Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

zeek / zeek Public

Notifications Fork 1.2k Star 6.4k

Code Issues 156 Pull requests 10 Discussions Actions Projects Wiki Security Insights

Files

691b099

Go to file

.github
auxil
ci
cmake
doc
docker
man
scripts
base
files
frameworks
misc
packet-protocols
protocols
conn
dce-rpc
README
__load__.zeek
consts.zeek
dpd.sig
main.zeek
dhcp
dnp3
dns
ftp
http
imap
irc
krb
modbus
mqtt
mysql
ntlm
ntp
pop3
radius

zeek / scripts / base / protocols / dce-rpc / consts.zeek

fox-ds Add IType opnum mapping 4a19acb · 3 years ago History

Code Blame 2977 lines (2827 loc) · 198 KB Raw

```

module DCE_RPC;

export {
	const uuid_endpoint_map: table[string] of string = {
		["367abb81-9844-35f1-ad32-98f038001003"] = "svcctl",
		["86d35949-83c9-4044-b424-db363231fd0c"] = "ITaskSchedulerService",
		["378e52b0-c0a9-11cf-822d-00aa0051e40f"] = "sasec",
		["1ff70682-0a51-30e8-076d-740be8cee98b"] = "atsvc",
		["0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53"] = "idletask",
		["906b0ce0-c70b-1067-b317-00dd010662da"] = "IXnRemote",
		["ae33069b-a2a8-46ee-a235-ddfd339be281"] = "IRPCRemoteObject",
		["0b6edbfa-4a24-4fc6-8a23-942b1eca65d1"] = "IRPCAsyncNotify",
		["afa8bd80-7d8a-11c9-bef4-08002b102989"] = "mgmt",
		["f5cc59b4-4264-101a-8c59-08002b2f8426"] = "FrsRpc",
		["000001a0-0000-0000-c000-000000000046"] = "IRemoteSCMActivator",
		["00000143-0000-0000-c000-000000000046"] = "IRemUnknown2",
		["12345778-1234-abcd-ef00-0123456789ab"] = "lsarpc",
		["76f03f96-cdfd-44fc-a22c-64950a001209"] = "IRemoteWinspool",
		["12345678-1234-abcd-ef00-01234567cffb"] = "netlogon",
		["e3514235-4b06-11d1-ab04-00c04fc2dcd2"] = "drsuapi",
		["5261574a-4572-206e-b268-6b199213b4e4"] = "AsyncEMSMDB",
		["4d9f4ab8-7d1c-11cf-861e-0020af6e7c57"] = "IActivation",
		["99fcfec4-5260-101b-bbcb-00aa0021347a"] = "IObjectExporter",
		["e1af8308-5d1f-11c9-91a4-08002b14a0fa"] = "epmapper",
		["12345778-1234-abcd-ef00-0123456789ac"] = "samr",
		["4b324fc8-1670-01d3-1278-5a47bf6ee188"] = "srvsvc",
		["45f52c28-7f9f-101a-b52b-08002b2efabe"] = "winspipe",
		["6bffd098-a112-3610-9833-46c3f87e345a"] = "wkssvc",
		["3919286a-b10c-11d0-9ba8-00c04fd92ef5"] = "dssetup",
		["12345678-1234-abcd-ef00-0123456789ab"] = "spoolss",

		# Exchange
		["1544f5e0-613c-11d1-93df-00c04fd7bd09"] = "exchange_rfr",
		["f5cc5a18-4264-101a-8c59-08002b2f8426"] = "nspi",
		["a4f1db00-ca47-1067-b31f-00dd010662da"] = "exchange_mapi",

		# IWbem
		["9556dc99-828c-11cf-a37e-00aa003240c7"] = "IWbemServices",
		["f309ad18-d86a-11d0-a075-00c04fb68820"] = "IWbemLevel1Login",
		["d4781cd6-e5d3-44df-ad94-930efe48a887"] = "IWbemLoginClientID",
		["44aca674-e8fc-11d0-a07c-00c04fb68820"] = "IWbemContext interface",
		["674b6698-ee92-11d0-ad71-00c04fd8fdff"] = "IWbemContext unmarshaler",
		["dc12a681-737f-11cf-884d-00aa004b2e24"] = "IWbemClassObject interface"
		["4590f812-1d3a-11d0-891f-00aa004b2e24"] = "IWbemClassObject unmarshale
		["9a653086-174f-11d2-b5f9-00104b703efd"] = "IWbemClassObject interface"
		["c49e32c6-bc8b-11d2-85d4-00105a1f8304"] = "IWbemBackupRestoreEx interf
		["7c857801-7381-11cf-884d-00aa004b2e24"] = "IWbemObjectSink interface",
		["027947e1-d731-11ce-a357-000000000001"] = "IEnumWbemClassObject interf
		["44aca675-e8fc-11d0-a07c-00c04fb68820"] = "IWbemCallResult interface",
		["c49e32c7-bc8b-11d2-85d4-00105a1f8304"] = "IWbemBackupRestore interfac
		["a359dec5-e813-4834-8a2a-ba7f1d777d76"] = "IWbemBackupRestoreEx interf
		["f1e9c5b2-f59b-11d2-b362-00105a1f8177"] = "IWbemRemoteRefresher interf
		["2c9273e0-1dc3-11d3-b364-00105a1f8177"] = "IWbemRefreshingServices int
		["423ec01e-2e35-11d2-b604-00104b703efd"] = "IWbemWCOSmartEnum interface
		["1c1c45ee-4395-11d2-b60b-00104b703efd"] = "IWbemFetchSmartEnum interfa
		["541679AB-2E5F-11d3-B34E-00104BCC4B4A"] = "IWbemLoginHelper interface"
```

› rdp
› rfb
› sip
› smb
› smtp
› snmp

```
	["541679AB-2E5F-11D3-B34E-00104BCC4B4A"] = "IWbemLoginHelper interface
	["51c82175-844e-4750-b0d8-ec255555bc06"] = "KMS",
	["50abc2a4-574d-40b3-9d66-ee4fd5fba076"] = "dnsserver",
	["3faf4738-3a21-4307-b46c-fdda9bb8c0d5"] = "AudioSrv",
	["c386ca3e-9061-4a72-821e-498d83be188f"] = "AudioRpc",
	["6bffd098-a112-3610-9833-012892020162"] = "browser",
	["91ae6020-9e3c-11cf-8d7c-00aa00c091be"] = "ICertPassage",
	["c8cb7687-e6d3-11d2-a958-00c04f682e16"] = "DAV RPC SERVICE",
	["82273fdc-e32a-18c3-3f78-827929dc23ea"] = "eventlog",
	["3d267954-eeb7-11d1-b94e-00c04fa3080d"] = "HydraLsPipe",
	["894de0c0-0d55-11d3-a322-00c04fa321a1"] = "InitShutdown",
	["d95afe70-a6d5-4259-822e-2c84da1ddb0d"] = "WindowsShutdown",
	["8d0ffe72-d252-11d0-bf8f-00c04fd9126b"] = "IKeySvc",
	["68b58241-c259-4f03-a2e5-a2651dcbc930"] = "IKeySvc2",
	["0d72a7d4-6148-11d1-b4aa-00c04fb66ea0"] = "ICertProtect",
	["f50aac00-c7f3-428e-a022-a6b71bfb9d43"] = "ICatDBSvc",
	["338cd001-2244-31f1-aaaa-900038001003"] = "winreg",
	["3dde7c30-165d-11d1-ab8f-00805f14db40"] = "BackupKey", # https://msdn.
	["3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5"] = "RpcSrvDHCPC",
	["3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6"] = "dhcpcsvc6",
	["2f59a331-bf7d-48cb-9ec5-7c090d76e8b8"] = "lcrpc",
	["5ca4a760-ebb1-11cf-8611-00a0245420ed"] = "winstation_rpc",
	["12b81e99-f207-4a4c-85d3-77b42f76fd14"] = "ISeclogon",
	["d6d70ef0-0e3b-11cb-acc3-08002b1d29c3"] = "NsiS",
	["d3fbb514-0e3b-11cb-8fad-08002b1d29c3"] = "NsiC",
	["d6d70ef0-0e3b-11cb-acc3-08002b1d29c4"] = "NsiM",
	["17fdd703-1827-4e34-79d4-24a55c53bb37"] = "msgsvc",
	["5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc"] = "msgsvcsend",
	["8d9f4e40-a03d-11ce-8f69-08003e30051b"] = "pnp",
	["57674cd0-5200-11ce-a897-08002b2e9c6d"] = "lls_license",
	["342cfd40-3c6c-11ce-a893-08002b2e9c6d"] = "llsrpc",
	["4fc742e0-4a10-11cf-8273-00aa004ae673"] = "netdfs",
	["83da7c00-e84f-11d2-9807-00c04f8ec850"] = "sfcapi",
	["2f5f3220-c126-1076-b549-074d078619da"] = "nddeapi",

	# Added from BZAR
	["0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7"] = "authzr",
	["e3d0d746-d2af-40fd-8a7a-0d7078bb7092"] = "BitsPeerAuth",
	["b97db8b2-4c63-11cf-bff6-08002be23f2f"] = "clusapi",
	["d61a27c6-8f53-11d0-bfa0-00a024151983"] = "CNtmsSvr",
	["6bffd098-a112-3610-9833-46c3f874532d"] = "dhcpsrv",
	["5b821720-f63b-11d0-aad2-00c04fc324db"] = "dhcpsrv2",
	["8f09f000-b7ed-11ce-bbd2-00001a181cad"] = "dimsvc",
	["7c44d7d4-31d5-424c-bd5e-2b3e1f323d22"] = "dsaop",
	["77df7a80-f298-11d0-8358-00a024c480a8"] = "dscomm",
	["708cca10-9569-11d1-b2a5-0060977d8118"] = "dscomm2",
	["df1941c5-fe89-4e79-bf10-463657acf44d"] = "efsrpc",
	["c681d488-d850-11d0-8c52-00c04fd90f7e"] = "efsrpc2",
	["ea0a3165-4834-11d2-a6f8-00c04fa346cc"] = "fax",
	["6099fc12-3eff-11d0-abd0-00c04fd91a4e"] = "faxclient",
	["a8e0653c-2744-4389-a61d-7373df8b2292"] = "FileServerVssAgent",
	["897e2e5f-93f3-4376-9c9c-fd2277495c27"] = "FrsTransport",
	["4bb8ab1d-9ef9-4100-8eb6-dd4b4e418b72"] = "IADProxy",
	["c4b0c7d9-abe0-4733-a1e1-9fdedf260c7a"] = "IADProxy2",
	["03837516-098b-11d8-9414-505054503030"] = "IAlertDataCollector",
	["0383751a-098b-11d8-9414-505054503030"] = "IApiTracingDataCollector",
	["d99e6e71-fc88-11d0-b498-00a0c90312f3"] = "ICertAdminD",
	["7fe0d935-dda6-443f-85d0-1cfb58fe41dd"] = "ICertAdminD2",
	["d99e6e70-fc88-11d0-b498-00a0c90312f3"] = "ICertRequestD",
	["5422fd3a-d4b8-4cef-a12e-e87d4ca22e90"] = "ICertRequestD2",
	["879c8bbe-41b0-11d1-be11-00c04fb6bf70"] = "IClientSink",
	["03837514-098b-11d8-9414-505054503030"] = "IConfigurationDataCollector
```

```
		["88143fd0-c28d-4b2b-8fef-8d882f6a9390",0x0B] = "RpcGetAllSessionsEx",

		# TermServNotification - MSDN Ref: Terminal Services Runtime Interface
		["11899a43-2b68-4a76-92e3-a3d6ad8c26ce",0x00] = "RpcWaitForSessionState
		["11899a43-2b68-4a76-92e3-a3d6ad8c26ce",0x01] = "RpcRegisterAsyncNotifi
		["11899a43-2b68-4a76-92e3-a3d6ad8c26ce",0x02] = "RpcWaitAsyncNotificati
		["11899a43-2b68-4a76-92e3-a3d6ad8c26ce",0x03] = "RpcUnRegisterAsyncNoti

		# TermSrvSession - MSDN Ref: Terminal Services Runtime Interface Protoc
		["484809d6-4239-471b-b5bc-61df8c23ac48",0x00] = "RpcWaitForSessionState
		["484809d6-4239-471b-b5bc-61df8c23ac48",0x01] = "RpcRegisterAsyncNotifi
		["484809d6-4239-471b-b5bc-61df8c23ac48",0x02] = "RpcWaitAsyncNotificati
		["484809d6-4239-471b-b5bc-61df8c23ac48",0x03] = "RpcUnRegisterAsyncNoti

		# trksvr - MSDN Ref: Distributed Link Tracking: Central Manager Protoco
		["4da1c422-943d-11d1-acae-00c04fc2aa3f",0x00] = "LnkSvrMessage",
		["4da1c422-943d-11d1-acae-00c04fc2aa3f",0x01] = "LnkSvrMessageCallback"

		# trkwks - MSDN Ref: Distributed Link Tracking: Workstation Protocol [m
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x00] = "Opnum0NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x01] = "Opnum1NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x02] = "Opnum2NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x03] = "Opnum3NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x04] = "Opnum4NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x05] = "Opnum5NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x06] = "Opnum6NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x07] = "Opnum7NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x08] = "Opnum8NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x09] = "Opnum9NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x0A] = "Opnum10NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x0B] = "Opnum11NotUsedOnWire",
		["300f3532-38cc-11d0-a3f0-0020af6b0add",0x0C] = "LnkSearchMachine",

		# TsProxyRpcInterface - MSDN Ref: Terminal Services Gateway Server Prot
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x00] = "Opnum0NotUsedOnWire",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x01] = "TsProxyCreateTunnel",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x02] = "TsProxyAuthorizeTunnel
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x03] = "TsProxyMakeTunnelCall"
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x04] = "TsProxyCreateChannel",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x05] = "Opnum5NotUsedOnWire",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x06] = "TsProxyCloseChannel",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x07] = "TsProxyCloseTunnel",
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x08] = "TsProxySetupReceivePip
		["44e265dd-7daf-42cd-8560-3cdb6e7a2729",0x09] = "TsProxySendToServer",

		# TSVIPPublic - MSDN Ref: Terminal Services Runtime Interface Protocol
		["53b46b02-c73b-4a3e-8dee-b16b80672fc0",0x00] = "RpcGetSessionIP",

		# W32Time - MSDN Ref: W32Time Remote Protocol [ms-w32t]
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x00] = "W32TimeSync",
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x01] = "W32TimeGetNetlogonServ
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x02] = "W32TimeQueryProviderSt
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x03] = "W32TimeQuerySource",
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x04] = "W32TimeQueryProviderCo
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x05] = "W32TimeQueryConfigurat
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x06] = "W32TimeQueryStatus",
		["8fb6d884-2388-11d0-8c35-00c04fda2795",0x07] = "W32TimeLog",

		# WdsRpcInterface - MSDN Ref: Windows Deployment Services Control Proto
		["1a927394-352e-4553-ae3f-7cf4aafca620",0x00] = "WdsRpcMessage",

		# winsi2 - MSDN Ref: Remote Administrative Interface: WINS [ms-raiw]
		["811109bf-a4e1-11d1-ab54-00a0c91e9b45",0x00] = "R_WinsTombstoneDbRecs"
```

```
                ["811109bf-a4e1-11d1-ab54-00a0c91e9b45",0x01] = "R_WinsCheckAccess",

                # Witness - MSDN Ref: Service Witness Protocol [ms-swn]
                ["ccd8c074-d0e5-4a40-92b4-d074faa6ba28",0x00] = "WitnessrGetInterfaceLi
                ["ccd8c074-d0e5-4a40-92b4-d074faa6ba28",0x01] = "WitnessrRegister",
                ["ccd8c074-d0e5-4a40-92b4-d074faa6ba28",0x02] = "WitnessrUnRegister",
                ["ccd8c074-d0e5-4a40-92b4-d074faa6ba28",0x03] = "WitnessrAsyncNotify",
                ["ccd8c074-d0e5-4a40-92b4-d074faa6ba28",0x04] = "WitnessrRegisterEx",

        } &redef &default=function(uuid: string, i: count): string { return fmt("unknow
}
```