



# **MSRPC NULL sessions**

## **Exploitation and protection**

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

- Introduction to NULL sessions
- NULL sessions internals
- Tools to exploit NULL sessions
- NULL sessions restrictions
- Default NULL session restrictions on Windows systems
  - Windows 2000
  - Windows XP (SP0, SP1a), Windows XP SP2
  - Windows Server 2003, Windows Server 2003 SP1
  - Active Directory domain controllers
- Hardening recommendations
- Conclusion

- NULL sessions have already been discussed in the past
  - Still, interesting and new things to discuss
- NULL sessions are used to anonymously call RPC operations on a remote system
  - NULL sessions are **unauthenticated** SMB sessions
  - SMB is Windows core network protocol, **not to be confused with NetBIOS!**
  - SMB operates over
    - 139/TCP (NetBIOS over TCP/IP transport)
    - 445/TCP (raw SMB transport, directly into TCP)
  - Recent Windows systems also run RPC services over TCP/IP
    - It is also possible to anonymously call RPC operations over TCP/IP

## Steps to establish a NULL session

- TCP connection to port 445/tcp or 139/tcp
  - NetBIOS session establishment if the NetBT transport is used (139/tcp)
- SMB session establishment, authenticated with NULL credentials (empty login and password)
- Connection to **IPC\$** share
- Opening of a named pipe
  - Ex : `\pipe\samr` to reach the SAM RPC server
- Binding to a DCE-RPC interface
  - A DCE-RPC interface is identified by a UUID
  - No additional authentication required, already done at the SMB level
- Call of RPC operations

# NULL session: network trace

	Source	Destination	Protocol	Info
1	192.70.106.76	192.70.106.144	TCP	55777 > 445 [SYN] Seq=719055985 Ack=0 Win=65535 Len=0 MSS=
2	192.70.106.144	192.70.106.76	TCP	445 > 55777 [SYN, ACK] Seq=3192492925 Ack=719055986 Win=16
3	192.70.106.76	192.70.106.144	TCP	55777 > 445 [ACK] Seq=719055986 Ack=3192492926 Win=33304 L
4	192.70.106.76	192.70.106.144	SMB	Negotiate Protocol Request
5	192.70.106.144	192.70.106.76	SMB	Negotiate Protocol Response
6	192.70.106.76	192.70.106.144	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
7	192.70.106.144	192.70.106.76	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STf
8	192.70.106.76	192.70.106.144	SMB	Session Setup AndX Request, NTLMSSP_AUTH
9	192.70.106.144	192.70.106.76	SMB	Session Setup AndX Response
10	192.70.106.76	192.70.106.144	SMB	Tree Connect AndX Request, Path: \\192.70.106.144\IPC\$
11	192.70.106.144	192.70.106.76	SMB	Tree Connect AndX Response
12	192.70.106.76	192.70.106.144	SMB	NT Create AndX Request, Path: \samr
13	192.70.106.144	192.70.106.76	SMB	NT Create AndX Response, FID: 0x400b
14	192.70.106.76	192.70.106.144	DCERPC	Bind: call_id: 1 UUID: SAMR
15	192.70.106.144	192.70.106.76	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 4280 max_recv: 4280
16	192.70.106.76	192.70.106.144	SAMR	SamrConnect request[Long frame (10 bytes)]
17	192.70.106.144	192.70.106.76	SAMR	SamrConnect response
18	192.70.106.76	192.70.106.144	SAMR	SamrEnumerateDomainsInSamServer request
19	192.70.106.144	192.70.106.76	SAMR	SamrEnumerateDomainsInSamServer response
20	192.70.106.76	192.70.106.144	SAMR	SamrCloseHandle request, ConnectAnon handle
21	192.70.106.144	192.70.106.76	SAMR	SamrCloseHandle response

## How a NULL session can fail?

- SMB-related ports (445/tcp, 139/tcp) filtered or disabled
  - IP filtering, Server service not bound to the network adapter, ...
- Server service refusing unauthenticated SMB sessions
  - Only theoretical, never happens in practice
- **IPC\$** share disabled
  - Before Windows XP, **IPC\$** might be deleted (`net share IPC$ /delete`)
- **Named pipe can not be opened anonymously**
  - XP SP2, W2K3 SP1: named pipe might be forbidden, even for authenticated sessions (named pipe firewall)
- DCE-RPC server refusing unauthenticated bind requests
- Individual operations inside a DCE-RPC interface implementing access control

- Interesting named pipes for NULL sessions
  - `\pipe\samr`: SAM (Security Account Manager) RPC server
  - `\pipe\lsarpc`: LSA (Local Security Authority) RPC server
  - `\pipe\netlogon`: Netlogon RPC server
  - `\pipe\svcctl`: SCM (Service Control Manager) RPC server
  - `\pipe\eventlog`: Eventlog service RPC server
  - `\pipe\srvsvc`: Server service RPC server
  - `\pipe\wkssvc`: Workstation service RPC server
- Details of these interfaces:
  - [http://www.hsc.fr/ressources/articles/win\\_net\\_srv/](http://www.hsc.fr/ressources/articles/win_net_srv/)

## Hardcoded named pipes (1/2)

- The [NullSessionPipes](#) registry value is supposed to contain named pipes allowed to be opened anonymously
- Up to Windows XP SP2 and Windows 2003 SP1, 6 named pipes are **always implicitly allowed to be opened anonymously**
  - [\pipe\lsarpc](#) [\pipe\samr](#) [\pipe\netlogon](#)
  - [\pipe\wkssvc](#) [\pipe\svrsvc](#) [\pipe\browser](#)
- **Particularly misleading**, as these 6 named pipes do not appear in the [NullSessionPipes](#) registry value
- Sidenote: [NullSessionPipes](#) can not be modified to protect against recent MSRPC vulnerabilities
  - [wkssvc](#) vulnerability (MS03-049)
  - [dssetup](#) vulnerability (MS04-011)

- Microsoft removed hardcoded named pipes in
  - Windows XP SP2
  - Windows 2003 SP1
- **NullSessionPipes** now explicitly contains
  - Windows XP SP2
    - `\pipe\browser`
  - Windows 2003 SP1
    - `\pipe\lsarpc`
    - `\pipe\samr`
    - `\pipe\netlogon`
    - `\pipe\browser`

- Windows named pipes are implemented by a file system driver
  - [npfs.sys](#) : named pipe file system driver
- Named pipes file system related tools (Sysinternals)
  - [pipelist](#): named pipes enumeration
  - [filemon](#): file systems activity, including npfs
  - [pipeacl](#): named pipes security descriptor viewer
- The npfs driver supports aliases
  - Alias names stored in the registry
    - [HKLM\SYSTEM\CurrentControlSet\Services\Npfs\Aliases\](#) key
    - Two values : [lsass](#) and [ntsvcs](#)
  - Some named pipes do not exist in the npfs namespace but are aliases of either [lsass](#) or [ntsvcs](#)

# Named pipes aliases

- Named pipe aliases
  - `\pipe\lsass` aliases :
    - Windows 2000: `\pipe\lsarpc`, `\pipe\samr`, `\pipe\netlogon`
    - Windows 2003: `\pipe\lsarpc`, `\pipe\samr`, `\pipe\netlogon`, `\pipe\protected_storage`
  - `\pipe\ntsvcs` aliases
    - Windows 2000: `\pipe\srvc`, `\pipe\wkssvc`, `\pipe\svccntl`, `\pipe\eventlog`, ...
    - Windows 2003: `\pipe\svccntl`, `\pipe\eventlog`
  - <http://www.hsc.fr/ressources/presentations/sambaxp2003/slide21.html>
- Immediate consequence
  - All aliases of `\pipe\lsass` are equivalent
  - All aliases of `\pipe\ntsvcs` are equivalent

# Named pipe and MSRPC

- MSRPC: all RPC services running inside a process can be reached using any opened endpoint
  - Most Windows services run RPC services and are executed in shared processes ([lsass.exe](#), [services.exe](#), [svchost.exe](#))
- RPC services need to register a security callback function to avoid this vulnerability
  - The security callback function must verify if the expected endpoint was used
  - [RpcServerRegister2\(\)](#) and [RpcServerRegisterIfEx\(\)](#) APIs
  - [http://msdn.microsoft.com/library/en-us/rpc/rpc/be\\_wary\\_of\\_other\\_rpc\\_endpoints\\_running\\_in\\_the\\_same\\_process.asp](http://msdn.microsoft.com/library/en-us/rpc/rpc/be_wary_of_other_rpc_endpoints_running_in_the_same_process.asp)

- **rpcclient**
  - Command-line tool implementing interesting MSRPC interfaces
  - Two versions (Samba-TNG, Samba), supporting different set of MSRPC operations
  - Samba4's rpcclient currently in development (using Python wrappers)
- **Nessus NASL scripts**
  - Tenable recently developed new SMB and MSRPC implementations for Nessus
  - Some NASL scripts can be used standalone, with the [nasl](#) command

- Opening a named pipe that can be opened anonymously
  - Either one of the six hardcoded named pipes or one appearing in `NullSessionPipes`
- Binding to the RPC interface supported by the named pipe
- Examples
  - Opening `\pipe\lsarpc` and binding to `lsarpc`
  - Opening `\pipe\samr` and binding to `samr`
  - Opening `\pipe\netlogon` and binding to `netlogon`
  - Opening `\pipe\svrsvc` and binding to `svrsvc`
  - Opening `\pipe\wkssvc` and binding to `wkssvc`
  - ...

# Using NULL sessions: the new way

- Opening a named pipe that can be opened anonymously
  - Either one of the six hardcoded named pipes or one appearing in [NullSessionPipes](#)
- Binding to **one of the RPC interfaces** run by services running inside the process that created the named pipe
- Examples
  - Opening [\pipe\{srvsvc,wkssvc,browser}](#) and binding to [svcctl](#) or [eventlog](#)
    - Supported by Windows 2000's [services.exe](#) process (fixed by Update Rollup 1 for Windows 2000 SP4)
  - Opening [\pipe\browser](#) and binding to [wkssvc](#) or [srvsvc](#) in Windows XP SP2 and Windows Server 2003 SP1

# Modifying named pipes

- Most RPC implementations hardcode named pipes for each RPC service
  - Example: MSRPC (Windows implementation), rpcclient, ...
- Named pipe names have to be modified on the fly
  - SMB signing does not exist for NULL sessions
  - [netsed](#) is the perfect tool to modify named pipe names
    - thanks to Thomas Seyrat for suggesting it
- Tricks for named pipe name substitution
  - Maintain Unicode encoding
  - Remove \ when the substituted name is one character shorter
  - Add one or several \ when the substituted name is longer

# Anonymous enumeration of Windows 2000 services

Name	Description	Sta...	Startup Type	Log On As
Alerter		Started		Local System
DHCP Client		Started		Local System
Distributed File System		Started		Local System
Distributed Link Tracking Client		Started		Local System
DNS Client		Started		Local System
Event Log		Started		Local System
License Logging Service		Started		Local System
Logical Disk Manager		Started		Local System
Network Connections		Started		Local System
Plug and Play		Started		Local System
Protected Storage		Started		Local System
Remote Registry Service		Started		Local System
Removable Storage		Started		Local System
RunAs Service		Started		Local System
Server		Started		Local System
System Event Notification		Started		Local System
TCP/IP NetBIOS Helper Service		Started		Local System
VMware Tools Service		Started		Local System
Windows Management Instrumentation		Started		Local System
Workstation		Started		Local System
Remote Procedure Call (RPC)	Provides the end...	Started	Automatic	Local System
Security Accounts Manager	Stores security in...	Started	Automatic	Local System
COM+ Event System	Provides automat...	Started	Manual	Local System
Telephony	Provides Telepho...	Started	Manual	Local System
Windows Management Instrumentation Driver...	Provides systems...	Started	Manual	Local System
Computer Browser				Local System

# NULL session restrictions: registry values and security options (1/2)

- **RestrictAnonymous** (Windows NT 4.0 and >)
  - Windows NT 4.0: **0** or 1
  - Windows 2000: **0**, 1 or 2 (disable NULL sessions)
    - *Additional restrictions for anonymous connections* security option
  - Windows XP and Windows 2003: **0** or 1
    - *Network access: Do not allow anonymous enumeration of SAM accounts and shares* security option
- **EveryoneIncludesAnonymous** (Windows XP, Windows 2003)
  - *Network access: Let Everyone permissions apply to anonymous users*
  - Disabled by default (**EVERYONE** does not include **ANONYMOUS LOGON**)

# NULL session restrictions: registry values and security options (2/2)

- **RestrictAnonymousSam** (Windows XP, Windows 2003)
  - *Network access: Do not allow anonymous enumeration of SAM accounts*
  - Enabled by default, preventing anonymous access to **samr**
- *Network access: Allow anonymous SID/Name translation*
  - Disabled by default
  - Modifies the security descriptor on LSA policy object, to deny or allow anonymous SID to name translation
- **TurnOffAnonymousBlock** (Windows 2003)
  - Not present by default, preventing anonymous access to **lsarpc**
  - When present and set to 1, allow anonymous access to **lsarpc**

# NULL session restrictions in Windows 2000 (1/2)

- 6 hardcoded named pipes
- **RestrictAnonymous** set to 0 by default
  - 0: no restriction
  - 1: prevent direct enumeration of accounts and groups using **samr**
  - 2: prevent NULL sessions (anonymous connections to **IPC\$** denied)
- Anonymous access to **samr**
  - Detailed user accounts enumeration
  - Group memberships (including **BUILTIN\Administrators**)
  - Prevented by setting **RestrictAnonymous** to 1
- Anonymous access to **lsarpc**
  - Can be used to translate SID to names to indirectly discover user accounts when **RestrictAnonymous** is set to 1

# NULL session restrictions in Windows 2000 (2/2)

- Anonymous access to [wkssvc](#) and [srvsvc](#)
  - Some hardcoded restrictions, documented in MSDN (*Security requirements* section)
  - Some additional restrictions for [srvsvc](#) operations when [RestrictAnonymous](#) is set to 1
  - Security descriptors for [srvsvc](#) operations stored under the [DefaultSecurity](#) registry key
  - Can be modified in Windows XP and Windows Server 2003 with the TweakUI for Windows XP tool

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.145 -U '%'
Server: \\192.70.106.145:      User:      Domain:
Connection:      OK
[192.70.106.145]$ srvinfo
Server Info Level 101:
      192.70.106.145 Wk Sv NT SNT
      platform_id      :      500
      os version       :      5.0
[192.70.106.145]$ enumusers
SAM Enumerate Users
User RID:      1f4  User Name: Administrator
User RID:      1f5  User Name: Guest
User RID:      3e8  User Name: TsInternetUser
User RID:      3e9  User Name: user
[192.70.106.145]$ samaliasmem BUILTIN\administrators
SAM Query Alias: administrators
From: GARBAREK To: \\192.70.106.145 Domain: BUILTIN SID: S-1-5-32
      Alias Members:
      -----
      W2KDFLT\Administrator (User)
[192.70.106.145]$ █
```

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.145 -U '%'
Server: \\192.70.106.145:      User:      Domain:
wConnection:      OK
[192.70.106.145]$ wksinfo
Name:      W2KDFLT
Domain:    WORKGROUP
Platform:  500
Version:   5.0
[192.70.106.145]$ enumusers
SAM Enumerate Users
SAMR_OPEN_DOMAIN: NT_STATUS_ACCESS_DENIED
SAMR_OPEN_DOMAIN: NT_STATUS_ACCESS_DENIED
enumusers: FAILED
[192.70.106.145]$ lsaquery
LSA Query Info Policy
Domain Member      - Domain: WORKGROUP SID: S-0-0
Domain Controller - Domain: W2KDFLT SID: S-1-5-21-1644491937-299502267-839522115
[192.70.106.145]$ lookupsids S-1-5-21-1644491937-299502267-839522115-1000
Lookup SIDS:
SID: S-1-5-21-1644491937-299502267-839522115-1000 -> W2KDFLT\TsInternetUser (1: User)
[192.70.106.145]$ lookupsids S-1-5-21-1644491937-299502267-839522115-1001
Lookup SIDS:
SID: S-1-5-21-1644491937-299502267-839522115-1001 -> W2KDFLT\user (1: User)
[192.70.106.145]$ █
```

No. .	Source	Destination	Protocol	Info
1	192.70.106.76	192.70.106.145	TCP	49345 > 139 [SYN] Seq=126373878 Ack=0 Win=65535 Len=0 MS
2	192.70.106.145	192.70.106.76	TCP	139 > 49345 [SYN, ACK] Seq=3551907474 Ack=126373879 Win=
3	192.70.106.76	192.70.106.145	TCP	49345 > 139 [ACK] Seq=126373879 Ack=3551907475 Win=33304
4	192.70.106.76	192.70.106.145	NBSS	Session request, to *SMBSERVER<20> from GARBAREK<00>
5	192.70.106.145	192.70.106.76	NBSS	Positive session response
6	192.70.106.76	192.70.106.145	SMB	Negotiate Protocol Request
7	192.70.106.145	192.70.106.76	SMB	Negotiate Protocol Response
8	192.70.106.76	192.70.106.145	SMB	Session Setup AndX Request, User: anonymous
9	192.70.106.145	192.70.106.76	SMB	Session Setup AndX Response
10	192.70.106.76	192.70.106.145	SMB	Tree Connect AndX Request, Path: \\192.70.106.145\IPC\$
11	192.70.106.145	192.70.106.76	SMB	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
12	192.70.106.76	192.70.106.145	SMB	Logoff AndX Request
13	192.70.106.145	192.70.106.76	SMB	Logoff AndX Response
14	192.70.106.76	192.70.106.145	TCP	49345 > 139 [FIN, ACK] Seq=126374314 Ack=3551907770 Win=
15	192.70.106.145	192.70.106.76	TCP	139 > 49345 [FIN, ACK] Seq=3551907770 Ack=126374315 Win=
16	192.70.106.76	192.70.106.145	TCP	49345 > 139 [ACK] Seq=126374315 Ack=3551907771 Win=33303

# NULL session restrictions in Windows XP (SP0 and SP1a)

- 6 hardcoded named pipes
- Anonymous access to **samr** forbidden
  - **RestrictAnonymousSam** registry value set to 1 by default
- Anonymous access to **lsarpc** allowed
  - However, anonymous SID to name translation forbidden
  - Security option **Network access: Allow anonymous SID/Name translation** disabled by default
- Anonymous access to **wkssvc** and **srvsvc** allowed
  - **RestrictAnonymous** set to 0 by default
  - If set to 1, some additional restrictions for **srvsvc** operations

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.142 -U '%'
Server: \\192.70.106.142:      User:      Domain:
Connection:      OK
[192.70.106.142]$ wksinfo
Name:            XPSP1A
Domain:          AD
Platform:        500
Version:         5.1
[192.70.106.142]$ lsaquery
LSA Query Info Policy
Domain Member    - Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
Domain Controller - Domain: XPSP1A SID: S-1-5-21-1085031214-746137067-839522115
[192.70.106.142]$ enumusers
SAM Enumerate Users
SAMR_CONNECT: NT_STATUS_ACCESS_DENIED
enumusers: FAILED
[192.70.106.142]$ lookupsids S-1-5-21-1085031214-746137067-839522115-500
LSA_LOOKUP_SIDS: NT_STATUS_ACCESS_DENIED
lookupsids: FAILED
[192.70.106.142]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-1001
LSA_LOOKUP_SIDS: NT_STATUS_ACCESS_DENIED
lookupsids: FAILED
[192.70.106.142]$ █
```

# NULL session restrictions in Windows XP SP2

- `\pipe\samr`, `\pipe\lsarpc` and `\pipe\netlogon` no longer hardcoded
  - Prevents all anonymous access to RPC services running inside `lsass.exe` (including `samr` and `lsarpc`)
- One interesting named pipe remaining: `\pipe\browser`
  - Can be used to reach another RPC interface running in the same `svchost.exe` instance, such as
    - Workstation service RPC server (`wkssvc`)
    - Server service RPC server (`srvsvc`)
- `RestrictAnonymous` set to 0 by default
  - When set to 1, restricts some operations of `srvsvc`

No. .	Source	Destination	Protocol	Info
1	192.70.106.76	192.70.106.146	SMB	NT Create AndX Request, Path: \samr
2	192.70.106.146	192.70.106.76	SMB	NT Create AndX Response, Error: STATUS_ACCESS_DENIED
3	192.70.106.76	192.70.106.146	TCP	63159 > 139 [ACK] Seq=897556804 Ack=3292921825 Win=33
4	192.70.106.76	192.70.106.146	SMB	NT Create AndX Request, Path: \lsarpc
5	192.70.106.146	192.70.106.76	SMB	NT Create AndX Response, Error: STATUS_ACCESS_DENIED
6	192.70.106.76	192.70.106.146	TCP	63159 > 139 [ACK] Seq=897556899 Ack=3292921864 Win=33
7	192.70.106.76	192.70.106.146	SMB	NT Create AndX Request, Path: \srvsvc
8	192.70.106.146	192.70.106.76	SMB	NT Create AndX Response, Error: STATUS_ACCESS_DENIED
9	192.70.106.76	192.70.106.146	TCP	63159 > 139 [ACK] Seq=897556994 Ack=3292921903 Win=33
10	192.70.106.76	192.70.106.146	SMB	NT Create AndX Request, Path: \wkssvc
11	192.70.106.146	192.70.106.76	SMB	NT Create AndX Response, Error: STATUS_ACCESS_DENIED
12	192.70.106.76	192.70.106.146	TCP	63159 > 139 [ACK] Seq=897557089 Ack=3292921942 Win=33
13	192.70.106.76	192.70.106.146	SMB	NT Create AndX Request, Path: \browser
14	192.70.106.146	192.70.106.76	SMB	NT Create AndX Response, FID: 0x4000
15	192.70.106.76	192.70.106.146	DCERPC	Bind: call_id: 1 UUID: RPC_BROWSER # Bind: call_id: 1
16	192.70.106.146	192.70.106.76	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 4280 max_recv:
17	192.70.106.76	192.70.106.146	RPC_BROW	BrowserrQueryOtherDomains request # BrowserrQueryOthe
18	192.70.106.146	192.70.106.76	RPC_BROW	BrowserrQueryOtherDomains response[Long frame (24 byt
19	192.70.106.76	192.70.106.146	SMB	Close Request, FID: 0x4000
20	192.70.106.146	192.70.106.76	SMB	Close Response
21	192.70.106.76	192.70.106.146	TCP	63159 > 139 [ACK] Seq=897557554 Ack=3292922332 Win=33

# NULL session restrictions in Windows 2003

- 6 hardcoded named pipes
- Anonymous access to **samr** forbidden
  - **RestrictAnonymousSam** registry value set to 1 by default
- Anonymous access to **lsarpc** forbidden
  - Default setting for a Windows 2003 system
  - Can be allowed by adding and setting **TurnOffAnonymousBlock** to 1
  - In addition, the security option **Network access: Allow anonymous SID/Name translation** is disabled by default
- Anonymous access to **wkssvc** and **srvsvc** allowed
  - **RestrictAnonymous** set to 0 by default
  - If set to 1, some additional restrictions for **srvsvc** operations

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.151 -U '%'
Server: \\192.70.106.151:      User:      Domain:
Connection:      OK
[192.70.106.151]$ srvinfo
Server Info Level 101:
      192.70.106.151 Wk Sv NT SNT
      platform_id      :      500
      os version       :      5.2
[192.70.106.151]$ wksinfo
Name:      SERVEUR
Domain:    WORKGROUP
Platform:  500
Version:   5.2
[192.70.106.151]$ lsaquery
LSA_OPENPOLICY: NT_STATUS_ACCESS_DENIED
lsa_open_policy failed
lsaquery: FAILED
[192.70.106.151]$ enumusers
SAMR_CONNECT: NT_STATUS_ACCESS_DENIED
please use 'lsaquery' first, to ascertain the SID
enumusers: FAILED
[192.70.106.151]$ █
```

# NULL session restrictions in Windows 2003 SP1

- `\pipe\samr`, `\pipe\lsarpc`, `\pipe\netlogon`, `\pipe\browser` present in `NullSessionPipes`
- Anonymous access to `samr` forbidden
  - `RestrictAnonymousSam` registry value set to 1 by default
- Anonymous access to `lsarpc` forbidden
  - Default setting for a Windows 2003 SP1 system
- Anonymous access to `wkssvc` and `srvsvc` still possible through `\pipe\browser`
  - `RestrictAnonymous` set to 0 by default
  - If set to 1, some additional restrictions for `srvsvc` operations

# NULL session restrictions in Active Directory domain controllers: samr

- **samr** interface
  - Active Directory uses the **Pre-Windows 2000 Compatible Access** local group to grant or revoke anonymous access to Active Directory objects
  - On Windows 2000 Active Directory domain controllers, **EVERYONE** is included in **Pre-Windows 2000 Compatible Access**, allowing anonymous enumeration of Active Directory accounts
  - On Windows 2003, **EVERYONE** does no longer include **ANONYMOUS LOGON**, thus anonymous enumeration is only possible if **ANONYMOUS LOGON** explicitly appears in **Pre-Windows 2000 Compatible Access**
  - **RestrictAnonymous** (Windows 2000) and **RestrictAnonymousSam** (Windows 2003) settings have no effect on **samr** restrictions on Active Directory domain controllers

# Windows Server 2003 domain controller (with ANONYMOUS LOGON)

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.144 -U '%' 16:4
Server: \\192.70.106.144:      User:      Domain:
IsConnection:  WARNING: remote site seems to require smb signing, which we do not (yet) support
OK
[192.70.106.144]$ lsaquery
LSA Query Info Policy
Domain Member      - Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
Domain Controller - Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
[192.70.106.144]$ enumusers
SAM Enumerate Users
User RID:      1f4  User Name: Administrator
User RID:      1f5  User Name: Guest
User RID:      1f6  User Name: krbtgt
User RID:      3e9  User Name: SUPPORT_388945a0
User RID:      3eb  User Name: IUSR_W2K3DFLT
User RID:      3ec  User Name: IWAM_W2K3DFLT
User RID:      456  User Name: jbm
[192.70.106.144]$ samaliasmem BUILTIN\administrators
SAM Query Alias: administrators
From: GARBAREK To: \\192.70.106.144 Domain: BUILTIN SID: S-1-5-32
Alias Members:
-----
AD\Administrator (User)
AD\Enterprise Admins (Domain Group)
AD\Domain Admins (Domain Group)

[192.70.106.144]$ samgroupmem "Domain admins"
SAM Query Group: Domain admins
From: GARBAREK To: \\192.70.106.144 Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
Members:
-----
Administrator (User)
```

# Windows Server 2003 domain controller (without ANONYMOUS LOGON)

```
jbm@garbarek ~> /usr/local/samba/bin/rpcclient -S 192.70.106.144 -U '%'
Server: \\192.70.106.144:          User:          Domain:
Connection:      WARNING: remote site seems to require smb signing, which we do not (yet) su
OK
[192.70.106.144]$ lsquery
LSA Query Info Policy
Domain Member    - Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
Domain Controller - Domain: AD SID: S-1-5-21-2330557087-2467616270-843640848
[192.70.106.144]$ enumusers
SAM Enumerate Users
SAMR_CONNECT: NT_STATUS_ACCESS_DENIED
enumusers: FAILED
[192.70.106.144]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-500
Lookup SIDS:
SID: S-1-5-21-2330557087-2467616270-843640848-500 -> AD\Administrator (1: User)
[192.70.106.144]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-501
Lookup SIDS:
SID: S-1-5-21-2330557087-2467616270-843640848-501 -> AD\Guest (1: User)
[192.70.106.144]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-502
Lookup SIDS:
SID: S-1-5-21-2330557087-2467616270-843640848-502 -> AD\krbtgt (1: User)
[192.70.106.144]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-1000
Lookup SIDS:
SID: S-1-5-21-2330557087-2467616270-843640848-1000 -> AD\HelpServicesGroup (4: Local Group)
[192.70.106.144]$ lookupsids S-1-5-21-2330557087-2467616270-843640848-1001
Lookup SIDS:
SID: S-1-5-21-2330557087-2467616270-843640848-1001 -> AD\SUPPORT_388945a0 (1: User)
[192.70.106.144]$ █
```

- Before Windows XP SP2 and Windows 2003 SP1
  - 6 hardcoded named pipes always implicitly allowed for NULL sessions
- Windows 2000 is the **only system where NULL sessions can be completely disabled**
  - With `RestrictAnonymous == 2`
- `RestrictAnonymous == 2` is not supported in Windows XP and Windows Server 2003 (equivalent to 1)

- Windows 2000
  - Not protected by default against NULL sessions
  - Setting [RestrictAnonymous](#) to 1 does not really improve security, using 2 is highly recommended on workstations and servers
  - Apply Update Rollup Package 1 for Windows 2000 SP4
- Windows XP
  - Protected by default against access to [samr](#) and [lsarpc](#)
  - In XP SP2, [\pipe\browser](#) can be used to reach [srvsvc](#) or [wkssvc](#)
- Windows 2003
  - Protection equivalent to Windows XP
- Active Directory domain controllers
  - Typically not protected by default against account enumeration via [samr](#)

- If server-side SMB support is not needed, disable SMB
  - Only possible for isolated (not part of a Windows domain) systems
  - If needed, remote administration still possible using Terminal Services or SSH
- To disable SMB support
  - Disable NetBIOS over TCP/IP support
  - Stop the server (lanmanserver) service
- More details on Windows network services hardening
  - [http://www.hsc.fr/tips/min\\_srv\\_res\\_win.en.html](http://www.hsc.fr/tips/min_srv_res_win.en.html)
  - [http://www.hsc.fr/tips/min\\_w2k3\\_net\\_srv.html](http://www.hsc.fr/tips/min_w2k3_net_srv.html)

- Windows 2000
  - Set [RestrictAnonymous](#) to 2 (disable NULL sessions)
  - Apply Update Rollup Package 1 for Windows 2000 SP4
- Windows XP
  - Set [RestrictAnonymous](#) to 1
  - Windows XP SP2: set [NullSessionPipes](#) to "" (empty string)
- Windows 2003
  - Set [RestrictAnonymous](#) to 1
  - Set [TurnOffAnonymousBlock](#) to 0
  - Windows 2003 SP1: consider setting [NullSessionPipes](#) to "" (empty string), at least remove [browser](#)

- Active Directory domain controllers
  - Windows 2000: remove **EVERYONE** from the **Pre-Windows 2000 Compatible Access** alias
  - Windows 2003: verify that **ANONYMOUS LOGON** is not in the **Pre-Windows 2000 Compatible Access** alias
  - Windows 2003: set **TurnOffAnonymousBlock** to 0

- Using the named pipe firewall available in XP SP2 and W2K3 SP1
  - Named pipe filtering can be **dynamically** enabled by setting the [PipeFirewallActive](#) registry value to 1 (not present by default)
  - Named pipe filtering applies to **all SMB sessions** (NULL sessions and authenticated sessions)
  - List of allowed named pipes specified in the [AllowedPipes](#) registry value ([REG\\_MULTI\\_SZ](#))
  - Setting [PipeFirewallActive](#) to 1 and [AllowedPipes](#) to "" (empty string) is the equivalent of removing the [IPC\\$](#) share

- Windows NULL sessions are here to stay
  - Still needed in some environments for backward compatibility
  - Used as attack vectors to exploit recent MSRPC vulnerabilities (MS03-049, MS04-011)
- A good knowledge of network protocols and Windows internals are recommended to understand NULL sessions
- A third-party MSRPC implementation is required to exploit NULL sessions effectively
- Recent Windows systems are more and more protected against NULL sessions
  - Additional hardening measures are still required

- *Windows network services internals*
  - [http://www.hsc.fr/ressources/articles/win\\_net\\_srv/](http://www.hsc.fr/ressources/articles/win_net_srv/)
  - Includes a detailed section about MSRPC NULL sessions
- *Windows 2000, Null Sessions and MSRPC* (Todd Sabin)
  - <http://www.bindview.com/Services/RAZOR/Resources/nullsess.ppt>
- ethereal
  - <http://www.ethereal.com/>
  - <http://wiki.ethereal.com/>
- rpcclient
  - <http://www.samba-tng.org/>
  - <http://www.samba.org/>