



Sign in

fortra / impacket Public

Notifications

Fork 3.6k

Star 13.5k

Code

Issues 196

Pull requests 151

Actions

Projects

Security

Insights

impacket / examples / dcomexec.py

...



Executable File · 657 lines (574 loc) · 28.2 KB

Code

Blame

Raw



```
1  #!/usr/bin/env python
2  # Impacket - Collection of Python classes for working with network protocols.
3  #
4  # SECUREAUTH LABS. Copyright (C) 2021 SecureAuth Corporation. All rights reserved.
5  #
6  # This software is provided under a slightly modified version
7  # of the Apache Software License. See the accompanying LICENSE file
8  # for more information.
9  #
10 # Description:
11 #   A similar approach to psexec but executing commands through DCOM.
12 #   You can select different objects to be used to execute the commands.
13 #   Currently supported objects are:
14 #       1. MMC20.Application (49B2791A-B1AE-4C90-9B8E-E860BA07F889) - Tested Windows 7, Windows 10, S
15 #       2. ShellWindows (9BA05972-F6A8-11CF-A442-00A0C90A8F39) - Tested Windows 7, Windows 10, Server
16 #       3. ShellBrowserWindow (C08AFD90-F2A1-11D1-8455-00A0C91F3880) - Tested Windows 10, Server 2012
17 #
18 #   Drawback is it needs DCOM, hence, I have to be able to access
19 #   DCOM ports at the target machine.
20 #
21 #   Original discovery by Matt Nelson (@enigma0x3):
22 #   https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
23 #   https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
24 #
25 # Author:
26 #   beto (@agsolino)
```

```
27     # Marcello (@byt3bl33d3r)
28     #
29     # Reference for:
30     # DCOM
31     #
32     # ToDo:
33     # [ ] Kerberos auth not working, invalid_checksum is thrown. Most probably sequence numbers out c
34     #     getInterface() method
35     #
36
37     from __future__ import division
38     from __future__ import print_function
39     import argparse
40     import cmd
41     import logging
42     import ntpath
43     import os
44     import sys
45     import time
46     from base64 import b64encode
47
48     from six import PY2, PY3
49     from impacket import version
50     from impacket.dcerpc.v5.dcom.oaut import IID_IDispatch, string_to_bin, IDispatch, DISPPARAMS, DISPA
51         VARIANT, VARENUM, DISPATCH_METHOD
52     from impacket.dcerpc.v5.dcomrt import DCOMConnection, CONVERSION
53     from impacket.dcerpc.v5.dcomrt import OBJREF, FLAGS_OBJREF_CUSTOM, OBJREF_CUSTOM, OBJREF_HANDLER, \
54         OBJREF_EXTENDED, OBJREF_STANDARD, FLAGS_OBJREF_HANDLER, FLAGS_OBJREF_STANDARD, FLAGS_OBJREF_EXT
55         IRemUnknown2, INTERFACE
56     from impacket.dcerpc.v5.dtypes import NULL
57     from impacket.examples import logger
58     from impacket.examples.utils import parse_target
59     from impacket.smbconnection import SMBConnection, SMB_DIALECT, SMB2_DIALECT_002, SMB2_DIALECT_21
60     from impacket.krb5.keytab import Keytab
61
62     OUTPUT_FILENAME = '__' + str(time.time())[:5]
63     CODEC = sys.stdout.encoding
64
65     class DCOMEXEC:
66     def __init__(self, command='', username='', password='', domain='', hashes=None, aesKey=None, s
67         noOutput=False, doKerberos=False, kdcHost=None, dcomObject=None, shell_type=None):
68         self.__command = command
69         self.__username = username
70         self.__password = password
71         self.__domain = domain
72         self.__lmhash = ''
```

```
73         self.__nthash = ''
74         self.__aesKey = aesKey
75         self.__share = share
76         self.__noOutput = noOutput
77         self.__doKerberos = doKerberos
78         self.__kdcHost = kdcHost
79         self.__dcomObject = dcomObject
80         self.__shell_type = shell_type
81         self.shell = None
82         if hashes is not None:
83             self.__lmhash, self.__nthash = hashes.split(':')
84
85     def getInterface(self, interface, resp):
86         # Now let's parse the answer and build an Interface instance
87         objRefType = OBJREF(b''.join(resp))['flags']
88         objRef = None
89         if objRefType == FLAGS_OBJREF_CUSTOM:
90             objRef = OBJREF_CUSTOM(b''.join(resp))
91         elif objRefType == FLAGS_OBJREF_HANDLER:
92             objRef = OBJREF_HANDLER(b''.join(resp))
93         elif objRefType == FLAGS_OBJREF_STANDARD:
94             objRef = OBJREF_STANDARD(b''.join(resp))
95         elif objRefType == FLAGS_OBJREF_EXTENDED:
96             objRef = OBJREF_EXTENDED(b''.join(resp))
97         else:
98             logging.error("Unknown OBJREF Type! 0x%x" % objRefType)
99
100         return IRemUnknown2(
101             INTERFACE(interface.get_cinstance(), None, interface.get_ipidRemUnknown(), objRef['std'],
102                        oxid=objRef['std']['oxid'], oid=objRef['std']['oxid'],
103                        target=interface.get_target()))
104
105     def run(self, addr, silentCommand=False):
106         if self.__noOutput is False and silentCommand is False:
107             smbConnection = SMBConnection(addr, addr)
108             if self.__doKerberos is False:
109                 smbConnection.login(self.__username, self.__password, self.__domain, self.__lmhash,
110                                    self.__nthash, self.__aesKey, kdcHost=self.__kdcHost)
111             else:
112                 smbConnection.kerberosLogin(self.__username, self.__password, self.__domain, self.__lmhash,
113                                              self.__nthash, self.__aesKey, kdcHost=self.__kdcHost)
114
115             dialect = smbConnection.getDialect()
116             if dialect == SMB_DIALECT:
117                 logging.info("SMBv1 dialect used")
118             elif dialect == SMB2_DIALECT_002:
119                 logging.info("SMBv2.0 dialect used")
```

```
110         logging.info('Server process open %s',
```



```
584                                     '(128 or 256 bits)')
585     group.add_argument('-dc-ip', action='store', metavar = "ip address", help='IP Address of the dc
586                                     'omitted it use the domain part (FQDN) specified in the target parameter')
587     group.add_argument('-A', action="store", metavar = "authfile", help="smbclient/mount.cifs-style
588                                     "See smbclient man page's -
589     group.add_argument('-keytab', action="store", help='Read keys for SPN from keytab file')
590
591     if len(sys.argv)==1:
592         parser.print_help()
593         sys.exit(1)
594
595     options = parser.parse_args()
596
597     # Init the example's logger theme
598     logger.init(options.ts)
599
600     if options.codec is not None:
601         CODEC = options.codec
602     else:
603         if CODEC is None:
604             CODEC = 'utf-8'
605
606     if ' '.join(options.command) == ' ' and options.nooutput is True:
607         logging.error("-nooutput switch and interactive shell not supported")
608         sys.exit(1)
609     if options.silentcommand and options.command == ' ':
610         logging.error("-silentcommand switch and interactive shell not supported")
611         sys.exit(1)
612
613     if options.debug is True:
614         logging.getLogger().setLevel(logging.DEBUG)
615         # Print the Library's installation path
616         logging.debug(version.getInstallationPath())
617     else:
618         logging.getLogger().setLevel(logging.INFO)
619
620     if options.com_version is not None:
621         try:
622             .
623             .
624             .
625             .
626             .
627             .
628             .
629             .
630             .
631             .
632             .
633             .
634             .
635             .
636             .
637             .
638             .
639             .
640             .
641             .
642             .
643             .
644             .
645             .
646             .
647             .
648             .
649             .
650             .
651             .
652             .
653             .
654             .
655             .
656             .
657             .
658             .
659             .
660             .
661             .
662             .
663             .
664             .
665             .
666             .
667             .
668             .
669             .
670             .
671             .
672             .
673             .
674             .
675             .
676             .
677             .
678             .
679             .
680             .
681             .
682             .
683             .
684             .
685             .
686             .
687             .
688             .
689             .
690             .
691             .
692             .
693             .
694             .
695             .
696             .
697             .
698             .
699             .
700             .
701             .
702             .
703             .
704             .
705             .
706             .
707             .
708             .
709             .
710             .
711             .
712             .
713             .
714             .
715             .
716             .
717             .
718             .
719             .
720             .
721             .
722             .
723             .
724             .
725             .
726             .
727             .
728             .
729             .
730             .
731             .
732             .
733             .
734             .
735             .
736             .
737             .
738             .
739             .
740             .
741             .
742             .
743             .
744             .
745             .
746             .
747             .
748             .
749             .
750             .
751             .
752             .
753             .
754             .
755             .
756             .
757             .
758             .
759             .
760             .
761             .
762             .
763             .
764             .
765             .
766             .
767             .
768             .
769             .
770             .
771             .
772             .
773             .
774             .
775             .
776             .
777             .
778             .
779             .
780             .
781             .
782             .
783             .
784             .
785             .
786             .
787             .
788             .
789             .
790             .
791             .
792             .
793             .
794             .
795             .
796             .
797             .
798             .
799             .
800             .
801             .
802             .
803             .
804             .
805             .
806             .
807             .
808             .
809             .
810             .
811             .
812             .
813             .
814             .
815             .
816             .
817             .
818             .
819             .
820             .
821             .
822             .
823             .
824             .
825             .
826             .
827             .
828             .
829             .
830             .
831             .
832             .
833             .
834             .
835             .
836             .
837             .
838             .
839             .
840             .
841             .
842             .
843             .
844             .
845             .
846             .
847             .
848             .
849             .
850             .
851             .
852             .
853             .
854             .
855             .
856             .
857             .
858             .
859             .
860             .
861             .
862             .
863             .
864             .
865             .
866             .
867             .
868             .
869             .
870             .
871             .
872             .
873             .
874             .
875             .
876             .
877             .
878             .
879             .
880             .
881             .
882             .
883             .
884             .
885             .
886             .
887             .
888             .
889             .
890             .
891             .
892             .
893             .
894             .
895             .
896             .
897             .
898             .
899             .
900             .
901             .
902             .
903             .
904             .
905             .
906             .
907             .
908             .
909             .
910             .
911             .
912             .
913             .
914             .
915             .
916             .
917             .
918             .
919             .
920             .
921             .
922             .
923             .
924             .
925             .
926             .
927             .
928             .
929             .
930             .
931             .
932             .
933             .
934             .
935             .
936             .
937             .
938             .
939             .
940             .
941             .
942             .
943             .
944             .
945             .
946             .
947             .
948             .
949             .
950             .
951             .
952             .
953             .
954             .
955             .
956             .
957             .
958             .
959             .
960             .
961             .
962             .
963             .
964             .
965             .
966             .
967             .
968             .
969             .
970             .
971             .
972             .
973             .
974             .
975             .
976             .
977             .
978             .
979             .
980             .
981             .
982             .
983             .
984             .
985             .
986             .
987             .
988             .
989             .
990             .
991             .
992             .
993             .
994             .
995             .
996             .
997             .
998             .
999             .
1000            .
1001            .
1002            .
1003            .
1004            .
1005            .
1006            .
1007            .
1008            .
1009            .
1010            .
1011            .
1012            .
1013            .
1014            .
1015            .
1016            .
1017            .
1018            .
1019            .
1020            .
1021            .
1022            .
1023            .
1024            .
1025            .
1026            .
1027            .
1028            .
1029            .
1030            .
1031            .
1032            .
1033            .
1034            .
1035            .
1036            .
1037            .
1038            .
1039            .
1040            .
1041            .
1042            .
1043            .
1044            .
1045            .
1046            .
1047            .
1048            .
1049            .
1050            .
1051            .
1052            .
1053            .
1054            .
1055            .
1056            .
1057            .
1058            .
1059            .
1060            .
1061            .
1062            .
1063            .
1064            .
1065            .
1066            .
1067            .
1068            .
1069            .
1070            .
1071            .
1072            .
1073            .
1074            .
1075            .
1076            .
1077            .
1078            .
1079            .
1080            .
1081            .
1082            .
1083            .
1084            .
1085            .
1086            .
1087            .
1088            .
1089            .
1090            .
1091            .
1092            .
1093            .
1094            .
1095            .
1096            .
1097            .
1098            .
1099            .
1100            .
1101            .
1102            .
1103            .
1104            .
1105            .
1106            .
1107            .
1108            .
1109            .
1110            .
1111            .
1112            .
1113            .
1114            .
1115            .
1116            .
1117            .
1118            .
1119            .
1120            .
1121            .
1122            .
1123            .
1124            .
1125            .
1126            .
1127            .
1128            .
1129            .
1130            .
1131            .
1132            .
1133            .
1134            .
1135            .
1136            .
1137            .
1138            .
1139            .
1140            .
1141            .
1142            .
1143            .
1144            .
1145            .
1146            .
1147            .
1148            .
1149            .
1150            .
1151            .
1152            .
1153            .
1154            .
1155            .
1156            .
1157            .
1158            .
1159            .
1160            .
1161            .
1162            .
1163            .
1164            .
1165            .
1166            .
1167            .
1168            .
1169            .
1170            .
1171            .
1172            .
1173            .
1174            .
1175            .
1176            .
1177            .
1178            .
1179            .
1180            .
1181            .
1182            .
1183            .
1184            .
1185            .
1186            .
1187            .
1188            .
1189            .
1190            .
1191            .
1192            .
1193            .
1194            .
1195            .
1196            .
1197            .
1198            .
1199            .
1200            .
1201            .
1202            .
1203            .
1204            .
1205            .
1206            .
1207            .
1208            .
1209            .
1210            .
1211            .
1212            .
1213            .
1214            .
1215            .
1216            .
1217            .
1218            .
1219            .
1220            .
1221            .
1222            .
1223            .
1224            .
1225            .
1226            .
1227            .
1228            .
1229            .
1230            .
1231            .
1232            .
1233            .
1234            .
1235            .
1236            .
1237            .
1238            .
1239            .
1240            .
1241            .
1242            .
1243            .
1244            .
1245            .
1246            .
1247            .
1248            .
1249            .
1250            .
1251            .
1252            .
1253            .
1254            .
1255            .
1256            .
1257            .
1258            .
1259            .
1260            .
1261            .
1262            .
1263            .
1264            .
1265            .
1266            .
1267            .
1268            .
1269            .
1270            .
1271            .
1272            .
1273            .
1274            .
1275            .
1276            .
1277            .
1278            .
1279            .
1280            .
1281            .
1282            .
1283            .
1284            .
1285            .
1286            .
1287            .
1288            .
1289            .
1290            .
1291            .
1292            .
1293            .
1294            .
1295            .
1296            .
1297            .
1298            .
1299            .
1300            .
1301            .
1302            .
1303            .
1304            .
1305            .
1306            .
1307            .
1308            .
1309            .
1310            .
1311            .
1312            .
1313            .
1314            .
1315            .
1316            .
1317            .
1318            .
1319            .
1320            .
1321            .
1322            .
1323            .
1324            .
1325            .
1326            .
1327            .
1328            .
1329            .
1330            .
1331            .
1332            .
1333            .
1334            .
1335            .
1336            .
1337            .
1338            .
1339            .
1340            .
1341            .
1342            .
1343            .
1344            .
1345            .
1346            .
1347            .
1348            .
1349            .
1350            .
1351            .
1352            .
1353            .
1354            .
1355            .
1356            .
1357            .
1358            .
1359            .
1360            .
1361            .
1362            .
1363            .
1364            .
1365            .
1366            .
1367            .
1368            .
1369            .
1370            .
1371            .
1372            .
1373            .
1374            .
1375            .
1376            .
1377            .
1378            .
1379            .
1380            .
1381            .
1382            .
1383            .
1384            .
1385            .
1386            .
1387            .
1388            .
1389            .
1390            .
1391            .
1392            .
1393            .
1394            .
1395            .
1396            .
1397            .
1398            .
1399            .
1400            .
1401            .
1402            .
1403            .
1404            .
1405            .
1406            .
1407            .
1408            .
1409            .
1410            .
1411            .
1412            .
1413            .
1414            .
1415            .
1416            .
1417            .
1418            .
1419            .
1420            .
1421            .
1422            .
1423            .
1424            .
1425            .
1426            .
1427            .
1428            .
1429            .
1430            .
1431            .
1432            .
1433            .
1434            .
1435            .
1436            .
1437            .
1438            .
1439            .
1440            .
1441            .
1442            .
1443            .
1444            .
1445            .
1446            .
1447            .
1448            .
1449            .
1450            .
1451            .
1452            .
1453            .
1454            .
1455            .
1456            .
1457            .
1458            .
1459            .
1460            .
1461            .
1462            .
1463            .
1464            .
1465            .
1466            .
1467            .
1468            .
1469            .
1470            .
1471            .
1472            .
1473            .
1474            .
1475            .
1476            .
1477            .
1478            .
1479            .
1480            .
1481            .
1482            .
1483            .
1484            .
1485            .
1486            .
1487            .
1488            .
1489            .
1490            .
1491            .
1492            .
1493            .
1494            .
1495            .
1496            .
1497            .
1498            .
1499            .
1500            .
1501            .
1502            .
1503            .
1504            .
1505            .
1506            .
1507            .
1508            .
1509            .
1510            .
1511            .
1512            .
1513            .
1514            .
1515            .
1516            .
1517            .
1518            .
1519            .
1520            .
1521            .
1522            .
1523            .
1524            .
1525            .
1526            .
1527            .
1528            .
1529            .
1530            .
1531            .
1532            .
1533            .
1534            .
1535            .
1536            .
1537            .
1538            .
1539            .
1540            .
1541            .
1542            .
1543            .
1544            .
1545            .
1546            .
1547            .
1548            .
1549            .
1550            .
1551            .
1552            .
1553            .
1554            .
1555            .
1556            .
1557            .
1558            .
1559            .
1560            .
1561            .
1562            .
1563            .
1564            .
1565            .
1566            .
1567            .
1568            .
1569            .
1570            .
1571            .
1572            .
1573            .
1574            .
1575            .
1576            .
1577            .
1578            .
1579            .
1580            .
1581            .
1582            .
1583            .
1584            .
1585            .
1586            .
1587            .
1588            .
1589            .
1590            .
1591            .
1592            .
1593            .
1594            .
1595            .
1596            .
1597            .
1598            .
1599            .
1600            .
1601            .
1602            .
1603            .
1604            .
1605            .
1606            .
1607            .
1608            .
1609            .
1610            .
1611            .
1612            .
1613            .
1614            .
1615            .
1616            .
1617            .
1618            .
1619            .
1620            .
1621            .
1622            .
1623            .
1624            .
1625            .
1626            .
1627            .
1628            .
1629            .
1630            .
1631            .
1632            .
1633            .
1634            .
1635            .
1636            .
1637            .
1638            .
1639            .
1640            .
1641            .
1642            .
1643            .
1644            .
1645            .
1646            .
1647            .
1648            .
1649            .
1650            .
1651            .
1652            .
1653            .
1654            .
1655            .
1656            .
1657            .
1658            .
1659            .
1660            .
1661            .
1662            .
1663            .
1664            .
1665            .
1666            .
1667            .
1668            .
1669            .
1670            .
1671            .
1672            .
1673            .
1674            .
1675            .
1676            .
1677            .
1678            .
1679            .
1680            .
1681            .
1682            .
1683            .
1684            .
1685            .
1686            .
1687            .
1688            .
1689            .
1690            .
1691            .
1692            .
1693            .
1694            .
1695            .
1696            .
1697            .
1698            .
1699            .
1700            .
1701            .
1702            .
1703            .
1704            .
1705            .
1706            .
1707            .
1708            .
1709            .
1710            .
1711            .
1712            .
1713            .
1714            .
1715            .
1716            .
1717            .
1718            .
1719            .
1720            .
1721            .
1722            .
1723            .
1724            .
1725            .
1726            .
1727            .
1728            .
1729            .
1730            .
1731            .
1732            .
1733            .
1734            .
1735            .
1736            .
1737            .
1738            .
1739            .
1740            .
1741            .
1742            .
1743            .
1744            .
1745            .
1746            .
1747            .
1748            .
1749            .
1750            .
1751            .
1752            .
1753            .
1754            .
1755            .
1756            .
1757            .
1758            .
1759            .
1760            .
1761            .
1762            .
1763            .
1764            .
1765            .
1766            .
1767            .
1768            .
1769            .
1770            .
1771            .
1772            .
1773            .
1774            .
1775            .
1776            .
1777            .
1778            .
1779            .
1780            .
1781            .
1782            .
1783            .
1784            .
1785            .
1786            .
1787            .
1788            .
1789            .
1790            .
1791            .
1792            .
1793            .
1794            .
1795            .
1796            .
1797            .
1798            .
1799            .
1800            .
1801            .
1802            .
1803            .
1804            .
1805            .
1806            .
1807            .
1808            .
1809            .
1810            .
1811            .
1812            .
1813            .
1814            .
1815            .
1816            .
1817            .
1818            .
1819            .
1820            .
1821            .
1822            .
1823            .
1824            .
1825            .
1826            .
1827            .
1828            .
1829            .
1830            .
1831            .
1832            .
1833            .
1834            .
1835            .
1836            .
1837            .
1838            .
1839            .
1840            .
1841            .
1842            .
1843            .
1844            .
1845            .
1846            .
1847            .
1848            .
1849            .
1850            .
1851            .
1852            .
1853            .
1854            .
1855            .
1856            .
1857            .
1858            .
1859            .
1860            .
1861            .
1862            .
1863            .
1864            .
1865            .
1866            .
1867            .
1868            .
1869            .
1870            .
1871            .
1872            .
1873            .
1874            .
1875            .
1876            .
1877            .
1878            .
1879            .
1880            .
1881            .
1882            .
1883            .
1884            .
1885            .
1886            .
1887            .
1888            .
1889            .
1890            .
1891            .
1892            .
1893            .
1894            .
1895            .
1896            .
1897            .
1898            .
1899            .
1900            .
1901            .
1902            .
1903            .
1904            .
1905            .
1906            .
1907            .
1908            .
1909            .
1910            .
1911            .
1912            .
1913            .
1914            .
1915            .
1916            .
1917            .
1918            .
1919            .
1920            .
1921            .
1922            .
1923            .
1924            .
1925            .
1926            .
1927            .
1928            .
1929            .
1930            .
1931            .
1932            .
1933            .
1934            .
1935            .
1936            .
1937            .
1938            .
1939            .
1940            .
1941            .
1942            .
1943            .
1944            .
1945            .
1946            .
1947            .
1948            .
1949            .
1950            .
1951            .
1952            .
1953            .
1954            .
1955            .
1956            .
1957            .
1958            .
1959            .
1960            .
1961            .
1962            .
1963            .
1964            .
1965            .
1966            .
1967            .
1968            .
1969            .
1970            .
1971            .
1972            .
1973            .
1974            .
1975            .
1976            .
1977            .
1978            .
1979            .
1980            .
1981            .
1982            .
1983            .
1984            .
1985            .
1986            .
1987            .
1988            .
1989            .
1990            .
1991            .
1992            .
1993            .
1994            .
1995            .
1996            .
1997            .
1998            .
1999            .
2000            .
2001            .
2002            .
2003            .
2004            .
2005            .
2006            .
2007            .
2008            .
2009            .
2010            .
2011            .
2012            .
2013            .
2014            .
2015            .
2016            .
2017            .
2018            .
2019            .
2020            .
2021            .
2022            .
2023            .
2024            .
2025            .
2026            .
2027            .
2028            .
2029            .
2030            .
2031            .
2032            .
2033            .
2034            .
2035            .
2036            .
2037            .
2038            .
2039            .
2040            .
2041            .
2042            .
2043            .
2044            .
2045            .
2046            .
2047            .
2048            .
2049            .
2050            .
2051            .
2052            .
2053            .
2054            .
2055            .
2056            .
2057            .
2058            .
2059            .
2060            .
2061            .
2062            .
2063            .
2064            .
2065            .
2066            .
2067            .
2068            .
2069            .
2070            .
2071            .
2072            .
2073            .
2074            .
2075            .
2076            .
2077            .
2078            .
2079            .
2080            .
2081            .
2082            .
2083            .
2084            .
2085            .
2086            .
2087            .
2088            .
2089            .
2090            .
2091            .
2092            .
2093            .
2094            .
2095            .
2096            .
2097            .
2098            .
2099            .
2100            .
2101            .
2102            .
2103            .
2104            .
2105            .
2106            .
2107            .
2108            .
2109            .
2110            .
2111            .
2112            .
2113            .
2114            .
2115            .
2116            .
2117            .
2118            .
2119            .
2120            .
2121            .
2122            .
2123            .
2124            .
2125            .
2126            .
2127            .
2128            .
2129            .
2130            .
2131            .
2132            .
2133            .
2134            .
2135            .
2136            .
2137            .
2138            .
2139            .
2140            .
2141            .
2142            .
2143            .
2144            .
2145            .
2146            .
2147            .
2148            .
2149            .
2150            .
2151            .
2152            .
2153            .
2154            .
2155            .
2156            .
2157            .
2158            .
2159            .
2160            .
2161            .
2162            .
2163            .
2164            .
2165            .
2166            .
2167            .
2168            .
2169            .
2170            .
2171            .
2172            .
2173            .
2174            .
2175            .
2176            .
2177            .
2178            .
2179            .
2180            .
2181            .
2182            .
2183            .
2184            .
2185            .
2186            .
2187            .
2188            .
2189            .
2190            .
2191            .
2192            .
2193            .
2194            .
2195            .
2196            .
2197            .
2198            .
2199            .
2200            .
2201            .
2202            .
2203            .
2204            .
2205            .
2206            .
2207            .
2208            .
2209            .
2210            .
2211            .
2212            .
2213            .
2214            .
2215            .
2216            .
2217            .
2218            .
2219            .
2220            .
2221            .
2222            .
2223            .
2224            .
2225            .
2226            .
2227            .
2228            .
2229            .
2230            .
2231            .
2232            .
2233            .
2234            .
2235            .
2236            .
2237            .
2238            .
2239            .
2240            .
2241            .
2242            .
2243            .
2244            .
2245            .
2246            .
2247            .
2248            .
2249            .
2250            .
2251            .
2252            .
2253            .
2254            .
2255            .
2256            .
2257            .
2258            .
2259            .
2260            .
2261            .
2262            .
2263            .
2264            .
2265            .
2266            .
2267            .
2268            .
2269            .
2270            .
2271            .
2272            .
2273            .
2274            .
2275            .
2276            .
2277            .
2278            .
2279            .
2280            .
2281            .
2282            .
2283            .
2284            .
2285            .
2286            .
2287            .
2288            .
2289            .
2290            .
2291            .
2292            .
2293            .
2294            .
2295            .
2296            .
2297            .
2298            .
2299            .
2300            .
2301            .
2302            .
2303            .
2304            .
2305            .
2306            .
2307            .
2308            .
2309            .
2310            .
2311            .
2312            .
2313            .
2314            .
2315            .
2316            .
2317            .
2318            .
2319            .
2320            .
2321            .
2322            .
2323            .
2324            .
2325            .
2326            .
2327            .
2328            .
2329            .
2330            .
2331            .
2332            .
2333            .
2334            .
2335            .
2336            .
2337            .
2338            .
2339            .
2340            .
2341            .
2342            .
2343            .
2344            .
2345            .
2346            .
2347            .
2348            .
2349            .
2350            .
2351            .

```

```
622         major_version, minor_version = options.com_version.split('.')
623         COMVERSION.set_default_version(int(major_version), int(minor_version))
624     except Exception:
625         logging.error("Wrong COMVERSION format, use dot separated integers e.g. \"5.7\"")
626         sys.exit(1)
627
628     domain, username, password, address = parse_target(options.target)
629
630     try:
631         if options.A is not None:
632             (domain, username, password) = load_smbclient_auth_file(options.A)
633             logging.debug('loaded smbclient auth file: domain=%s, username=%s, password=%s' % (repr(
634
635         if domain is None:
636             domain = ''
637
638         if options.keytab is not None:
639             Keytab.loadKeysFromKeytab(options.keytab, username, domain, options)
640             options.k = True
641
642         if password == '' and username != '' and options.hashes is None and options.no_pass is False:
643             from getpass import getpass
644             password = getpass("Password:")
645
646         if options.aesKey is not None:
647             options.k = True
648
649         executer = DCOMEXEC(' '.join(options.command), username, password, domain, options.hashes,
650                             options.share, options.nooutput, options.k, options.dc_ip, options.obje
651         executer.run(address, options.silentcommand)
652     except (Exception, KeyboardInterrupt) as e:
653         if logging.getLogger().level == logging.DEBUG:
654             import traceback
655             traceback.print_exc()
656         logging.error(str(e))
657     sys.exit(0)
```