Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

🔍

Sign in

Sign up


jpalanco / alienvault-ossimPublic

🔔 Notifications

 Fork93

 Star119

<> Code⌚ Issues5🔗 Pull requests1⌚ Actions📁 Projects📖 Wiki🛡 Security📈 Insights

alienvault-ossim / os-sim / agent / src / ParserUtil.py

...

 Jose Ramon Palanco Updated

f74359c · 5 years ago🕒 History

```
1      #
2      # License:
3      #
4      #   Copyright (c) 2003-2006 ossim.net
5      #   Copyright (c) 2007-2014 AlienVault
6      #   All rights reserved.
7      #
8      #   This package is free software; you can redistribute it and/or modify
9      #   it under the terms of the GNU General Public License as published by
10     #   the Free Software Foundation; version 2 dated June, 1991.
11     #   You may not use, modify or distribute this program under any other version
12     #   of the GNU General Public License.
13     #
14     #   This package is distributed in the hope that it will be useful,
15     #   but WITHOUT ANY WARRANTY; without even the implied warranty of
16     #   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
17     #   GNU General Public License for more details.
18     #
19     #   You should have received a copy of the GNU General Public License
20     #   along with this package; if not, write to the Free Software
21     #   Foundation, Inc., 51 Franklin St, Fifth Floor, Boston,
22     #   MA 02110-1301 USA
23     #
24     #
25     # On Debian GNU/Linux systems, the complete text of the GNU General
26     # Public License can be found in `/usr/share/common-licenses/GPL-2'.
27     #
28     # Otherwise you can read it here: http://www.gnu.org/licenses/gpl-2.0.txt
29     #
30
31     #
32     # GLOBAL IMPORTS
33     #
34     import datetime
35     import json
36     import os
37     import pickle
38     import re
39     import socket
40     import time
41     from hashlib import md5
42
43     import GeoIP
44
45     GEOIPDB = GeoIP.open("/usr/share/geoip/GeoLiteCity.dat", GeoIP.GEOIP_STANDARD)
46     #
47     # LOCAL IMPORTS
48     #
49
50     from SiteProtectorMap import *
51     from NetScreenMap import *
52     from Logger import Logger
53
54     logger = Logger.logger
55
56     #
57     # GLOBAL VARIABLES
```

```
57     # GLOBAL VARIABLES
58     #
59     DEFAULT_ID = '99999'
60     DATE_FORMAT_FILE_PATH = '/etc/ossim/agent/plugins/date_config/date_formats.json'
61     CUSTOM_FORMATS_LOADED = False
62     HOST_RESOLV_CACHE = {}
63
64     ✓ PROTO_TABLE = {
65         '1': 'icmp',
66         '6': 'tcp',
67         '17': 'udp',
68     }
69
70     HOST_BLACK_LIST = {}
71
72     ✓ FIXED_MONTH_TRANSLATE = {
73         # ENGLISH
74         'jan': 1,
75         'feb': 2,
```



```
832         '%%4554': 'Undefined Access (no effect) Bit 10',
833         '%%4555': 'Undefined Access (no effect) Bit 11',
834         '%%4556': 'Undefined Access (no effect) Bit 12',
835         '%%4557': 'Undefined Access (no effect) Bit 13',
836         '%%4558': 'Undefined Access (no effect) Bit 14',
837         '%%4559': 'Undefined Access (no effect) Bit 15',
838         '%%4560': 'Force thread termination',
839         '%%4561': 'Suspend or resume thread',
840         '%%4562': 'Send an alert to thread',
841         '%%4563': 'Get thread context',
842         '%%4564': 'Set thread context',
843         '%%4565': 'Set thread information',
844         '%%4566': 'Query thread information',
845         '%%4567': 'Assign a token to the thread',
846         '%%4568': 'Cause thread to directly impersonate another thread',
847         '%%4569': 'Directly impersonate this thread',
848         '%%4570': 'Undefined Access (no effect) Bit 10',
849         '%%4571': 'Undefined Access (no effect) Bit 11',
850         '%%4572': 'Undefined Access (no effect) Bit 12',
851         '%%4573': 'Undefined Access (no effect) Bit 13',
852         '%%4574': 'Undefined Access (no effect) Bit 14',
853         '%%4575': 'Undefined Access (no effect) Bit 15',
854         '%%4576': 'Query timer state',
855         '%%4577': 'Modify timer state',
856         '%%4578': 'Undefined Access (no effect) Bit 2',
857         '%%4579': 'Undefined Access (no effect) Bit 3',
858         '%%4580': 'Undefined Access (no effect) Bit 4',
859         '%%4581': 'Undefined Access (no effect) Bit 5',
860         '%%4582': 'Undefined Access (no effect) Bit 6',
861         '%%4584': 'Undefined Access (no effect) Bit 8',
862         '%%4585': 'Undefined Access (no effect) Bit 9',
863         '%%4586': 'Undefined Access (no effect) Bit 10',
864         '%%4587': 'Undefined Access (no effect) Bit 11',
865         '%%4588': 'Undefined Access (no effect) Bit 12',
866         '%%4589': 'Undefined Access (no effect) Bit 13',
867         '%%4590': 'Undefined Access (no effect) Bit 14',
868         '%%4591': 'Undefined Access (no effect) Bit 15',
869         '%%4592': 'AssignAsPrimary',
870         '%%4593': 'Duplicate',
871         '%%4594': 'Impersonate',
872         '%%4595': 'Query',
873         '%%4596': 'QuerySource',
874         '%%4597': 'AdjustPrivileges',
875         '%%4598': 'AdjustGroups',
876         '%%4599': 'AdjustDefaultDacl',
877         '%%4600': 'Undefined Access (no effect) Bit 8',
```



Files



f74359c



Go to file

> alienvault-agent-generator

> alienvault-api

> alienvault-crosscorrelation-free

> alienvault-directives-free

> alienvault-doctor

> alienvault-dummies-ami

> alienvault-dummies-config

> alienvault-dummies-hyperv

```
878         '%4601': 'Undefined Access (no effect) Bit 9',
879         '%4602': 'Undefined Access (no effect) Bit 10',
880         '%4603': 'Undefined Access (no effect) Bit 11',
881         '%4604': 'Undefined Access (no effect) Bit 12',
882         '%4605': 'Undefined Access (no effect) Bit 13',
883         '%4606': 'Undefined Access (no effect) Bit 14',
884         '%4607': 'Undefined Access (no effect) Bit 15',
885         '%4608': 'Create instance of object type',
886         '%4609': 'Undefined Access (no effect) Bit 1',
887         '%4610': 'Undefined Access (no effect) Bit 2',
888         '%4611': 'Undefined Access (no effect) Bit 3',
889         '%4612': 'Undefined Access (no effect) Bit 4',
890         '%4613': 'Undefined Access (no effect) Bit 5',
891         '%4614': 'Undefined Access (no effect) Bit 6',
892         '%4615': 'Undefined Access (no effect) Bit 7',
893         '%4616': 'Undefined Access (no effect) Bit 8',
894         '%4617': 'Undefined Access (no effect) Bit 9',
895         '%4618': 'Undefined Access (no effect) Bit 10',
896         '%4619': 'Undefined Access (no effect) Bit 11',
897         '%4620': 'Undefined Access (no effect) Bit 12',
898         '%4621': 'Undefined Access (no effect) Bit 13',
899         '%4622': 'Undefined Access (no effect) Bit 14',
900         '%4623': 'Undefined Access (no effect) Bit 15',
901         '%4864': 'Query State',
902         '%4865': 'Modify State',
903         '%5120': 'Channel read message',
904         '%5121': 'Channel write message',
905         '%5122': 'Channel query information',
906         '%5123': 'Channel set information',
907         '%5124': 'Undefined Access (no effect) Bit 4',
908         '%5125': 'Undefined Access (no effect) Bit 5',
909         '%5126': 'Undefined Access (no effect) Bit 6',
910         '%5127': 'Undefined Access (no effect) Bit 7',
911         '%5128': 'Undefined Access (no effect) Bit 8',
912         '%5129': 'Undefined Access (no effect) Bit 9',
913         '%5130': 'Undefined Access (no effect) Bit 10',
914         '%5131': 'Undefined Access (no effect) Bit 11',
915         '%5132': 'Undefined Access (no effect) Bit 12',
916         '%5133': 'Undefined Access (no effect) Bit 13',
917         '%5134': 'Undefined Access (no effect) Bit 14',
918         '%5135': 'Undefined Access (no effect) Bit 15',
919         '%5136': 'Assign process',
920         '%5137': 'Set Attributes',
921         '%5138': 'Query Attributes',
922         '%5139': 'Terminate Job',
923         '%5140': 'Set Security Attributes',
924         '%5141': 'Undefined Access (no effect) Bit 5',
925         '%5142': 'Undefined Access (no effect) Bit 6',
926         '%5143': 'Undefined Access (no effect) Bit 7',
927         '%5144': 'Undefined Access (no effect) Bit 8',
928         '%5145': 'Undefined Access (no effect) Bit 9',
929         '%5146': 'Undefined Access (no effect) Bit 10',
930         '%5147': 'Undefined Access (no effect) Bit 11',
931         '%5148': 'Undefined Access (no effect) Bit 12',
932         '%5149': 'Undefined Access (no effect) Bit 13',
```

alienvault-ossim / os-sim / agent / src / ParserUtil.py

↑ Top

Code



































Blame

1146 lines (1016 loc) · 46.7 KB

Raw



```
937         '%5378': 'InitializeServer',
938         '%5379': 'CreateDomain',
939         '%5380': 'EnumerateDomains',
940         '%5381': 'LookupDomain',
941         '%5382': 'Undefined Access (no effect) Bit 6',
942         '%5383': 'Undefined Access (no effect) Bit 7',
943         '%5384': 'Undefined Access (no effect) Bit 8',
944         '%5385': 'Undefined Access (no effect) Bit 9',
945         '%5386': 'Undefined Access (no effect) Bit 10',
946         '%5387': 'Undefined Access (no effect) Bit 11',
947         '%5388': 'Undefined Access (no effect) Bit 12',
948         '%5389': 'Undefined Access (no effect) Bit 13',
949         '%5390': 'Undefined Access (no effect) Bit 14',
950         '%5391': 'Undefined Access (no effect) Bit 15',
951         '%5392': 'ReadPasswordParameters',
952         '%5393': 'WritePasswordParameters',
```

- >  alienvault-dummy-common
- >  alienvault-dummy-database
- >  alienvault-dummy-framework
- >  alienvault-dummy-sensor-ids
- >  alienvault-dummy-sensor
- >  alienvault-dummy-server
- >  alienvault-libs
- >  alienvault-plugins
- >  alienvault-reporting
- >  alienvault-rhythm
- ▼  os-sim
- ▼  agent
- >  debian
- ▼  src
- >  doc
- >  etc
-  Agent.py
-  Config.py
-  Conn.py
-  Control.py
-  ControlError.py
-  ControllInventory.py
-  ControlNmap.py
-  ControlSniffer.py
-  ControlUtil.py
-  ControlVAScanner.py
-  Database.py
-  Detector.py
-  Event.py
-  EventList.py
-  Exceptions.py
-  InventoryTask.py
-  InventoryTask_LDAP.py
-  InventoryTask NMAP.py

```
953 '%5394': 'ReadOtherParameters',
954 '%5395': 'WriteOtherParameters',
955 '%5396': 'CreateUser',
956 '%5397': 'CreateGlobalGroup',
957 '%5398': 'CreateLocalGroup',
958 '%5399': 'GetLocalGroupMembership',
959 '%5400': 'ListAccounts',
960 '%5401': 'LookupIDs',
961 '%5402': 'AdministerServer',
962 '%5408': 'ReadInformation',
963 '%5409': 'WriteAccount',
964 '%5410': 'AddMember',
965 '%5411': 'RemoveMember',
966 '%5412': 'ListMembers',
967 '%5424': 'AddMember',
968 '%5425': 'RemoveMember',
969 '%5426': 'ListMembers',
970 '%5427': 'ReadInformation',
971 '%5428': 'WriteAccount',
972 '%5440': 'ReadGeneralInformation',
973 '%5441': 'ReadPreferences',
974 '%5442': 'WritePreferences',
975 '%5443': 'ReadLogon',
976 '%5444': 'ReadAccount',
977 '%5445': 'WriteAccount',
978 '%5446': 'ChangePassword (with knowledge of old password)',
979 '%5447': 'SetPassword (without knowledge of old password)',
980 '%5448': 'ListGroups',
981 '%5449': 'ReadGroupMembership',
982 '%5450': 'ChangeGroupMembership',
983 '%5632': 'View non-sensitive policy information',
984 '%5633': 'View system audit requirements',
985 '%5634': 'Get sensitive policy information',
986 '%5635': 'Modify domain trust relationships',
987 '%5636': 'Create special accounts (for assignment of user rights)',
988 '%5637': 'Create a secret object',
989 '%5638': 'Create a privilege',
990 '%5639': 'Set default quota limits',
991 '%5640': 'Change system audit requirements',
992 '%5641': 'Administer audit log attributes',
993 '%5642': 'Enable/Disable LSA',
994 '%5643': 'Lookup Names/SIDs',
995 '%5648': 'Change secret value',
996 '%5649': 'Query secret value',
997 '%5664': 'Query trusted domain name/SID',
998 '%5665': 'Retrieve the controllers in the trusted domain',
999 '%5666': 'Change the controllers in the trusted domain',
1000 '%5667': 'Query the Posix ID offset assigned to the trusted domain',
1001 '%5668': 'Change the Posix ID offset assigned to the trusted domain',
1002 '%5680': 'Query account information',
1003 '%5681': 'Change privileges assigned to account',
1004 '%5682': 'Change quotas assigned to account',
1005 '%5683': 'Change logon capabilities assigned to account',
1006 '%6656': 'Enumerate desktops',
1007 '%6657': 'Read attributes',
1008 '%6658': 'Access Clipboard',
1009 '%6659': 'Create desktop',
1010 '%6660': 'Write attributes',
1011 '%6661': 'Access global atoms',
1012 '%6662': 'Exit windows',
1013 '%6663': 'Unused Access Flag',
1014 '%6664': 'Include this windowstation in enumerations',
1015 '%6665': 'Read screen',
1016 '%6672': 'Read Objects',
1017 '%6673': 'Create window',
1018 '%6674': 'Create menu',
1019 '%6675': 'Hook control',
1020 '%6676': 'Journal (record)',
1021 '%6677': 'Journal (playback)',
1022 '%6678': 'Include this desktop in enumerations',
1023 '%6679': 'Write objects',
1024 '%6680': 'Switch to this desktop',
1025 '%6912': 'Administer print server',
1026 '%6913': 'Enumerate printers',
```

```
1027         '%6930': 'Full Control',
1028         '%6931': 'Print',
1029         '%6948': 'Administer Document',
1030         '%7168': 'Connect to service controller',
1031         '%7169': 'Create a new service',
1032         '%7170': 'Enumerate services',
1033         '%7171': 'Lock service database for exclusive access',
1034         '%7172': 'Query service database lock state',
1035         '%7173': 'Set last-known-good state of service database',
1036         '%7184': 'Query service configuration information',
1037         '%7185': 'Set service configuration information',
1038         '%7186': 'Query status of service',
1039         '%7187': 'Enumerate dependencies of service',
1040         '%7188': 'Start the service',
1041         '%7189': 'Stop the service',
1042         '%7190': 'Pause or continue the service',
1043         '%7191': 'Query information from service',
1044         '%7192': 'Issue service-specific control commands',
1045         '%7424': 'DDE Share Read',
1046         '%7425': 'DDE Share Write',
1047         '%7426': 'DDE Share Initiate Static',
1048         '%7427': 'DDE Share Initiate Link',
1049         '%7428': 'DDE Share Request',
1050         '%7429': 'DDE Share Advise',
1051         '%7430': 'DDE Share Poke',
1052         '%7431': 'DDE Share Execute',
1053         '%7432': 'DDE Share Add Items',
1054         '%7433': 'DDE Share List Items',
1055         '%7680': 'Create Child',
1056         '%7681': 'Delete Child',
1057         '%7682': 'List Contents',
1058         '%7683': 'Write Self',
1059         '%7684': 'Read Property',
1060         '%7685': 'Write Property',
1061         '%7686': 'Delete Tree',
1062         '%7687': 'List Object',
1063         '%7688': 'Control Access'}
1064
1065     for id, text in ids.iteritems():
1066         if string.find(id) >= 0:
1067             string_translated = string_translated + text + ", "
1068
1069
1070
1071
1072
1073     HOST_RESOLV_DYNAMIC_CACHE = {}
1074
1075     # Dynamic host-ip cache.
1076     def refreshCache(data):
1077         """ Refresh the HOST dynamic cache """
1078         # action="refresh_asset_list" list={ossim-unstable-pro=192.168.2.18,crosa=192.1
1079         logger.debug("Updating dynamic host cache... %s" % data)
1080         # HostResolv.HOST_RESOLV_DYNAMIC_CACHE.clear()
1081         pattern = "action=\"refresh_asset_list\"\\s+list=({?P<list>.*})"
1082         ipv4_reg = "\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}"
1083         hostname_valid = "(([a-zA-Z]|[a-zA-Z][a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z]|[A
1084         reg_comp = re.compile(pattern)
1085         res = reg_comp.match(data)
1086         host_list = []
1087         new_cache = {}
1088         if res is not None:
1089             tmp_list = res.group('list')
1090             if tmp_list is not None:
1091                 host_list = tmp_list.split(';')
1092                 logger.debug("HOST_LIST: %s" % host_list)
1093                 for asset in host_list:
1094                     if asset == '':
1095                         continue
1096                     ip, hostnames = asset.split('=')
1097                     hostname_list = hostnames.split(',')
1098                     logger.debug("IP = %s , hostnamelist: %s" % (ip, hostname_list))
1099                     for hostname in hostname_list:
1100                         hostname = hostname.strip()
1101                         hostname = hostname.lower()
```

```
1102             if re.match(ipv4_reg, ip) and re.match(hostname_valid, hostname):
1103                 if new_cache.has_key(hostname):
1104                     if ip not in new_cache[hostname]:
1105                         new_cache[hostname].append(ip)
1106             else:
1107                 new_cache[hostname] = []
1108                 new_cache[hostname].append(ip)
1109
1110         HostResolv.HOST_RESOLV_DYNAMIC_CACHE = new_cache
1111
1112         HostResolv.printCache()
1113         HostResolv.saveHostCache()
1114
1115     refreshCache = staticmethod(refreshCache)
1116
1117     def saveHostCache():
1118         logger.info("Saving dynamic host cache in /etc/ossim/agent/host_cache.dic")
1119         pickle.dump(HostResolv.HOST_RESOLV_DYNAMIC_CACHE, open("/etc/ossim/agent/host_c
1120
1121     saveHostCache = staticmethod(saveHostCache)
1122
1123     def loadHostCache():
1124         if os.path.isfile("/etc/ossim/agent/host_cache.dic"):
1125             try:
1126                 logger.debug("Loading dynamic host cache from '/etc/ossim/agent/host_ca
1127                 HostResolv.HOST_RESOLV_DYNAMIC_CACHE = pickle.load(open("/etc/ossim/age
1128                 HostResolv.printCache()
1129             except:
1130                 logger.warning("Deleting corrupt file host_cache_pro.dic")
1131                 os.remove("/etc/ossim/agent/host_cache_pro.dic")
1132                 return False
1133         else:
1134             return False
1135
1136         return True
1137
1138     loadHostCache = staticmethod(loadHostCache)
1139
1140     def printCache():
1141         logger.debug("----- Dynamic cache -----")
1142         for host, ip in HostResolv.HOST_RESOLV_DYNAMIC_CACHE.items():
1143             logger.debug("%s ----->> %s" % (host, ip))
1144         logger.debug("-----")
1145
1146     printCache = staticmethod(printCache)
```