Windows network services internals

HiverCon 2003

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

Agenda

- TCP/IP stack
- SMB/CIFS
- MSRPC
- References

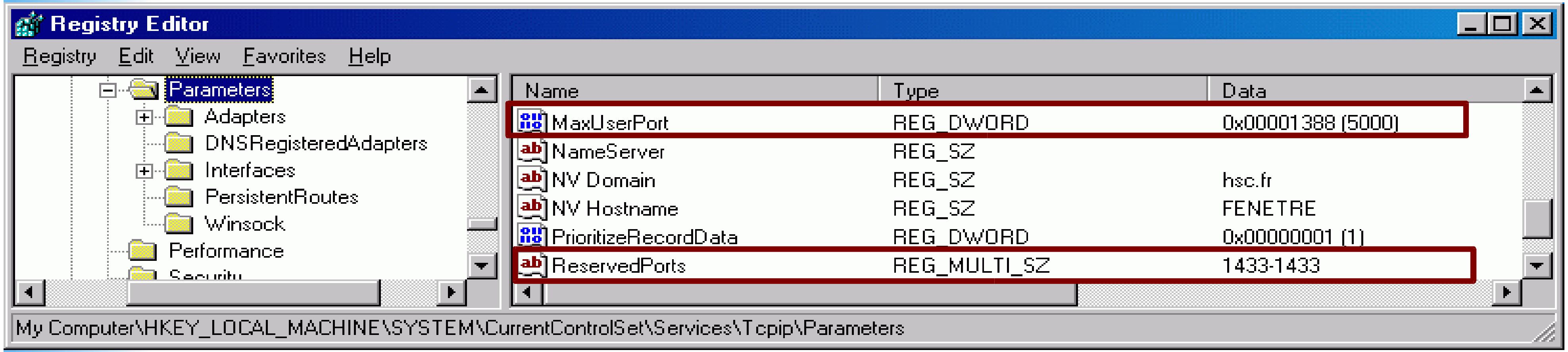
TCP/IP stack

- Ephemeral ports allocation policy
- netstat bugs
- Identifying processes behind sockets
- Lack of privileged ports
- TCP sockets hijacking

Ephemeral ports

- Ephemeral ports
  - Typically used for TCP or UDP clients
    - Also used for RPC services running on TCP or UDP (hence the portmapper service)
  - Default range: 1025-5000
    - Highest port: MaxUserPort registry value
    - Exceptions in this range: ReservedPorts registry value
    - **Do not** appear in the registry by default

Ephemeral ports range configuration



Name	Type	Data
MaxUserPort	REG_DWORD	0x00001388 (5000)
NameServer	REG_SZ	
NV Domain	REG_SZ	hsc.fr
NV Hostname	REG_SZ	FENETRE
PrioritizeRecordData	REG_DWORD	0x00000001 (1)
ReservedPorts	REG_MULTI_SZ	1433-1433

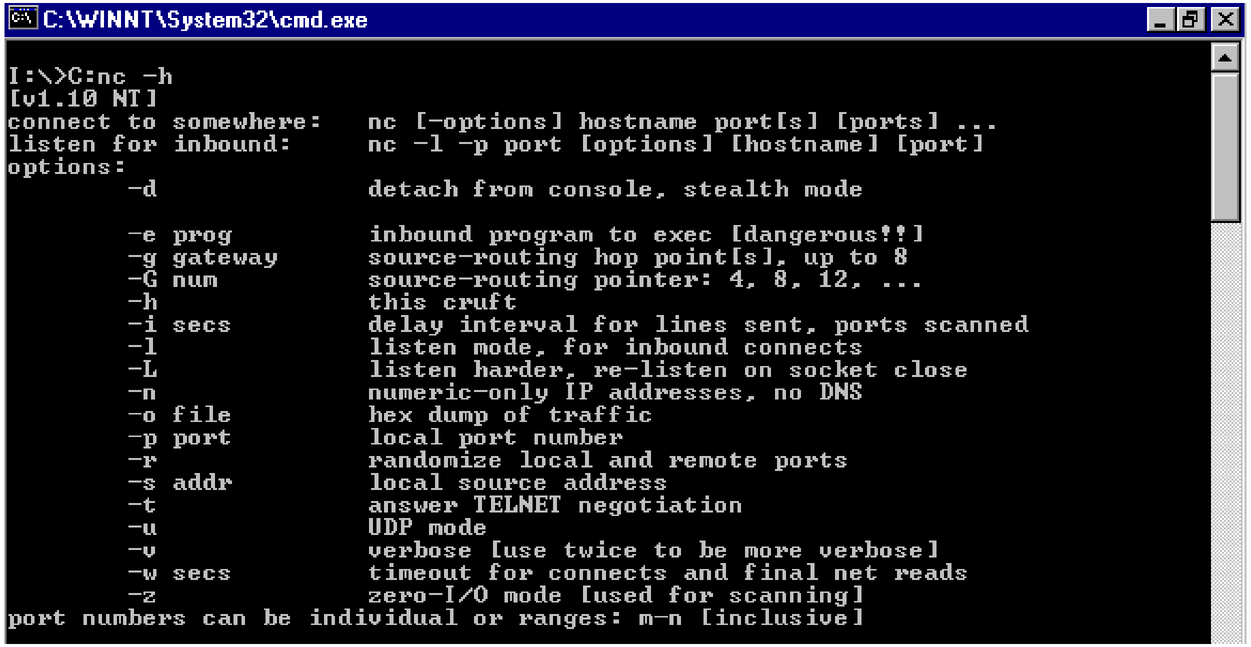
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Ephemeral ports allocation policy

- Ephemeral ports usages
  - TCP & UDP clients typically do not specify a source port, thus an ephemeral port is allocated
  - RPC services also run on dynamic ports
    - After system startup, RPC services typically use ports immediately higher than 1024 (1025, 1026, 1028, ...)
- Ephemeral ports allocation
  - Incremental, starting from 1025
  - Shared between TCP and UDP

nc.exe: TCP/UDP client or server

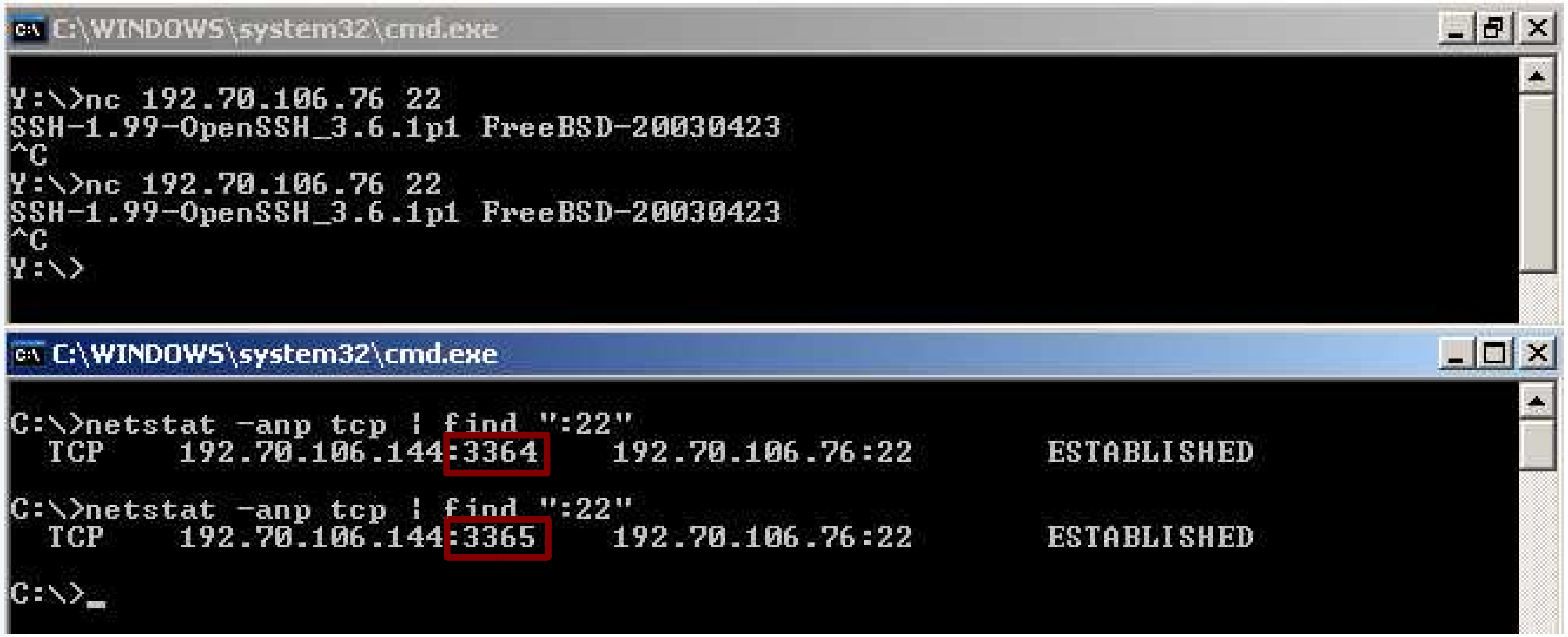
- nc.exe (netcat)
  - Windows port of the well-known nc Unix utility
    - http://www.atstake.com/research/tools/network_utilities/nc11nt.zip
  - Usages: TCP/UDP client or server



```
I:\>C:nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Ephemeral ports: TCP clients

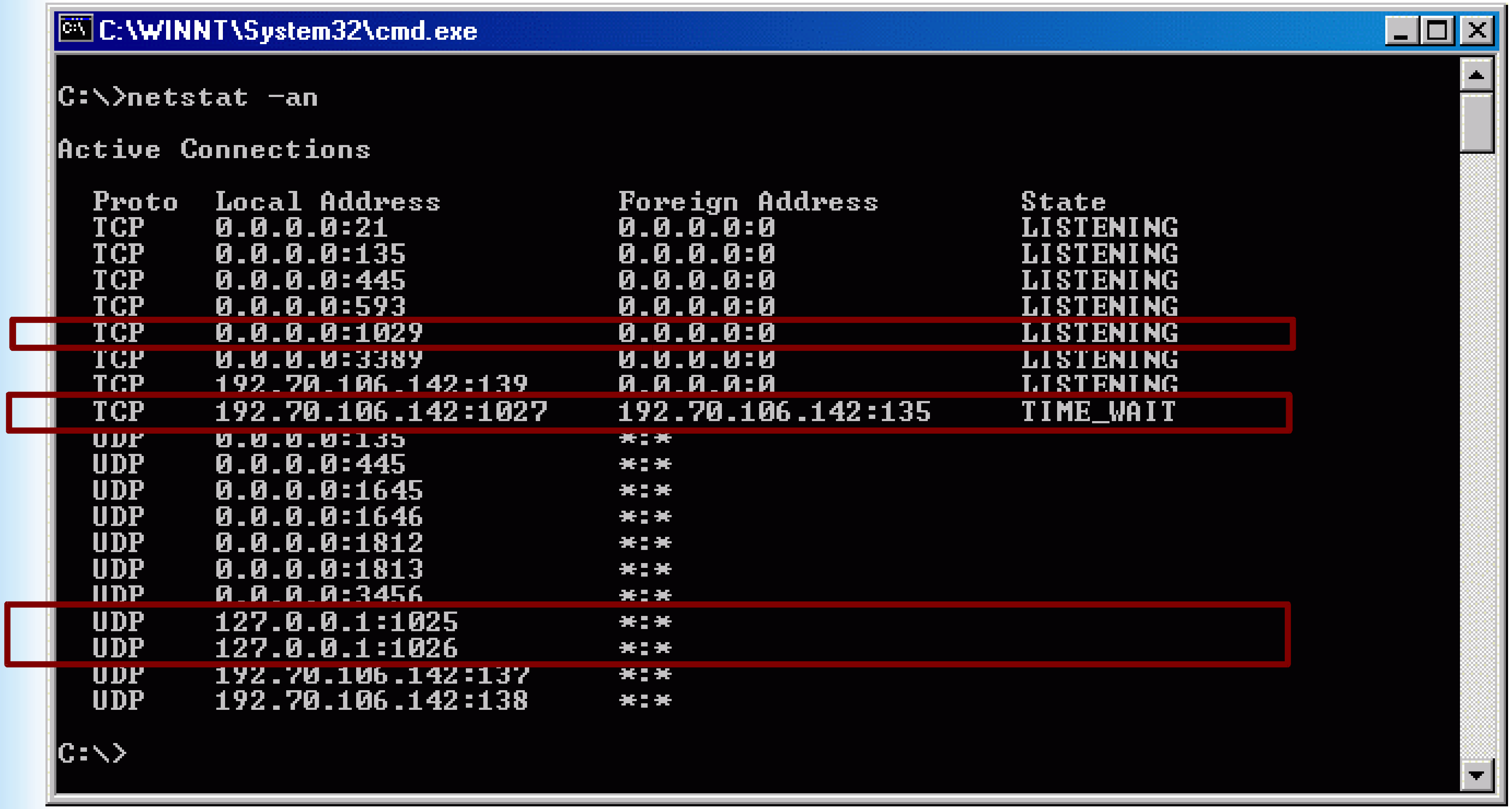
- First TCP client: source port 3364/tcp
- Second TCP client: source port 3365/tcp
- Next UDP client: 3366/udp



```
Y:\>nc 192.70.106.76 22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030423
^C
Y:\>nc 192.70.106.76 22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030423
^C
Y:\>
```

```
C:\>netstat -anp tcp | find ":22"
  TCP    192.70.106.144:3364    192.70.106.76:22       ESTABLISHED

C:\>netstat -anp tcp | find ":22"
  TCP    192.70.106.144:3365    192.70.106.76:22       ESTABLISHED

C:\>_
```

Ephemeral ports example

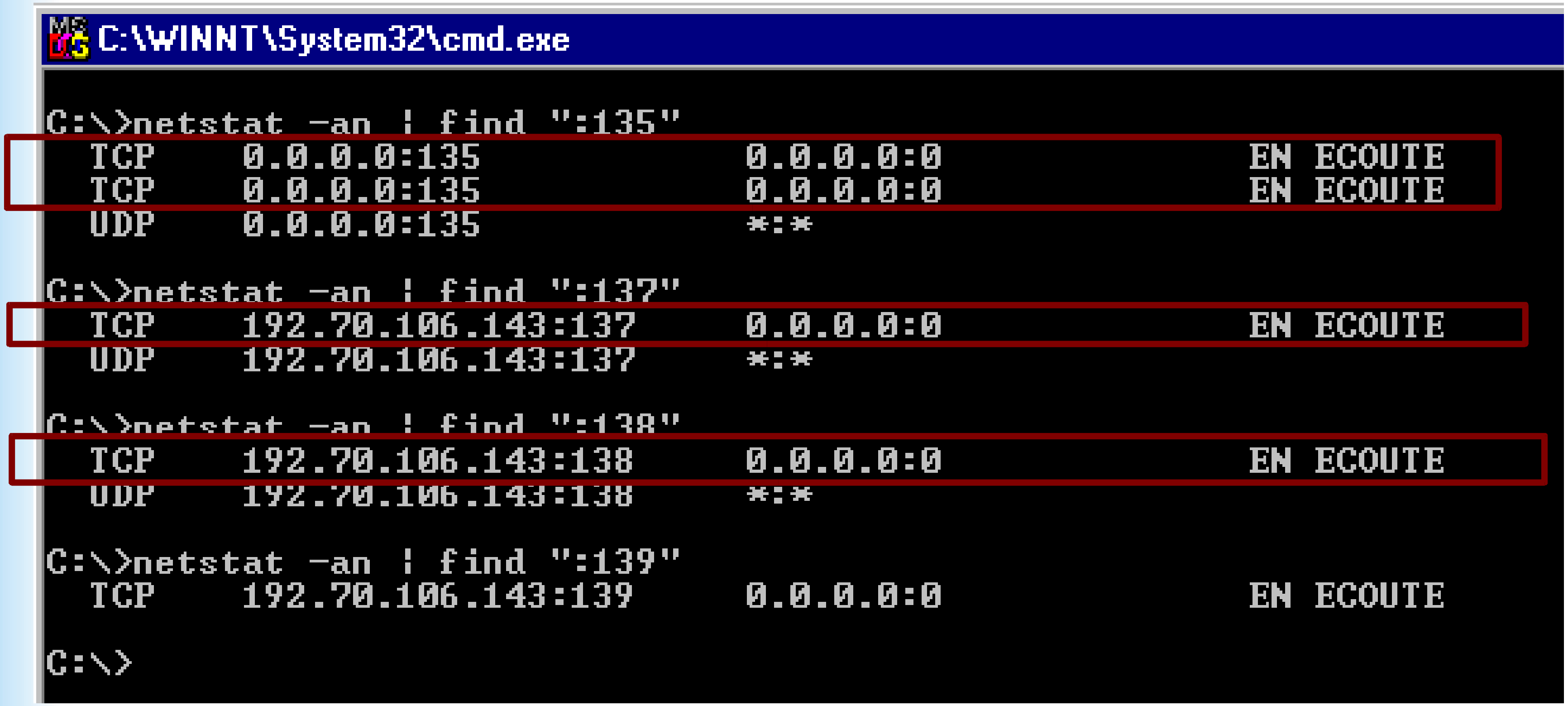


```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    192.70.106.142:139     0.0.0.0:0              LISTENING
  TCP    192.70.106.142:1027    192.70.106.142:135     TIME_WAIT
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1645           *:*
  UDP    0.0.0.0:1646           *:*
  UDP    0.0.0.0:1812           *:*
  UDP    0.0.0.0:1813           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    127.0.0.1:1025         *:*
  UDP    127.0.0.1:1026         *:*
  UDP    192.70.106.142:137     *:*
  UDP    192.70.106.142:138     *:*

C:\>
```

netstat bugs history

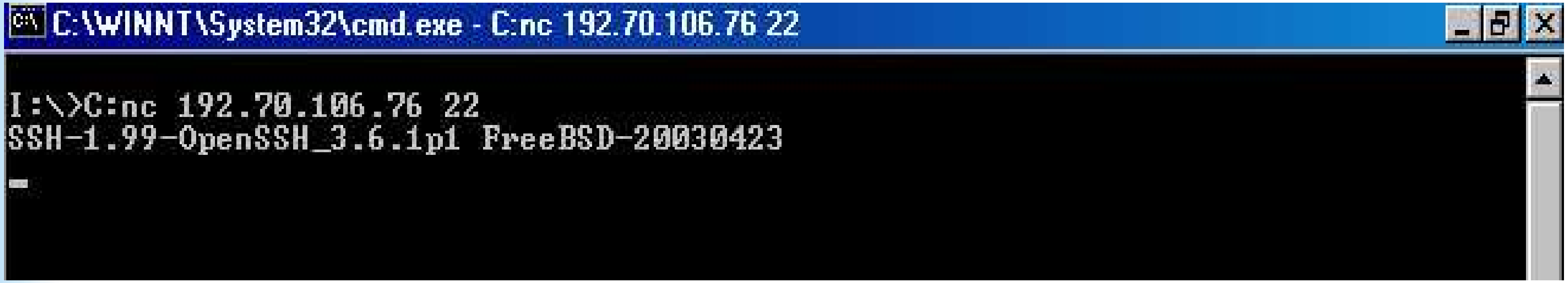
- netstat bugs
  - NT 4.0 < SP3: LISTENING sockets not displayed
    - http://support.microsoft.com/?id=131482
  - NT 4.0: for each bound UDP socket, a LISTENING TCP socket with the same port is displayed
    - http://support.microsoft.com/?id=194171
  - NT 4.0 and W2K: source ports used for outgoing TCP connections are displayed as LISTENING
  - Windows Server 2003: no known bug...

netstat bugs: UDP -> TCP (NT 4)

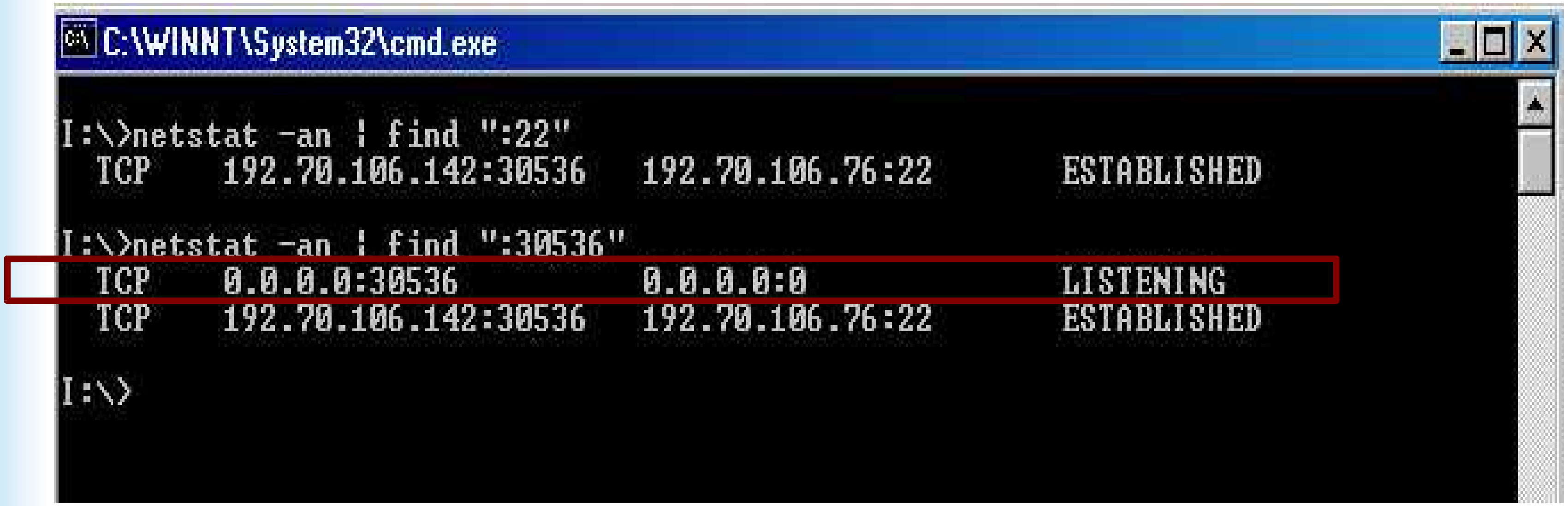


```
C:\>netstat -an | find ":135"
  TCP    0.0.0.0:135            0.0.0.0:0              EN ECOUTE
  TCP    0.0.0.0:135            0.0.0.0:0              EN ECOUTE
  UDP    0.0.0.0:135            *:*

C:\>netstat -an | find ":137"
  TCP    192.70.106.143:137     0.0.0.0:0              EN ECOUTE
  UDP    192.70.106.143:137     *:*

C:\>netstat -an | find ":138"
  TCP    192.70.106.143:138     0.0.0.0:0              EN ECOUTE
  UDP    192.70.106.143:138     *:*

C:\>netstat -an | find ":139"
  TCP    192.70.106.143:139     0.0.0.0:0              EN ECOUTE

C:\>
```

netstat bugs: LISTENING bug (W2K)

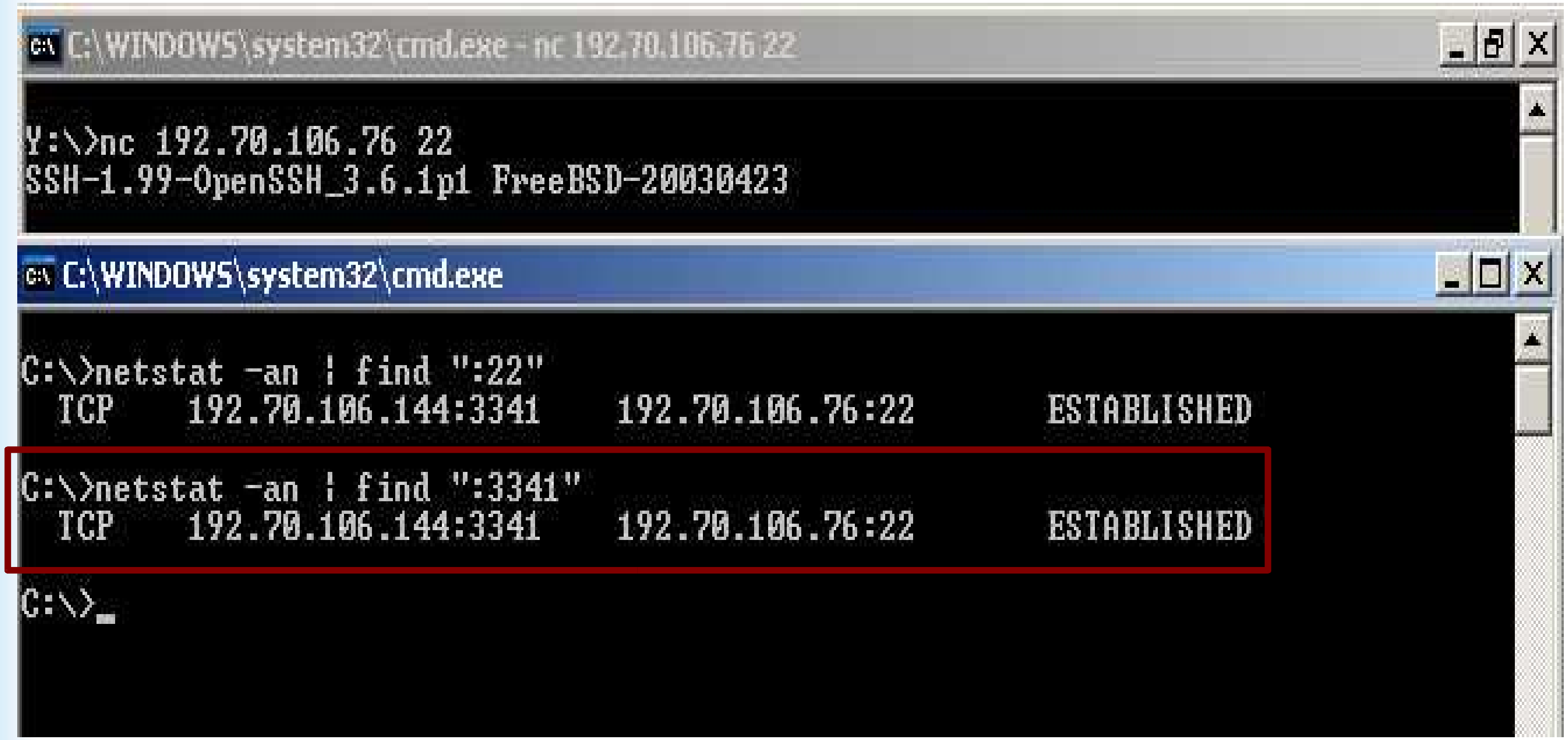


```
I:\>C:nc 192.70.106.76 22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030423
_
```



```
I:\>netstat -an | find ":22"
  TCP    192.70.106.142:30536   192.70.106.76:22       ESTABLISHED

I:\>netstat -an | find ":30536"
  TCP    0.0.0.0:30536          0.0.0.0:0              LISTENING
  TCP    192.70.106.142:30536   192.70.106.76:22       ESTABLISHED

I:\>
```

W2K3: LISTENING bug fixed



C:\WINDOWS\system32\cmd.exe - nc 192.70.106.76 22

```
Y:\>nc 192.70.106.76 22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030423
```

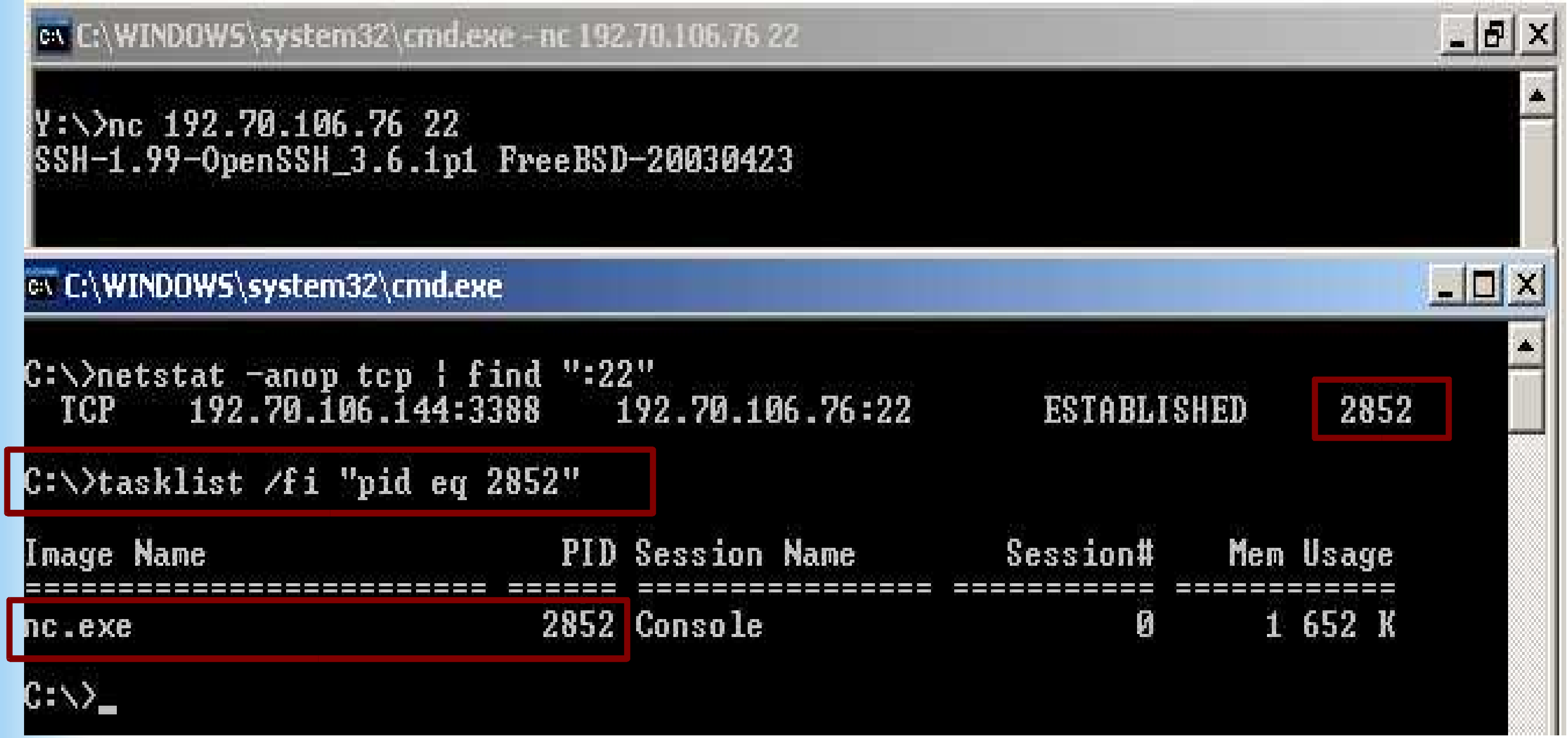
C:\WINDOWS\system32\cmd.exe

```
C:\>netstat -an ¦ find ":22"
  TCP    192.70.106.144:3341    192.70.106.76:22       ESTABLISHED

C:\>netstat -an ¦ find ":3341"
  TCP    192.70.106.144:3341    192.70.106.76:22       ESTABLISHED

C:\>_
```

Identifying processes behind sockets

- Identifying processes behind sockets is a common administration task
- Before WXP, not possible without third-party tools
  - netstat -o option (XP and W2K3) + tasklist command (XP and W2K3)
    - http://support.microsoft.com/?id=281336
  - Third-party tools
    - TCPview (sysinternals)
      - http://www.sysinternals.com/ntw2k/source/tcpview.shtml
    - fport (Foundstone)
      - http://www.foundstone.com/knowledge/proddesc/fport.html

netstat -o option: XP, W2K3

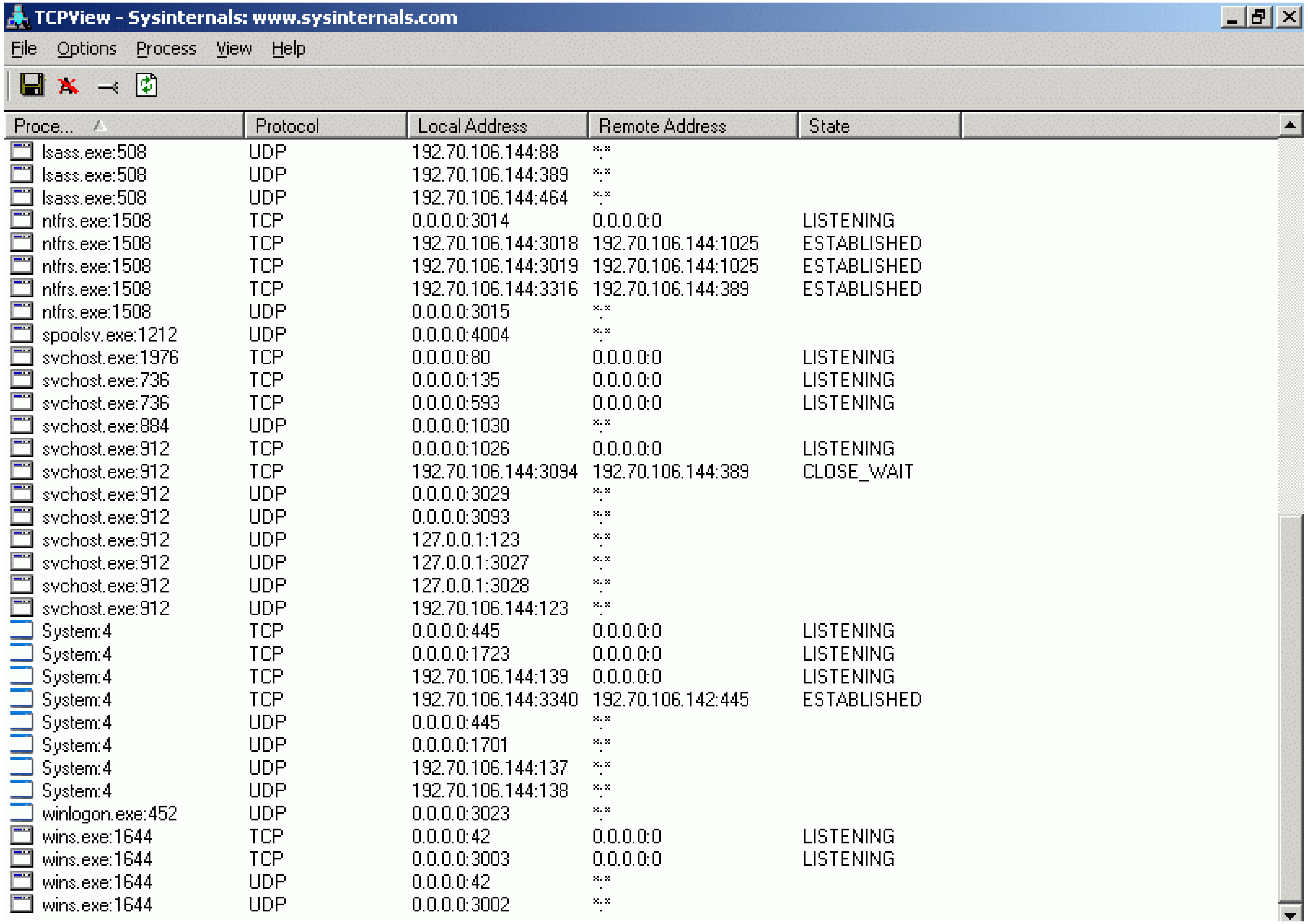

C:\WINDOWS\system32\cmd.exe - nc 192.70.106.76 22

```
Y:\>nc 192.70.106.76 22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030423
```

C:\WINDOWS\system32\cmd.exe

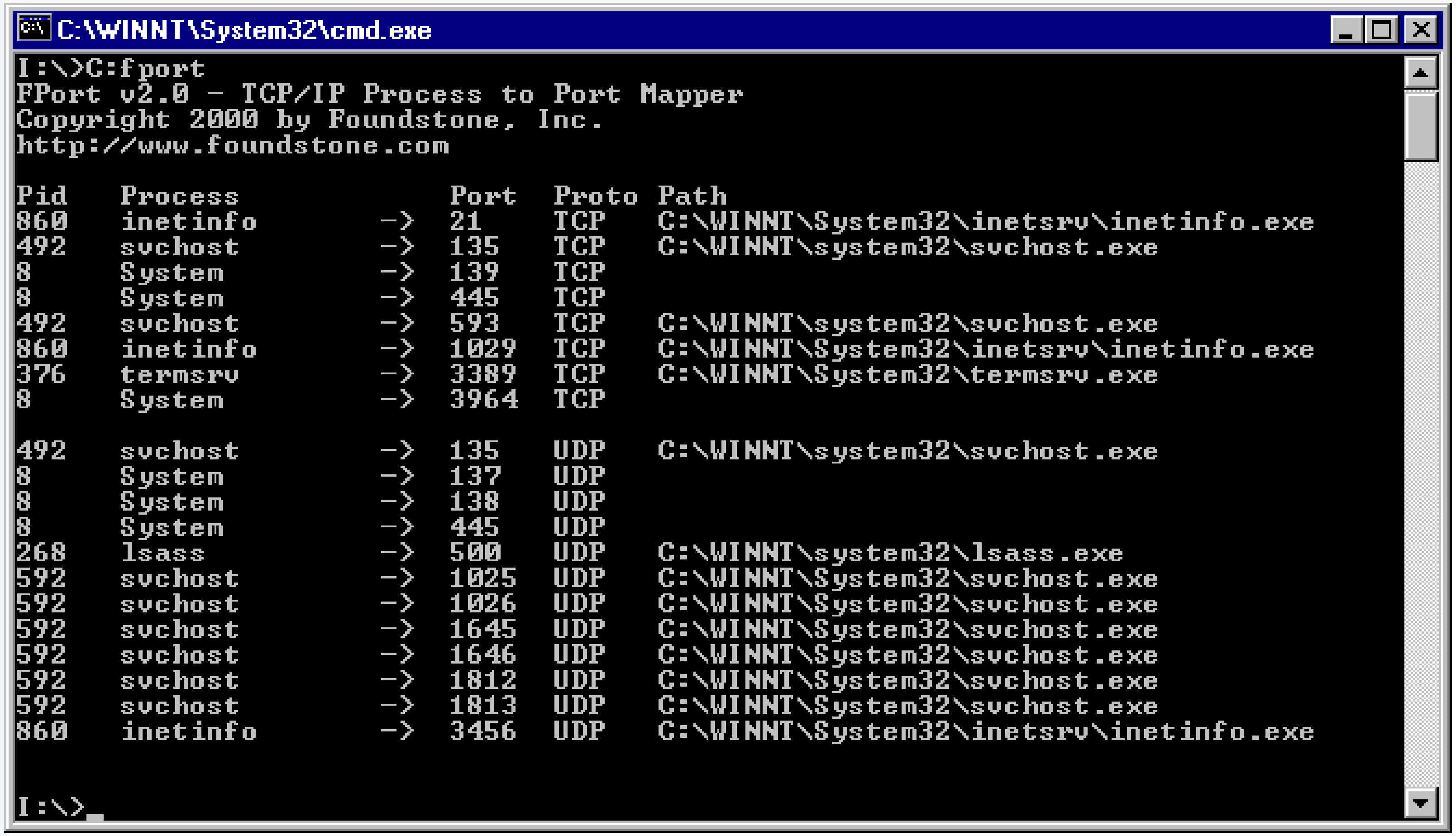
```
C:\>netstat -anop tcp | find ":22"
  TCP    192.70.106.144:3388    192.70.106.76:22       ESTABLISHED     2852

C:\>tasklist /fi "pid eq 2852"

Image Name                   PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
nc.exe                      2852 Console                 0      1 652 K

C:\>_
```

TCPView


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

Proce...	Protocol	Local Address	Remote Address	State
lsass.exe:508	UDP	192.70.106.144:88	*:*	
lsass.exe:508	UDP	192.70.106.144:389	*:*	
lsass.exe:508	UDP	192.70.106.144:464	*:*	
ntfrs.exe:1508	TCP	0.0.0.0:3014	0.0.0.0:0	LISTENING
ntfrs.exe:1508	TCP	192.70.106.144:3018	192.70.106.144:1025	ESTABLISHED
ntfrs.exe:1508	TCP	192.70.106.144:3019	192.70.106.144:1025	ESTABLISHED
ntfrs.exe:1508	TCP	192.70.106.144:3316	192.70.106.144:389	ESTABLISHED
ntfrs.exe:1508	UDP	0.0.0.0:3015	*:*	
spoolsv.exe:1212	UDP	0.0.0.0:4004	*:*	
svchost.exe:1976	TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
svchost.exe:736	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
svchost.exe:736	TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
svchost.exe:884	UDP	0.0.0.0:1030	*:*	
svchost.exe:912	TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
svchost.exe:912	TCP	192.70.106.144:3094	192.70.106.144:389	CLOSE_WAIT
svchost.exe:912	UDP	0.0.0.0:3029	*:*	
svchost.exe:912	UDP	0.0.0.0:3093	*:*	
svchost.exe:912	UDP	127.0.0.1:123	*:*	
svchost.exe:912	UDP	127.0.0.1:3027	*:*	
svchost.exe:912	UDP	127.0.0.1:3028	*:*	
svchost.exe:912	UDP	192.70.106.144:123	*:*	
System:4	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
System:4	TCP	0.0.0.0:1723	0.0.0.0:0	LISTENING
System:4	TCP	192.70.106.144:139	0.0.0.0:0	LISTENING
System:4	TCP	192.70.106.144:3340	192.70.106.142:445	ESTABLISHED
System:4	UDP	0.0.0.0:445	*:*	
System:4	UDP	0.0.0.0:1701	*:*	
System:4	UDP	192.70.106.144:137	*:*	
System:4	UDP	192.70.106.144:138	*:*	
winlogon.exe:452	UDP	0.0.0.0:3023	*:*	
wins.exe:1644	TCP	0.0.0.0:42	0.0.0.0:0	LISTENING
wins.exe:1644	TCP	0.0.0.0:3003	0.0.0.0:0	LISTENING
wins.exe:1644	UDP	0.0.0.0:42	*:*	
wins.exe:1644	UDP	0.0.0.0:3002	*:*	

Fport



```
I:\>C:fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
860   inetinfo       ->  21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
492   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
492   svchost        ->  593   TCP   C:\WINNT\system32\svchost.exe
860   inetinfo       ->  1029  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
376   termsrv        ->  3389  TCP   C:\WINNT\System32\termsrv.exe
8     System         ->  3964  TCP

492   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
268   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
592   svchost        ->  1025  UDP   C:\WINNT\System32\svchost.exe
592   svchost        ->  1026  UDP   C:\WINNT\System32\svchost.exe
592   svchost        ->  1645  UDP   C:\WINNT\System32\svchost.exe
592   svchost        ->  1646  UDP   C:\WINNT\System32\svchost.exe
592   svchost        ->  1812  UDP   C:\WINNT\System32\svchost.exe
592   svchost        ->  1813  UDP   C:\WINNT\System32\svchost.exe
860   inetinfo       ->  3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe


I:\>_
```

Lack of privileged ports

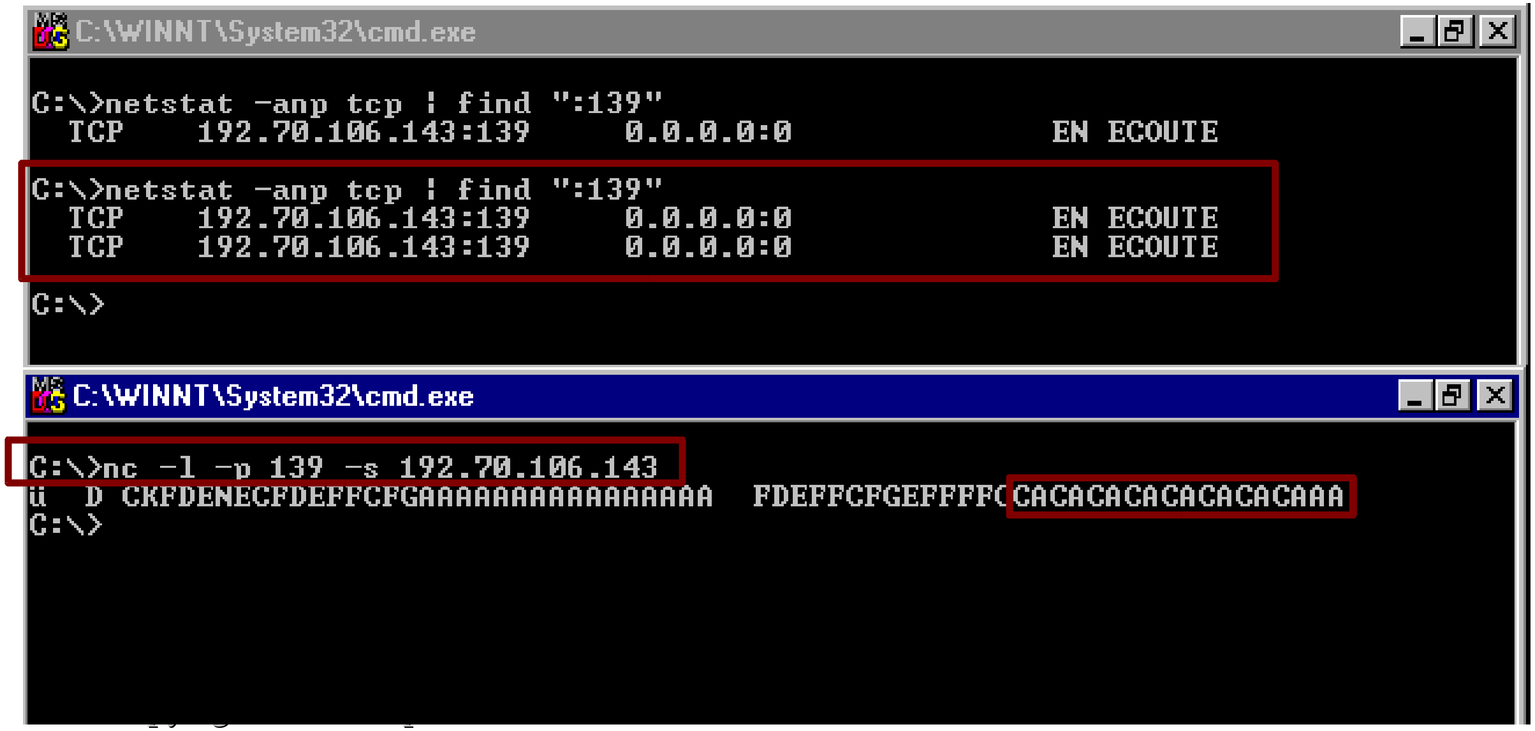
- Privileged ports
  - Used to restrict ports < 1024,typically used by TCP servers, to system administrators
    - Examples: 25/tcp (SMTP), 80/tcp (HTTP), 2049/tcp (NFS, exception)
  - Windows TCP/IP stack: no privileged ports
    - Any user can bind a TCP server to any port
    - Can be used to disrupt running services

TCP server hijacking

- TCP server hijacking
  - Became widely known with the release of a Windows port of the netcat utility
      - http://www.insecure.org/sploits/NT.port-binding-vulnerability.html
  - Technical reasons:
    - Lack of privileged ports
    - SO_REUSEADDR socket option
  - Well-known example
    - NT4 SMB server hijacking
    - NetBT (NetBIOS over TCP/IP) session port (139/tcp)

NT4: SMB server hijacking

- SMB server hijacking
  - nc listener, bound to exactly the same port and address as the SMB server
  - Last server (nc) receives incoming TCP connections!



```
C:\>netstat -anp tcp | find ":139"
  TCP    192.70.106.143:139     0.0.0.0:0              EN ECOUTE

C:\>netstat -anp tcp | find ":139"
  TCP    192.70.106.143:139     0.0.0.0:0              EN ECOUTE
  TCP    192.70.106.143:139     0.0.0.0:0              EN ECOUTE

C:\>
```

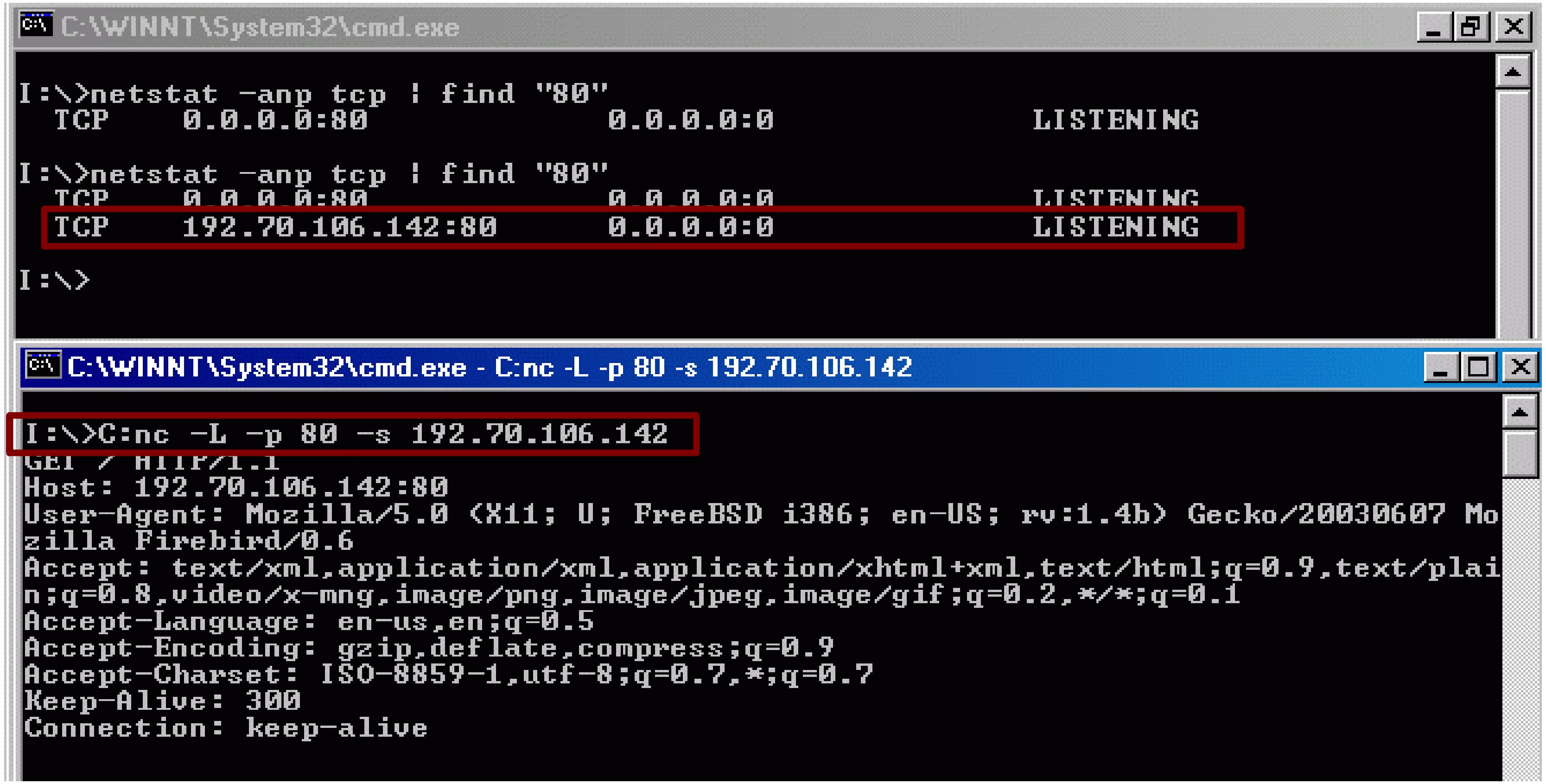
```
C:\>nc -l -p 139 -s 192.70.106.143
ü  D CKFDENECFDEFFCFGAAAAAAAAAAAAAAAA  FDEFFCFGEFFFFFCCACACACACACACAAA
C:\>
```

IIS5 hijacking

- IIS5 HTTP service
  - Bound by default to 0.0.0.0:80
  - Lack of privileged ports
    - A second TCP server can be bound to 80/tcp
    - Using a specific IPv4 address (with SO_REUSEADDR)
  - TCP connections to the specific IPv4 address
    - Received by the second TCP server
    - Not IIS5!

IIS5 hijacking: example

- nc listener receives HTTP requests, hijacking IIS5 HTTP service


C:\WINNT\System32\cmd.exe
C:\WINNT\System32\cmd.exe - C:nc -L -p 80 -s 192.70.106.142

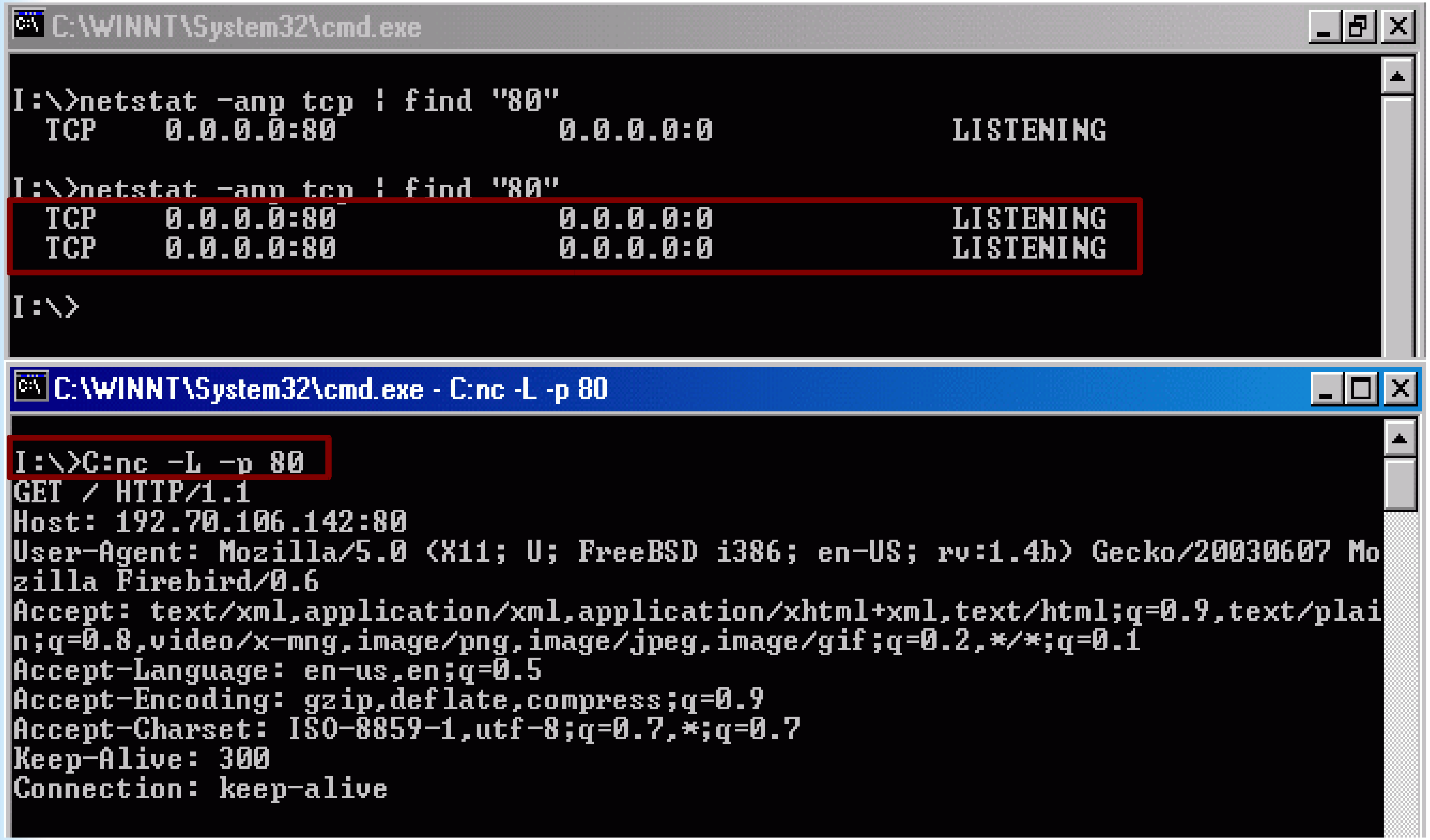
```
I:\>netstat -anp tcp | find "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING

I:\>netstat -anp tcp | find "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    192.70.106.142:80      0.0.0.0:0              LISTENING

I:\>
```

```
I:\>C:nc -L -p 80 -s 192.70.106.142
GET / HTTP/1.1
Host: 192.70.106.142:80
User-Agent: Mozilla/5.0 (X11; U; FreeBSD i386; en-US; rv:1.4b) Gecko/20030607 Mo
zilla Firebird/0.6
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plai
n;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate,compress;q=0.9
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

TCP duplicate bindings

- Duplicate bindings
  - Two TCP servers bound to exactly the same local address (IPv4 address, TCP port)
    - Ex: 0.0.0.0:80 and 0.0.0.0:80, x.y.z.t:42 and x.y.z.t:42
    - Usually not supported by TCP/IP implementations
    - Supported by Windows...
      - Question: which TCP server receives TCP connections?
      - Last server in NT 4.0
      - Random server in W2K
        - http://support.microsoft.com/?id=307175

IIS5 duplicate bindings


C:\WINNT\System32\cmd.exe

```
I:\>netstat -anp tcp | find "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING

I:\>netstat -anp tcp | find "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING

I:\>
```

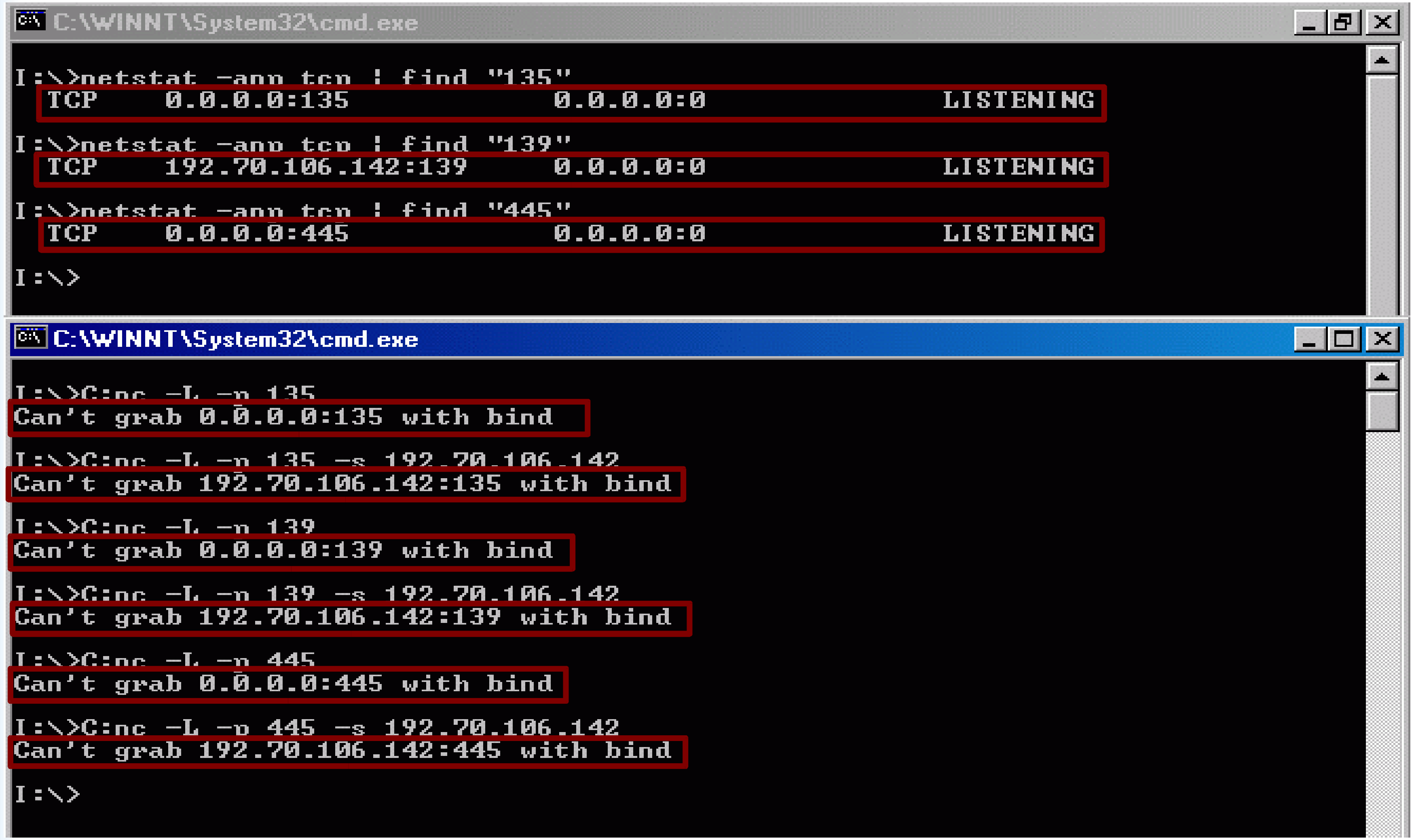
C:\WINNT\System32\cmd.exe - C:nc -L -p 80

```
I:\>C:nc -L -p 80
GET / HTTP/1.1
Host: 192.70.106.142:80
User-Agent: Mozilla/5.0 (X11; U; FreeBSD i386; en-US; rv:1.4b) Gecko/20030607 Mo
zilla Firebird/0.6
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plai
n;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate,compress;q=0.9
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

Avoiding TCP server hijacking

- SO_EXCLUSIVEADDRUSE socket option
  - Introduced in Windows NT 4.0 SP4
    - " The SO_EXCLUSIVEADDRUSE option prevents other sockets from being forcibly bound to the same address and port, a practice enabled by the SO_REUSEADDR option; such reuse can be executed by malicious applications to disrupt the application "
    - Not used by all Microsoft products...
      - Example: IIS 5, as seen before
      - In W2K
        - Used by RPC services listening on TCP/IP or UDP/IP
        - Used by SQL Server (1433/tcp)
        - Used by NetBT driver (137/udp, 138/udp, 139/tcp, 445/tcp)

SO_EXCLUSIVEADDRUSE: W2K

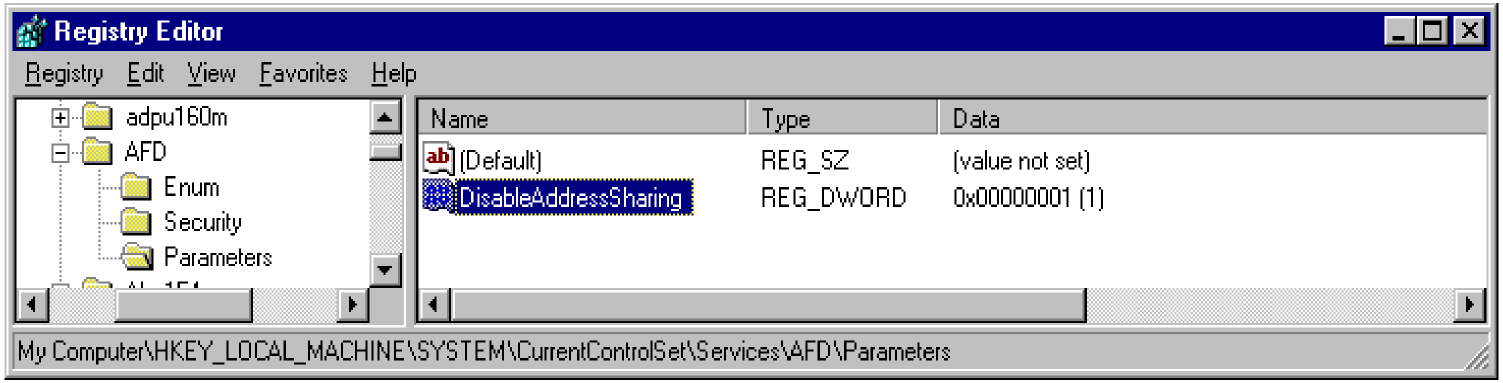


```
I:\>netstat -anp tcp | find "135"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING

I:\>netstat -anp tcp | find "139"
  TCP    192.70.106.142:139     0.0.0.0:0              LISTENING

I:\>netstat -anp tcp | find "445"
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING

I:\>
```

```
I:\>C:nc -L -p 135
Can't grab 0.0.0.0:135 with bind

I:\>C:nc -L -p 135 -s 192.70.106.142
Can't grab 192.70.106.142:135 with bind

I:\>C:nc -L -p 139
Can't grab 0.0.0.0:139 with bind

I:\>C:nc -L -p 139 -s 192.70.106.142
Can't grab 192.70.106.142:139 with bind

I:\>C:nc -L -p 445
Can't grab 0.0.0.0:445 with bind

I:\>C:nc -L -p 445 -s 192.70.106.142
Can't grab 192.70.106.142:445 with bind

I:\>
```

SO_EXCLUSIVEADDRUSE: afd driver

- Winsock API
  - Implemented by the Afd driver
    - Creates TDI file objects to represent TCP or UDP sockets
    - SO_EXCLUSIVEADDRUSE socket option
      - Corresponds to a NULL value for the ShareAccess parameter of the ZwCreateFile() function used to create TDI file objects
    - DisableAddressSharing registry value: global protection, when set to 1



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableAddressSharing	REG_DWORD	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters

SMB/CIFS

- SMB/CIFS introduction
- SMB transport
- SMB implementation
- SMB administration
- SMB as transport protocol: DCE RPC over SMB

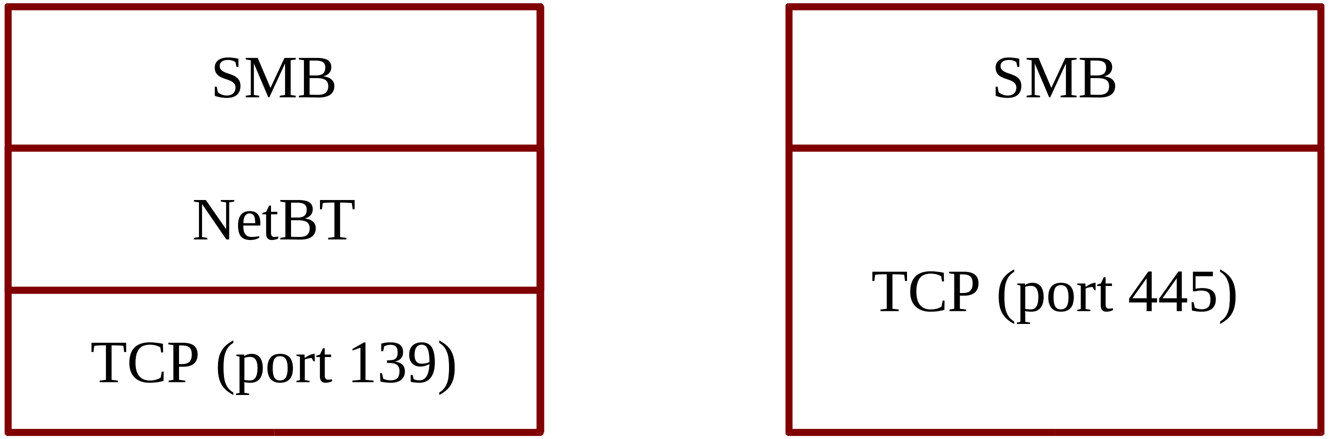
SMB/CIFS: introduction

- SMB/CIFS
  - SMB: Server Message Block protocol
    - Network protocol behind Windows networking
      - Ressources sharing (files and printer)
    - Renamed by MS to CIFS around 1996/1997
      - Common Internet File System
    - Frequently confused with NetBT (NetBIOS over TCP/IP)
      - NetBT is only a transport protocol for SMB/CIFS
    - Proprietary protocol, mostly documented by the work of the Samba team (open-source SMB/CIFS implementation)
      - Reference documentation: Implementing CIFS, written by Christopher R. Hertel
        - http://www.ubiqx.org/cifs/

SMB transport

- SMB transport
  - Before W2K: SMB typically carried into NetBT
    - NetBIOS over TCP/IP:139/tcp
  - W2K >: SMB can be carried directly into TCP
    - NetBT layer removed
      - nbss pseudo-header maintained for backward compatibility
    - Raw SMB transport: 445/tcp

SMB transport: NT 4 vs W2K



SMB

NetBT

TCP (port 139)

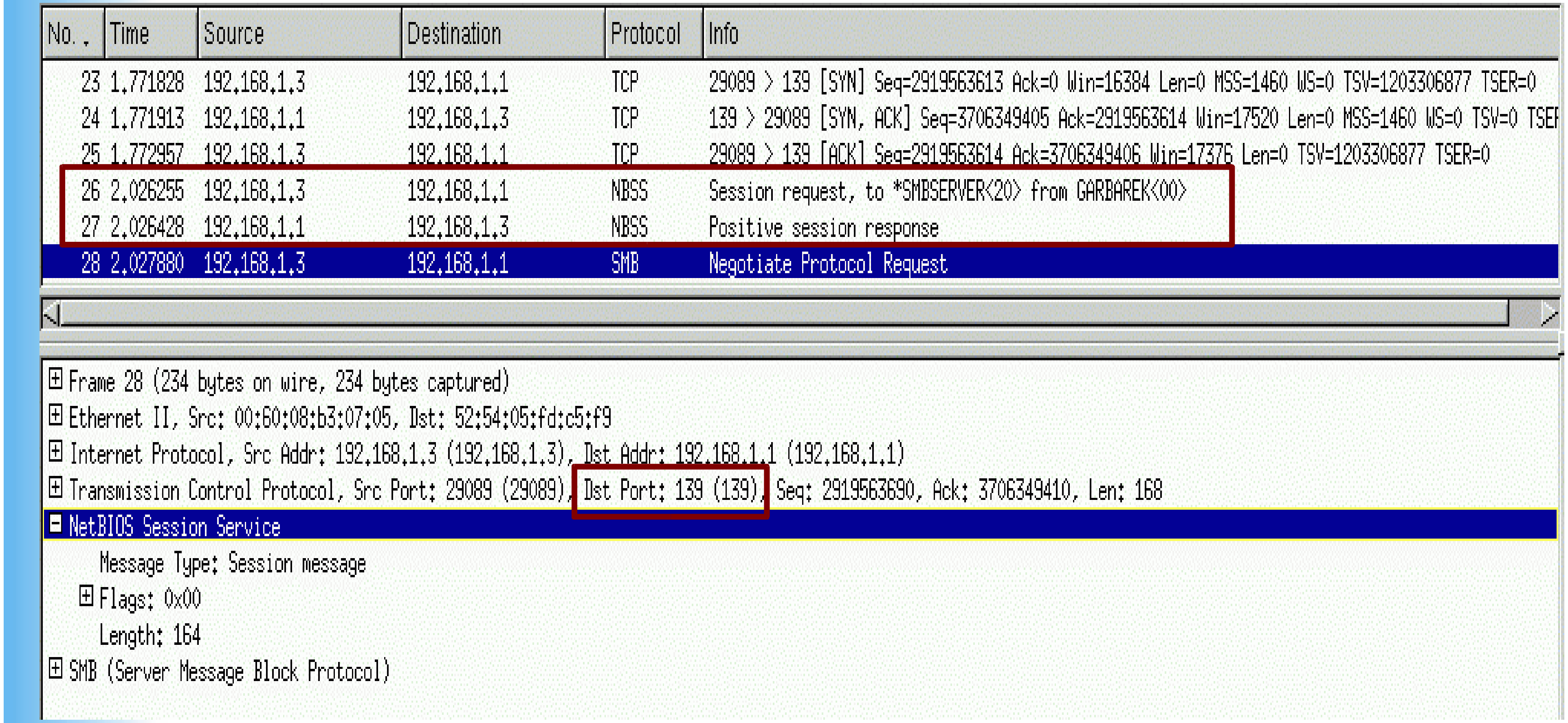
SMB

TCP (port 445)

Windows NT

Windows 2000 >

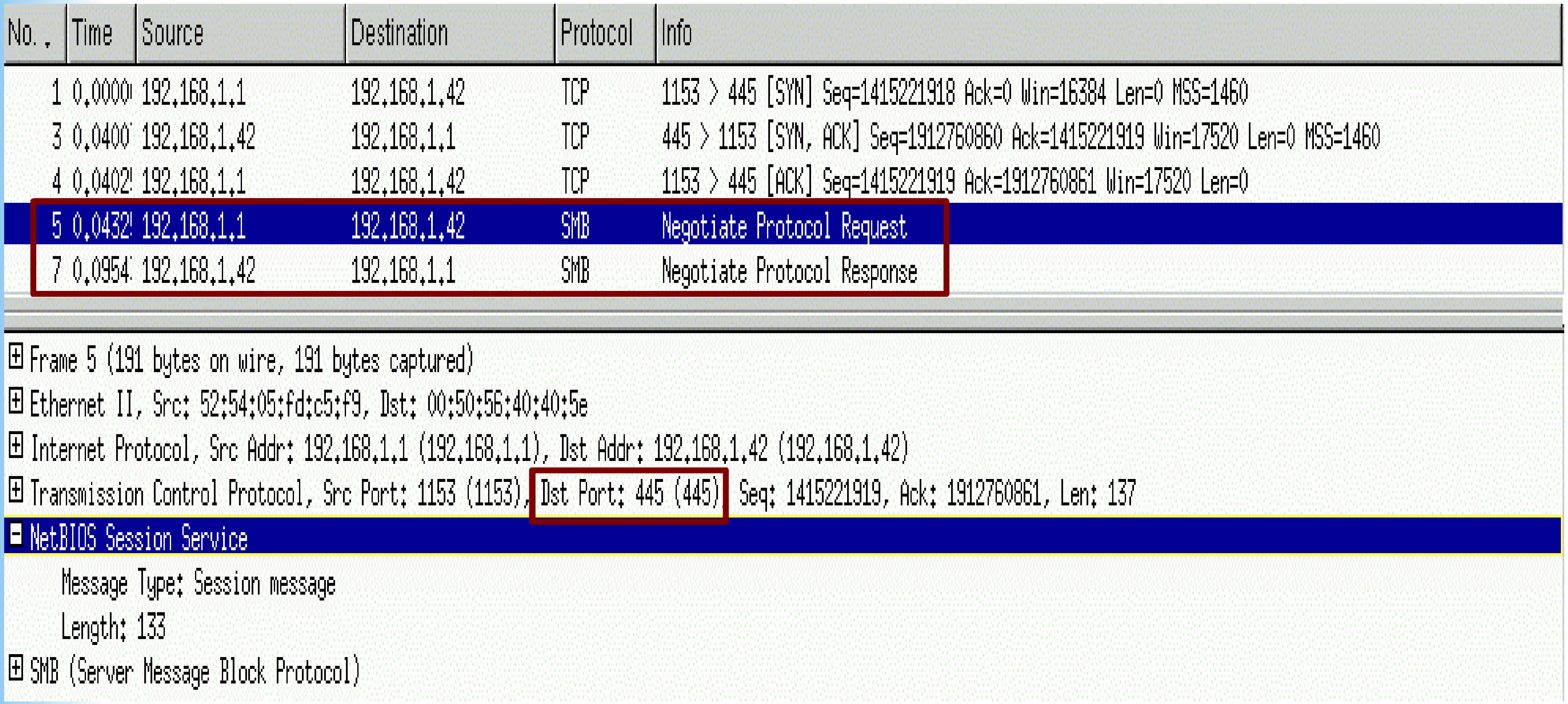
SMB NetBT transport: on the wire



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 TSEF
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)
```

Raw SMB transport: on the wire



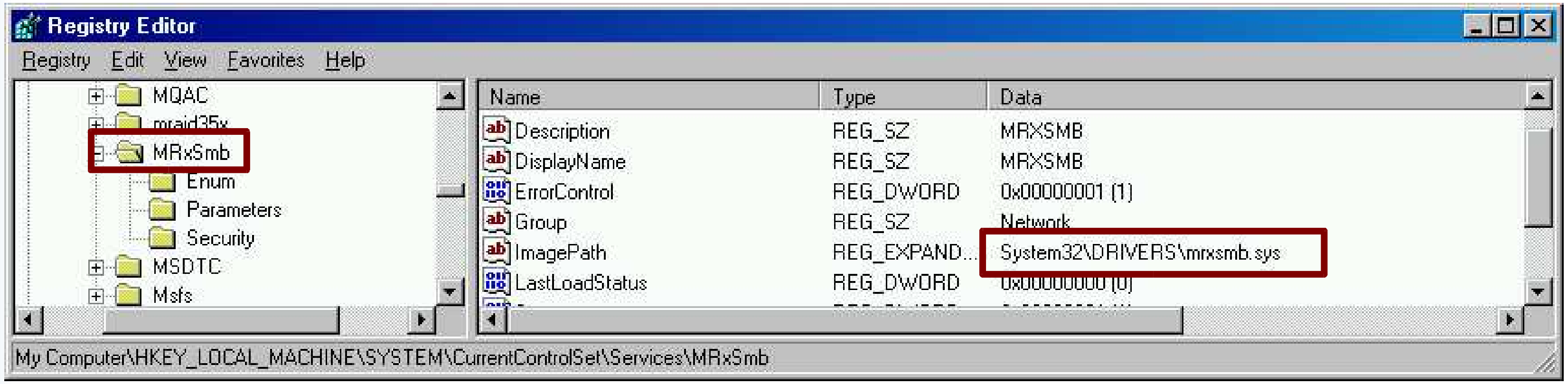
```
No. . Time    Source        Destination   Protocol  Info
    1 0.0000  192.168.1.1   192.168.1.42  TCP       1153 > 445 [SYN] Seq=1415221918 Ack=0 Win=16384 Len=0 MSS=1460
    3 0.0400  192.168.1.42  192.168.1.1   TCP       445 > 1153 [SYN, ACK] Seq=1912760860 Ack=1415221919 Win=17520 Len=0 MSS=1460
    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)
```

SMB implementation

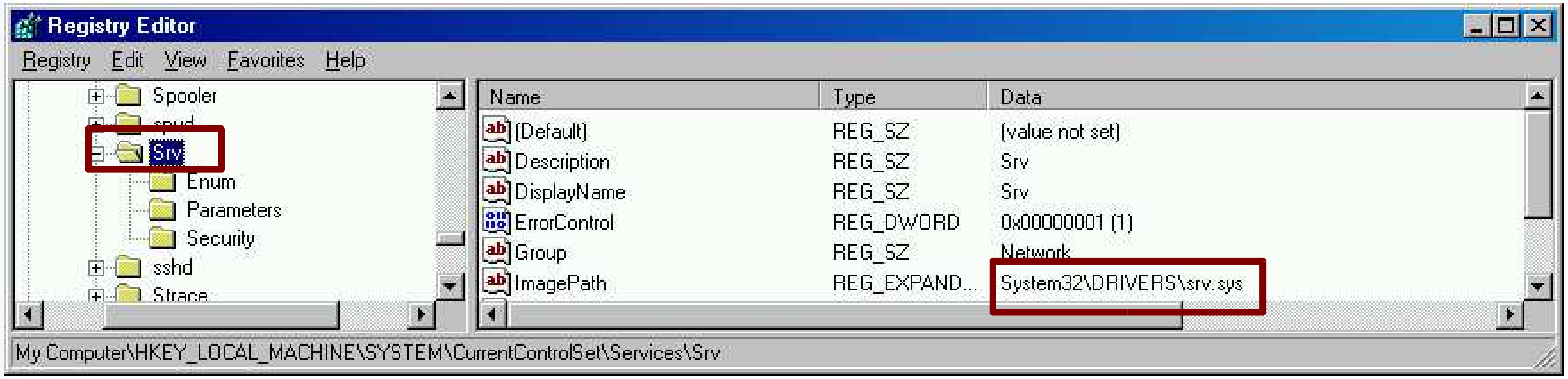
- kernel-mode drivers
  - Client-side: redirector
    - rdr.sys (NT), mrxsmb.sys (W2K and >)
  - Server-side: server (srv.sys)
- User-mode services
  - lanmanworkstation: redirector configuration
  - lanmanserver: server configuration

SMB implementation: drivers



Name	Type	Data
Description	REG_SZ	MRXSMB
DisplayName	REG_SZ	MRXSMB
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	Network
ImagePath	REG_EXPAND...	System32\DRIVERS\mrxsmb.sys
LastLoadStatus	REG_DWORD	0x00000000 (0)

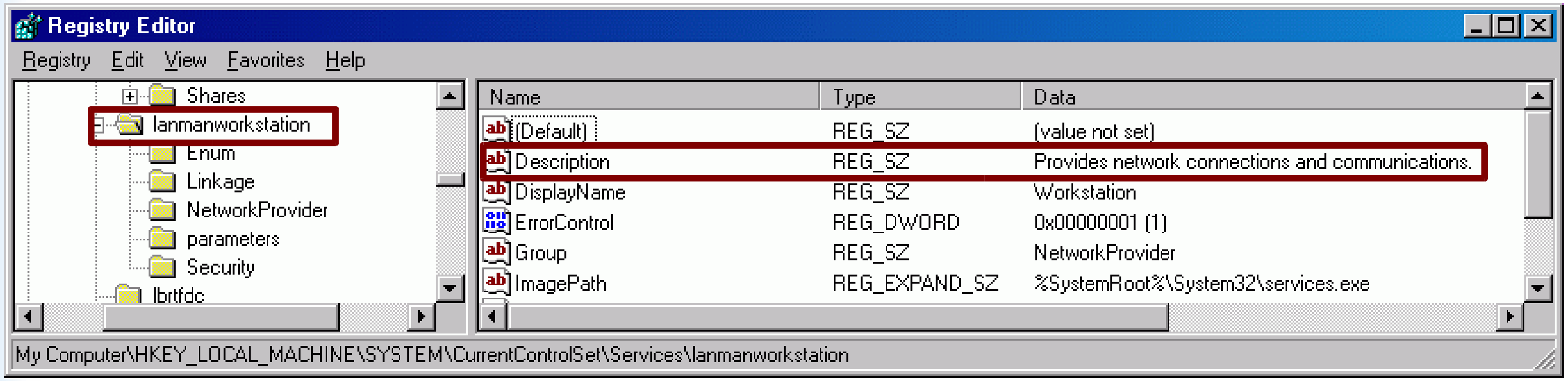
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb



Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Srv
DisplayName	REG_SZ	Srv
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	Network
ImagePath	REG_EXPAND...	System32\DRIVERS\srv.sys

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Srv

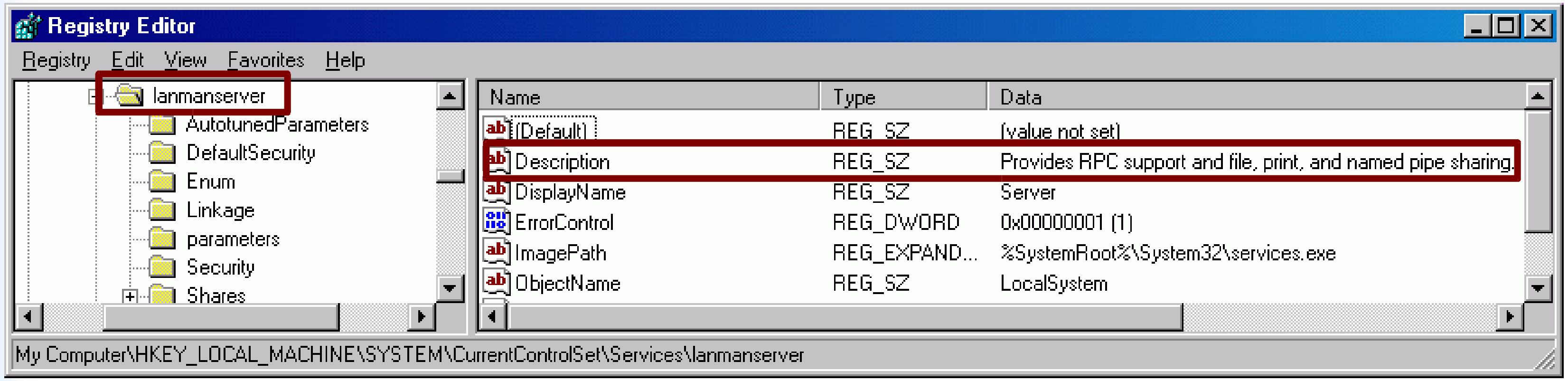
SMB implementation: services



Shares
lanmanworkstation
Enum
Linkage
NetworkProvider
parameters
Security
lbrtfdc

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Provides network connections and communications.
DisplayName	REG_SZ	Workstation
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	NetworkProvider
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\services.exe

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation



lanmanserver
AutotunedParameters
DefaultSecurity
Enum
Linkage
parameters
Security
Shares

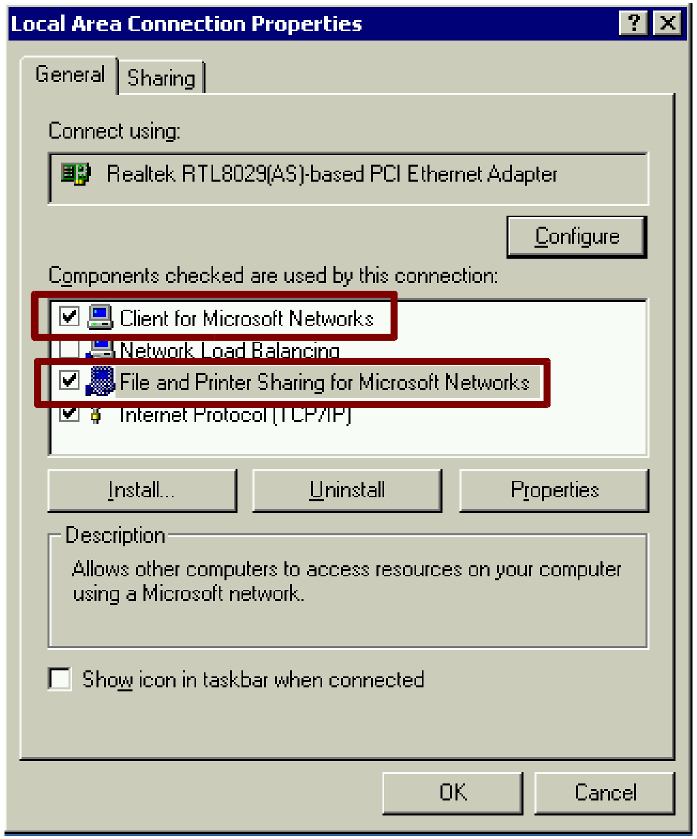
Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Provides RPC support and file, print, and named pipe sharing.
DisplayName	REG_SZ	Server
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND...	%SystemRoot%\System32\services.exe
ObjectName	REG_SZ	LocalSystem

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver

SMB bindings

- SMB bindings
  - Per network adapter
    - Client-side: Client for Microsoft Networks
    - Server-side: File and Printer Sharing for Microsoft Networks
  - Configuration
    - GUI: network adapter properties
    - CLI: net config rdr, net config srv

SMB bindings: GUI



Local Area Connection Properties

General | Sharing

Connect using:

Realtek RTL8029(AS)-based PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks

□ Network Load Balancing

☑ File and Printer Sharing for Microsoft Networks

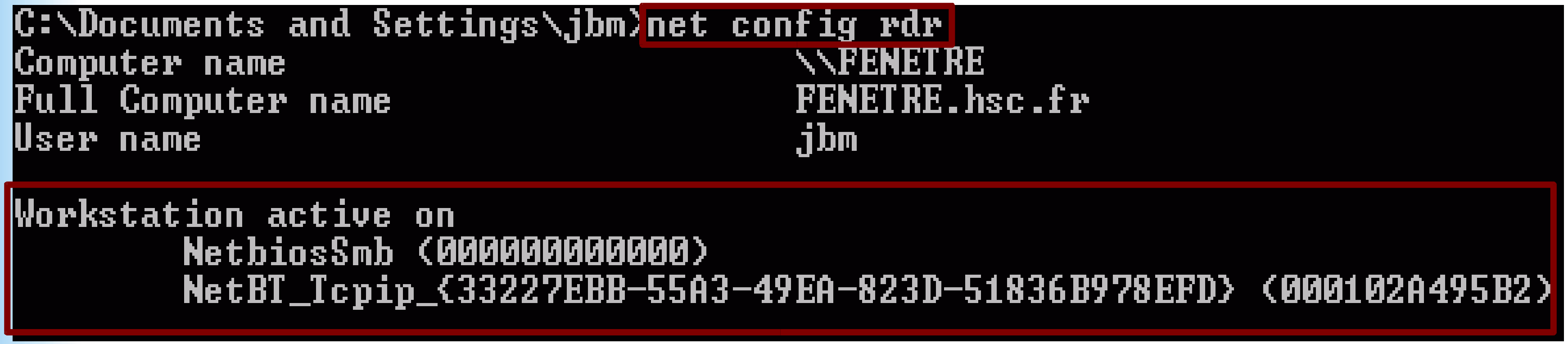
☑ Internet Protocol (TCP/IP)

Description

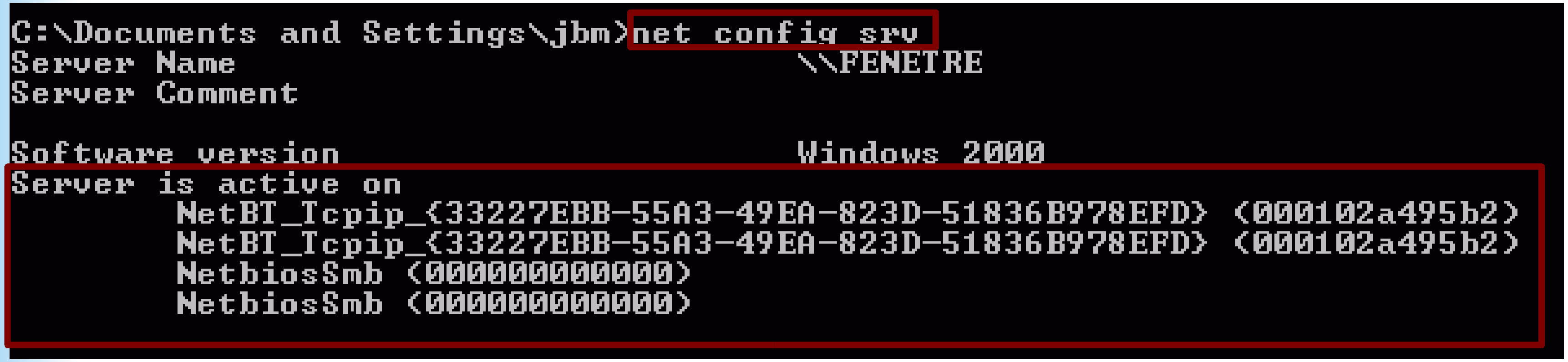
Allows other computers to access resources on your computer using a Microsoft network.

□ Show icon in taskbar when connected

SMB bindings: CLI



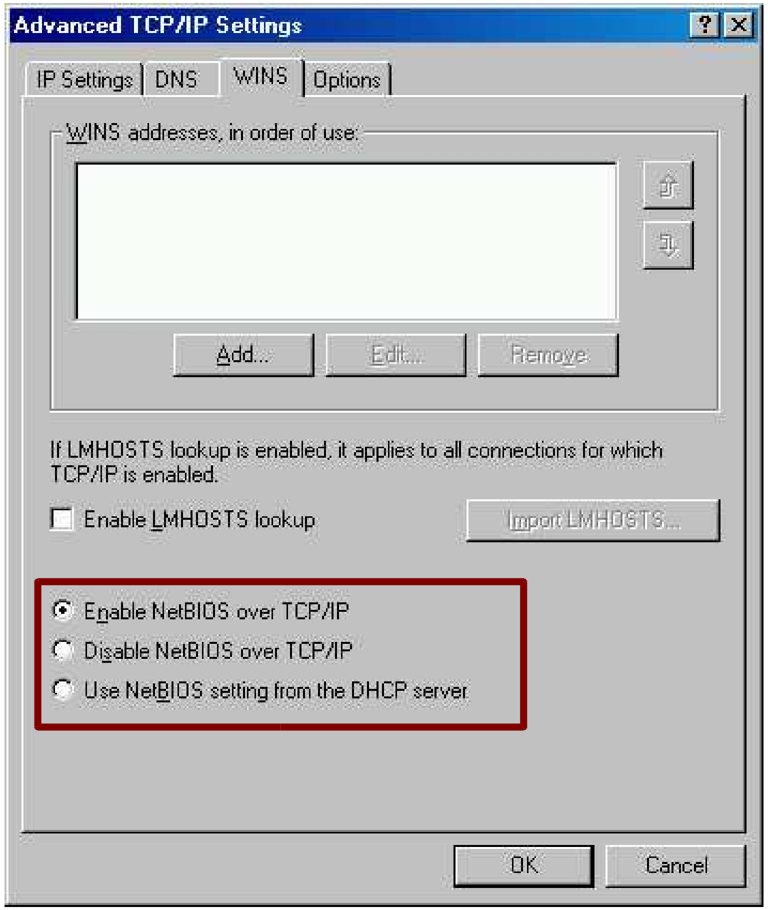
```
C:\Documents and Settings\jbm>net config rdr
Computer name                        \\FENETRE
Full Computer name                   FENETRE.hsc.fr
User name                            jbm

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{33227EBB-55A3-49EA-823D-51836B978EFD} (000102A495B2)
```



```
C:\Documents and Settings\jbm>net config srv
Server Name                          \\FENETRE
Server Comment

Software version                     Windows 2000
Server is active on
        NetBT_Tcpip_{33227EBB-55A3-49EA-823D-51836B978EFD} (000102a495b2)
        NetBT_Tcpip_{33227EBB-55A3-49EA-823D-51836B978EFD} (000102a495b2)
        NetbiosSmb (000000000000)
        NetbiosSmb (000000000000)
```

SMB transport configuration

- NetBT transport



Advanced TCP/IP Settings

WINS addresses, in order of use:

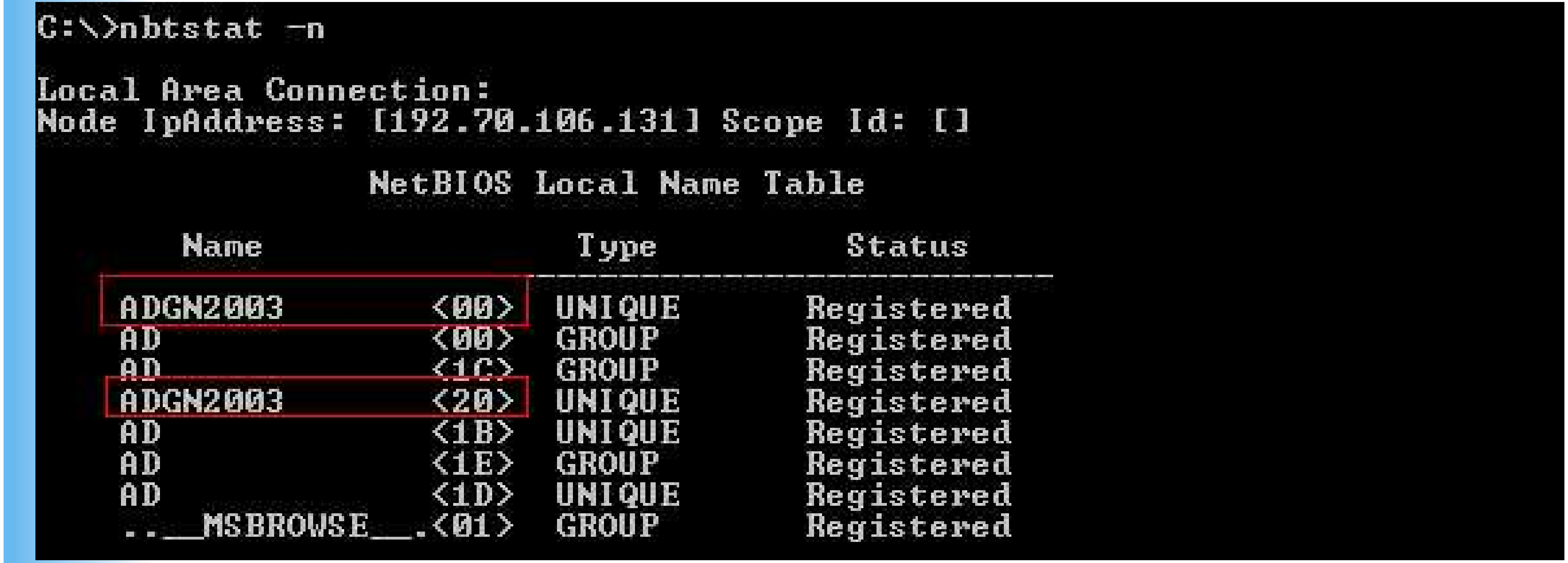
If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

□ Enable LMHOSTS lookup

● Enable NetBIOS over TCP/IP
○ Disable NetBIOS over TCP/IP
○ Use NetBIOS setting from the DHCP server

NetBT: NetBIOS names

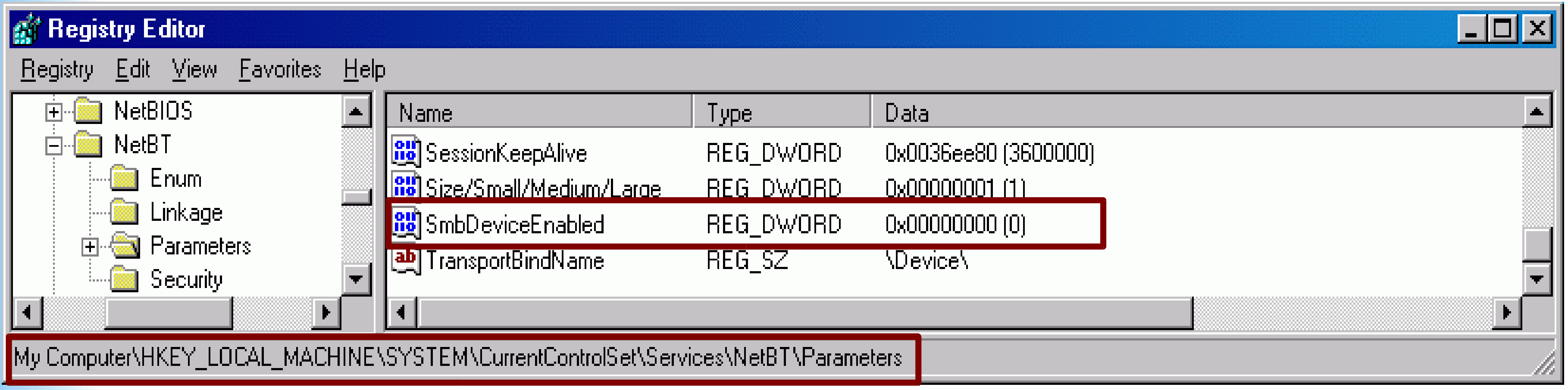
- NetBIOS names
  - Name suffix identifies nature of the service
    - <00>: redirector service, <20>: server service



```
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
```

SMB transport: raw SMB

- raw SMB transport
  - Global device: NetbiosSmb
    - Created by the NetBT driver
    - Can not be bound/unbound to a specific network adapter
    - SmbDeviceEnabled registry value

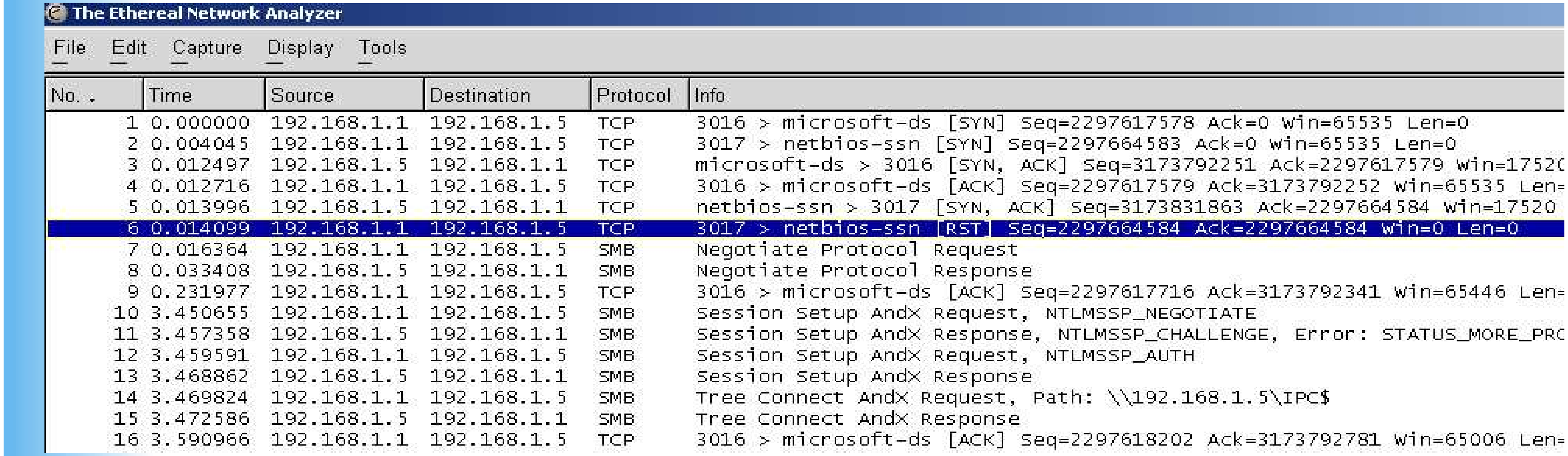


Name	Type	Data
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
SmbDeviceEnabled	REG_DWORD	0x00000000 (0)
TransportBindName	REG_SZ	\Device\

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

SMB transport choice

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

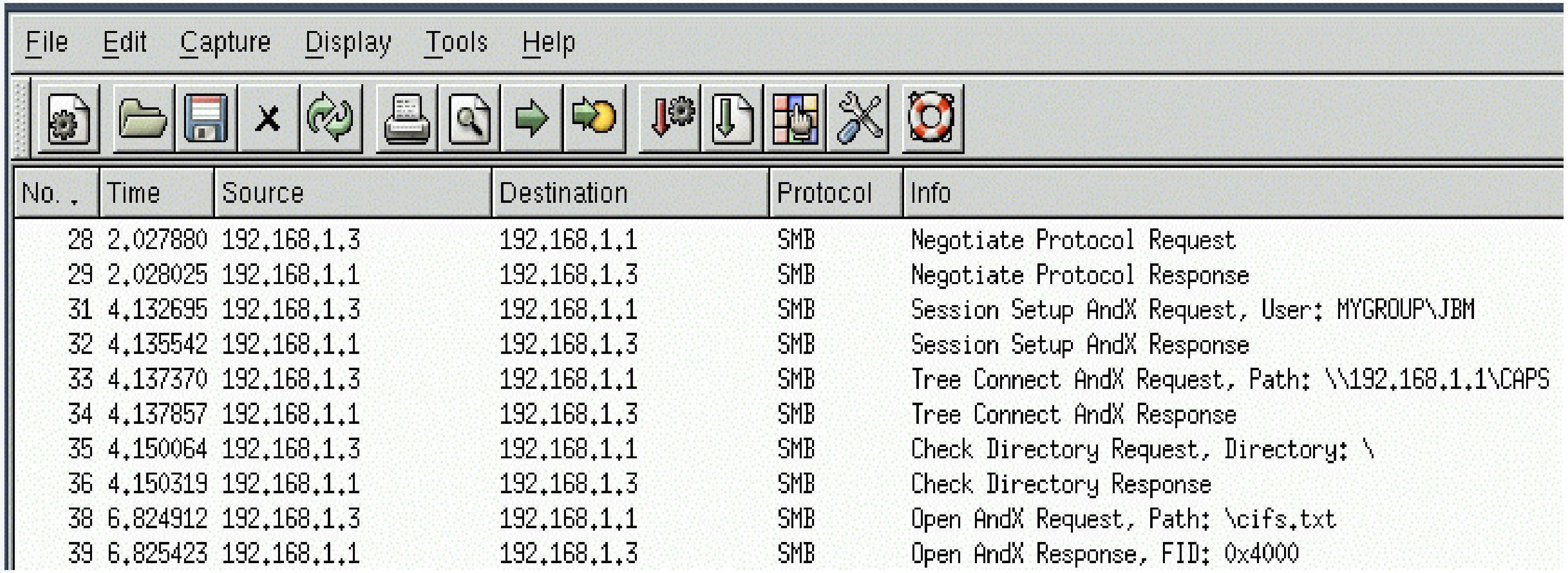


```
No. .   Time      Source       Destination  Protocol  Info
   1 0.000000  192.168.1.1  192.168.1.5  TCP       3016 > microsoft-ds [SYN] Seq=2297617578 Ack=0 Win=65535 Len=0
   2 0.004045  192.168.1.1  192.168.1.5  TCP       3017 > netbios-ssn [SYN] Seq=2297664583 Ack=0 Win=65535 Len=0
   3 0.012497  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_PR
  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=
```

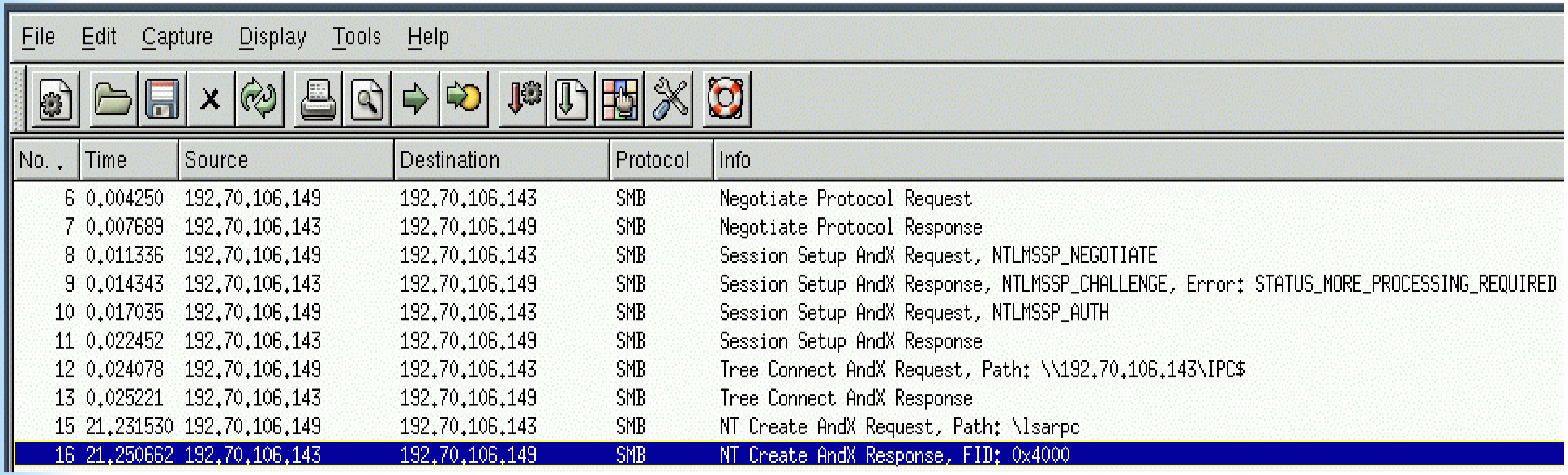
SMB key concepts

- SMB key concepts
  - Share: group of shared ressources
    - Files share
      - Ex: administrative shares (C$, ADMIN$)
    - Shared printers
    - IPC$: special share
      - Gives access, over the network, to named pipes
  - SMB session
    - The SMB protocol is session-oriented
    - A SMB session starts with authentication
    - Use of a network authentication protocol
      - (NT)LM
      - Kerberos

SMB session: examples



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

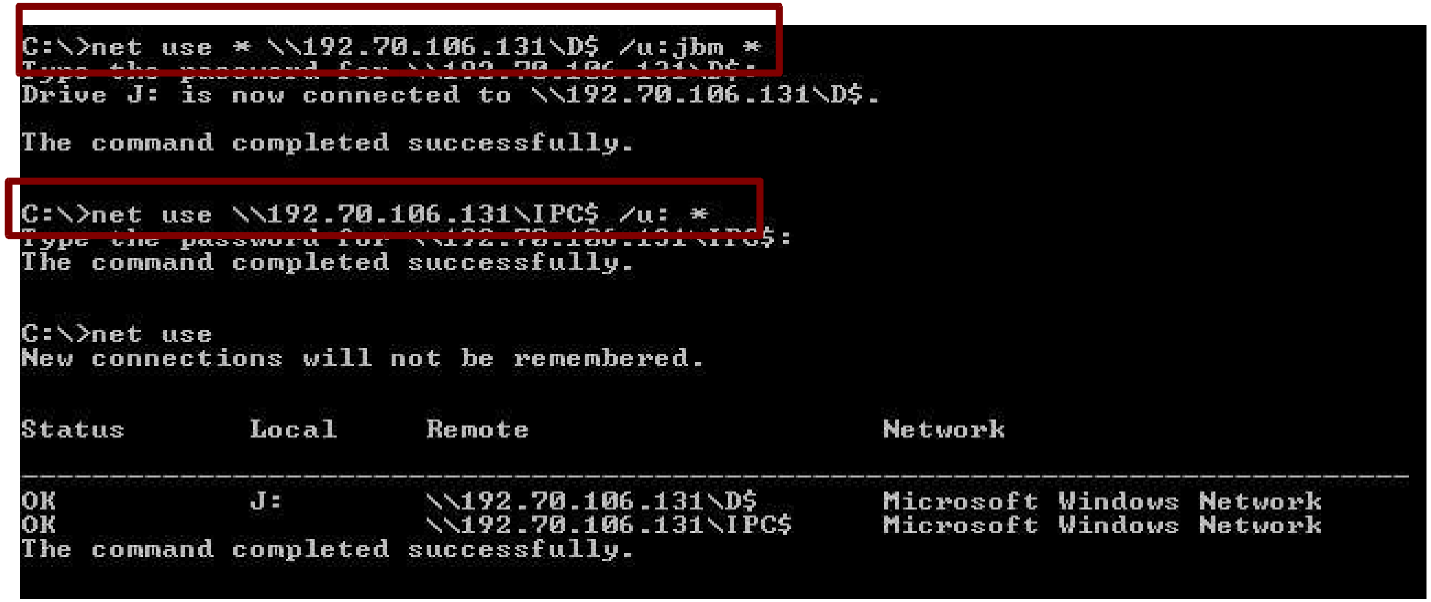


No.	Time	Source	Destination	Protocol	Info
6	0.004250	192.70.106.149	192.70.106.143	SMB	Negotiate Protocol Request
7	0.007689	192.70.106.143	192.70.106.149	SMB	Negotiate Protocol Response
8	0.011336	192.70.106.149	192.70.106.143	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
9	0.014343	192.70.106.143	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

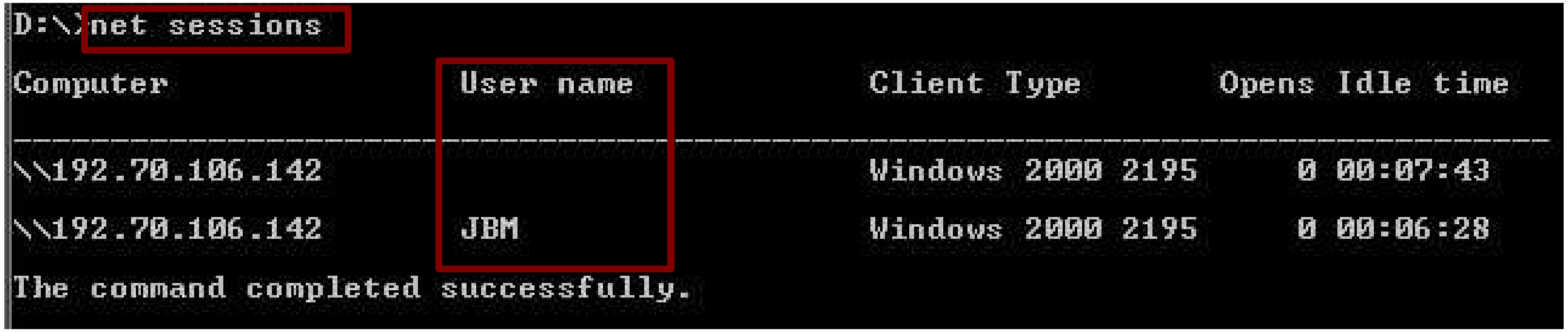
Using the redirector

- 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**

net use: examples



```
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.
```

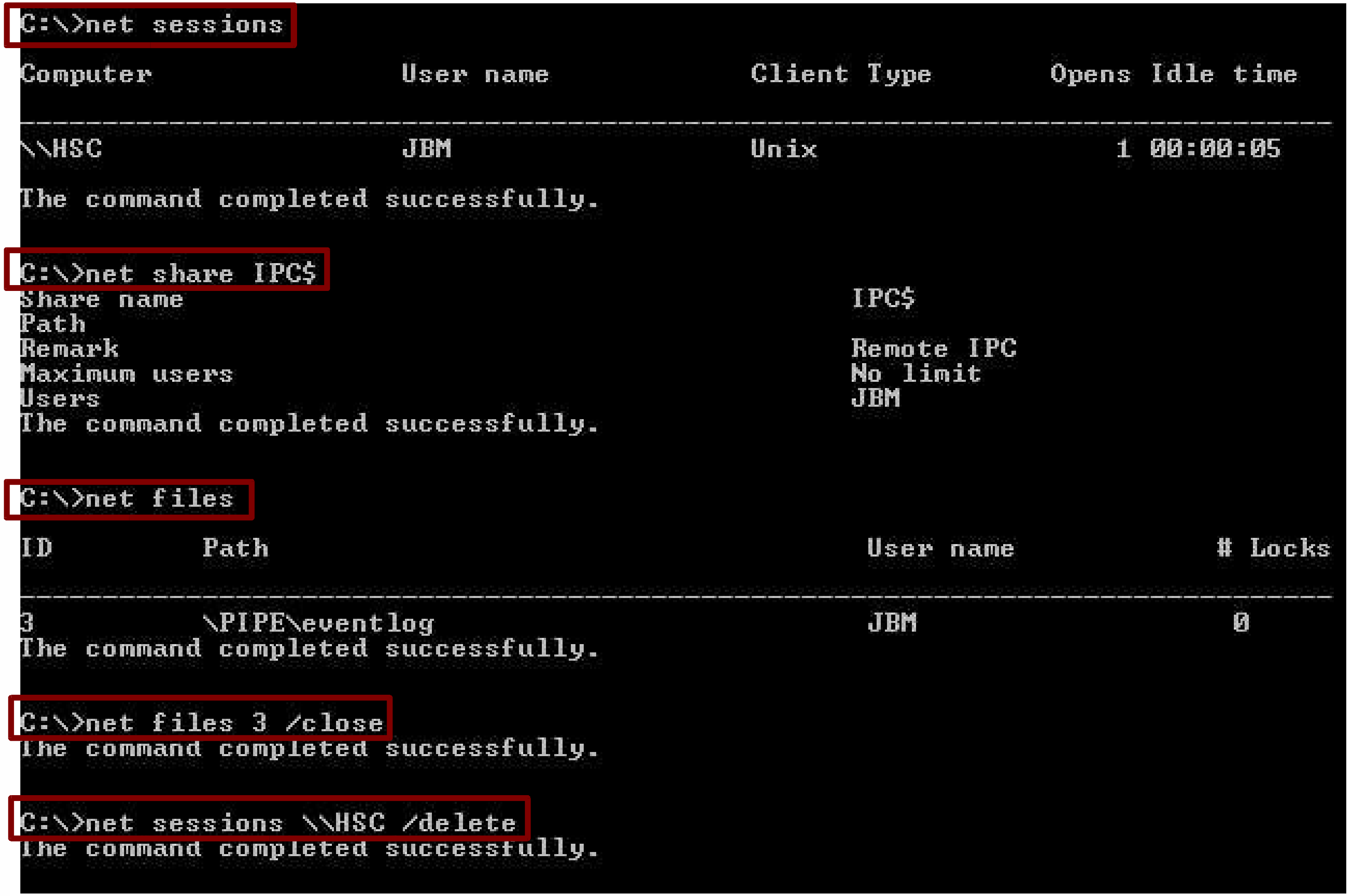


```
D:\>net sessions

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.
```

SMB 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 sessions management



```
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.
```

SMB as a transport protocol

- SMB as a transport protocol
  - IPC$ share: gives access to named pipes over the network
  - Named pipes are used to transport remote procedure calls
  - DCE RPC over SMB
    - Named pipes are used as DCE RPC endpoints

MSRPC

- MSRPC introduction
- Typical MSRPC protocol sequences
  - named pipes: ncacn_np
  - LPC ports: ncalrpc
  - TCP/IP: ncacn_ip_tcp, ncadg_ip_udp
- NULL sessions
- RPC services examples
- MSRPC security

MSRPC: introduction

- Microsoft implementation of DCE RPC
  - Used in all versions of Windows NT, at all levels
    - Typical use: NT domains, remote administration, DCOM
    - A brief history of Windows
      - http://www.advogato.org/article/596.html
- 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

MSRPC transport

- MSRPC typical protocol sequences
  - ncacn_np: named pipes (using SMB)
  - ncalrpc: LPC (Local Procedure Calls) ports
  - ncacn_ip_tcp, ncadg_ip_udp: TCP or UDP ports
  - Other transports: ncacn_http (HTTP transport), IPX/SPX, NetBeui..

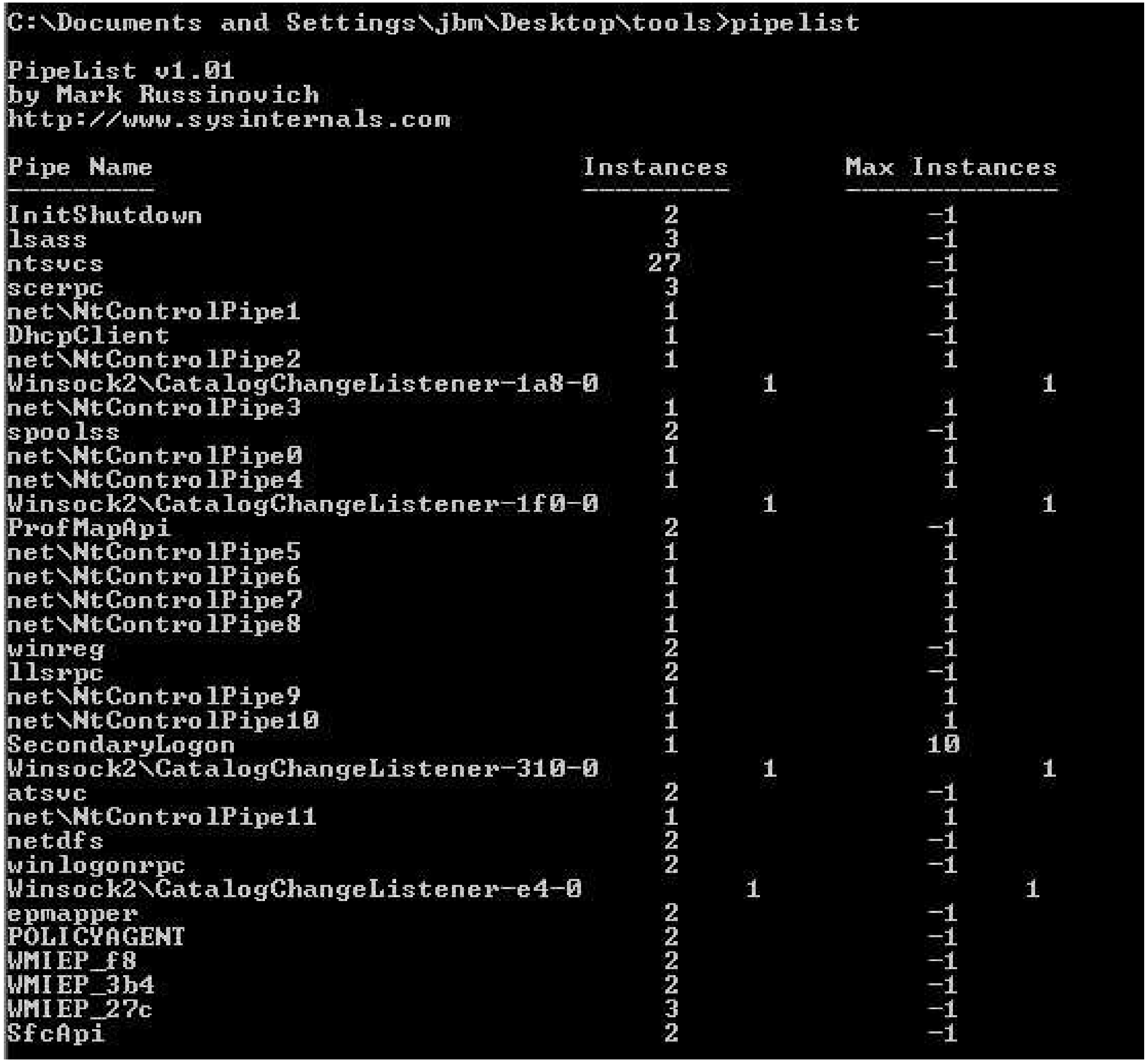
MSRPC services classification

- MSRPC services classification
  - ncacn_np RPC services
    - NT 4.0 domains
    - remote administration tools
  - ncacn_ip_tcp and ncadg_ip_udp RPC services
    - Active Directory domains
    - DCOM

Named pipes

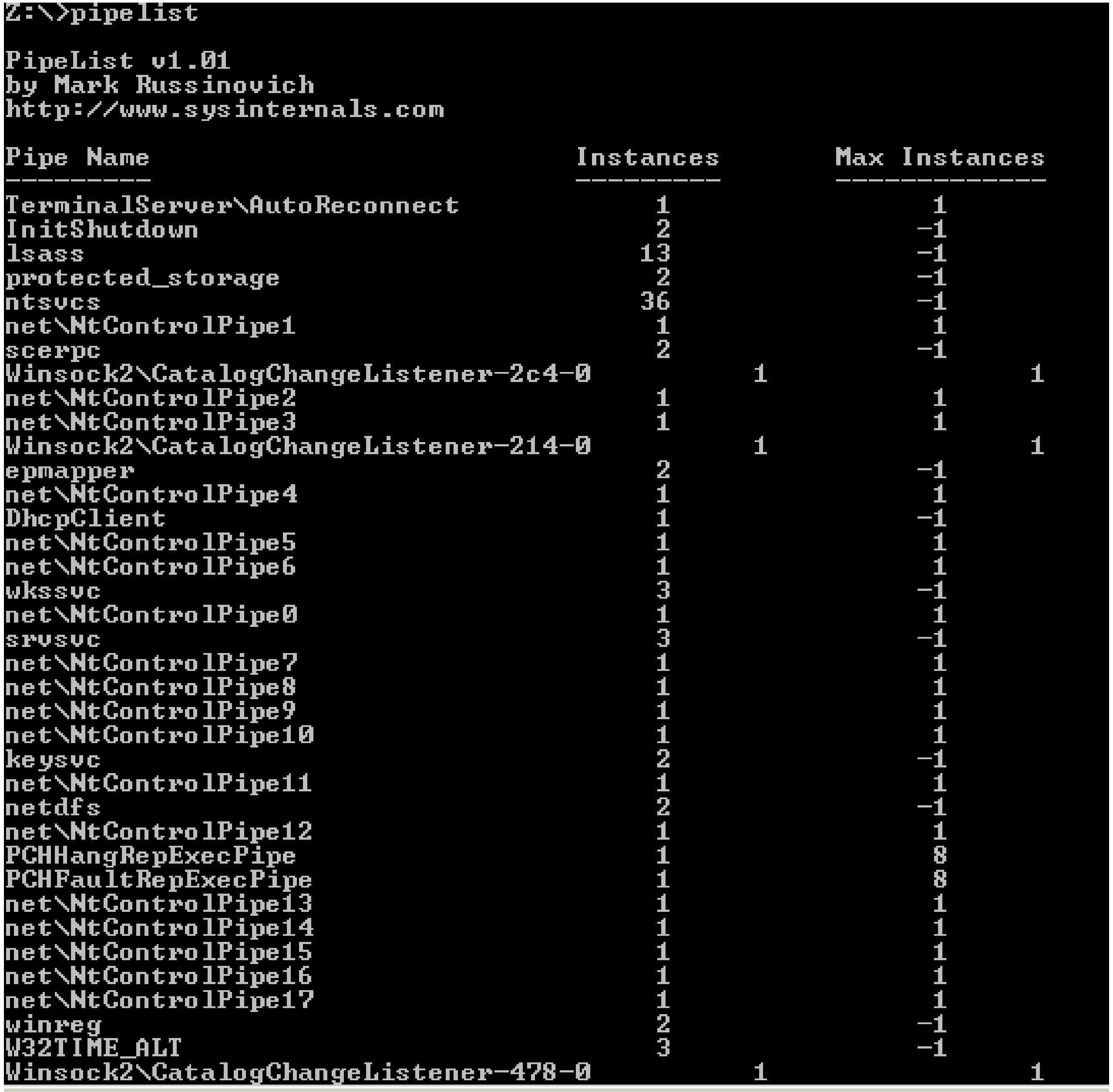
- Inter-Process Communication (IPC) mechanism
  - Locally or over the network (using SMB)
- Implemented by a file system driver
  - npfs.sys (Ex: \Device\NamedPipes\lsass)
- Named pipes enumeration tool
  - pipelist (sysinternals.com)

Named pipes: W2K



```
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: W2K3

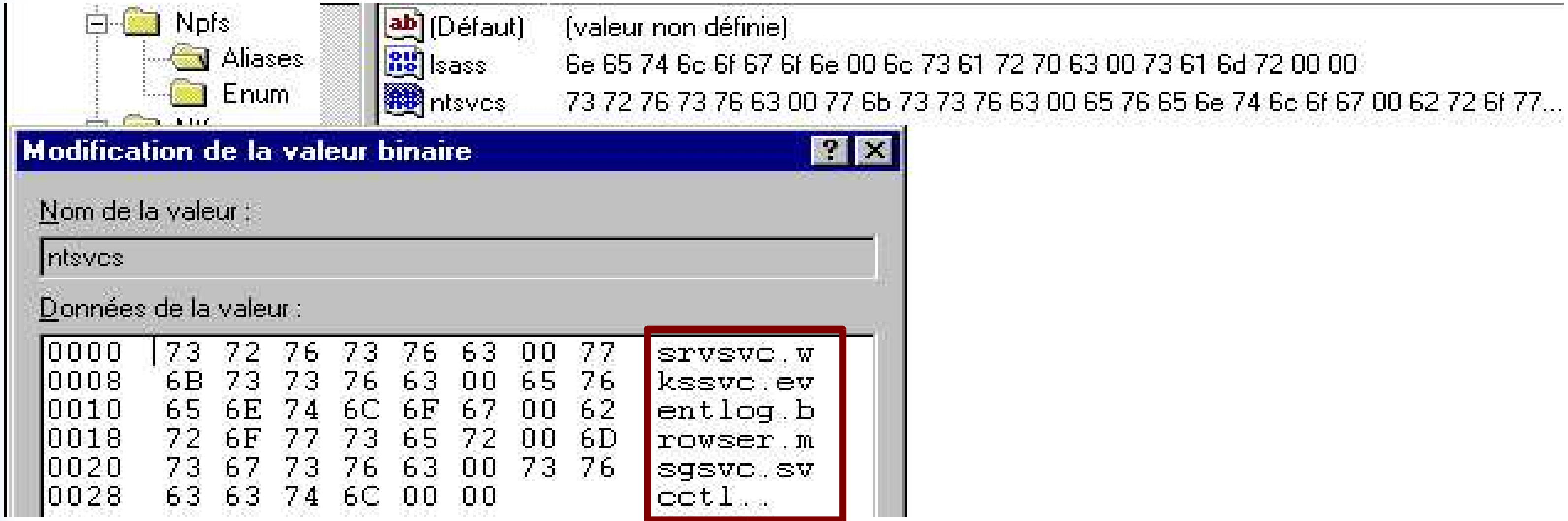


```
Z:\>pipelist

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

Pipe Name                          Instances       Max Instances
---------                          ---------       -------------
TerminalServer\AutoReconnect             1                1
InitShutdown                             2               -1
lsass                                   13               -1
protected_storage                        2               -1
ntsvcs                                  36               -1
net\NtControlPipe1                       1                1
scerpc                                   2               -1
Winsock2\CatalogChangeListener-2c4-0           1                1
net\NtControlPipe2                       1                1
net\NtControlPipe3                       1                1
Winsock2\CatalogChangeListener-214-0           1                1
epmapper                                 2               -1
net\NtControlPipe4                       1                1
DhcpClient                               1               -1
net\NtControlPipe5                       1                1
net\NtControlPipe6                       1                1
wkssvc                                   3               -1
net\NtControlPipe0                       1                1
srvsvc                                   3               -1
net\NtControlPipe7                       1                1
net\NtControlPipe8                       1                1
net\NtControlPipe9                       1                1
net\NtControlPipe10                      1                1
keysvc                                   2               -1
net\NtControlPipe11                      1                1
netdfs                                   2               -1
net\NtControlPipe12                      1                1
PCHHangRepExecPipe                       1                8
PCHFaultRepExecPipe                      1                8
net\NtControlPipe13                      1                1
net\NtControlPipe14                      1                1
net\NtControlPipe15                      1                1
net\NtControlPipe16                      1                1
net\NtControlPipe17                      1                1
winreg                                   2               -1
W32TIME_ALT                              3               -1
Winsock2\CatalogChangeListener-478-0           1                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}

npfs aliases: registry values



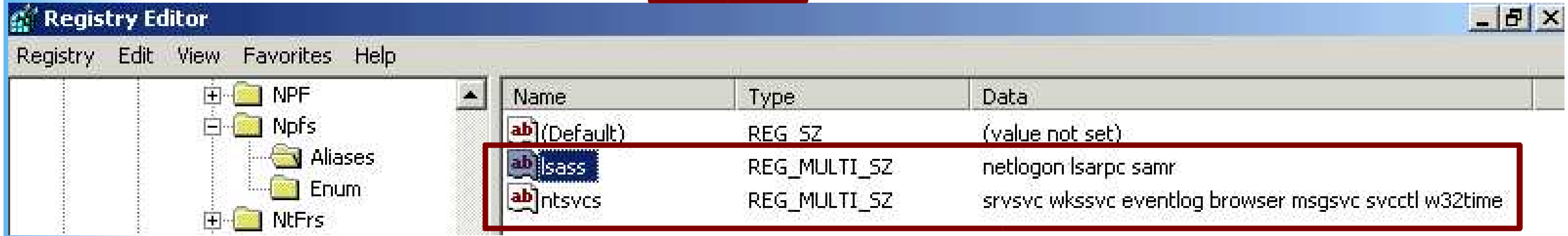
```
(Défaut)   (valeur non définie)
lsass      6e 65 74 6c 6f 67 6f 6e 00 6c 73 61 72 70 63 00 73 61 6d 72 00 00
ntsvcs     73 72 76 73 76 63 00 77 6b 73 73 76 63 00 65 76 65 6e 74 6c 6f 67 00 62 72 6f 77...
```

Modification de la valeur binaire

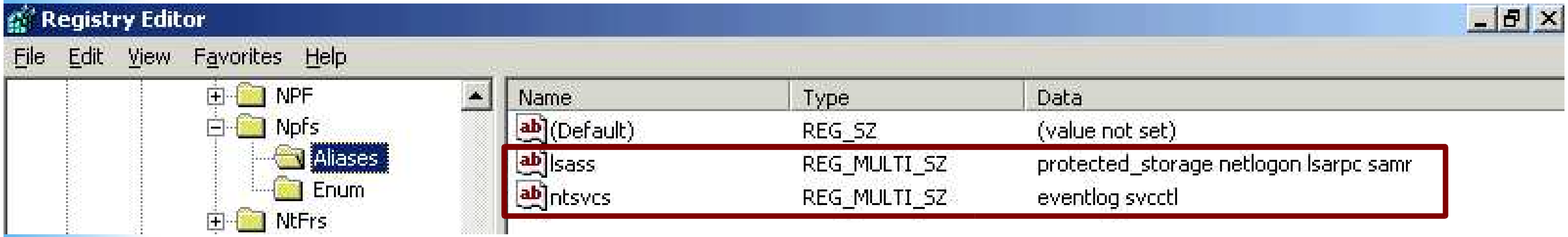
Nom de la valeur : ntsvcs

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

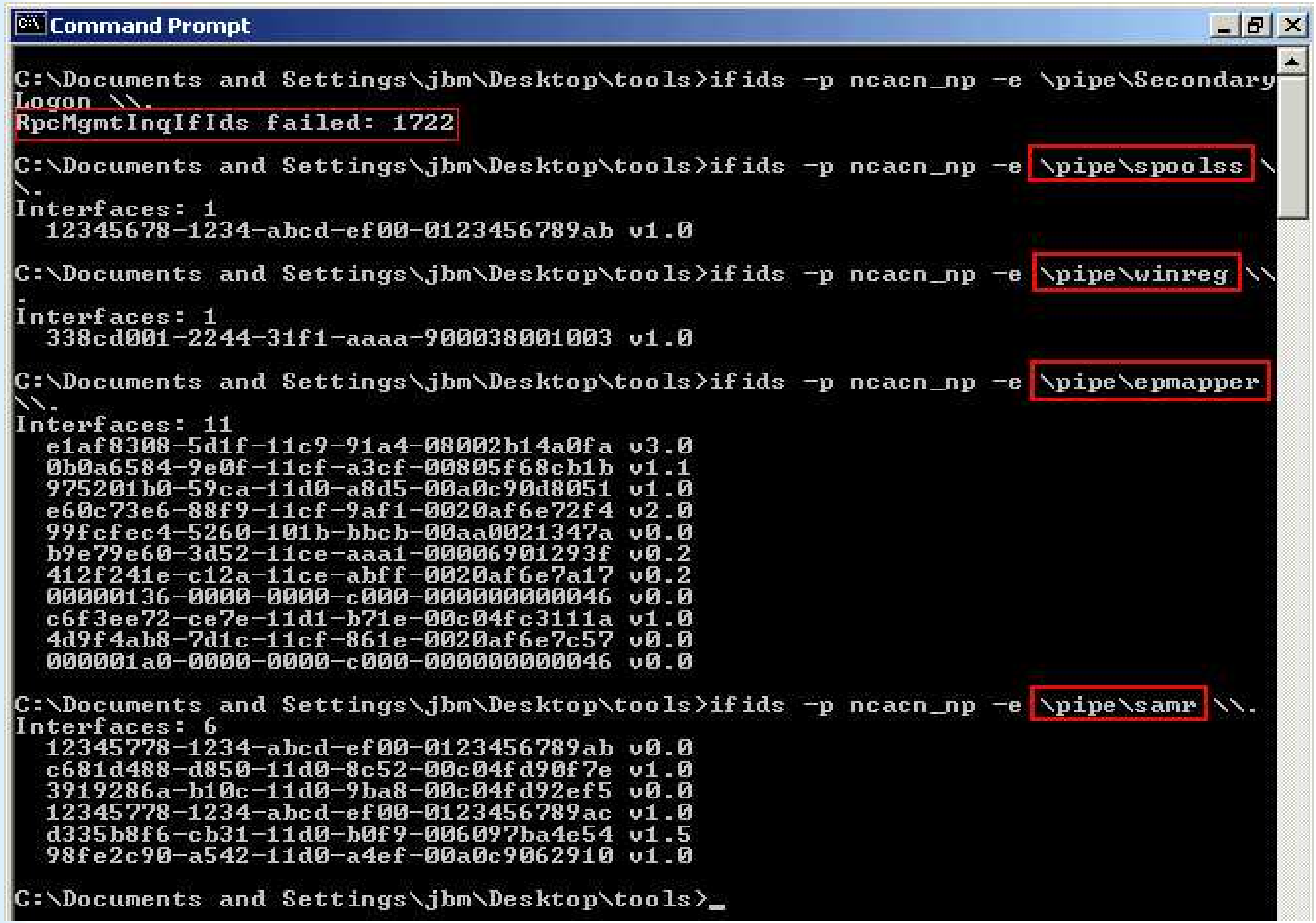


Name	Type	Data
(Default)	REG_SZ	(value not set)
lsass	REG_MULTI_SZ	protected_storage netlogon lsarpc samr
ntsvcs	REG_MULTI_SZ	eventlog svcctl

DCE RPC remote mgmt interface

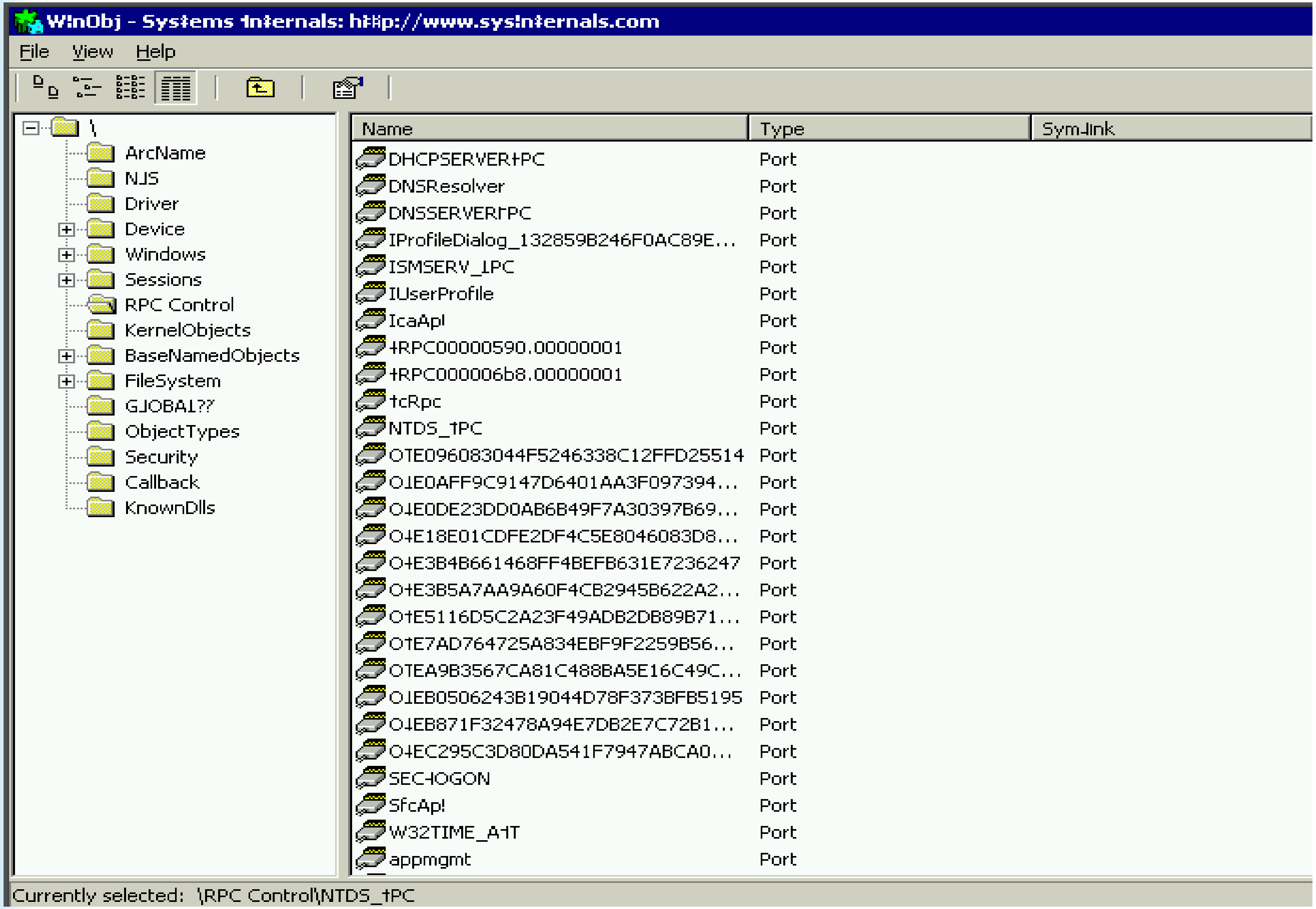
- DCE RPC mgmt interface
  - interface: set of related operations
  - management interface
    - Implicitly supported by any DCE RPC service
    - ifids tool (Todd Sabin)
  - Identification of named pipes used as MSRPC endpoints, using ifids
    - Ifids -p ncacn_np -e \pipe\pipe_name \\UNC_name

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>_
```

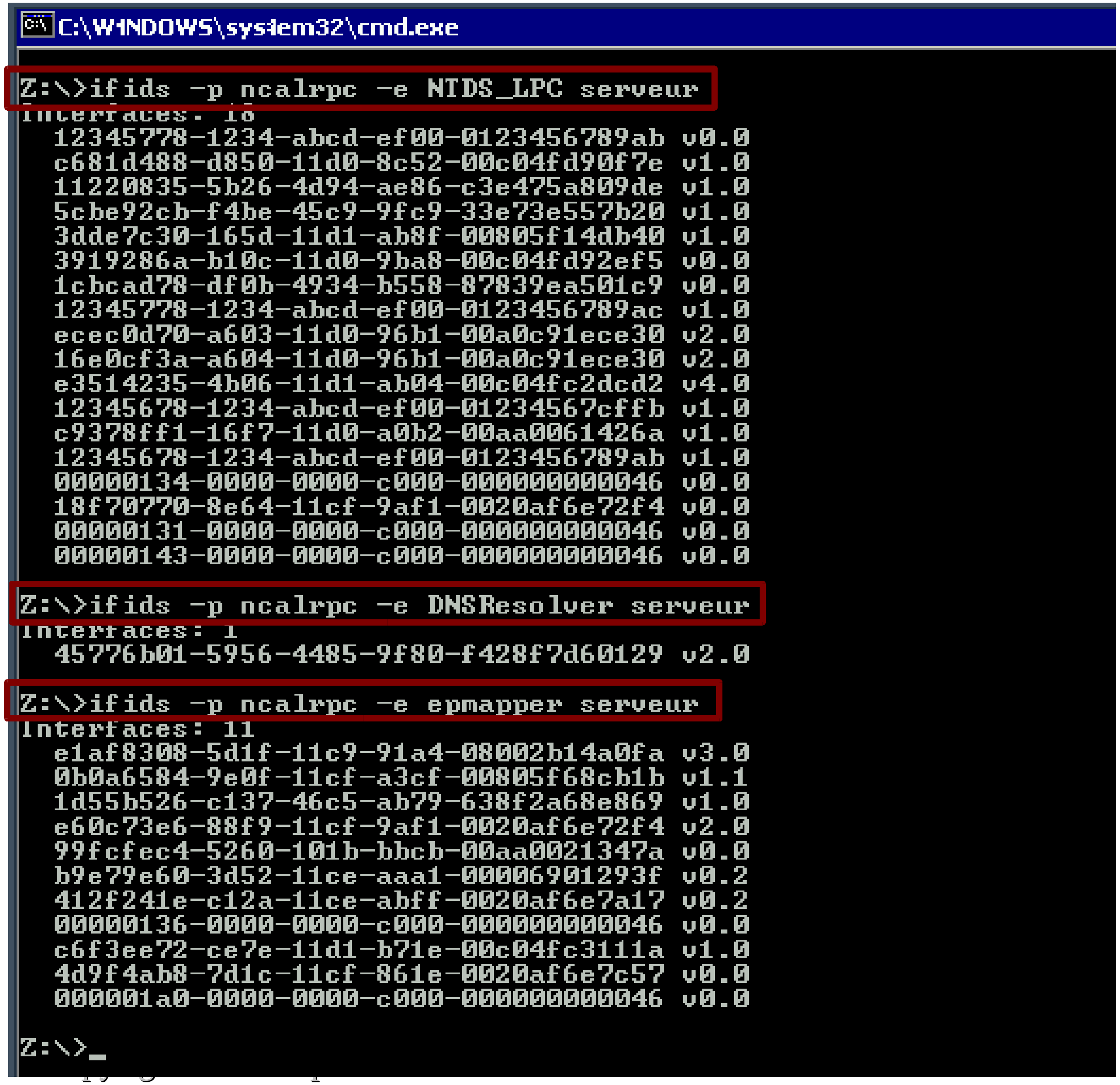
ncalrpc: LPC port endpoints



Name	Type	SymLink
DHCPSERVER+PC	Port	
DNSResolver	Port	
DNSSERVERΓPC	Port	
IProfileDialog_132859B246F0AC89E...	Port	
ISMSERV_ⅠPC	Port	
IUserProfile	Port	
IcaApl	Port	
+RPC00000590.00000001	Port	
+RPC000006b8.00000001	Port	
tcRpc	Port	
NTDS_tPC	Port	
OTE096083044F5246338C12FFD25514	Port	
OⅠE0AFF9C9147D6401AA3F097394...	Port	
O+E0DE23DD0AB6B49F7A30397B69...	Port	
O+E18E01CDFE2DF4C5E8046083D8...	Port	
O+E3B4B661468FF4BEFB631E7236247	Port	
O+E3B5A7AA9A60F4CB2945B622A2...	Port	
O+E5116D5C2A23F49ADB2DB89B71...	Port	
OTE7AD764725A834EBF9F2259B56...	Port	
OTEA9B3567CA81C488BA5E16C49C...	Port	
OⅠEB0506243B19044D78F373BFB5195	Port	
O+EB871F32478A94E7DB2E7C72B1...	Port	
O+EC295C3D80DA541F7947ABCA0...	Port	
SEC+OGON	Port	
SfcAp!	Port	
W32TIME_A+T	Port	
appmgmt	Port	

Currently selected: \RPC Control\NTDS_tPC

ifids: LPC ports endpoints



```
Z:\>ifids -p ncalrpc -e NTDS_LPC serveur
Interfaces: 18
  12345778-1234-abcd-ef00-0123456789ab v0.0
  c681d488-d850-11d0-8c52-00c04fd90f7e v1.0
  11220835-5b26-4d94-ae86-c3e475a809de v1.0
  5cbe92cb-f4be-45c9-9fc9-33e73e557b20 v1.0
  3dde7c30-165d-11d1-ab8f-00805f14db40 v1.0
  3919286a-b10c-11d0-9ba8-00c04fd92ef5 v0.0
  1cbcad78-df0b-4934-b558-87839ea501c9 v0.0
  12345778-1234-abcd-ef00-0123456789ac v1.0
  ecec0d70-a603-11d0-96b1-00a0c91ece30 v2.0
  16e0cf3a-a604-11d0-96b1-00a0c91ece30 v2.0
  e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0
  12345678-1234-abcd-ef00-01234567cffb v1.0
  c9378ff1-16f7-11d0-a0b2-00aa0061426a v1.0
  12345678-1234-abcd-ef00-0123456789ab v1.0
  00000134-0000-0000-c000-000000000046 v0.0
  18f70770-8e64-11cf-9af1-0020af6e72f4 v0.0
  00000131-0000-0000-c000-000000000046 v0.0
  00000143-0000-0000-c000-000000000046 v0.0

Z:\>ifids -p ncalrpc -e DNSResolver serveur
Interfaces: 1
  45776b01-5956-4485-9f80-f428f7d60129 v2.0

Z:\>ifids -p ncalrpc -e epmapper serveur
Interfaces: 11
  e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
  0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.1
  1d55b526-c137-46c5-ab79-638f2a68e869 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

Z:\>_
```

NULL sessions

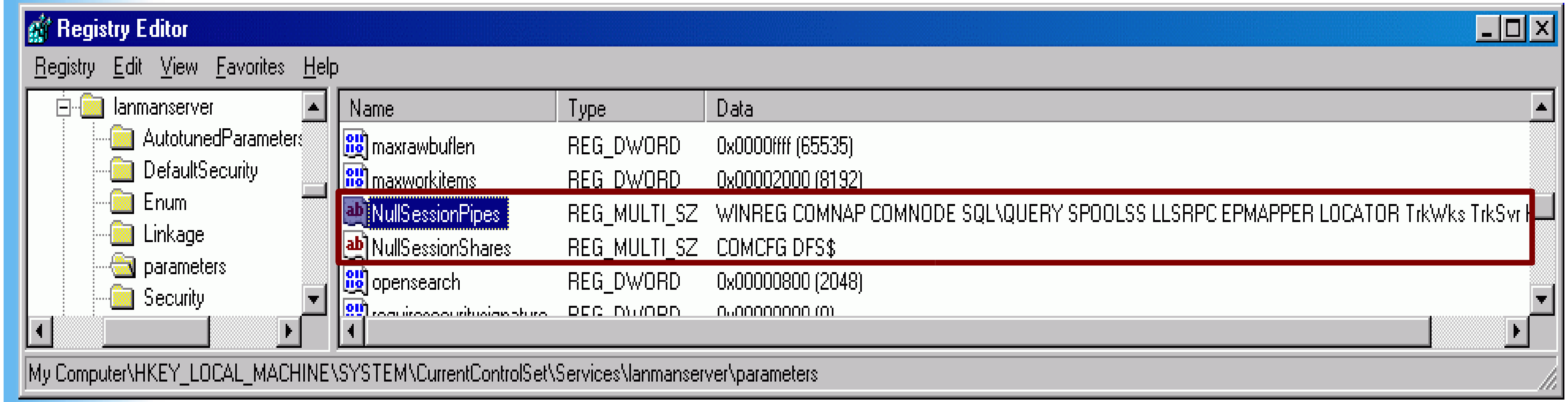
- NULL session
  - Unauthenticated SMB session to the IPC$ share
    - Actually, authentication is realized with empty username and password, hence the NULL session terminology
    - Can be used by an attacker to gather information about a remote system
    - Using RPC calls over the ncacn_np transport

NULL sessions: access control

- Access controls involved in a NULL session
  - IPC$ share connection: always (implictly) permitted
    - IPC$ missing in the NullSessionShares registry value
  - Named pipes access: named pipe dependent
    - NullSessionPipes registry value + hardcoded names
  - Runtime (RPC operations) checks
    - At runtime + DACL on SAM and LSA objects
    - Access control, using the impersonation token of the NULL session

NULL sessions: registry values

- Registry values
  - NullSessionShares: shares to which it is possible to connect with a NULL session
  - NullSessionPipes: named pipes that can be opened in the context of a NULL session to IPC$

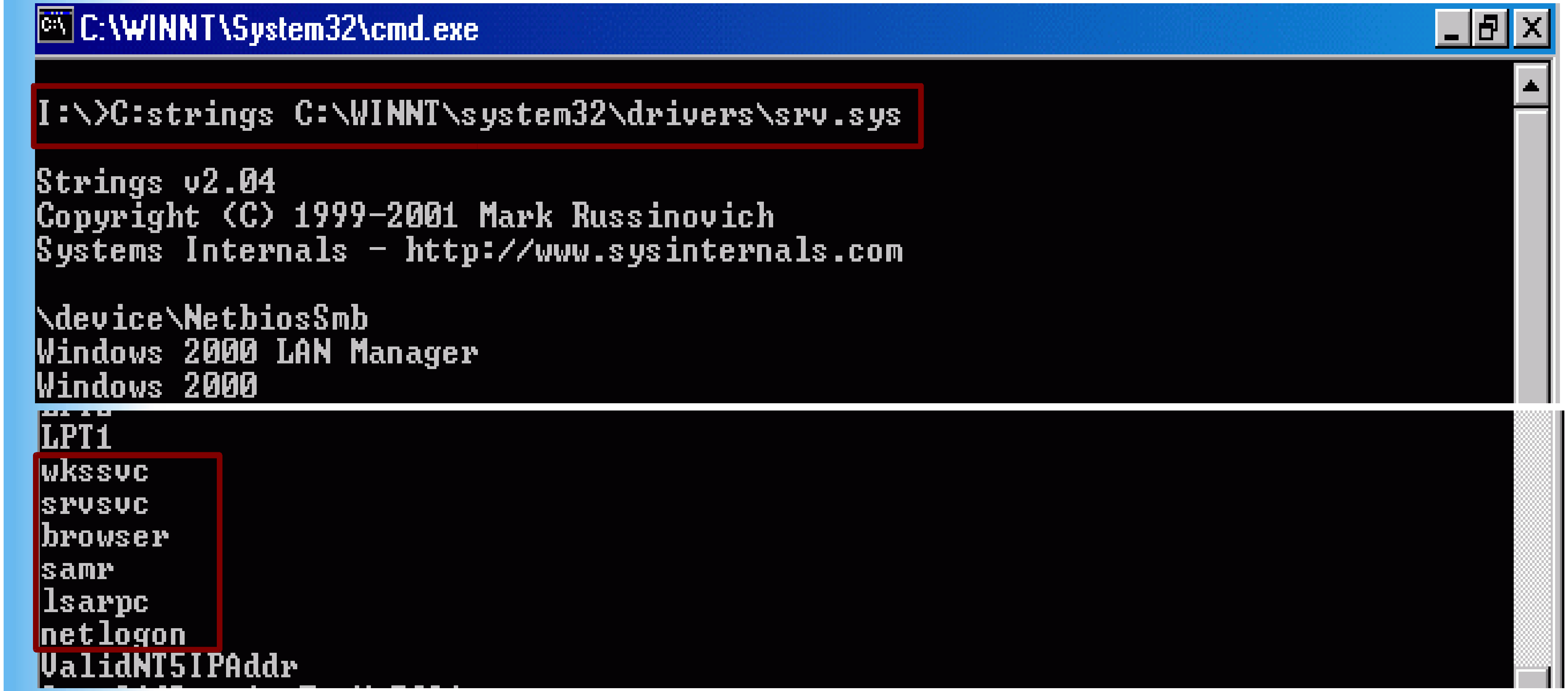


Name	Type	Data
maxrawbuflen	REG_DWORD	0x0000ffff (65535)
maxworkitems	REG_DWORD	0x00002000 (8192)
NullSessionPipes	REG_MULTI_SZ	WINREG COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC EPMAPPER LOCATOR TrkWks TrkSvr
NullSessionShares	REG_MULTI_SZ	COMCFG DFS$
opensearch	REG_DWORD	0x00000800 (2048)
requiresecuritysignature	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

NULL sessions: implictly allowed named pipes

- Hardcoded named pipes (srv.sys)
  - \pipe\{lsarpc,samr,netlogon,wkssvc,srvsvc,browser}



```
I:\>C:strings C:\WINNT\system32\drivers\srv.sys

Strings v2.04
Copyright (C) 1999-2001 Mark Russinovich
Systems Internals - http://www.sysinternals.com

\device\NetbiosSmb
Windows 2000 LAN Manager
Windows 2000
```

```
LPT1
wkssvc
srvsvc
browser
samr
lsarpc
netlogon
ValidNT5IPAddr
```

NULL session: impersonation token

- NULL session impersonation token
  - By default, contains the EVERYONE SID
    - Anything allowed for the EVERYONE SID is possible in a NULL session
  - Registry values
    - RestrictAnonymous: NT4, W2K
      - When set to 2, removes EVERYONE from the token
    - EveryoneIncludesAnonymous: WXP, W2K3
      - When unset, equivalent to RestrictAnonymous == 2

RPC services: NT 4.0 domains

- NT 4.0 domains
  - Use RPC services, using named pipes endpoints
  - Typical named pipes
    - lsarpc: LSA (Local Security Authority) RPC service
    - samr: SAM (Security Account Manager) RPC service
    - netlogon : netlogon RPC service

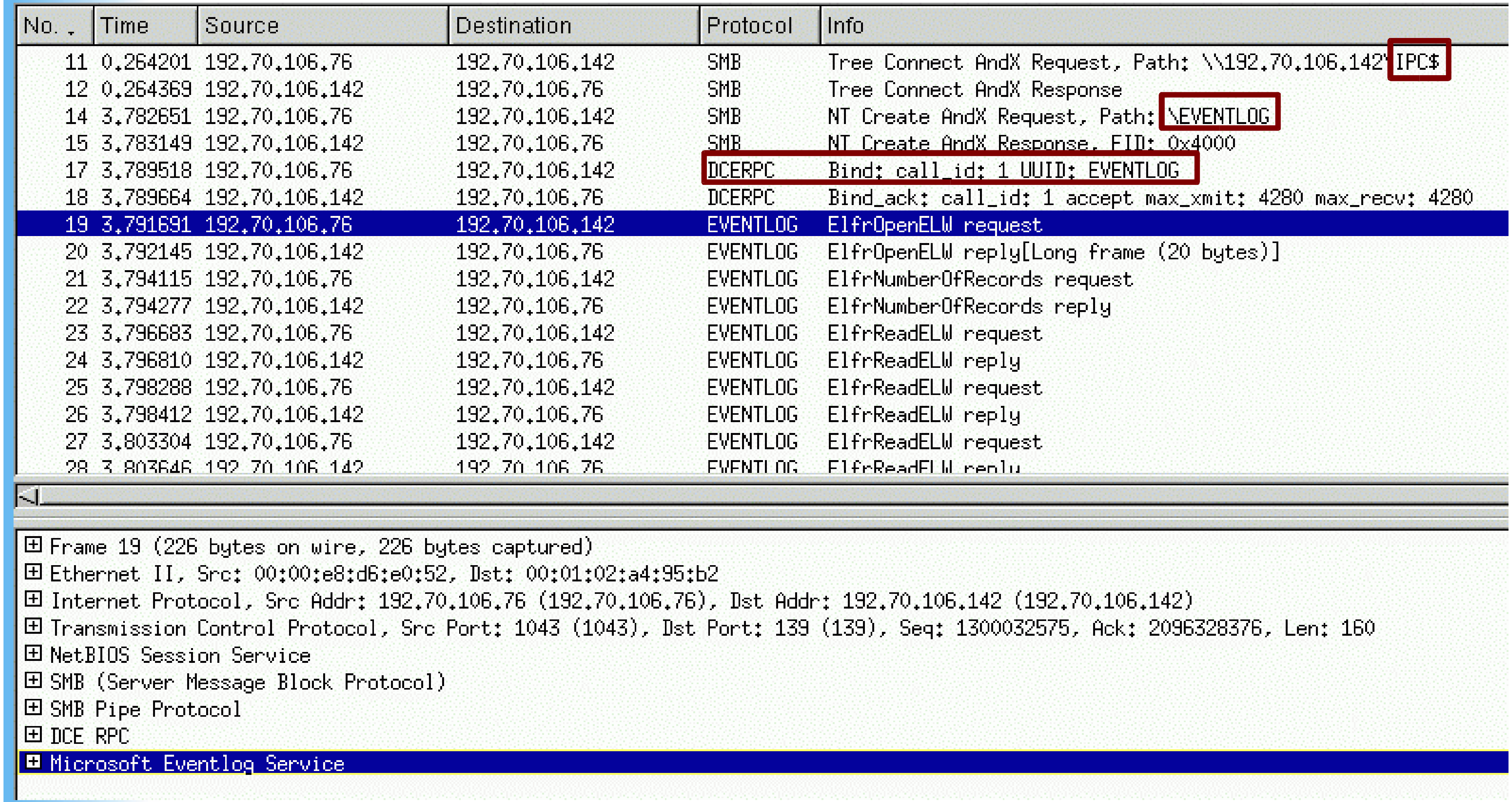
RPC services: administration tools

- Windows administration tools
  - Administration API use RPC functions
  - Different transports are used for a local or a remote system
    - Local system: ncalrpc or ncacn_np transports
    - Remote system: ncacn_np transport

RPC-based administration tools

- RPC-based administration tools
  - server manager, services manager, registry editor, event viewer, IIS administration, dns server, task scheduler, certificate service, ...
  - Named pipes (endpoints) names identify the service
    - svcctl (services management), winreg (remote registry), inetinfo (iis5), eventlog (eventlog service), ...
  - New administration tools use WMI
    - thus DCOM, thus RPC services over TCP/IP

Remote administration: example



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
```

MSRPC security: transport protocols

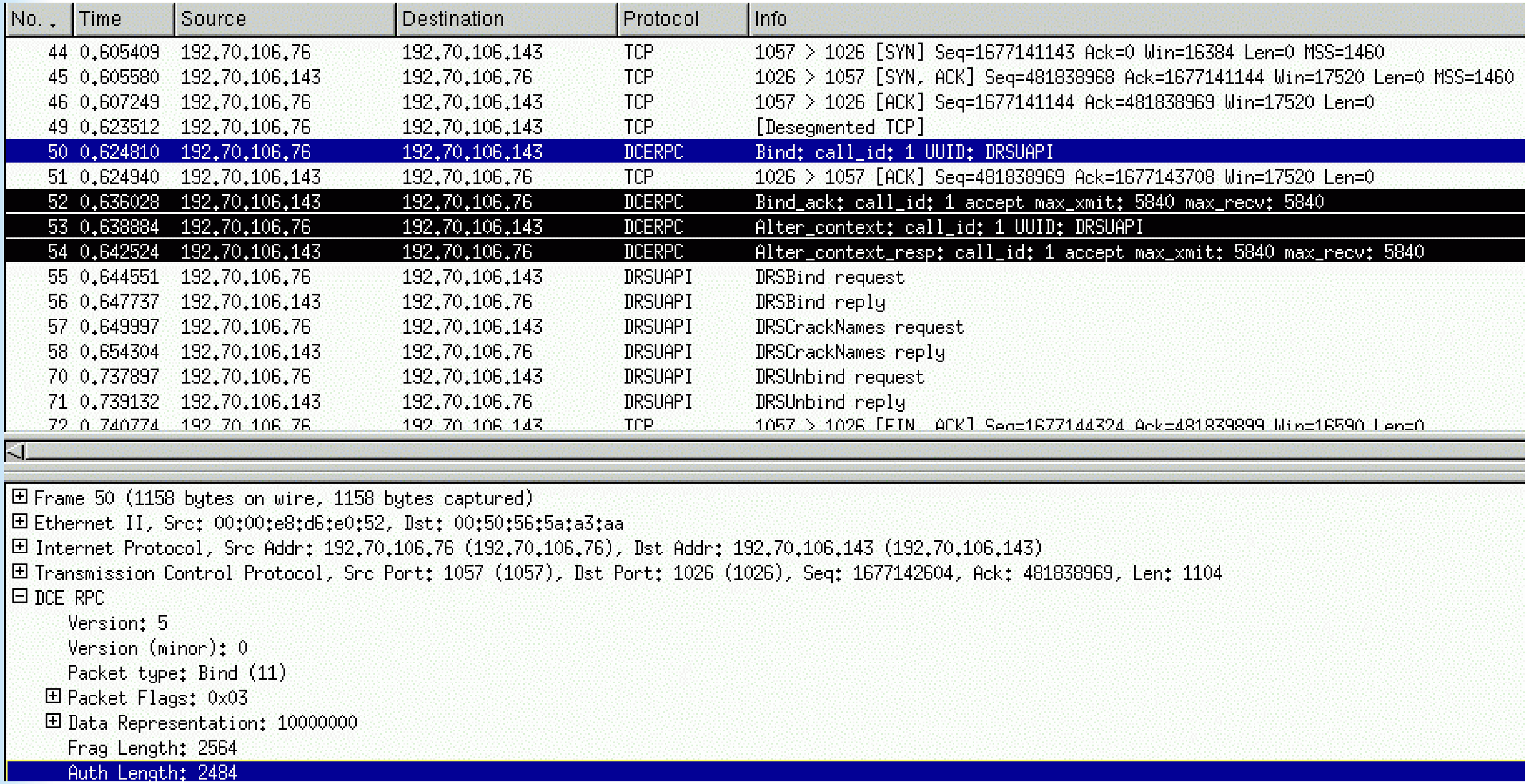
- Protocol sequences that can be reached remotely
  - A RPC service that listen on TCP/IP can be reached remotely
    - Most RPC services listening on TCP/IP are bound to all network interfaces (0.0.0.0)
    - For some RPC services, it is possible to configure interfaces binding restrictions
      - http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html
  - A RPC service that listen on named pipes can be reached remotely
    - If the server service is running and bound to a network adapter

MSRPC security: authentication

- RPC services: authentication
  - ncacn_np (named pipes)
    - Authenticated at the SMB level (SMB session authentication)
      - But NULL sessions allow unauthenticated calls to RPC services
  - ncacn_ip_tcp, ncadg_ip_udp
    - Most Active Directory RPC services require authentication
      - at the DCE RPC level
        - Bind, Alter Context DCE RPC PDUs
    - Legacy RPC services do not require authentication
      - Example: MSRPC services running in the Messenger service
        - MS03-043 security bulletin, vulnerability published by LSD

RPC authentication: ncacn_ip_tcp

- SPNEGO authentication (NTLM or Kerberos V)



No.	Time	Source	Destination	Protocol	Info
44	0.605409	192.70.106.76	192.70.106.143	TCP	1057 > 1026 [SYN] Seq=1677141143 Ack=0 Win=16384 Len=0 MSS=1460
45	0.605580	192.70.106.143	192.70.106.76	TCP	1026 > 1057 [SYN, ACK] Seq=481838968 Ack=1677141144 Win=17520 Len=0 MSS=1460
46	0.607249	192.70.106.76	192.70.106.143	TCP	1057 > 1026 [ACK] Seq=1677141144 Ack=481838969 Win=17520 Len=0
49	0.623512	192.70.106.76	192.70.106.143	TCP	[Desegmented TCP]
50	0.624810	192.70.106.76	192.70.106.143	DCERPC	Bind: call_id: 1 UUID: DRSUAPI
51	0.624940	192.70.106.143	192.70.106.76	TCP	1026 > 1057 [ACK] Seq=481838969 Ack=1677143708 Win=17520 Len=0
52	0.636028	192.70.106.143	192.70.106.76	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840
53	0.638884	192.70.106.76	192.70.106.143	DCERPC	Alter_context: call_id: 1 UUID: DRSUAPI
54	0.642524	192.70.106.143	192.70.106.76	DCERPC	Alter_context_resp: call_id: 1 accept max_xmit: 5840 max_recv: 5840
55	0.644551	192.70.106.76	192.70.106.143	DRSUAPI	DRSBind request
56	0.647737	192.70.106.143	192.70.106.76	DRSUAPI	DRSBind reply
57	0.649997	192.70.106.76	192.70.106.143	DRSUAPI	DRSCrackNames request
58	0.654304	192.70.106.143	192.70.106.76	DRSUAPI	DRSCrackNames reply
70	0.737897	192.70.106.76	192.70.106.143	DRSUAPI	DRSUnbind request
71	0.739132	192.70.106.143	192.70.106.76	DRSUAPI	DRSUnbind reply
72	0.740774	192.70.106.76	192.70.106.143	TCP	1057 > 1026 [FIN, ACK] Seq=1677144324 Ack=481839899 Win=16590 Len=0

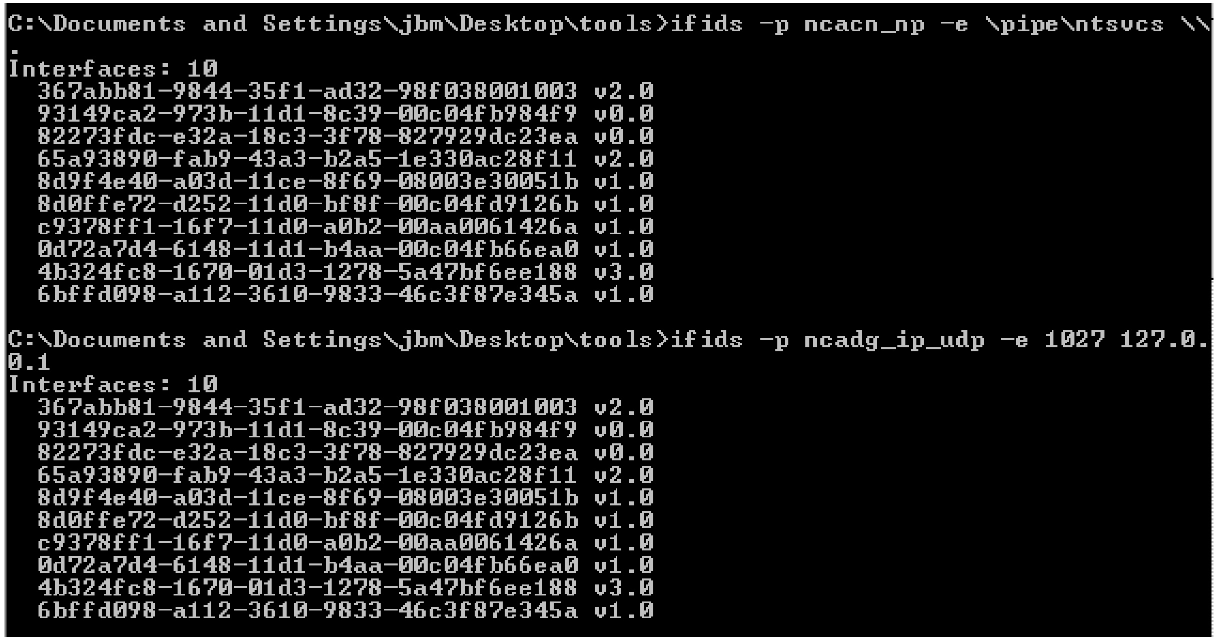
```
⊞ Frame 50 (1158 bytes on wire, 1158 bytes captured)
⊞ Ethernet II, Src: 00:00:e8:d6:e0:52, Dst: 00:50:56:5a:a3:aa
⊞ Internet Protocol, Src Addr: 192.70.106.76 (192.70.106.76), Dst Addr: 192.70.106.143 (192.70.106.143)
⊞ Transmission Control Protocol, Src Port: 1057 (1057), Dst Port: 1026 (1026), Seq: 1677142604, Ack: 481838969, Len: 1104
⊟ DCE RPC
     Version: 5
     Version (minor): 0
     Packet type: Bind (11)
   ⊞ Packet Flags: 0x03
   ⊞ Data Representation: 10000000
     Frag Length: 2564
     Auth Length: 2484
```

MSRPC implementation quirks

- MSRPC implementation quirks
  - Inside a given process, all RPC services can be reached using any opened endpoints!
    - If one RPC service listens on a TCP port or a named pipe, all RPC services running in the hosting process can be reached using this endpoint
    - Even if a RPC service only listens on a local-only transport (ncalrpc), it might be exposed to the outside
    - Most Windows services run in shared processes (services.exe, svchost.exe)
      - thus RPC services run by Windows services can be reached using any opened endpoint

services.exe RPC services: example

- services.exe RPC services
  - All RPC services running inside W2K services.exe process can be reached, using either a named pipe or a UDP port as endpoint



```
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
```

RPC services protection

- RPC services protection
  - RPC services exposure problem acknowledged by Microsoft
    - New APIs: RpcServerRegisterIfEx(), RpcServerRegisterIf2()
    - Allow specification of a security-callback function, on a per-interface basis
    - Can be used to verify that the protocol sequence used by a client is legal
      - Example: W2K3 lsasrv.dll: 3 RPC services use RpcServerRegisterIfEx() with a security-callback function that verifies the protocol sequence
        - Ex: 1cbcad78-df0b-4934-b558-87839ea501c9 v0.0 (dsrole)
          - Only reachable locally, via the dsrole LPC port

ncalrpc vs ncacn_np

- Many RPC services are locally used by Windows components
  - ncalrpc protocol sequence
  - However, some RPC services also listen on ncacn_np protocol sequence at the same time
    - Not very clear why (when RPC services are not supposed to be reached remotely)
    - Example of the File Protection Subsystem RPC service
      - Typically a local-only RPC interface
      - W2K and WXP endpoints: SfcApi named pipe, SfcApi LPC port
      - Windows Server 2003 endpoint: SfcApi LPC port **only**
    - It seems that Windows Server 2003 RPC services choose more carefully their protocol sequences

MSRPC vulnerabilities

- MSRPC vulnerabilities
  - Past vulnerabilities
    - MS01-041: Malformed RPC Request Can Cause Service Failure
    - MS01-048: Malformed RPC Request to RPC Endpoint Mapper can Cause RPC Service to Fail (Windows NT 4.0)
    - MS03-001: Unchecked Buffer in Locator Service Could Lead to Code Execution
    - MS03-010: Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks

MSRPC vulnerabilities, cont.

- MSRPC vulnerabilities
  - Recent vulnerabilities
    - MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution
      - Published by the LSD research group: http://www.lsd-pl.net
      - Vulnerability affecting RPC interfaces in the rpcss service, which opens the following endpoints
        - 135/tcp (ncacn_ip_tcp), 135/udp (ncadg_ip_udp), \pipe\epmapper (ncacn_np), epmapper LPC port (ncalrpc)
        - Typically exploitable via 135/tcp
    - Other vulnerability discovered
      - Microsoft Windows 2000 RPC DCOM Interface DOS AND Privilege Escalation Vulnerability
        - Flashsky (Xfocus)

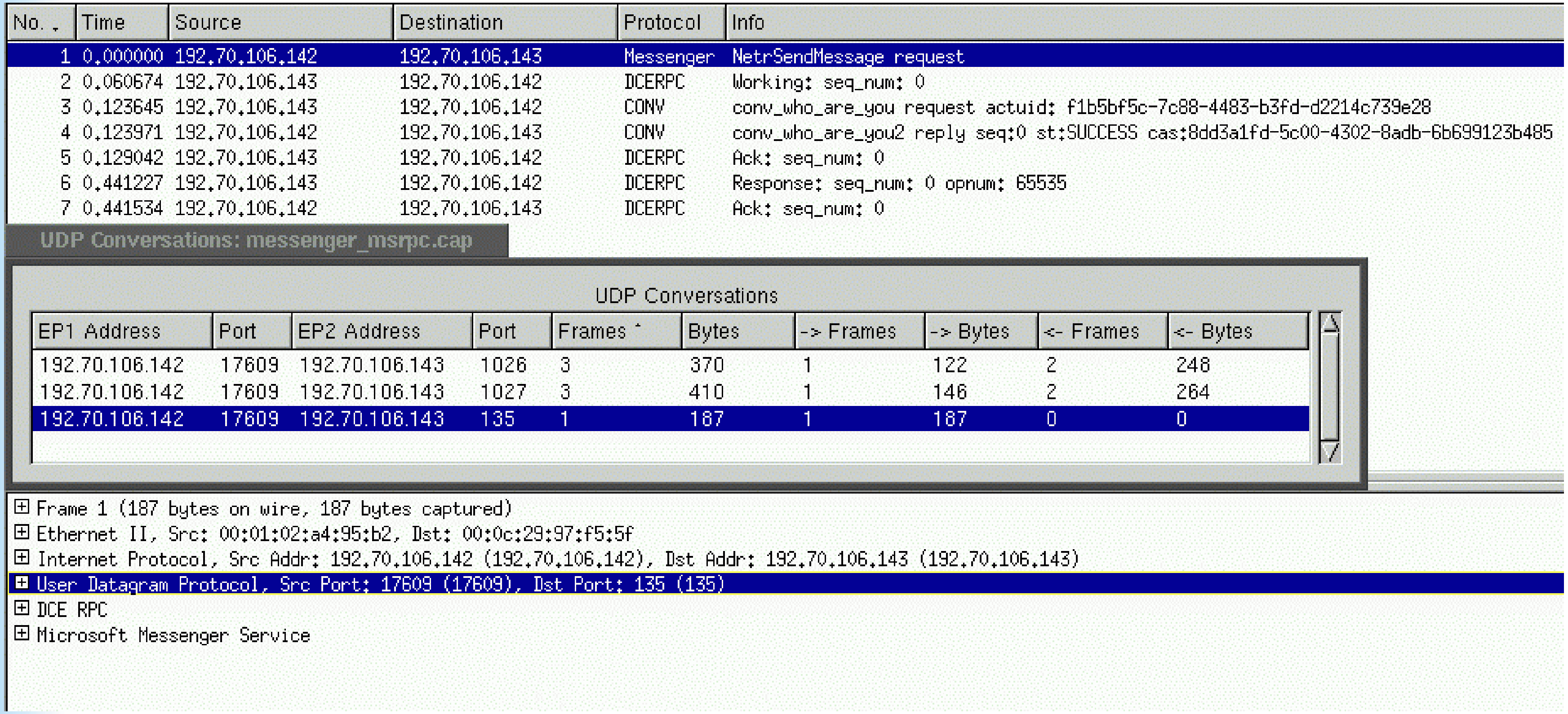
MSRPC vulnerabilities, cont.

- MSRPC vulnerabilities, cont.
  - Recent vulnerabilities
    - MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution
      - Was supposed to fix three additional vulnerabilities of RPC/ORPC services running in the rpcss service
      - Discovered by Tenable Network Security (Xue Yong Zhi and Renaud Deraison), NSFOCUS Security Team and eEye
      - It seems that a denial of service attack is still possible on systems with MS03-039 applied (as disussed on bugtraq@ on 2003/10/10)

MSRPC vulnerabilities, cont.

- MSRPC vulnerabilities, cont.
  - Recent vulnerabilities
    - MS03-043: Buffer Overrun in Messenger Service Could Allow Code Execution
      - Published by LSD
      - Windows Messenger service runs two RPC services, which can be used to send popup messages over MSRPC, via UDP (ncadg_ip_udp)
        - In addition to the traditional SMB transport
      - The RPC transport was already "exploited" to send popup spam (see http://www.mynetwatchman.com/kb/security/articles/popupspam/)
      - Another specificity of the MSRPC implementation is that it is possible to reach a RPC service listening on ncadg_ip_udp via 135/udp
        - See next slide

Messenger RPC service (ncadg_ip_udp)



```
No. .  Time     Source          Destination     Protocol   Info
    1 0.000000 192.70.106.142  192.70.106.143  Messenger  NetrSendMessage request
    2 0.060674 192.70.106.143  192.70.106.142  DCERPC     Working: seq_num: 0
    3 0.123645 192.70.106.143  192.70.106.142  CONV       conv_who_are_you request actuid: f1b5bf5c-7c88-4483-b3fd-d2214c739e28
    4 0.123971 192.70.106.142  192.70.106.143  CONV       conv_who_are_you2 reply seq:0 st:SUCCESS cas:8dd3a1fd-5c00-4302-8adb-6b699123b485
    5 0.129042 192.70.106.143  192.70.106.142  DCERPC     Ack: seq_num: 0
    6 0.441227 192.70.106.143  192.70.106.142  DCERPC     Response: seq_num: 0 opnum: 65535
    7 0.441534 192.70.106.142  192.70.106.143  DCERPC     Ack: seq_num: 0
```

UDP Conversations

EP1 Address	Port	EP2 Address	Port	Frames	Bytes	-> Frames	-> Bytes	<- Frames	<- Bytes
192.70.106.142	17609	192.70.106.143	1026	3	370	1	122	2	248
192.70.106.142	17609	192.70.106.143	1027	3	410	1	146	2	264
192.70.106.142	17609	192.70.106.143	135	1	187	1	187	0	0

```
⊞ Frame 1 (187 bytes on wire, 187 bytes captured)
⊞ Ethernet II, Src: 00:01:02:a4:95:b2, Dst: 00:0c:29:97:f5:5f
⊞ Internet Protocol, Src Addr: 192.70.106.142 (192.70.106.142), Dst Addr: 192.70.106.143 (192.70.106.143)
⊞ User Datagram Protocol, Src Port: 17609 (17609), Dst Port: 135 (135)
⊞ DCE RPC
⊞ Microsoft Messenger Service
```

MSRPC security: conclusion

- MSRPC implementation is apparently fragile...
  - .. but MSRPC is here to stay
    - core Windows technology
  - Possible workarounds
    - Minimizing running RPC services
    - Using IP filtering
      - Including ports used by additional protocol sequences
        - 139/tcp, 445/tcp for ncacn_np
        - 593/tcp for ncacn_http

References: books

- 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.
    - http://www.ubiqx.org/cifs

References: tools

- Tools
  - Sysinternals tools
    - Filemon, regmon, Process Exploter, PsTools, TCPView, TDIMon, ...
    - http://www.sysinternals.com
  - Todd Sabin's tools
    - RPC Tools, PipeACL Tools, ACL tools
    - http://razor.bindview.com
  - Dave Aitel's SPIKE toolkit
    - dcedump, ifids
    - http://www.immunitysec.com

Reference: Ethereal

- Ethereal: open-source network analyzer
  - Simply the best network analyzer! (Unix & Windows)
  - Windows-related protocols particularly well dissected
    - NetBT, SMB/CIFS
    - DCE RPC (most packet-dcerpc-* dissectors are for MSRPC interfaces)
    - Network authentication protocols: NTLMSSP, Kerberos V (including SPNEGO)
    - Looking at Windows network trafic is the only way to understand how Windows networks really work!
  - http://www.ethereal.com

References: TCP/IP stack

- Windows TCP/IP stack
  - Windows Network Data and Packet Filtering
    - http://www.ndis.com/papers/winpktfilter.htm
  - Microsoft Windows 2000 TCP/IP Implementation Details
    - http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.asp

References: other publications

- Other publications
  - Documents
    - Windows network services internals
      - Research paper on which this presentation is based
      - http://www.hsc.fr/ressources/articles/win_net_srv/
    - Minimizing Windows network services
      - Describes a possible methodology to close all TCP and UDP ports on a Windows system
      - http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html
  - Presentation
    - Windows network services for Samba folks
      - http://www.hsc.fr/ressources/presentations/sambaxp2003/

Thanks!

- Thanks to people working on Windows systems research!
  - Samba community
  - Ethereal community
  - Security community
  - You know who you are!

Questions?

Thank you!