

Forum:[Hack Forums](#)

Thread: [./Dark Legion/Exploiting Windows Services: A Hacker's Guide to RPC Operations](#)

Dread.Reaper - March 31, 2023, 3:26 pm

@Genuine@

Exploiting Windows Services: A Hacker's Guide to RPC Operations

Written By: Dread.Reaper - Dark Legion

Introduction:

As an attacking hacker, my goal is to find and exploit vulnerabilities in systems to gain unauthorized access to sensitive information or cause damage to the target. In order to do this, I need to have a deep understanding of the technologies and protocols that are used by my targets. One area of interest for me is the Remote Procedure Call (RPC) interface, which is commonly used in Windows-based systems for various functions, including file and printer sharing, user authentication, and domain management.

This technical document presents a comprehensive list of functions that can be called through the RPC interface, along with their descriptions and parameters. As an attacking hacker, this document provides me with valuable insight into the inner workings of the RPC interface and the underlying technologies that it interacts with. By studying this document, I can identify potential vulnerabilities or weaknesses in the RPC interface that can be exploited to gain unauthorized access to the target system.

For example, the "change_trust_pw" function in the NETLOGON section of the document may be of interest to me as an attacking hacker. This function allows for the changing of the trust account password, which is used for authenticating between domains. If I can exploit a vulnerability in this function or obtain the password through other means, I may be able to gain unauthorized access to the target domain or use it to launch further attacks.

Similarly, the "addprinter" and "deldriverex" functions in the SPOOLSS section of the document may be of interest to me as an attacking hacker looking to exploit vulnerabilities in the printing subsystem. By studying the descriptions and parameters of these functions, I can identify potential weaknesses in the system and develop exploits to take advantage of them.

Overall, this technical document provides valuable information to an attacking hacker looking to gain unauthorized access to a Windows-based system. By understanding the functions and parameters of the RPC interface, an attacker can identify potential vulnerabilities and develop exploits to take advantage of them. As a defender, it is important to be aware of these potential vulnerabilities and take steps to mitigate them, such as keeping systems up to date with the latest security patches and implementing strict access controls.

Options:

BINDING-STRING|HOST:

When connecting to a dcerpc service, you need to specify a binding string. The format is `TRANSPORT:host[options]`, where `TRANSPORT` is either `ncacn_np` (named pipes) for SMB or `ncacn_ip_tcp` for DCERPC over TCP/IP. "host" is an IP or hostname or netbios name. "options" can include a SMB pipe name if using the `ncacn_np` transport or a TCP port number if using the `ncacn_ip_tcp` transport, otherwise, they will be auto-determined.

- `-c|--command=<command string>`:

Execute semicolon-separated commands.

- `-I|--dest-ip IP-address`:

IP address is the address of the server to connect to. It should be specified in standard "a.b.c.d" notation. Normally, the client would attempt to locate a named SMB/CIFS server by looking it up via the NetBIOS name resolution mechanism described above in the name resolve order parameter above. Using this parameter will force the client to assume that the server is on the machine with the specified IP address, and the NetBIOS name component of the resource being connected to will be ignored.

- -p|--port port:

This number is the TCP port number that will be used when making connections to the server. The standard (well-known) TCP port number for an SMB/CIFS server is 139, which is the default.

- -?|--help:

Print a summary of command-line options.

- --usage:

Display brief usage message.

- -d|--debuglevel=DEBUGLEVEL:

Level is an integer from 0 to 10. The default value if this parameter is not specified is 1 for client applications. The higher this value, the more detail will be logged to the log files about the activities of the server.

- --debug-stdout:

This will redirect debug output to STDOUT. By default, all clients are logging to STDERR.

- --configfile=<configuration file>:

The file specified contains the configuration details required by the client.

- --option=<name>=<value>:

Set the smb.conf(5) option "<name>" to value "<value>" from the command line.

- -l|--log-basename=logdirectory:

Base directory name for log/debug files.

- --leak-report:

Enable talloc leak reporting on exit.

- --leak-report-full:

Enable full talloc leak reporting on exit.

- -V|--version:

Prints the program version number.

- -R|--name-resolve=NAME-RESOLVE-ORDER:

This option is used to determine what naming services and in what order to resolve host names to IP addresses. The option takes a space-separated string of different name resolution options.

- -O|--socket-options=SOCKETOPTIONS:

TCP socket options to set on the client socket.

- -m|--max-protocol=MAXPROTOCOL:

The value of the parameter (a string) is the highest protocol level that will be supported by the client.

- -n|--netbiosname=NETBIOSNAME:

This option allows you to override the NetBIOS name that Samba uses for itself.

- --netbios-scope=SCOPE:

This specifies a NetBIOS scope that nmblookup will use to communicate with when generating NetBIOS names.

- -W|--workgroup=WORKGROUP

Set the SMB domain of the username. This overrides the default domain which is the domain defined in smb.conf. If the domain specified is the same as the servers NetBIOS name, it causes the client to log on using the servers local SAM (as opposed to the Domain SAM).

- -r|--realm=REALM

Set the realm for the domain.

- -U|--user=[DOMAIN]USERNAME[%PASSWORD]

Sets the SMB username or username and password. If %PASSWORD is not specified, the user will be prompted. The client will first check the USER environment variable, then the LOGNAME

variable and if either exists, the value is used. If these environmental variables are not found, the username found in a Kerberos Credentials cache may be used.

A third option is to use a credentials file which contains the plaintext of the username and password. See the -A switch for more details.

- -N|--no-pass

If specified, this parameter suppresses the normal password prompt from the client to the user. This is useful when accessing a service that does not require a password.

- --password

Specify the password on the commandline.

- --pw-nt-hash

The supplied password is the NT hash.

- -A|--authentication-file=filename

This option allows you to specify a file from which to read the username and password used in the connection.

- -P|--machine-pass

Use stored machine account password.

- --simple-bind-dn=DN

DN to use for a simple bind.

- --use-kerberos=desired|required|off

This parameter determines whether Samba client tools will try to authenticate using Kerberos.

- --use-krb5-ccache=CCACHE

Specifies the credential cache location for Kerberos authentication.

- --use-winbind-ccache

Try to use the credential cache by winbind.

- --client-protection=sign|encrypt|off

Sets the connection protection the client tool should use.

LSARPC:

- lsquery: Query info policy
- lookupsids: Convert SIDs to names
- lookupsids3: Convert SIDs to names
- lookupsids_level: Convert SIDs to names
- lookupnames: Convert names to SIDs
- lookupnames4: Convert names to SIDs
- lookupnames_level: Convert names to SIDs
- enumtrust: Enumerate trusted domains
- enumprivs: Enumerate privileges
- getdispname: Get the privilege name
- lsenumsid: Enumerate the LSA SIDS
- lscreateaccount: Create a new Lsa account
- lsenumprivsaccount: Enumerate the privileges of an SID
- lsenumacctrights: Enumerate the rights of an SID
- lsaddpriv: Assign a privilege to a SID
- lsdelpriv: Revoke a privilege from a SID
- lsaddacctrights: Add rights to an account
- lsremoveacctrights: Remove rights from an account
- lslookupprivvalue: Get a privilege value given its name
- lsquerysecobj: Query LSA security object
- lsquerytrustdominfo: Query LSA trusted domains info (given a SID)
- lsquerytrustdominfobyname: Query LSA trusted domains info (given a name), only works for Windows > 2k
- lsquerytrustdominfo bysid: Query LSA trusted domains info (given a SID)
- lssettrustdominfo: Set LSA trusted domain info

- getusername: Get username
- createsecret: Create Secret
- deletesecret: Delete Secret
- querysecret: Query Secret
- setsecret: Set Secret
- retrieveprivatedata: Retrieve Private Data
- storeprivatedata: Store Private Data
- createtrustdom: Create Trusted Domain
- deletetrustdom: Delete Trusted Domain

LSARPC-DS:

- dsroledominfo: Get Primary Domain Information

DFS:

- dfsversion: Query DFS support
- dfsadd: Add a DFS share
- dfsremove: Remove a DFS share
- dfsgetinfo: Query DFS share info
- dfsenum: Enumerate dfs shares
- dfsenumex: Enumerate dfs shares

SHUTDOWN:

- shutdowninit: syntax: shutdown [-m message]
- shutdownabort: syntax: shutdownabort

SRVSVC:

- srvinfo: Server query info
- netshareenum: Enumerate shares
- netshareenumall: Enumerate all shares
- netsharegetinfo: Get Share Info
- netsharesetinfo: Set Share Info
- netsharesetdfsflags: Set DFS flags
- netfileenum: Enumerate open files
- netremotetod: Fetch remote time of day
- netnamevalidate: Validate sharename
- netfilegetsec: Get File security
- netsessdel: Delete Session
- netsessenum: Enumerate Sessions
- netdiskenum: Enumerate Disks
- netconnenum: Enumerate Connections
- netshareadd: Add share
- netsharedel: Delete share

Want Longer Tutorials? Gift me Ub3r!