`rpcclient` es una herramienta de línea de comandos en sistemas operativos basados en Linux que se utiliza para interactuar con los servicios de RPC (Remote Procedure Call) en servidores remotos. RPC es un mecanismo utilizado para permitir que los programas soliciten servicios de otros programas en computadoras en una red.

La herramienta `rpcclient` se utiliza principalmente para interactuar con servicios que utilizan RPC, como los servicios proporcionados por los sistemas basados en Windows, como Active Directory, Servicios de Dominio de Windows (DNS), y otros servicios que se comunican a través de RPC.

Algunas de las acciones comunes que puedes realizar con `rpcclient` incluyen:

1. \*\*Autenticación\*\*: `rpcclient` puede ser utilizado para autenticarse con un servidor remoto. Esto es especialmente útil cuando estás trabajando con servicios de autenticación como Active Directory.

2. \*\*Consulta de información\*\*: Puedes usar `rpcclient` para obtener información sobre el servidor remoto, como listas de usuarios, grupos, recursos compartidos de red, etc.

3. \*\*Gestión de cuentas de usuario y grupos\*\*: `rpcclient` permite realizar operaciones como agregar, eliminar o modificar cuentas de usuario y grupos en el servidor remoto.

4. \*\*Diagnóstico y depuración\*\*: `rpcclient` también se puede usar con fines de diagnóstico y depuración para verificar la conectividad con el servidor RPC, probar el acceso a servicios específicos, etc.

En resumen, `rpcclient` es una herramienta poderosa para interactuar con servicios basados en RPC en sistemas remotos, proporcionando una manera de administrar y diagnosticar estos servicios desde la línea de comandos en sistemas Linux.

─$ rpcclient -U "corp/empleado1%@ng01\*Apolo" WS01.corp.local

rpcclient $> doble tab para que nos muestre todas las funciones

Display all 224 possibilities? (y or n)

?

adddriver

addform

addpermachineconnection

addprinter

AsyncNotify

capabilities

change\_trust\_pw

chgpasswd

chgpasswd2

chgpasswd3

chgpasswd4

clusapi\_create\_enum

clusapi\_create\_enumex

clusapi\_get\_cluster\_name

clusapi\_get\_cluster\_version

clusapi\_get\_cluster\_version2

clusapi\_get\_quorum\_resource

clusapi\_get\_resource\_state

clusapi\_offline\_resource

clusapi\_online\_resource

clusapi\_open\_cluster

clusapi\_open\_resource

clusapi\_pause\_node

clusapi\_resume\_node

createdomalias

createdomgroup

createdomuser

createprinteric

createsecret

createtrustdom

debug

debuglevel

deldriver

deldriverex

deletealias

deletedomgroup

deletedomuser

deleteform

deletesecret

deletetrustdom

delpermachineconnection

deregisterdnsrecords

dfsadd

dfsenum

dfsenumex

dfsgetinfo

dfsremove

dfsversion

dscracknames

dsenumdomtrusts

dsgetdcinfo

dsgetncchanges

dsr\_enumtrustdom

dsr\_getdcname

dsr\_getdcnameex

dsr\_getdcnameex2

dsr\_getforesttrustinfo

dsr\_getsitename

dsroledominfo

dswriteaccountspn

echoaddone

echodata

enumalsgroups

enumdata

enumdataex

enumdomains

enumdomgroups

enumdomusers

enumdrivers

enumforms

enumjobs

enumkey

enummonitors

enumpermachineconnections

enumports

enumprinters

enumprivs

enumprocdatatypes

enumprocs

enumtrust

epmlookup

epmmap

eventlog\_backuplog

eventlog\_loginfo

eventlog\_numrecord

eventlog\_oldestrecord

eventlog\_readlog

eventlog\_registerevsource

eventlog\_reportevent

eventlog\_reporteventsource

exit

fetch\_attributes

fetch\_properties

fss\_create\_expose

fss\_delete

fss\_get\_mapping

fss\_get\_sup\_version

fss\_has\_shadow\_copy

fss\_is\_path\_sup

fss\_recovery\_complete

getanydcname

getcoreprinterdrivers

getdata

getdataex

getdcname

getdcsitecoverage

getdispinfoidx

getdispname

getdompwinfo

getdriver

getdriverdir

getdriverpackagepath

getform

GetInterfaceList

getjob

getprinter

getprintprocdir

getpwuid

gettrustrid

getusername

getusrdompwinfo

help

list

logonctrl

logonctrl2

logongetdomaininfo

lookupdomain

lookupnames

lookupnames4

lookupnames\_level

lookupsids

lookupsids3

lookupsids\_level

lsaaddacctrights

lsaaddpriv

lsacreateaccount

lsadelpriv

lsaenumacctrights

lsaenumprivsaccount

lsaenumsid

lsalookupprivvalue

lsaquery

lsaquerysecobj

lsaquerytrustdominfo

lsaquerytrustdominfobyname

lsaquerytrustdominfobysid

lsaremoveacctrights

lsasettrustdominfo

netconnenum

netdiskenum

netfileenum

netfilegetsec

netnamevalidate

netremotetod

netrenumtrusteddomains

netrenumtrusteddomainsex

netsessdel

netsessenum

netshareadd

netsharedel

netshareenum

netshareenumall

netsharegetinfo

netsharesetdfsflags

netsharesetinfo

ntsvcs\_getdevlist

ntsvcs\_getdevlistsize

ntsvcs\_getdevregprop

ntsvcs\_getversion

ntsvcs\_hwprofflags

ntsvcs\_hwprofinfo

ntsvcs\_validatedevinst

openprinter

openprinter\_ex

playgdiscriptonprinteric

printercmp

queryaliasinfo

queryaliasmem

querydispinfo

querydispinfo2

querydispinfo3

querydominfo

querygroup

querygroupmem

querymultiplevalues

querymultiplevalues2

querysecret

queryuser

queryuseraliases

queryusergroups

quit

Register

RegisterEx

retrieveprivatedata

rffpcnex

samlogon

samlookupnames

samlookuprids

samquerysecobj

setdriver

setform

setjob

setprinter

setprinterdata

setprintername

setsecret

setuserinfo

setuserinfo2

sinkdata

sourcedata

srvinfo

storeprivatedata

timeout

uidtosid

UnRegister

winreg\_enumkey

winspool\_AsyncCorePrinterDriverInstalled

winspool\_AsyncOpenPrinter

wkssvc\_enumeratecomputernames

wkssvc\_enumerateusers

wkssvc\_getjoininformation

wkssvc\_messagebuffersend

wkssvc\_wkstagetinfo

Lista

Aquí tienes una lista con una descripción de todas las funciones de los comandos que proporcionaste:

2. \*\*enumports\*\*: Enumera los puertos disponibles en el sistema.

3. \*\*netdiskenum\*\*: Enumera los recursos compartidos de red disponibles.

4. \*\*adddriver\*\*: Agrega un controlador de impresora al servidor de impresión.

5. \*\*enumprinters\*\*: Enumera las impresoras disponibles en la red.

6. \*\*addform\*\*: Agrega un formulario de papel a la base de datos de impresoras.

7. \*\*enumprivs\*\*: Enumera los privilegios asignados a un usuario o grupo.

8. \*\*adddriver\*\*: Agrega un controlador de impresora al servidor de impresión.

9. \*\*enumprocdatatypes\*\*: Enumera los tipos de datos de proceso.

10. \*\*addform\*\*: Agrega un formulario de papel a la base de datos de impresoras.

11. \*\*addpermachineconnection\*\*: Agrega una conexión permanente a un recurso compartido en un servidor remoto.

12. \*\*enumprinters\*\*: Enumera las impresoras disponibles en la red.

13. \*\*AsyncNotify\*\*: Notifica de manera asíncrona un cambio en un recurso compartido de red.

14. \*\*enumprocs\*\*: Enumera los procesos en ejecución en el sistema.

15. \*\*capabilities\*\*: Enumera las capacidades del servidor.

16. \*\*epmlookup\*\*: Busca una entrada en la tabla de conexión de extremo de RPC.

17. \*\*change\_trust\_pw\*\*: Cambia la contraseña de una relación de confianza.

18. \*\*epmmap\*\*: Muestra la tabla de mapeo de extremos de RPC.

19. \*\*chgpasswd\*\*: Cambia la contraseña de un usuario.

20. \*\*eventlog\_backuplog\*\*: Realiza una copia de seguridad de un archivo de registro de eventos.

21. \*\*chgpasswd2\*\*: Cambia la contraseña de un usuario utilizando un método alternativo.

22. \*\*eventlog\_loginfo\*\*: Obtiene información sobre un registro de eventos.

23. \*\*chgpasswd3\*\*: Cambia la contraseña de un usuario utilizando un método alternativo.

24. \*\*eventlog\_numrecord\*\*: Obtiene el número total de registros de eventos.

25. \*\*chgpasswd4\*\*: Cambia la contraseña de un usuario utilizando un método alternativo.

26. \*\*eventlog\_oldestrecord\*\*: Obtiene la fecha y hora del registro de eventos más antiguo.

27. \*\*clusapi\_create\_enum\*\*: Crea un enumerador de recursos.

28. \*\*eventlog\_readlog\*\*: Lee un archivo de registro de eventos.

29. \*\*clusapi\_create\_enumex\*\*: Crea un enumerador de recursos extendido.

30. \*\*eventlog\_registerevsource\*\*: Registra una fuente de eventos.

31. \*\*clusapi\_get\_cluster\_name\*\*: Obtiene el nombre del clúster.

32. \*\*eventlog\_reportevent\*\*: Registra un evento en el registro de eventos.

33. \*\*clusapi\_get\_cluster\_version\*\*: Obtiene la versión del clúster.

34. \*\*eventlog\_reporteventsource\*\*: Registra un evento en el registro de eventos asociado a una fuente.

35. \*\*clusapi\_get\_cluster\_version2\*\*: Obtiene información detallada sobre la versión del clúster.

36. \*\*exit\*\*: Sale de la sesión actual de rpcclient.

37. \*\*clusapi\_get\_quorum\_resource\*\*: Obtiene información sobre el recurso de cuórum.

38. \*\*fetch\_attributes\*\*: Obtiene los atributos de un objeto.

39. \*\*clusapi\_get\_resource\_state\*\*: Obtiene el estado de un recurso.

40. \*\*fetch\_properties\*\*: Obtiene las propiedades de un objeto.

41. \*\*clusapi\_offline\_resource\*\*: Pone offline un recurso.

42. \*\*fss\_create\_expose\*\*: Crea un punto de montaje de FSS (File System Shadow Copy).

43. \*\*clusapi\_online\_resource\*\*: Pone online un recurso.

44. \*\*fss\_delete\*\*: Elimina un punto de montaje de FSS.

45. \*\*clusapi\_open\_cluster\*\*: Abre un controlador de clúster.

46. \*\*fss\_get\_mapping\*\*: Obtiene el mapeo de un punto de montaje de FSS.

47. \*\*clusapi\_open\_resource\*\*: Abre un recurso de clúster.

48. \*\*fss\_get\_sup\_version\*\*: Obtiene la versión de un punto de montaje de FSS compatible.

49. \*\*clusapi\_pause\_node\*\*: Pausa un nodo del clúster.

50. \*\*fss\_has\_shadow\_copy\*\*: Verifica si un volumen tiene copias en sombra.

51. \*\*clusapi\_resume\_node\*\*: Reanuda un nodo del clúster.

52. \*\*fss\_is\_path\_sup\*\*: Verifica si un camino es compatible con FSS.

53. \*\*createdomalias\*\*: Crea un alias de dominio.

54. \*\*fss\_recovery\_complete\*\*: Marca la recuperación de FSS como completa.

55. \*\*createdomgroup\*\*: Crea un grupo de dominio.

56. \*\*getanydcname\*\*: Obtiene el nombre de un controlador de dominio.

57. \*\*createdomuser\*\*: Crea un usuario de dominio.

58. \*\*getcoreprinterdrivers\*\*: Obtiene los controladores de impresora básicos.

59. \*\*createprinteric\*\*: Crea una impresora.

60. \*\*getdata\*\*: Obtiene datos de un objeto.

61. \*\*createsecret\*\*: Crea un secreto en la base de datos de secretos.

62. \*\*getdataex\*\*: Obtiene datos extendidos de un objeto.

63. \*\*createtrustdom\*\*: Crea una relación de confianza entre dominios.

64. \*\*getdcname\*\*: Obtiene el nombre de un controlador de dominio.

65. \*\*debug\*\*: Establece o muestra el nivel de depuración.

66. \*\*getdcsitecoverage\*\*: Obtiene la cobertura de sitios del controlador de dominio.

67. \*\*debuglevel\*\*: Establece el nivel de depuración.

68. \*\*getdispinfoidx\*\*: Obtiene el índice de un identificador de visualización.

69. \*\*deldriver\*\*: Elimina un controlador de impresora.

70. \*\*getdompwinfo\*\*: Obtiene información sobre la política de contraseña de un dominio.

71. \*\*deldriverex\*\*: Elimina un controlador de impresora extendido.

72. \*\*getdriver\*\*: Obtiene información sobre un controlador de impresora.

73. \*\*deletealias\*\*: Elimina un alias de dominio.

74. \*\*getdriverdir\*\*: Obtiene el directorio de los controladores de impresora.

75. \*\*deletedomgroup\*\*: Elimina un grupo de dominio.

76. \*\*getdriverpackagepath\*\*: Obtiene la ruta del paquete del controlador de impresora.

77. \*\*deletedomuser\*\*: Elimina un usuario de dominio.

78. \*\*deleteform\*\*: Elimina un formulario de papel.

79. \*\*deletesecret\*\*: Elimina un secreto de la base de datos de secretos.

80. \*\*deletetrustdom\*\*: Elimina una relación de confianza entre dominios.

81. \*\*delpermachineconnection\*\*: Elimina una conexión permanente a un recurso compartido en un servidor remoto.

82. \*\*deregisterdnsrecords\*\*: Cancela el registro de registros DNS.

83. \*\*dfsadd\*\*: Agrega un enlace DFS.

84. \*\*dfsenum\*\*: Enumera las raíces DFS disponibles.

85. \*\*dfsenumex\*\*: Enumera las raíces DFS disponibles.

86. \*\*dfsgetinfo\*\*: Obtiene información sobre una raíz DFS.

87. \*\*dfsremove\*\*: Elimina un enlace DFS.

88. \*\*dfsversion\*\*: Obtiene la versión del servicio DFS.

89. \*\*dscracknames\*\*: Convierte nombres en identificadores de seguridad y viceversa.

90. \*\*dsenumdomtrusts\*\*: Enumera las relaciones de confianza de dominio.

91. \*\*dsgetdcinfo\*\*: Obtiene información sobre un controlador de dominio.

92. \*\*dsgetncchanges\*\*: Obtiene los cambios realizados en un NC (Naming Context) desde un momento específico.

93. \*\*dsr\_enumtrustdom\*\*: Enumera las relaciones de confianza de dominio.

94. \*\*dsr\_getdcname\*\*: Obtiene el nombre de un controlador de dominio.

95. \*\*dsr\_getdcnameex\*\*: Obtiene el nombre de un controlador de dominio extendido.

96. \*\*dsr\_getdcnameex2\*\*: Obtiene el nombre de un controlador de dominio extendido.

97. \*\*dsr\_getforesttrustinfo\*\*: Obtiene información sobre la confianza en el bosque.

98. \*\*dsr\_getsitename\*\*: Obtiene el nombre del sitio del controlador de dominio.

99. \*\*dsroledominfo\*\*: Obtiene información sobre el rol de un controlador de dominio.

100. \*\*dswriteaccountspn\*\*: Escribe el nombre del servicio principal (SPN) para una cuenta de usuario.

101. \*\*echoaddone\*\*: Incrementa un valor.

102. \*\*echodata\*\*: Envía datos al servidor.

103. \*\*enumalsgroups\*\*: Enumera los grupos en un dominio.

104. \*\*enumdata\*\*: Enumera los datos de un objeto.

105. \*\*enumdataex\*\*: Enumera los datos extendidos de un objeto.

106. \*\*enumdomains\*\*: Enumera los dominios disponibles.

107. \*\*enumdrivers\*\*: Enumera los controladores de impresora.

108. \*\*enumforms\*\*: Enumera los formularios de papel disponibles.

109. \*\*enumjobs\*\*: Enumera los trabajos de impresión en la cola de impresión.

110. \*\*enumkey\*\*: Enumera las subclaves de un registro.

111. \*\*enummonitors\*\*: Enumera los monitores de impresora.

112. \*\*enumpermachineconnections\*\*: Enumera las conexiones permanentes a recursos compartidos en un servidor remoto.

113. \*\*enumprinters\*\*: Enumera las impresoras disponibles en la red.

114. \*\*enumprocs\*\*: Enumera los procesos en ejecución en el sistema.

115. \*\*enumprocdatatypes\*\*: Enumera los tipos de datos de proceso.

116. \*\*enumprivs\*\*: Enumera los privilegios asignados a un usuario o grupo.

117. \*\*enumtrust\*\*: Enumera la información sobre las relaciones de confianza entre los dominios.

118. \*\*eventlog\_backuplog\*\*: Realiza una copia de seguridad de un archivo de registro de eventos.

119. \*\*eventlog\_loginfo\*\*: Obtiene información sobre un registro de eventos.

120. \*\*eventlog\_numrecord\*\*: Obtiene el número total de registros de eventos.

121. \*\*eventlog\_oldestrecord\*\*: Obtiene la fecha y hora del registro de eventos más antiguo.

122. \*\*exit\*\*: Sale de la sesión actual de rpcclient.

123. \*\*fetch\_attributes\*\*: Obtiene los atributos de un objeto.

124. \*\*fetch\_properties\*\*: Obtiene las propiedades de un objeto.

125. \*\*fss\_create\_expose\*\*: Crea un punto de montaje de FSS (File System Shadow Copy).

126. \*\*fss\_delete\*\*: Elimina un punto de montaje de FSS.

127. \*\*fss\_get\_mapping\*\*: Obtiene el mapeo de un punto de montaje de FSS.

128. \*\*fss\_has\_shadow\_copy\*\*: Verifica si un volumen tiene copias en sombra.

129. \*\*fss\_is\_path\_sup\*\*: Verifica si un camino es compatible con FSS.

130. \*\*fss\_recovery\_complete\*\*: Marca la recuperación de FSS como completa.

131. \*\*getanydcname\*\*: Obtiene el nombre de un controlador de dominio.

132. \*\*getcoreprinterdrivers\*\*: Obtiene los controladores de impresora básicos.

133. \*\*getdata\*\*: Obtiene datos de un objeto.

134. \*\*getdataex\*\*: Obtiene datos extendidos de un objeto.

135. \*\*getdispinfoidx\*\*: Obtiene el índice de un identificador de visualización.

136. \*\*getdompwinfo\*\*: Obtiene información sobre la política de contraseña de un dominio.

137. \*\*getdriver\*\*: Obtiene información sobre un controlador de impresora.

138. \*\*getdriverdir\*\*: Obtiene el directorio de los controladores de impresora.

139. \*\*getdriverpackagepath\*\*: Obtiene la ruta del paquete del controlador de impresora.

140. \*\*getgroup\*\*: Obtiene información sobre un grupo.

1. **getjob**: Obtiene información sobre un trabajo de impresión.
2. **getprintprocdir**: Obtiene el directorio de procesadores de impresión.
3. **getprinter**: Obtiene información sobre una impresora.
4. **getprinterdata**: Obtiene datos asociados con una impresora.
5. **getprintername**: Obtiene el nombre de una impresora.
6. **getprintprocdir**: Obtiene el directorio de procesadores de impresión.

221. \*\*getpwuid\*\*: Obtiene información sobre un usuario a partir de su identificador de usuario (UID).

222. \*\*getusrdompwinfo\*\*: Obtiene información sobre la política de contraseña de usuario de un dominio.

223. \*\*getusername\*\*: Obtiene el nombre de usuario asociado con una sesión.

224. \*\*gettrustrid\*\*: Obtiene el RID (Relative Identifier) asociado con un nombre de confianza.

225. \*\*lsacreateaccount\*\*: Crea una nueva cuenta de usuario o grupo.

226. \*\*lsadelpriv\*\*: Elimina un privilegio de una cuenta.

227. \*\*lsaddacctrights\*\*: Agrega derechos de cuenta a una cuenta.

228. \*\*lsaenumacctrights\*\*: Enumera los derechos de cuenta de una cuenta.

229. \*\*lsaenumprivsaccount\*\*: Enumera los privilegios de una cuenta.

230. \*\*lsalookupprivvalue\*\*: Obtiene el valor de un privilegio.

231. \*\*lsaremoveacctrights\*\*: Elimina derechos de cuenta de una cuenta.

232. \*\*lsasettrustdominfo\*\*: Establece información para una relación de confianza.

233. \*\*lsalookup\*\*: Realiza una búsqueda en la base de datos LSA (Local Security Authority).

234. \*\*lsalookupprivvalue\*\*: Obtiene el valor de un privilegio.

235. \*\*lsaremoveacctrights\*\*: Elimina derechos de cuenta de una cuenta.

236. \*\*lsasettrustdominfo\*\*: Establece información para una relación de confianza.

237. \*\*netconnenum\*\*: Enumera las conexiones de red.

238. \*\*netfileenum\*\*: Enumera los archivos abiertos en un servidor remoto.

239. \*\*netremotetod\*\*: Obtiene la hora del sistema en un servidor remoto.

240. \*\*netshareenum\*\*: Enumera los recursos compartidos en un servidor remoto.

241. \*\*netsharesetinfo\*\*: Configura la información de un recurso compartido.

242. \*\*ntsvcs\_getdevlist\*\*: Obtiene una lista de dispositivos en el sistema.

243. \*\*ntsvcs\_getdevlistsize\*\*: Obtiene el tamaño de la lista de dispositivos en el sistema.

244. \*\*ntsvcs\_getdevregprop\*\*: Obtiene propiedades de registro de un dispositivo.

245. \*\*ntsvcs\_getversion\*\*: Obtiene la versión del servicio.

246. \*\*ntsvcs\_hwprofflags\*\*: Obtiene las banderas de perfil de hardware.

247. \*\*ntsvcs\_hwprofinfo\*\*: Obtiene información de perfil de hardware.

248. \*\*ntsvcs\_validatedevinst\*\*: Valida una instancia de dispositivo.

249. \*\*openprinter\*\*: Abre una impresora.

250. \*\*openprinter\_ex\*\*: Abre una impresora con opciones extendidas.

251. \*\*playgdiscriptonprinteric\*\*: Reproduce un script GDI en un controlador de impresora.

252. \*\*printercmp\*\*: Compara dos controladores de impresora.

253. \*\*queryaliasinfo\*\*: Obtiene información sobre un alias de dominio.

254. \*\*queryaliasmem\*\*: Obtiene información sobre la membresía de un alias de dominio.

255. \*\*querydispinfo\*\*: Obtiene información sobre una visualización.

256. \*\*querydispinfo2\*\*: Obtiene información detallada sobre una visualización.

257. \*\*querydispinfo3\*\*: Obtiene información detallada sobre una visualización.

258. \*\*querydominfo\*\*: Obtiene información sobre un dominio.

259. \*\*querygroup\*\*: Obtiene información sobre un grupo de dominio.

260. \*\*querygroupmem\*\*: Obtiene información sobre la membresía de un grupo de dominio.

261. \*\*querymultiplevalues\*\*: Obtiene múltiples valores de un objeto.

262. \*\*querymultiplevalues2\*\*: Obtiene múltiples valores de un objeto con opciones extendidas.

263. \*\*querysecret\*\*: Obtiene información sobre un secreto.

264. \*\*queryuser\*\*: Obtiene información sobre un usuario de dominio.

265. \*\*queryuseraliases\*\*: Obtiene información sobre los alias de un usuario de dominio.

266. \*\*queryusergroups\*\*: Obtiene información sobre los grupos de un usuario de dominio.

267. \*\*rffpcnex\*\*: Establece una conexión a un recurso compartido.

268. \*\*samlogon\*\*: Realiza un inicio de sesión en el sistema de cuentas de seguridad (SAM).

269. \*\*samlookupnames\*\*: Busca nombres en el sistema de cuentas de seguridad (SAM).

270. \*\*samlookuprids\*\*: Busca identificadores de recursos en el sistema de cuentas de seguridad (SAM).

271. \*\*samquerysecobj\*\*: Obtiene información sobre un objeto de seguridad.

272. \*\*setdriver\*\*: Establece un controlador de impresora para una impresora.

273. \*\*setform\*\*: Establece un formulario de papel para una impresora.

274. \*\*setjob\*\*: Establece información sobre un trabajo de impresión.

275. \*\*setprinter\*\*: Establece información sobre una impresora.

276. \*\*setprinterdata\*\*: Establece datos asociados con una impresora.

277. \*\*setprintername\*\*: Establece el nombre de una impresora.

278. \*\*setsecret\*\*: Establece información sobre un secreto.

279. \*\*setuserinfo\*\*: Establece información sobre un usuario de dominio.

280. \*\*setuserinfo2\*\*: Establece información detallada sobre un usuario de dominio.

281. \*\*sinkdata\*\*: Descarta datos.

282. \*\*sourcedata\*\*: Obtiene datos.

283. \*\*srvinfo\*\*: Obtiene información sobre el servidor.

284. \*\*storeprivatedata\*\*: Almacena datos privados.

285. \*\*timeout\*\*: Establece un tiempo de espera para las operaciones de RPC.

286. \*\*uidtosid\*\*: Convierte un identificador de usuario (UID) en un identificador de seguridad (SID).

287. \*\*UnRegister\*\*: Anula el registro de un nombre.

288. \*\*winreg\_enumkey\*\*: Enumera las subclaves de una clave del registro de Windows.

289. \*\*winspool\_AsyncCorePrinterDriverInstalled\*\*: Comprueba si se ha instalado un controlador de impresora principal de forma asíncrona.

290. \*\*winspool\_AsyncOpenPrinter\*\*: Abre una impresora de forma asíncrona.

291. \*\*wkssvc\_enumeratecomputernames\*\*: Enumera los nombres de los equipos.

292. \*\*wkssvc\_enumerateusers\*\*: Enumera los usuarios en un dominio.

293. \*\*wkssvc\_getjoininformation\*\*: Obtiene información sobre la pertenencia a un dominio.

294. \*\*wkssvc\_messagebuffersend\*\*: Envía un mensaje a un equipo.

295. \*\*wkssvc\_wkstagetinfo\*\*: Obtiene información sobre un equipo.

------------------------------------------------------------------------------------------------

🔗 1. Conexión a la Máquina Objetivo con rpcclient

📌 Conexión anónima

bash

Copiar

Editar

rpcclient -U "" 192.168.0.8

Si se conecta sin pedir contraseña, significa que los permisos de RPC permiten acceso anónimo.

📌 Conexión con credenciales

bash

Copiar

Editar

rpcclient -U "empleado1%@ng01\*Apolo" 192.168.0.8

Si devuelve NT\_STATUS\_LOGON\_FAILURE, las credenciales no son válidas o no tienen permisos sobre RPC.

📌 Conexión forzando NTLMv1

bash

Copiar

Editar

rpcclient -U "empleado1%@ng01\*Apolo" 192.168.0.8 --option='client ntlmv2 auth=no'

Algunos servidores Windows bloquean NTLMv2 y requieren NTLMv1.

🔍 2. Enumeración de Usuarios y Grupos

Si la conexión es exitosa, usa estos comandos dentro de rpcclient.

📌 Listar usuarios del sistema

bash

Copiar

Editar

enumdomusers

Devuelve un listado de usuarios en formato RID.

📌 Obtener información detallada de un usuario

bash

Copiar

Editar

queryuser <RID>

(Sustituye <RID> por un número de usuario obtenido con enumdomusers).

Ejemplo:

bash

Copiar

Editar

queryuser 1001

Muestra datos como:

Última sesión

Expiración de contraseña

Privilegios

📌 Listar grupos del sistema

bash

Copiar

Editar

enumdomgroups

Devuelve los grupos de seguridad dentro del sistema.

📌 Ver usuarios dentro de un grupo específico

bash

Copiar

Editar

querygroup <RID>

Ejemplo:

bash

Copiar

Editar

querygroup 512

Si 512 corresponde a Administrators, muestra los usuarios en ese grupo.

📌 Buscar usuarios con permisos elevados (Administrador)

bash

Copiar

Editar

enumalsgroups builtin

Esto puede revelar si el usuario tiene privilegios administrativos.

🖥 3. Información del Sistema

📌 Obtener información del servidor

bash

Copiar

Editar

srvinfo

Muestra detalles como:

Nombre del equipo

Sistema operativo

Versión del dominio

📌 Ver sesiones activas en el servidor

bash

Copiar

Editar

querydispinfo

Lista usuarios conectados y su estado.

📌 Listar servidores dentro de la red

bash

Copiar

Editar

netserverenum

Puede mostrar otros equipos activos en el dominio.

📁 4. Enumeración de Recursos Compartidos

📌 Listar carpetas compartidas

bash

Copiar

Editar

netshareenum

Si el acceso está permitido, devuelve algo como:

pgsql

Copiar

Editar

Share Type Comment

--------------------------------

C$ Disk Default Share

IPC$ Pipe Remote IPC

Si C$ está disponible y tienes credenciales válidas, puedes montarlo con smbclient.

📌 Obtener información sobre una carpeta compartida específica

bash

Copiar

Editar

netshareinfo <nombre\_del\_recurso>

Ejemplo:

bash

Copiar

Editar

netshareinfo C$

🛠 5. Explotación y Movimientos Laterales

Si tienes permisos altos, podrías intentar lo siguiente:

📌 Crear un usuario si tienes permisos de administrador

bash

Copiar

Editar

createuser hacker

📌 Agregar el usuario al grupo de administradores

bash

Copiar

Editar

addusers "hacker" "Administrators"

📌 Cambiar la contraseña de un usuario

bash

Copiar

Editar

setuserinfo <RID> <nuevo\_password>

Ejemplo:

bash

Copiar

Editar

setuserinfo 1001 "P@ssw0rd123"

📌 Forzar cierre de sesión de un usuario

bash

Copiar

Editar

samlogoff <RID>

Estos comandos te ayudarán a enumerar, identificar vulnerabilidades y moverte lateralmente dentro de un sistema con RPC activo. 🚀