Windows network services for Samba folks

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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
Agenda

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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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_Tcpipl)
    - 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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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)

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
net use

C: \ net use \192.70.106.131\B$ /try
 net use \192.70.106.131\PC$ /try

(net use command output)

Status Local Remote Network
OK \192.70.106.131\B$ Microsoft Windows Network
OK \192.70.106.131\PC$ Microsoft Windows Network

The command completed successfully.

(net use command output)

Computer User name Client Type Opens Idle time
\192.70.106.142 Windows 2000 21:95 0 00:07:43
\192.70.106.142 JBM Windows 2000 21:95 0 00:06:28

The command completed successfully.

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

```bash
C:\> net use \192.168.106.142\IPC$ /u:jbm
Type the password for \192.168.106.142\IPC$:
The command completed successfully.

C:\> net use \192.168.106.142\IPC$/u: w
Type the password for \192.168.106.142\IPC$:
System error 1219 has occurred.
The credentials supplied conflict with an existing set of credentials.

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

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Local</th>
<th>Remote</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>\192.168.106.142\IPC$</td>
<td></td>
<td>Microsoft Windows Network</td>
</tr>
<tr>
<td>OK</td>
<td>\fenetre.hsc.fr\IPC$</td>
<td></td>
<td>Microsoft Windows Network</td>
</tr>
</tbody>
</table>

The command completed successfully.

```text
Multiple sessions

<table>
<thead>
<tr>
<th>Computer</th>
<th>User name</th>
<th>Client Type</th>
<th>Opens Idle time</th>
</tr>
</thead>
<tbody>
<tr>
<td>\192.168.106.142</td>
<td></td>
<td>Windows 2000 2175</td>
<td>0:00:00:00</td>
</tr>
<tr>
<td>\192.168.106.142</td>
<td>JBM</td>
<td>Windows 2000 2175</td>
<td>0:00:00:21</td>
</tr>
</tbody>
</table>
```

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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$)

<table>
<thead>
<tr>
<th>Computer</th>
<th>User name</th>
<th>Client Type</th>
<th>Opened Idle time</th>
</tr>
</thead>
<tbody>
<tr>
<td>\HSC</td>
<td>JBM</td>
<td>Unix</td>
<td>1:00:00:00</td>
</tr>
</tbody>
</table>

The command completed successfully.

C:\\net share IPC$  
Share name: IPC$  
Path: \HSC  
Remain users: JBM  
The command completed successfully.

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

C:\\net files  
\HSC /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

(c) Jean-Baptiste Marchand - jbm@hsd.fr - samba eXPerience 2003
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)

![Pipe List](image)

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
## Named pipes (Windows XP)

![Pipe list screenshot]

(c) Jean-Baptiste Marchand - jbm@hsfr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
npfs aliases (NT, 2K, {XP, 2K3})

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
Ifids: named pipes endpoints

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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, Ptools, TCPView...

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

<table>
<thead>
<tr>
<th>Time</th>
<th>Process</th>
<th>Request</th>
<th>Path</th>
<th>Result</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:56:24</td>
<td>services.exe 200</td>
<td>OPEN</td>
<td>\192.168.254.4\user\</td>
<td>SUCCESS</td>
<td>Options: Open/Access</td>
</tr>
<tr>
<td>00:56:24</td>
<td>services.exe 200</td>
<td>QUERY INFORMATION</td>
<td>\192.168.254.4\user\</td>
<td>SUCCESS</td>
<td>FileReadDeviceInformation</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>OPEN</td>
<td>\192.168.254.4\</td>
<td>SUCCESS</td>
<td>Options: Open/Directory</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>QUERY INFORMATION</td>
<td>\192.168.254.4\user\</td>
<td>SUCCESS</td>
<td>FileReadInformation</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>CLOSE</td>
<td>\192.168.254.4\</td>
<td>SUCCESS</td>
<td>FileWriteInformation</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>QUERY INFORMATION</td>
<td>Documents and Settings\Users\Desktop\Tools</td>
<td>SUCCESS</td>
<td>Attributes: OA</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>QUERY INFORMATION</td>
<td>Documents and Settings\Users\Desktop\Tools</td>
<td>SUCCESS</td>
<td>Attributes: OA</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>OPEN</td>
<td>\192.168.254.4\</td>
<td>SUCCESS</td>
<td>Options: Open/Directory</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>QUERY INFORMATION</td>
<td>Documents and Settings\Users\Desktop\Tools</td>
<td>SUCCESS</td>
<td>FileReadInformation</td>
</tr>
<tr>
<td>00:56:36</td>
<td>cmd.exe 1026</td>
<td>QUERY INFORMATION</td>
<td>Documents and Settings\Users\Desktop\Tools</td>
<td>SUCCESS</td>
<td>FileWriteInformation</td>
</tr>
</tbody>
</table>

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXperience 2003
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
References

• Books
  • *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/](http://www.ubiqx.org/cifs/)

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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

(c) Jean-Baptiste Marchand - jbm@hsc.fr - samba eXPerience 2003
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!