MSRPC (Microsoft Remote Procedure Call)

`Default Port: 135, 593`

MSRPC (Microsoft Remote Procedure Call) is the modified version of DCE/RPC. It forms the basis of network-level service interoperability. MSRPC is the protocol standard for Windows processes that allows a program running on one host to execute a program on another host.

Connect

MSRPC services normally listen on ports `135 and 593`; however, they can also run on other ports.

Netcat

You can check the connection with the `netcat` tool:

```
nc -vn <TARGET_IP> 135
nc -vn <TARGET_IP> 593
```

Enumeration

Using Nmap

```
nmap -p 135,593 --script=msrpc-enum <TARGET_IP>
```

RPC Client

Windows has an embedded tool for interacting with MSRPC called RPC client that you can use for enumeration.

```
rpcclient -U "" -N <TARGET_IP>
#empty username (-U "")
#no password (-N)
```

```
> serverinfo
> lsaenumsid
> netshareenumall
```

Identifying Exposed RPC Services

Exposure of RPC services can be determined by querying the RPC locator service and individual endpoints using tools such as rpcdump. This tool identifies unique RPC services, denoted by IFID values, providing service details and communication bindings.

```
rpcdump [-p port] <IP>
```

Tools such as Metasploit can also be used to audit and interact with MSRPC services, primarily focusing on port 135.

```
use auxiliary/scanner/dcerpc/endpoint_mapper
use auxiliary/scanner/dcerpc/hidden
use auxiliary/scanner/dcerpc/management
use auxiliary/scanner/dcerpc/tcp_dcerpc_auditor
```

Among these options, all except tcp_dcerpc_auditor are specifically designed for targeting MSRPC on port 135.

Attack Vectors

MSRPC has several interfaces that could be potentially exploited for gaining unauthorized access, remote command execution, enumerating users and domains, accessing public SAM database elements, remotely starting and stopping services, accessing and modifying the system registry, and more. These interfaces include:

- LSA interface (`pipe\lsarpc`)
- LSA Directory Services (DS) interface (`pipe\lsarpc`)
- LSA SAMR interface (`pipe\samr`)
- Server services and Service control manager interface (`pipe\svcctl`), (`pipe\srvsvc`)
- Remote registry service (`pipe\winreg`)
- Task scheduler (`pipe\atsvc`)
- DCOM interface (`pipe\epmapper`)

You can also use the IOXIDResolver interface to identify IPv4 and IPv6 addresses of systems on the network.

MSRPC DCOM

MSRPC DCOM is one of the most dangerous services on Windows systems due to the amount of control it can give an attacker. It should be disabled if not needed. MSRPC endpoints can be abused to execute arbitary code on a remote computer.

```
nmap -p 135 --script=msrpc-dcom-interface-activation <TARGET_IP>
```