred over NetBT transport
  - If both transports are active, the redirector resets the TCP connection to port 139 (NetBT)

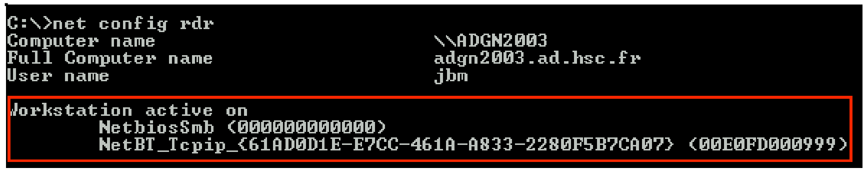


```
No. .   Time      Source        Destination   Protocol  Info
      1 0.000000  192.168.1.1   192.168.1.5   TCP       3016 > microsoft-ds [SYN] Seq=2297617578 Ack=0 Win=65535 Len=0
      2 0.004045  192.168.1.1   192.168.1.5   TCP       3017 > netbios-ssn [SYN] Seq=2297664583 Ack=0 Win=65535 Len=0
      3 0.012497  192.168.1.5   192.168.1.1   TCP       microsoft-ds > 3016 [SYN, ACK] Seq=3173792251 Ack=2297617579 Win=1752(
      4 0.012716  192.168.1.1   192.168.1.5   TCP       3016 > microsoft-ds [ACK] Seq=2297617579 Ack=3173792252 Win=65535 Len=
      5 0.013996  192.168.1.5   192.168.1.1   TCP       netbios-ssn > 3017 [SYN, ACK] Seq=3173831863 Ack=2297664584 Win=17520
      6 0.014099  192.168.1.1   192.168.1.5   TCP       3017 > netbios-ssn [RST] Seq=2297664584 Ack=2297664584 Win=0 Len=0
      7 0.016364  192.168.1.1   192.168.1.5   SMB       Negotiate Protocol Request
      8 0.033408  192.168.1.5   192.168.1.1   SMB       Negotiate Protocol Response
      9 0.231977  192.168.1.1   192.168.1.5   TCP       3016 > microsoft-ds [ACK] Seq=2297617716 Ack=3173792341 Win=65446 Len=
     10 3.450655  192.168.1.1   192.168.1.5   SMB       Session Setup AndX Request, NTLMSSP_NEGOTIATE
     11 3.457358  192.168.1.5   192.168.1.1   SMB       Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRC
     12 3.459591  192.168.1.1   192.168.1.5   SMB       Session Setup AndX Request, NTLMSSP_AUTH
     13 3.468862  192.168.1.5   192.168.1.1   SMB       Session Setup AndX Response
     14 3.469824  192.168.1.1   192.168.1.5   SMB       Tree Connect AndX Request, Path: \\192.168.1.5\IPC$
     15 3.472586  192.168.1.5   192.168.1.1   SMB       Tree Connect AndX Response
     16 3.590966  192.168.1.1   192.168.1.5   TCP       3016 > microsoft-ds [ACK] Seq=2297618202 Ack=3173792781 Win=65006 Len=
```

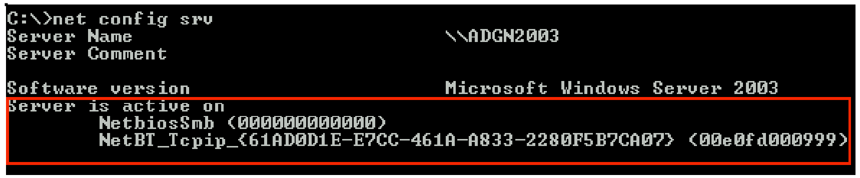
Transport configuration

- {server,redirector} transport configuration
  - GUI: network adapter properties
    - server: *File and Printer Sharing for Microsoft Networks*
    - redirector: *Client for Microsoft networks*
    - server and redirector: *Enable NetBIOS over TCP/IP*
  - CLI: net config srv, net config rdr
  - Raw SMB redirector transport always available
    - even with *Client for Microsoft networks* disabled

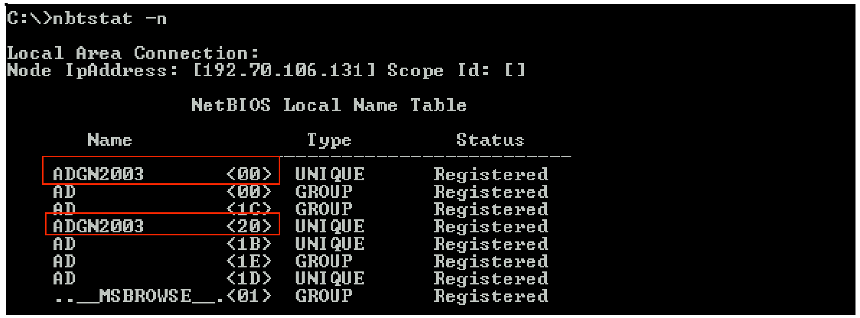
net config and nbtstat



```
C:\>net config rdr
Computer name                        \\ADGN2003
Full Computer name                   adgn2003.ad.hsc.fr
User name                            jbm

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{61AD0D1E-E7CC-461A-A833-2280F5B7CA07} (00E0FD000999)
```



```
C:\>net config srv
Server Name                          \\ADGN2003
Server Comment

Software version                     Microsoft Windows Server 2003
Server is active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{61AD0D1E-E7CC-461A-A833-2280F5B7CA07} (00e0fd000999)
```

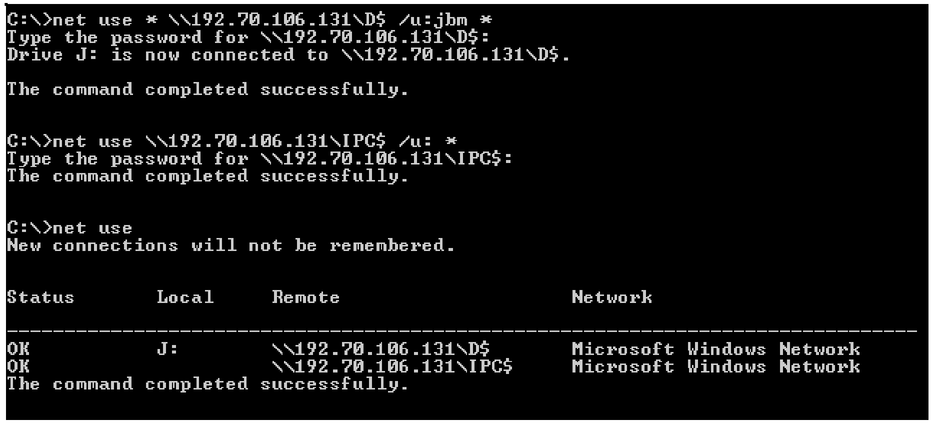


```
C:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.70.106.131] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    ADGN2003       <00>  UNIQUE      Registered
    AD             <00>  GROUP       Registered
    AD             <1C>  GROUP       Registered
    ADGN2003       <20>  UNIQUE      Registered
    AD             <1B>  UNIQUE      Registered
    AD             <1E>  GROUP       Registered
    AD             <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
```

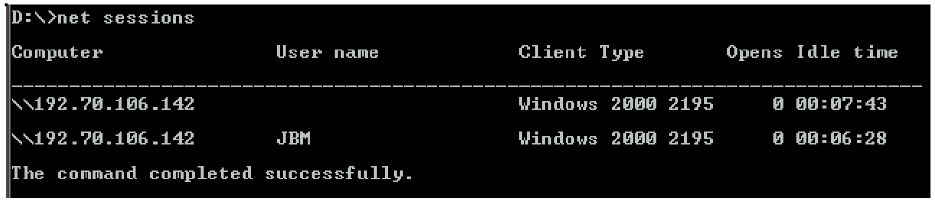
Using the redirector

- Establishing an SMB session: use records
  - *net use* command
    - Ex: net use * \\unc_name\share (cached credentials)
    - Ex: net use * \\192.168.1.42\myshare /u:jbm * (alternate credentials)
    - Ex: net use \\192.168.1.42\IPC$ /u: * (null session)
    - net use : enumerate use records in the **current logon session**
      - SMB sessions are established (and reestablished) seamlessly, once a use record is active

net use



```
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.
```



```
D:\>net sessions

Computer               User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------
\\192.70.106.142                            Windows 2000 2195     0 00:07:43

\\192.70.106.142       JBM                  Windows 2000 2195     0 00:06:28

The command completed successfully.
```

LSA credentials cache

- Local Security Authority credentials cache
  - {LM,NT} hashes caching in each logon session
  - Used by the MSV1_0 (NTLM) authentication package
    - And by Kerberos as well, once a TGT has expired and is no longer renewable
  - Transparent network authentication
    - current username and password are seamlessly reused
  - Alternate credentials can be specified with net use

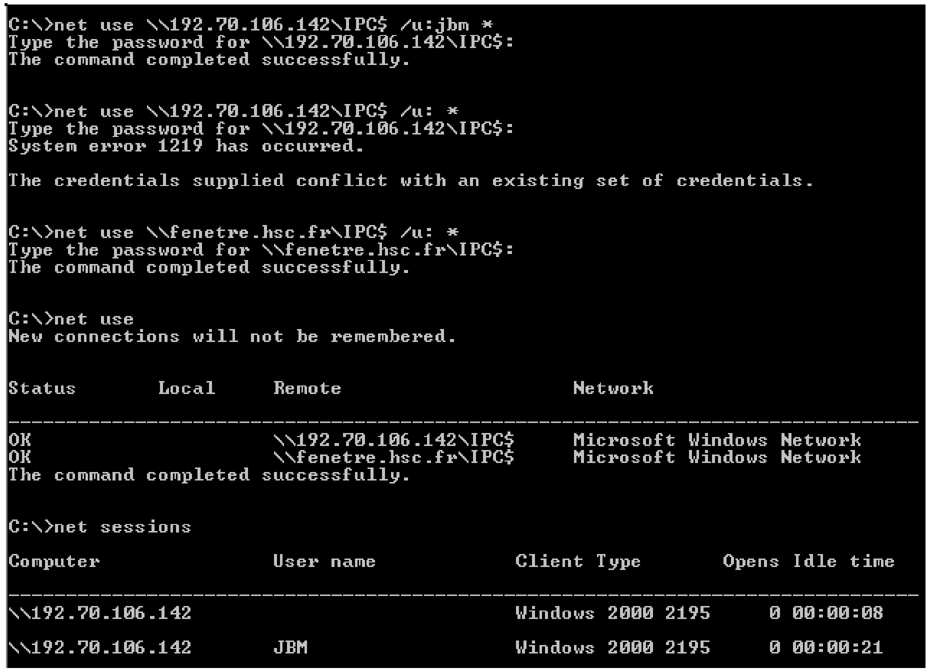
Redirector sessions cache

- Sessions cache
  - Established sessions are seamlessly used
  - Ex: using a remote administration tool on a remote machine
    - Any session established to the IPC$ share of the remote machine will be reused
    - Administration trick:
      - Establish a session with administrator credentials (using net use) to IPC$, before using remote administration tools

Sessions cache internals

- A session is uniquely identified by
  - Client: logon session id and network address
  - Server: server name
    - A different server name must be used to establish multiple sessions (with different credentials) to a given server
      - System error 1219 (*The credentials supplied conflict with an existing set of credentials*)
  - Trick: using NetBIOS name, IPv4 address or fqdn DNS name to establish multiple sessions to the same server, with different credentials

Multiple SMB sessions

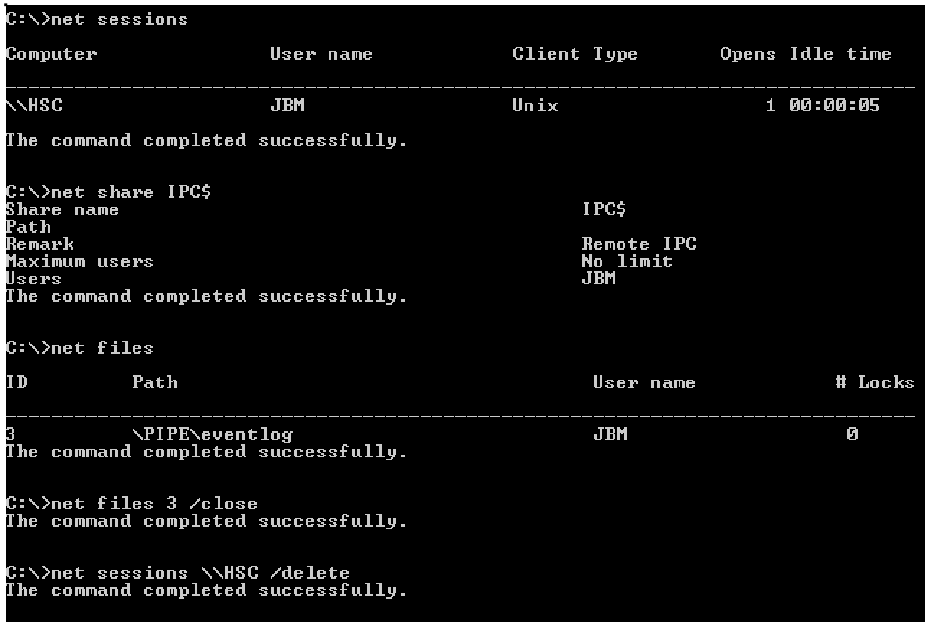


```
C:\>net use \\192.70.106.142\IPC$ /u:jbm *
Type the password for \\192.70.106.142\IPC$:
The command completed successfully.


C:\>net use \\192.70.106.142\IPC$ /u: *
Type the password for \\192.70.106.142\IPC$:
System error 1219 has occurred.

The credentials supplied conflict with an existing set of credentials.


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


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


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK                     \\192.70.106.142\IPC$     Microsoft Windows Network
OK                     \\fenetre.hsc.fr\IPC$     Microsoft Windows Network
The command completed successfully.


C:\>net sessions

Computer               User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------
\\192.70.106.142                            Windows 2000 2195     0 00:00:08

\\192.70.106.142       JBM                  Windows 2000 2195     0 00:00:21
```

File server administration

- Administration (*net* command)
  - Shares management: *net share*
  - Sessions management: *net sessions*
    - displays a list of established SMB sessions
    - can disconnect any session (*/delete*)
  - Shared resources management: *net files*
    - displays a list of accessed local resources
    - can close any shared resource (*/close*)

SMB session (IPC$)



```
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.
```

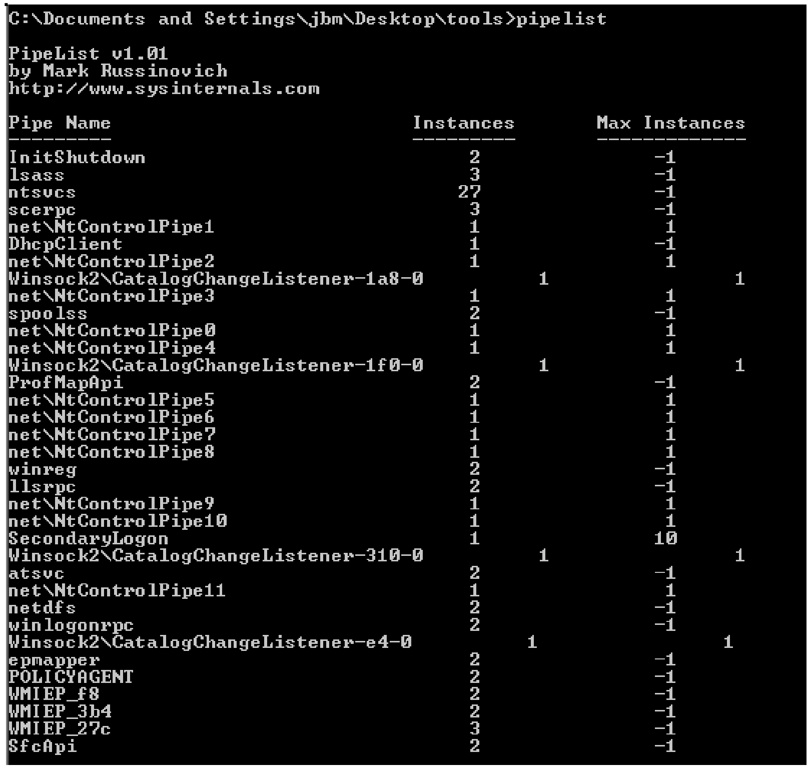
MSRPC

- Microsoft implementation of DCE RPC
  - Used in all versions of Windows NT, at all levels
    - Typical use: NT domains, remote administration, DCOM
- Transport independent
  - TCP/IP, IPX/SPX, NETBEUI,...
    - SMB transport (Windows-specific), using named pipes as DCE RPC endpoints
    - DCE RPC Protocol Data Units (PDUs) are sent over named pipes, using SMB commands

Named pipes

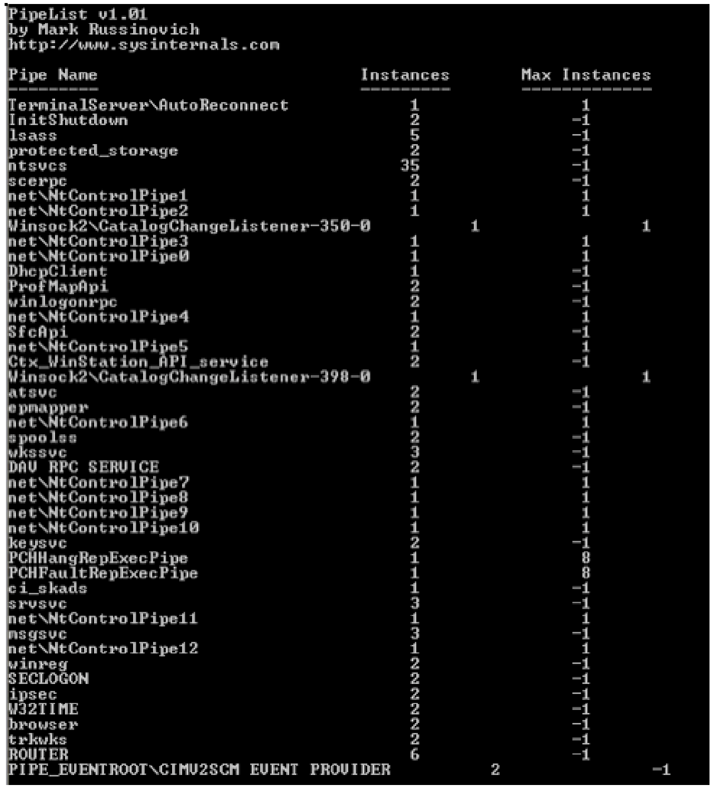
- Inter-Process Communication (IPC) mechanism
  - Locally or over the network (using SMB)
- Implemented by a file system driver
  - npfs.sys (Ex: \Device\NamedPipes\lsass)
- Named pipes enumeration
  - pipelist (sysinternals.com)

Named pipes (Windows 2K)



```
C:\Documents and Settings\jbm\Desktop\tools>pipelist

PipeList v1.01
by Mark Russinovich
http://www.sysinternals.com

Pipe Name                          Instances       Max Instances
---------                          ---------       -------------
InitShutdown                            2               -1
lsass                                   3               -1
ntsvcs                                 27               -1
scerpc                                  3               -1
net\NtControlPipe1                      1                1
DhcpClient                              1               -1
net\NtControlPipe2                      1                1
Winsock2\CatalogChangeListener-1a8-0          1                1
net\NtControlPipe3                      1                1
spoolss                                 2               -1
net\NtControlPipe0                      1                1
net\NtControlPipe4                      1                1
Winsock2\CatalogChangeListener-1f0-0          1                1
ProfMapApi                              2               -1
net\NtControlPipe5                      1                1
net\NtControlPipe6                      1                1
net\NtControlPipe7                      1                1
net\NtControlPipe8                      1                1
winreg                                  2               -1
llsrpc                                  2               -1
net\NtControlPipe9                      1                1
net\NtControlPipe10                     1                1
SecondaryLogon                          1               10
Winsock2\CatalogChangeListener-310-0          1                1
atsvc                                   2               -1
net\NtControlPipe11                     1                1
netdfs                                  2               -1
winlogonrpc                             2               -1
Winsock2\CatalogChangeListener-e4-0          1                1
epmapper                                2               -1
POLICYAGENT                             2               -1
WMIEP_f8                                2               -1
WMIEP_3b4                               2               -1
WMIEP_27c                               3               -1
SfcApi                                  2               -1
```

Named pipes (Windows XP)

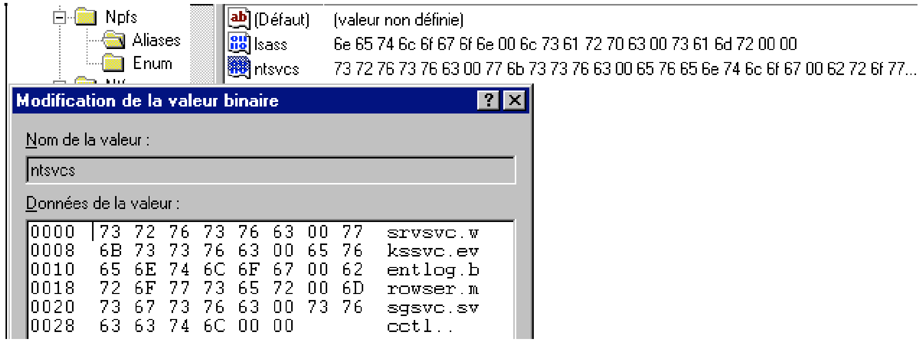


```
PipeList v1.01
by Mark Russinovich
http://www.sysinternals.com

Pipe Name                          Instances       Max Instances
---------                          ---------       -------------
TerminalServer\AutoReconnect             1               1
InitShutdown                             2              -1
lsass                                    5              -1
protected_storage                        2              -1
ntsvcs                                  35              -1
scerpc                                   2              -1
net\NtControlPipe1                       1               1
net\NtControlPipe2                       1               1
Winsock2\CatalogChangeListener-350-0           1                1
net\NtControlPipe3                       1               1
net\NtControlPipe0                       1               1
DhcpClient                               1              -1
ProfMapApi                               2              -1
winlogonrpc                              2              -1
net\NtControlPipe4                       1               1
SfcApi                                   2              -1
net\NtControlPipe5                       1               1
Ctx_WinStation_API_service               2              -1
Winsock2\CatalogChangeListener-398-0           1                1
atsvc                                    2              -1
epmapper                                 2              -1
net\NtControlPipe6                       1               1
spoolss                                  2              -1
wkssvc                                   3              -1
DAV RPC SERVICE                          2              -1
net\NtControlPipe7                       1               1
net\NtControlPipe8                       1               1
net\NtControlPipe9                       1               1
net\NtControlPipe10                      1               1
keysvc                                   2              -1
PCHHangRepExecPipe                       1               8
PCHFaultRepExecPipe                      1               8
ci_skads                                 1              -1
srvsvc                                   3              -1
net\NtControlPipe11                      1               1
msgsvc                                   3              -1
net\NtControlPipe12                      1               1
winreg                                   2              -1
SECLOGON                                 2              -1
ipsec                                    2              -1
W32TIME                                  2              -1
browser                                  2              -1
trkwks                                   2              -1
ROUTER                                   6              -1
PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER           2               -1
```

npfs aliases

- Named pipes aliases
  - Npfs\Aliases registry value
    - \pipe\lsass aliases
      - Windows NT, 2K, XP, Server 2003: \pipe\{netlogon, lsarpc, samr}
    - \pipe\ntsvcs aliases:
      - Windows NT, 2K: \pipe\{srvsvc, wkssvc, eventlog, browse, msgsvc, svcctl, w32time (W2K only)}
      - Windows XP, Server 2003: \pipe\{eventlog, svcctl}
    - \pipe\lanman (used by RAP calls) is *not a real* named pipe

npfs aliases (NT, 2K, {XP, 2K3})



(Défaut)	(valeur non définie)
lsass	6e 65 74 6c 6f 67 6f 6e 00 6c 73 61 72 70 63 00 73 61 6d 72 00 00
ntsvcs	73 72 76 73 76 63 00 77 6b 73 73 76 63 00 65 76 65 6e 74 6c 6f 67 00 62 72 6f 77...

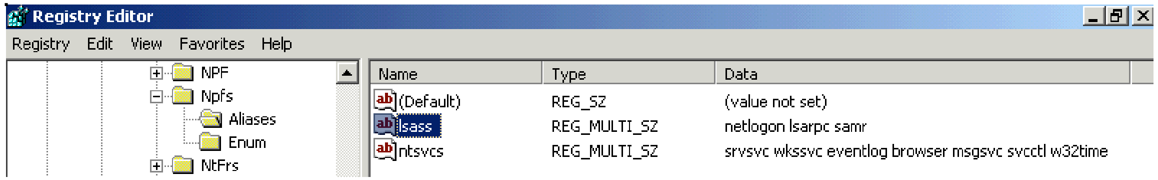
Modification de la valeur binaire

Nom de la valeur :

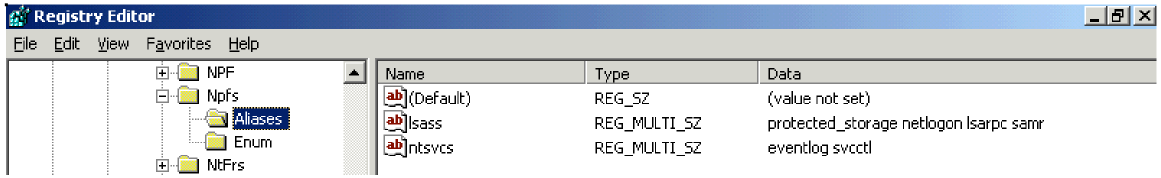
ntsvcs

Données de la valeur :

```
0000  73 72 76 73 76 63 00 77   srvsvc.w
0008  6B 73 73 76 63 00 65 76   kssvc.ev
0010  65 6E 74 6C 6F 67 00 62   entlog.b
0018  72 6F 77 73 65 72 00 6D   rowser.m
0020  73 67 73 76 63 00 73 76   sgsvc.sv
0028  63 63 74 6C 00 00         cctl..
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
lsass	REG_MULTI_SZ	netlogon lsarpc samr
ntsvcs	REG_MULTI_SZ	srvsvc wkssvc eventlog browser msgsvc svcctl w32time

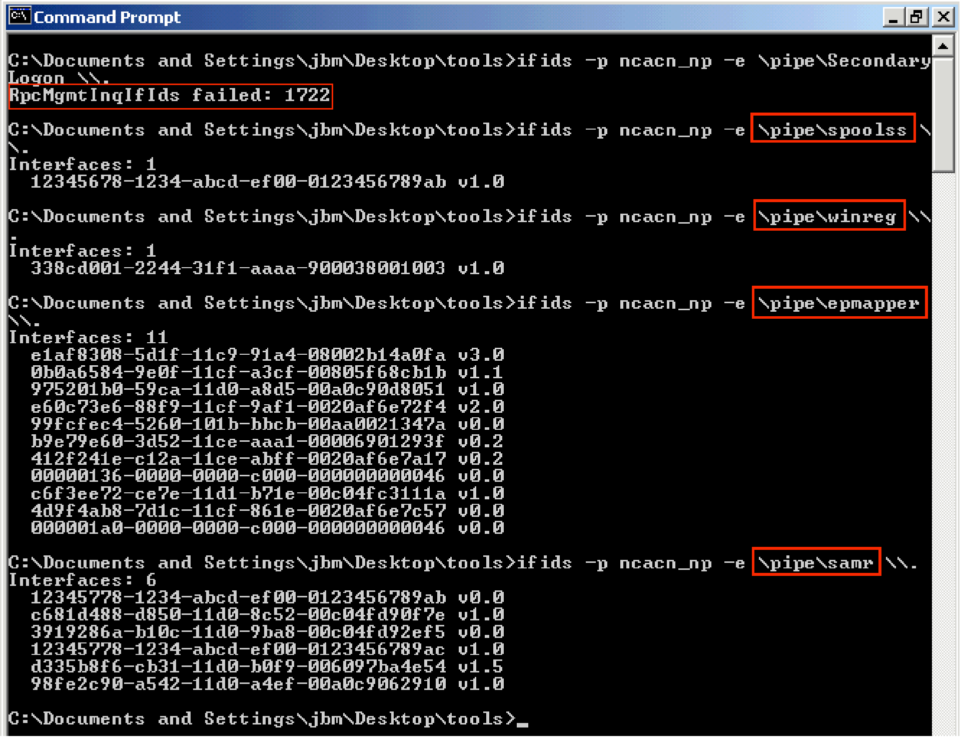


Name	Type	Data
(Default)	REG_SZ	(value not set)
lsass	REG_MULTI_SZ	protected_storage netlogon lsarpc samr
ntsvcs	REG_MULTI_SZ	eventlog svcctl

DCE RPC remote management interface

- DCE RPC mgmt interface
  - interface: set of related operations
  - management interface
    - Implicitly supported by any DCE RPC service
    - ifids tool (Todd Sabin)
- Identification of named pipes used as MSRPC endpoints, using ifids
  - ifids -p ncacn_np -e \pipe\pipe_name \\UNC_name

ifids: named pipes endpoints

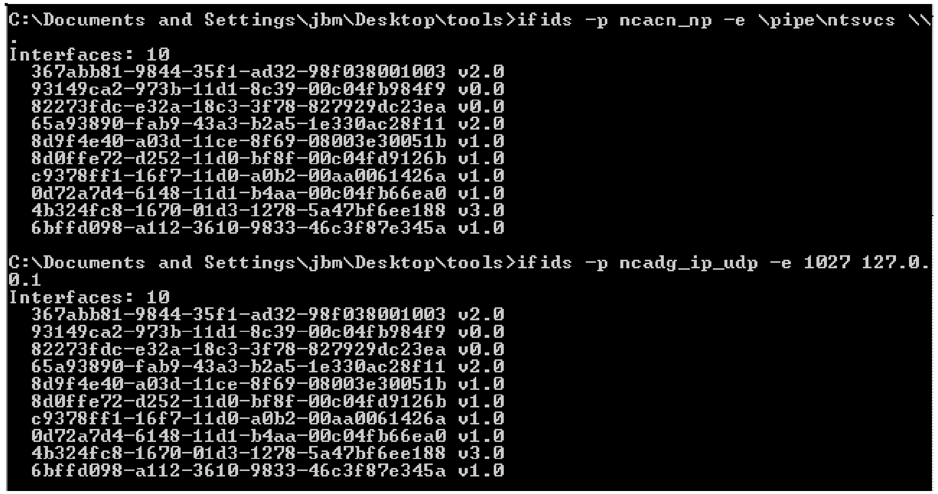


```
C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\Secondary
Logon \\.
RpcMgmtInqIfIds failed: 1722

C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\spoolss \
\.
Interfaces: 1
  12345678-1234-abcd-ef00-0123456789ab v1.0

C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\winreg \\
.
Interfaces: 1
  338cd001-2244-31f1-aaaa-900038001003 v1.0

C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\epmapper
\\.
Interfaces: 11
  e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
  0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.1
  975201b0-59ca-11d0-a8d5-00a0c90d8051 v1.0
  e60c73e6-88f9-11cf-9af1-0020af6e72f4 v2.0
  99fcfec4-5260-101b-bbcb-00aa0021347a v0.0
  b9e79e60-3d52-11ce-aaa1-00006901293f v0.2
  412f241e-c12a-11ce-abff-0020af6e7a17 v0.2
  00000136-0000-0000-c000-000000000046 v0.0
  c6f3ee72-ce7e-11d1-b71e-00c04fc3111a v1.0
  4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 v0.0
  000001a0-0000-0000-c000-000000000046 v0.0

C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\samr \\.
Interfaces: 6
  12345778-1234-abcd-ef00-0123456789ab v0.0
  c681d488-d850-11d0-8c52-00c04fd90f7e v1.0
  3919286a-b10c-11d0-9ba8-00c04fd92ef5 v0.0
  12345778-1234-abcd-ef00-0123456789ac v1.0
  d335b8f6-cb31-11d0-b0f9-006097ba4e54 v1.5
  98fe2c90-a542-11d0-a4ef-00a0c9062910 v1.0

C:\Documents and Settings\jbm\Desktop\tools>_
```

MSRPC supported interfaces

- Multiple interfaces
  - Inside a given process, all RPC services can be accessed using any endpoint on any transport
  - Most Windows services (daemons) are implemented in shared processes (services.exe, svchost.exe)
  - Consequence: ifids gives the list of all interfaces of all in-process RPC services

services.exe RPC services



```
C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncacn_np -e \pipe\ntsvcs \\
.
Interfaces: 10
  367abb81-9844-35f1-ad32-98f038001003 v2.0
  93149ca2-973b-11d1-8c39-00c04fb984f9 v0.0
  82273fdc-e32a-18c3-3f78-827929dc23ea v0.0
  65a93890-fab9-43a3-b2a5-1e330ac28f11 v2.0
  8d9f4e40-a03d-11ce-8f69-08003e30051b v1.0
  8d0ffe72-d252-11d0-bf8f-00c04fd9126b v1.0
  c9378ff1-16f7-11d0-a0b2-00aa0061426a v1.0
  0d72a7d4-6148-11d1-b4aa-00c04fb66ea0 v1.0
  4b324fc8-1670-01d3-1278-5a47bf6ee188 v3.0
  6bffd098-a112-3610-9833-46c3f87e345a v1.0

C:\Documents and Settings\jbm\Desktop\tools>ifids -p ncadg_ip_udp -e 1027 127.0.
0.1
Interfaces: 10
  367abb81-9844-35f1-ad32-98f038001003 v2.0
  93149ca2-973b-11d1-8c39-00c04fb984f9 v0.0
  82273fdc-e32a-18c3-3f78-827929dc23ea v0.0
  65a93890-fab9-43a3-b2a5-1e330ac28f11 v2.0
  8d9f4e40-a03d-11ce-8f69-08003e30051b v1.0
  8d0ffe72-d252-11d0-bf8f-00c04fd9126b v1.0
  c9378ff1-16f7-11d0-a0b2-00aa0061426a v1.0
  0d72a7d4-6148-11d1-b4aa-00c04fb66ea0 v1.0
  4b324fc8-1670-01d3-1278-5a47bf6ee188 v3.0
  6bffd098-a112-3610-9833-46c3f87e345a v1.0
```

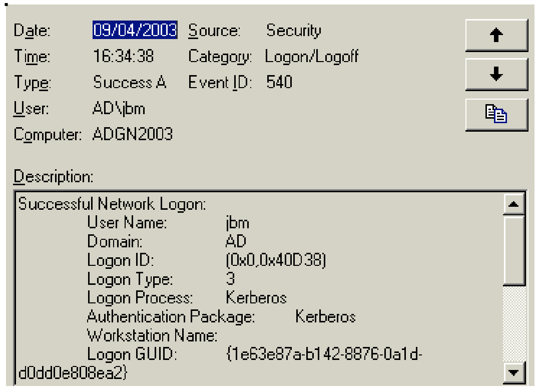
Network authentication

- SMB sessions are typically authenticated
    - Network authentication protocols
        - NTLM
        - Kerberos
    - A **network logon session** is established on the remote system
        - System threads servicing clients requests run in this logon session, with the security context of the authenticated user (impersonation token)

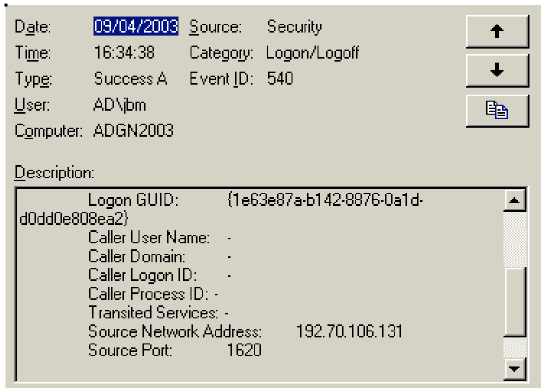
Auditing on a server

- Auditing policy
  - *Audit logon events (Success/Failure)*
  - Security events
    - Logon events
      - Windows NT: 528 (Successful Logon)
        - Logon Type == 3 (network logon session)
      - Windows 2K>: 540 (Successful Network Logon)
      - Interesting fields
        - User Name, Domain, Logon Type (3), Authentication Package, Workstation Name (NetBIOS name), Source Network Address (Windows Server 2003)

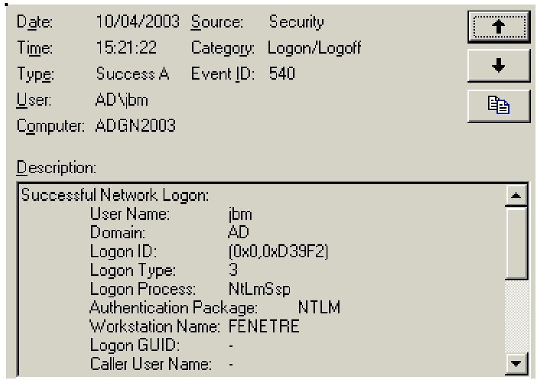
Security event 540



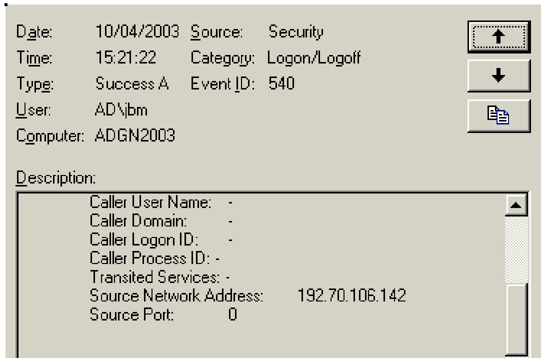
```
Date:     09/04/2003  Source:    Security
Time:     16:34:38    Category:  Logon/Logoff
Type:     Success A   Event ID:  540
User:     AD\jbm
Computer: ADGN2003

Description:
Successful Network Logon:
         User Name:          jbm
         Domain:             AD
         Logon ID:           (0x0,0x40D38)
         Logon Type:         3
         Logon Process:      Kerberos
         Authentication Package:       Kerberos
         Workstation Name:
         Logon GUID:         {1e63e87a-b142-8876-0a1d-
d0dd0e808ea2}
```



```
Date:     09/04/2003  Source:    Security
Time:     16:34:38    Category:  Logon/Logoff
Type:     Success A   Event ID:  540
User:     AD\jbm
Computer: ADGN2003

Description:
         Logon GUID:         {1e63e87a-b142-8876-0a1d-
d0dd0e808ea2}
         Caller User Name:   -
         Caller Domain:      -
         Caller Logon ID:    -
         Caller Process ID: -
         Transited Services: -
         Source Network Address:    192.70.106.131
         Source Port:         1620
```



```
Date:     10/04/2003  Source:    Security
Time:     15:21:22    Category:  Logon/Logoff
Type:     Success A   Event ID:  540
User:     AD\jbm
Computer: ADGN2003

Description:
Successful Network Logon:
         User Name:          jbm
         Domain:             AD
         Logon ID:           (0x0,0xD39F2)
         Logon Type:         3
         Logon Process:      NtLmSsp
         Authentication Package:       NTLM
         Workstation Name:  FENETRE
         Logon GUID:         -
         Caller User Name:   -
```



```
Date:     10/04/2003  Source:    Security
Time:     15:21:22    Category:  Logon/Logoff
Type:     Success A   Event ID:  540
User:     AD\jbm
Computer: ADGN2003

Description:
         Caller User Name:   -
         Caller Domain:      -
         Caller Logon ID:    -
         Caller Process ID: -
         Transited Services: -
         Source Network Address:    192.70.106.142
         Source Port:         0
```

Auditing on a domain controller

- Auditing policy:
  - *Audit account logon: Success/Failure*
  - Security events for domain authentications
    - Kerberos: 672-677
      - Successes: 672 (Authentication Ticket Granted), 673 (Service Ticket Granted), 674 (Ticket Granted Renewed)
      - Failures: 675 (Pre-authentication failed), 676 (Authentication Ticket Request Failed), 677 (Service Ticket Request Failed)
    - NTLM: 680 (Success), 681 (Failure)

Kerberos administration

- Kerberos logging
  - *Audit account logon* auditing category
    - Ticket granting and service tickets requests logging
      - Event 672-677 (security log)
  - Service tickets usage logging
    - MSKB #262177 (system log)
- Kerberos tools
  - Tickets management: klist, kerbtray, TktView

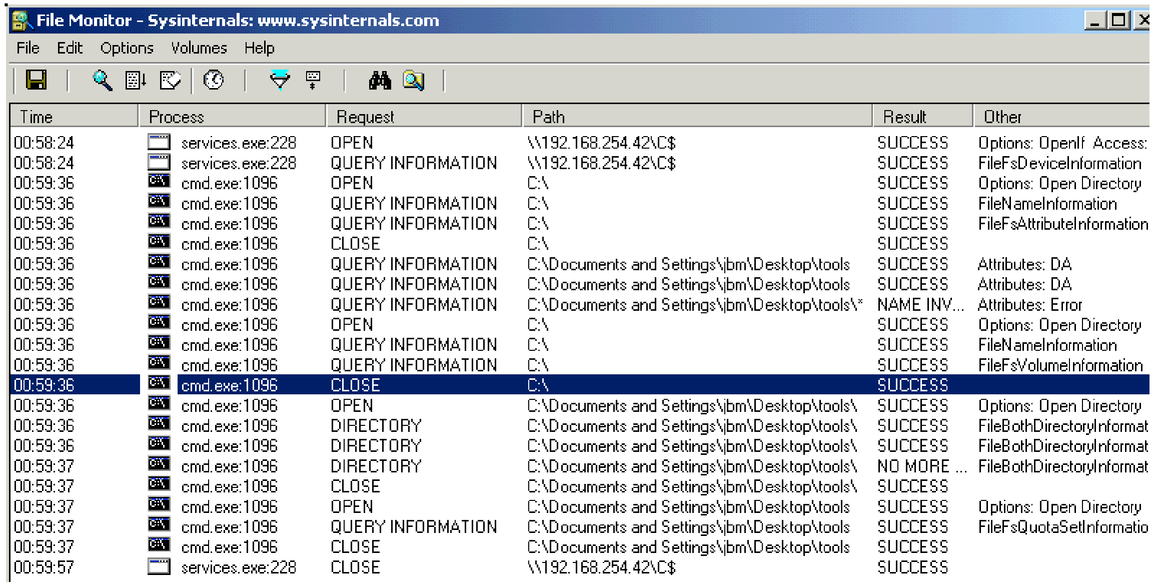
Sysinternals tools

- http://www.sysinternals.com/
  - Reference tools for advanced system administration and internals digging
  - Maintained by Mark Russinovitch (*Inside Windows 2000* author), Windows NT internals expert
  - Tools
    - Monitoring tools: Filemon, Regmon, Tokenmon, TDImon...
    - Administration tools: Process Explorer, Pstools, TCPView...

Monitoring file systems with Filemon

- Filemon
  - Can monitor all Windows file systems accesses (NTFS, NPFS (named pipes), MSFS (mailslots))
  - Can be used to debug many file systems related problems
    - Ex: permissions problems
  - Can monitor local redirector accesses

Filemon: example



Time	Process	Request	Path	Result	Other
00:58:24	services.exe:228	OPEN	\\192.168.254.42\C$	SUCCESS	Options: OpenIf Access:
00:58:24	services.exe:228	QUERY INFORMATION	\\192.168.254.42\C$	SUCCESS	FileFsDeviceInformation
00:59:36	cmd.exe:1096	OPEN	C:\	SUCCESS	Options: Open Directory
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\	SUCCESS	FileNameInformation
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\	SUCCESS	FileFsAttributeInformation
00:59:36	cmd.exe:1096	CLOSE	C:\	SUCCESS	
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\Documents and Settings\jbm\Desktop\tools	SUCCESS	Attributes: DA
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\Documents and Settings\jbm\Desktop\tools	SUCCESS	Attributes: DA
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\Documents and Settings\jbm\Desktop\tools\*	NAME INV...	Attributes: Error
00:59:36	cmd.exe:1096	OPEN	C:\	SUCCESS	Options: Open Directory
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\	SUCCESS	FileNameInformation
00:59:36	cmd.exe:1096	QUERY INFORMATION	C:\	SUCCESS	FileFsVolumeInformation
00:59:36	cmd.exe:1096	CLOSE	C:\	SUCCESS	
00:59:36	cmd.exe:1096	OPEN	C:\Documents and Settings\jbm\Desktop\tools\	SUCCESS	Options: Open Directory
00:59:36	cmd.exe:1096	DIRECTORY	C:\Documents and Settings\jbm\Desktop\tools\	SUCCESS	FileBothDirectoryInformat
00:59:36	cmd.exe:1096	DIRECTORY	C:\Documents and Settings\jbm\Desktop\tools\	SUCCESS	FileBothDirectoryInformat
00:59:37	cmd.exe:1096	DIRECTORY	C:\Documents and Settings\jbm\Desktop\tools\	NO MORE ...	FileBothDirectoryInformat
00:59:37	cmd.exe:1096	CLOSE	C:\Documents and Settings\jbm\Desktop\tools\	SUCCESS	
00:59:37	cmd.exe:1096	OPEN	C:\Documents and Settings\jbm\Desktop\tools	SUCCESS	Options: Open Directory
00:59:37	cmd.exe:1096	QUERY INFORMATION	C:\Documents and Settings\jbm\Desktop\tools	SUCCESS	FileFsQuotaSetInformatio
00:59:37	cmd.exe:1096	CLOSE	C:\Documents and Settings\jbm\Desktop\tools	SUCCESS	
00:59:57	services.exe:228	CLOSE	\\192.168.254.42\C$	SUCCESS	

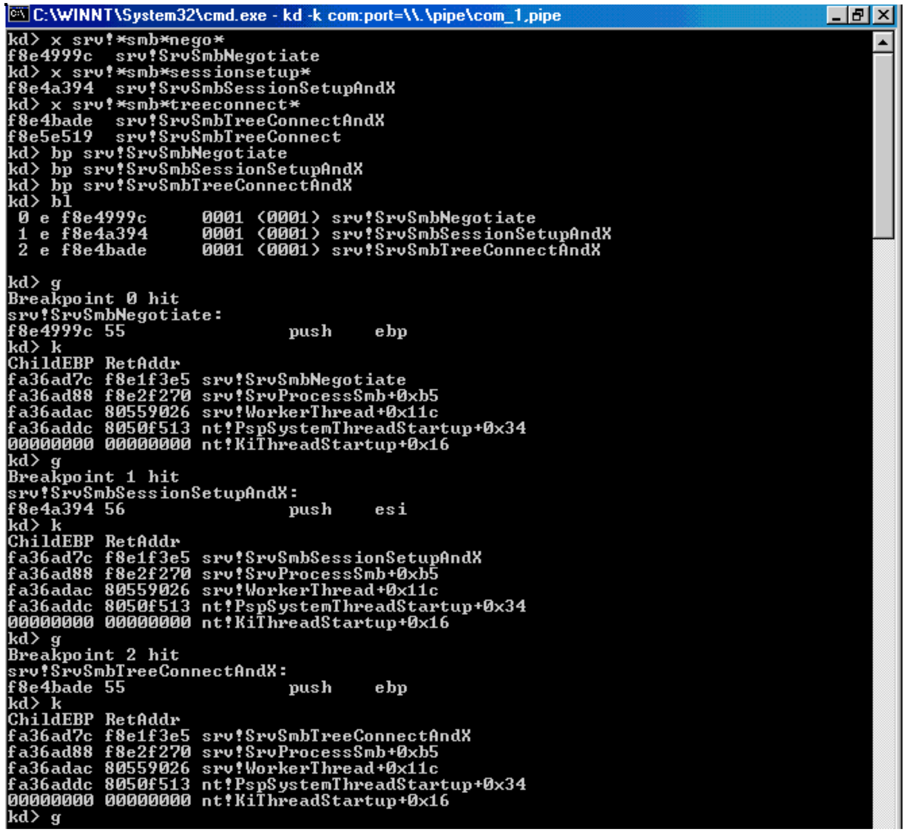
Monitoring registry accesses with Regmon

- Regmon
  - Can log all registry accesses at system boot
  - Can also be used to discover undocumented registry values
    - Ex: starting a driver or service with *net start* while regmon is running
    - Sometimes, the (driver or service) *Parameters* key must be manually created, to see queries for undocumented values

kd (kernel debugger)

- kd (Microsoft Debugging tools)
  - Some useful commands
    - Examining foo.sys driver symbols: kd> x foo!*
    - Setting a breakpoint for bar() function: kd> bp foo!bar
    - Resuming execution: kd> g
    - Displaying stack backtrace: kd> k
    - Executing a single instruction: kd> t *or* kd> p

srv.sys: SMB implementation



C:\WINNT\System32\cmd.exe - kd -k com:port=\\.\pipe\com_1,pipe

```
kd> x srv!*smb*nego*
f8e4999c  srv!SrvSmbNegotiate
kd> x srv!*smb*sessionsetup*
f8e4a394  srv!SrvSmbSessionSetupAndX
kd> x srv!*smb*treeconnect*
f8e4bade  srv!SrvSmbTreeConnectAndX
f8e5e519  srv!SrvSmbTreeConnect
kd> bp srv!SrvSmbNegotiate
kd> bp srv!SrvSmbSessionSetupAndX
kd> bp srv!SrvSmbTreeConnectAndX
kd> bl
 0 e f8e4999c     0001 (0001) srv!SrvSmbNegotiate
 1 e f8e4a394     0001 (0001) srv!SrvSmbSessionSetupAndX
 2 e f8e4bade     0001 (0001) srv!SrvSmbTreeConnectAndX

kd> g
Breakpoint 0 hit
srv!SrvSmbNegotiate:
f8e4999c 55               push    ebp
kd> k
ChildEBP RetAddr
fa36ad7c f8e1f3e5 srv!SrvSmbNegotiate
fa36ad88 f8e2f270 srv!SrvProcessSmb+0xb5
fa36adac 80559026 srv!WorkerThread+0x11c
fa36addc 8050f513 nt!PspSystemThreadStartup+0x34
00000000 00000000 nt!KiThreadStartup+0x16
kd> g
Breakpoint 1 hit
srv!SrvSmbSessionSetupAndX:
f8e4a394 56               push    esi
kd> k
ChildEBP RetAddr
fa36ad7c f8e1f3e5 srv!SrvSmbSessionSetupAndX
fa36ad88 f8e2f270 srv!SrvProcessSmb+0xb5
fa36adac 80559026 srv!WorkerThread+0x11c
fa36addc 8050f513 nt!PspSystemThreadStartup+0x34
00000000 00000000 nt!KiThreadStartup+0x16
kd> g
Breakpoint 2 hit
srv!SrvSmbTreeConnectAndX:
f8e4bade 55               push    ebp
kd> k
ChildEBP RetAddr
fa36ad7c f8e1f3e5 srv!SrvSmbTreeConnectAndX
fa36ad88 f8e2f270 srv!SrvProcessSmb+0xb5
fa36adac 80559026 srv!WorkerThread+0x11c
fa36addc 8050f513 nt!PspSystemThreadStartup+0x34
00000000 00000000 nt!KiThreadStartup+0x16
kd> g
```

References

- Books
  - *Inside Windows 2000*, Mark Russinovitch & David Salomon. Microsoft Press.
  - *Programming Windows Security*, Keith Brown. Addison Wesley.
  - *DCE/RPC over SMB: Samba and Windows NT Domain Internals*, Luke Kenneth Casson Leighton. MTP.
  - *Implementing CIFS,* Christopher R. Hertel. Prentice Hall (soon).
    - Available online: *http://www.ubiqx.org/cifs/*

References

- Internals tools
  - Sysinternals tools (www.sysinternals.com)
    - Filemon, Regmon, Process Explorer, PsTools, TCPView...
  - Todd Sabin's tools (razor.bindview.com)
    - RPC tools, PipeACL tools, ACL tools
  - SPIKE (Dave Aitel, www.immunitysec.com)
    - dcedump, ifids

References

- Kerberos tools
  - klist and kerbtray (http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/{klist-o,kerbtray-o}.asp)
  - TktView (http://www.develop.com/kbrown/security/samples.htm)

References

- Documentation
  - Security events
    - Audit Account Logon Events (http://www.winnetmag.com/Articles/Index.cfm?ArticleID=19677)
    - Tracking Logon and Logoff Activity in Win2K (http://www.win2000mag.com/Articles/Index.cfm?ArticleID=16430

Questions?

Thank you!