Description of the IPC$ share

The IPC$ is a hidden share maintained by the Server service (Disabling the service will remove the share). The IPC$ share is used for Inter Proces Communication by using RPC (Remote Procedure Call), allowing the client to send different commands to the server:

- List all shares
- List all users
- List files within a share
- Stop/Start services
- …

Certain commands can be accessed anonymously through a NULL session depending on the configuration of the server. If the command cannot be called anonymously, then the client has to authenticate. Access is granted if the client can provide proper credentials (username and password), that matches an account on the server. If not able to do this, then the user at the client machine will get an error like:

> **IPC$, The domain password you supplied is not correct*
>
> *You must supply a password to make this connection:*
>
> *Incorrect password or unknown username for:**

Note it is possible to access the IPC$ share of a server by using a different credentials, than those used when logging on the client machine. (Even if needing to use a domain-user to access a server from outside the domain).

> *net use q: \\10.0.0.2\c$ [password] /user:[domain\]username*

Note to block access to Remote Procedure Call (RPC), then one should ensure that the firewall blocks the following network ports: - TCP Port 135 - RPC Endpoint Mapper

- UDP Port 137 - Netbios
- UDP Port 138 - Netbios
- TCP Port 139 - Netbios
- TCP and UDP Port 445 - Named Pipes

Note Windows 95/98/Me doesn't support logon with different credentials. Therefore one have to make sure the userid and password on the Win9x machine matches one of the accounts on the WinNT machine. This can be done by using one of the following options:

- Create an account on the WinNT machine which matches the username and password (If any) used on the Win9x machine.
  - If the account already exist, then try to reenter the account password for the account (And check the password doesn't expire)
- Create an account on the Win9x machine which matches the username and password of an account on the WinNT machine and then logon to Win9x with the new account.
- Activate the guest account, though it is not recommended:
  - How to enable Win9x filesharing in Windows 2000
  - How to enable Win9x filesharing in Windows XP

Note if sure that the account is properly setup then one can configure an audit to see what account name is used to login to the machine.

More Info MS KB101150
More Info MS KB139592
More Info MS KB162325
More Info MS KB258717
More Info MS KB262916

Using NULL sessions to view shares and user accounts

It is possible to access the IPC$ share with a null session, after that one can access information about the machine configuration.

How to create a null session:

```
net use \\IP_ADDRESS\ipc$ “” /user:””
```

How to access shares after creation of null session:

```
net view \\IP_ADDRESS
```

How to list administrators after creation of null session:

```
local administrators \\IP_ADDRESS
```

How to list group members in “domain admins” after creation of null session:

```
global “domain admins” \\IP_ADDRESS
```

The utilities local.exe and global.exe. They are part of the Windows NT Resource Kit. WInfo is a 3rd party utility that also can exploit null sessions.

Disabling Netbios or blocking the ports 137-139 doesn’t close for Null-Sessions, unless one also closes the SMB on port 445.

Related Restrict access to NULL sessions

More Info MS KB132679
More Info MS KB289655

Credits The Hack FAQ

Creating file shares that are hidden

It is possible to create shares which aren't visible to people browsing the network. To make a hidden share, just add a $ in the end of name for the share:

```
\\machine\\hidden_share$
```

When accessing the shared resource then remember that $ is part of the share name.

- Hidden shares is merely a cosmetic feature, which allows one to remove irrelevant shares that the average user shouldn't have access to. Ex. shares needed only by a certain application.
- Hidden shares should NOT be used for protecting shares from unauthorized access, instead one should use normal access control with password.

Note that it is only Windows-Clients that abide to the rule of not showing "hidden" shares. Linux machines will see the "hidden" shares like any other shares. There also exist applications for Windows which allows to see "hidden" shares on remote machines.