Appendix A:**PenTester - Internal specification**

author: Marek Skrobacki

skrobul@skrobul.com

Contents

1 Namespace Documentation **1**

1.1 pentester Namespace Reference 1

1.2 pentester::hosts Namespace Reference 2

1.3 pentester::hosts::ifconfig Namespace Reference 3

1.4 pentester::hosts::metasploit Namespace Reference 4

1.5 pentester::hosts::models Namespace Reference 5

1.6 pentester::hosts::netscan Namespace Reference 6

1.7 pentester::hosts::views Namespace Reference 7

1.8 pentester::manage Namespace Reference 9

1.9 pentester::urls Namespace Reference 10

1.10 pentester::worker Namespace Reference 12

1.11 pentester::worker::models Namespace Reference 13

1.12 pentester::worker::views Namespace Reference 14

2 Class Documentation **17**

2.1 Configuration Class Reference 18

2.2 Configuration::Meta Class Reference 21

2.3 ConnectionError Class Reference 22

2.4 Host Class Reference 23

2.5 Host::Meta Class Reference 25

2.6 IFConfig Class Reference 26

2.7 Logs Class Reference 28

2.8 Logs::Meta Class Reference 30

2.9 MetaSploit Class Reference 31

2.10 MetaSploitLocal Class Reference 33

2.11 MetaSploitRemote Class Reference 35

2.12 models::Model Class Reference 37

2.13 MsfExecNotFound Class Reference 38

2.14 NetScan Class Reference 39
2.15 PluginError Class Reference 40
2.16 Service Class Reference 41
2.17 Service::Meta Class Reference 43
2.18 Session Class Reference 44
2.19 Session::Meta Class Reference 46
2.20 TIMEOUT Class Reference 47

3 File Documentation **49**

3.1 __init__.py File Reference 49
3.2 __init__.py File Reference 50
3.3 __init__.py File Reference 51
3.4 ifconfig.py File Reference 52
3.5 manage.py File Reference 53
3.6 metasploit.py File Reference 54
3.7 models.py File Reference 55
3.8 models.py File Reference 56
3.9 netscan.py File Reference 57
3.10 urls.py File Reference 58
3.11 views.py File Reference 59
3.12 views.py File Reference 60

Chapter 1

Namespace Documentation

1.1 pentester Namespace Reference

Namespaces

- namespace hosts
- namespace manage
- namespace urls
- namespace worker

1.2 pentester::hosts Namespace Reference

Namespaces

- namespace ifconfig
- namespace metasploit
- namespace models
- namespace netscan
- namespace views

1.3 pentester::hosts::ifconfig Namespace Reference

Classes

- class IFConfig

1.4 pentester::hosts::metasploit Namespace Reference

Classes

- class TIMEOUT
- class PluginError
- class ConnectionError
- class MsfExecNotFound
- class MetaSploit
- class MetaSploitLocal
- class MetaSploitRemote

Variables

- int MSFTIMEOUT = 120

1.4.1 Variable Documentation

1.4.1.1 int MSFTIMEOUT = 120

Definition at line 5 of file metasploit.py.

1.5 pentester::hosts::models Namespace Reference

Classes

- class Host
- class Service
- class Configuration

1.6 pentester::hosts::netscan Namespace Reference

Classes

- class NetScan

Variables

- tuple i = ifconfig.IFConfig.get_ifaces_up()

1.6.1 Variable Documentation

1.6.1.1 tuple i = ifconfig.IFConfig.get_ifaces_up()

Definition at line 55 of file netscan.py.

1.7 pentester::hosts::views Namespace Reference

Functions

- def ifaces
- def ifaceslist
- def iface_detail
- def index
- def createMenu
- def services
- def servupdate
- def addport
- def configuration
- def deletehost

1.7.1 Function Documentation

1.7.1.1 def pentester::hosts::views::addport (*request*)

```
Adds user-specified service to services table in database.
```

Definition at line 114 of file hosts/views.py.

1.7.1.2 def pentester::hosts::views::configuration (*request*)

```
This view is used to create, display or edit configuration
of our tool. Currently this view is used for setting path
to local meta sploit framework, or setting the IP address and destination
port of the remote meta sploit framework.
This view is based on Django generic views. If configuration object
does not exist in the database we create it. If exist, just display
and update it.
```

Definition at line 137 of file hosts/views.py.

1.7.1.3 def pentester::hosts::views::createMenu (*current*)

```
Returns a dictionary of menu items. If 'current' argument matches 'name' property of
particular menu item, it sets True, for 'current' property in dictionary.
```

Definition at line 57 of file hosts/views.py.

1.7.1.4 def pentester::hosts::views::deletehost (*request*, *hostid*)

```
Deletes all services associated with particular host and host itself
from the database. Takes host ID as an argument. After deleting object
from the model, redirects to the list of services.
```

Definition at line 169 of file hosts/views.py.

1.7.1.5 def pentester::hosts::views::iface_detail (*request*, *iface*)

```
Display detailed information about particular network interface in the
system.
```

Definition at line 35 of file hosts/views.py.

1.7.1.6 def pentester::hosts::views::ifaces (*request*)

```
Displays names of all network interfaces in the system.
```

Definition at line 9 of file hosts/views.py.

1.7.1.7 def pentester::hosts::views::ifaceslist ()

```
Gets list of network interfaces on the system and returns a list of
dictionaries with 'name', 'ip' and 'mask' keys. Works with conjunction
on IFConfig module.
```

Definition at line 23 of file hosts/views.py.

1.7.1.8 def pentester::hosts::views::index (*request*)

```
This view is used to render main application page.
All the work being done here is getting network interface list and
creating code for navigation menu.
```

Definition at line 49 of file hosts/views.py.

1.7.1.9 def pentester::hosts::views::services (*request*, *hostid* = None)

```
    Returns list of hosts correlated with services.
    If 'hostid' argument given, returns services of the particular host.
```

Definition at line 75 of file hosts/views.py.

1.7.1.10 def pentester::hosts::views::servupdate (*request*)

```
   Updates services table.
   Sets service to 'up' state if serviceXX box is checked in POST request.
   Otherwise sets service to 'down' state. After saving changes, redirects
   user to service list view.
```

Definition at line 98 of file hosts/views.py.

1.8 pentester::manage Namespace Reference

1.9 pentester::urls Namespace Reference

Variables

- dictionary lista_hostow
- dictionary logs_info
- dictionary sessions_info
- tuple urlpatterns

1.9.1 Variable Documentation

1.9.1.1 dictionary lista_hostow

Initial value:

```
{
                'queryset' : Host.objects.all(),
                'template_name' : 'host_list.html',
}
```

Definition at line 8 of file urls.py.

1.9.1.2 dictionary logs_info

Initial value:

```
{
            'queryset' : Logs.objects.all(),
            'template_name' : 'logs_list.html',
            'allow_empty' : True,
            'extra_context' : { 'menuitems' : createMenu('logs') },
}
```

Definition at line 12 of file urls.py.

1.9.1.3 dictionary sessions_info

Initial value:

```
{
                 'queryset' : map(lambda x: x.rhost, Session.objects.all()),
                 'template_name' : 'sess_list.html',
                 'allow_empty' : True,
                 'extra_context' : {'menuitems' : createMenu('results')}
}
```

Definition at line 18 of file urls.py.

1.9.1.4 tuple urlpatterns

Initial value:

```
patterns('',
     (r'^hosty/$',  list_detail.object_list, lista_hostow),
     (r'^logs/$', list_detail.object_list, logs_info),
     (r'^logs/clear/$', 'pentester.worker.views.clearlogs'),
     #(r'^results/$', list_detail.object_list, sessions_info),
     (r'results/$', 'pentester.worker.views.results'),
     (r'^deletehost/(?P<hostid>\d+)/$', 'pentester.hosts.views.deletehost'),
     (r'^if/$', 'pentester.hosts.views.ifaces'),
     (r'^if/(?P<iface>\w+)/$', 'pentester.hosts.views.iface_detail'),
     (r'^static/(?P<path>.*)$', 'django.views.static.serve', { 'document_root':'/home/skrobul/workspace/in
     (r'^services/update/', 'pentester.hosts.views.servupdate'),
     (r'^services/add/', 'pentester.hosts.views.addport'),
     (r'^services/(?P<hostid>.*)', 'pentester.hosts.views.services'),
     (r'^config/$', 'pentester.hosts.views.configuration'),
     (r'^scan/$', 'pentester.worker.views.scan'),
     (r'^scan/net/$', 'pentester.worker.views.netscan'),
     (r'^exploit/$', 'pentester.worker.views.exploit'),
     (r'^$', 'pentester.hosts.views.index'),
)
```

Definition at line 24 of file urls.py.

1.10 pentester::worker Namespace Reference

Namespaces

- namespace models
- namespace views

1.11 pentester::worker::models Namespace Reference

Classes

- class Logs
- class Session

1.12 pentester::worker::views Namespace Reference

Functions

- def getcfgobj
- def scan
- def netscan
- def isValidNetwork
- def exploit
- def clearlogs
- def results

1.12.1 Function Documentation

1.12.1.1 def pentester::worker::views::clearlogs (*request*)

```
Deletes all Log objects from database.
```

Definition at line 106 of file worker/views.py.

1.12.1.2 def pentester::worker::views::exploit (*request*)

```
Starts exploitation of hosts. Hosts addresses is retrieved from the
database (prior filled manually or by network scan). Results are collected
as text and inserted to the Logs table in the database. Additionaly
this method runs listing of currently opened sessions (after MetaSploit
exploitation), parses it, and inserts tuples (lhost,lport,rhost,rport)
describing opened sessions to the database.
```

Definition at line 73 of file worker/views.py.

1.12.1.3 def pentester::worker::views::getcfgobj ()

```
Internal method used for getting tool configuration (mainly MetaSploit parameters)
from the Configuration model. Returns Configuration objects if exist, or renders
error page with proper alert.
```

Definition at line 11 of file worker/views.py.

1.12.1.4 def pentester::worker::views::isValidNetwork (*net*)

Definition at line 62 of file worker/views.py.

1.12.1.5 def pentester::worker::views::netscan (*request*)

```
Performs an NMAP network scan on specified IP network (passed through POST['address']
argument). Scan is run by executing db_nmap command of the metasploit wrapper for NMAP.
Results are collected to the temporary XML file (-oX option in nmap), and then
parsed by MetaSploit Framework to the SQL database format.
```

Definition at line 43 of file worker/views.py.

1.12.1.6 def pentester::worker::views::results (*request*)

```
Processes list of currently opened sessions (successfully exploited hosts),
by taking their rhost value, and linking them to unordered list of IP
addresses of remote hosts. Afterwards list is passed to proper template
for display.
```

Definition at line 118 of file worker/views.py.

1.12.1.7 def pentester::worker::views::scan (*request*)

```
View that performs a scan for IP services on remote hosts contained in IP subnet
matching current subnet set on the particular network interface (this one specified
in request by POST['iface']
```

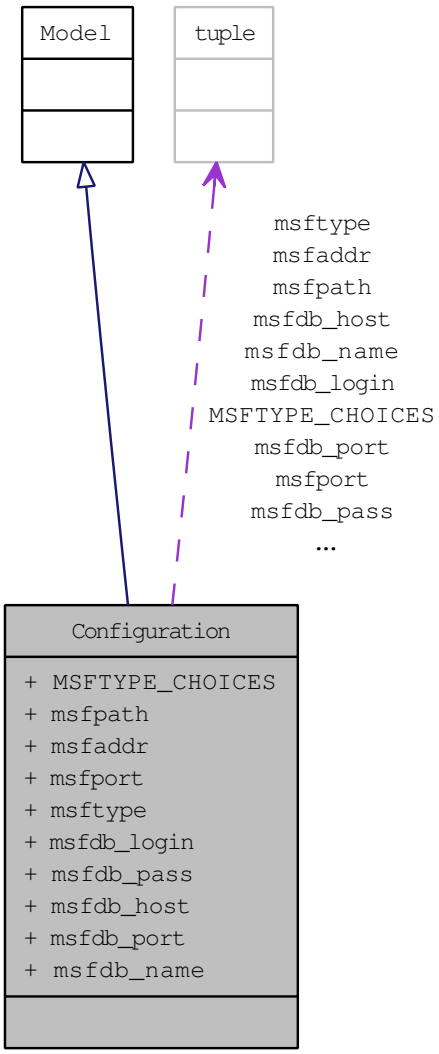
Definition at line 25 of file worker/views.py.

Chapter 2

Class Documentation

2.1 Configuration Class Reference

Inheritance diagram for Configuration:Collaboration diagram for Configuration:



Static Public Attributes

- tuple MSFTYPE_CHOICES
- tuple msfpath = models.CharField(maxlength=255,blank=True, null=True)
- tuple msfaddr = models.IPAddressField(blank=True,null=True)
- tuple msfport = models.PositiveIntegerField(blank=True,null=True)
- tuple msftype = models.CharField(maxlength=1,choices=MSFTYPE_CHOICES)
- tuple msfdb_login = models.CharField(maxlength=255)
- tuple msfdb_pass = models.CharField(maxlength=255)
- tuple msfdb_host = models.CharField(maxlength=255,default="localhost")
- tuple msfdb_port = models.PositiveIntegerField(default=5432)
- tuple msfdb_name = models.CharField(maxlength=128)

Classes

- class Meta

2.1.1 Detailed Description

Definition at line 26 of file hosts/models.py.

2.1.2 Member Data Documentation

2.1.2.1 tuple MSFTYPE_CHOICES [static]

Initial value:

```
(
                ('R', 'Remote'),
                ('L', 'Local')
        )
```

Definition at line 27 of file hosts/models.py.

2.1.2.2 tuple msfpath = models.CharField(maxlength=255,blank=True, null=True) [static]

Definition at line 33 of file hosts/models.py.

2.1.2.3 tuple msfaddr = models.IPAddressField(blank=True,null=True) [static]

Definition at line 34 of file hosts/models.py.

2.1.2.4 tuple msfport = models.PositiveIntegerField(blank=True,null=True) [static]

Definition at line 35 of file hosts/models.py.

2.1.2.5 tuple msftype = models.CharField(maxlength=1,choices=MSFTYPE_CHOICES) [static]

Definition at line 36 of file hosts/models.py.

2.1.2.6 tuple msfdb_login = models.CharField(maxlength=255) [static]

Definition at line 37 of file hosts/models.py.

2.1.2.7 tuple msfdb_pass = models.CharField(maxlength=255) [static]

Definition at line 38 of file hosts/models.py.

2.1.2.8 tuple msfdb_host = models.CharField(maxlength=255,default="localhost") [static]

Definition at line 39 of file hosts/models.py.

2.1.2.9 tuple msfdb_port = models.PositiveIntegerField(default=5432) [static]

Definition at line 40 of file hosts/models.py.

2.1.2.10 tuple msfdb_name = models.CharField(maxlength=128) [static]

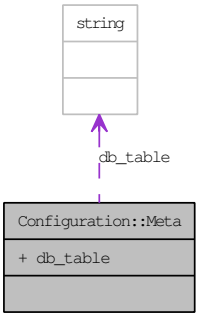
Definition at line 41 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.2 Configuration::Meta Class Reference

Collaboration diagram for Configuration::Meta:



Static Public Attributes

- string db_table = "configuration"

2.2.1 Detailed Description

Definition at line 31 of file hosts/models.py.

2.2.2 Member Data Documentation

2.2.2.1 string db_table = "configuration" [static]

Definition at line 32 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.3 ConnectionError Class Reference

Inheritance diagram for ConnectionError:Collaboration diagram for ConnectionError:

Public Member Functions

- def __init__
- def __str__

2.3.1 Detailed Description

Definition at line 23 of file metasploit.py.

2.3.2 Member Function Documentation

2.3.2.1 def __init__ (*self*)

Definition at line 24 of file metasploit.py.

2.3.2.2 def __str__ (*self*)

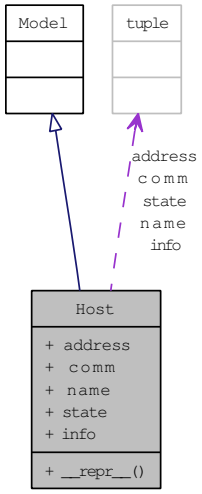
Definition at line 26 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.4 Host Class Reference

Inheritance diagram for Host:Collaboration diagram for Host:



Public Member Functions

- def __repr__

Static Public Attributes

- tuple address = models.CharField(maxlength=16,blank=True)
- tuple comm = models.CharField(maxlength=255,blank=True)
- tuple name = models.CharField(maxlength=255,blank=True)
- tuple state = models.CharField(maxlength=255,blank=True)
- tuple info = models.CharField(maxlength=1024,blank=True)

Classes

- class Meta

2.4.1 Detailed Description

Definition at line 3 of file hosts/models.py.

2.4.2 Member Function Documentation

2.4.2.1 def __repr__ (*self*)

Definition at line 12 of file hosts/models.py.

2.4.3 Member Data Documentation

2.4.3.1 tuple address = models.CharField(maxlength=16,blank=True) [static]

Definition at line 6 of file hosts/models.py.

2.4.3.2 tuple comm = models.CharField(maxlength=255,blank=True) [static]

Definition at line 7 of file hosts/models.py.

2.4.3.3 tuple name = models.CharField(maxlength=255,blank=True) [static]

Definition at line 8 of file hosts/models.py.

2.4.3.4 tuple state = models.CharField(maxlength=255,blank=True) [static]

Definition at line 9 of file hosts/models.py.

2.4.3.5 tuple info = models.CharField(maxlength=1024,blank=True) [static]

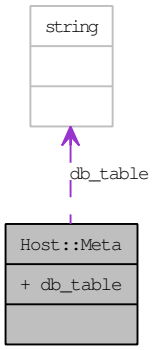
Definition at line 10 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.5 Host::Meta Class Reference

Collaboration diagram for Host::Meta:



Static Public Attributes

- string db_table = 'hosts'

2.5.1 Detailed Description

Definition at line 4 of file hosts/models.py.

2.5.2 Member Data Documentation

2.5.2.1 string db_table = 'hosts' [static]

Definition at line 5 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.6 IFConfig Class Reference

Public Member Functions

- def __init__
- def get_ip_address
- def get_netmask
- def get_ifaces_up
- def long2cidr

2.6.1 Detailed Description

```
Pozwala odczytać informacje o interfejsach sieciowych
    takie jak adres IP oraz maska podsieci
```

Definition at line 8 of file ifconfig.py.

2.6.2 Member Function Documentation

2.6.2.1 def __init__ (*self*)

Definition at line 11 of file ifconfig.py.

2.6.2.2 def get_ip_address (*ifname*)

```
Queries Linux kernel for IP addres of the particular interface
chosen by passing mandatory "ifname" argument. Returns string
containing IP addres in dotted-decimal format (eg. '4.2.2.2')
```

Definition at line 15 of file ifconfig.py.

2.6.2.3 def get_netmask (*ifname*, *long* = `False`)

```
Queries Linux kernel for netmask of the interface "ifname".
ifname argument should be given as a canonical name of the network interface
such as "eth0", "lo" etc. Method returns string containing netmask value
in one of two well known formats. If you pass True value as "long" argument
it will return netmask in long format (e.g. '255.255.255.0'). Otherwise
If you give 'False' value as "long" argument it will return netmask of
the interface in CIDR notation (eg. '/24')
```

Definition at line 28 of file ifconfig.py.

2.6.2.4 def get_ifaces_up ()

```
Queries Linux kernel for structure containing various information about
installed network interfaces. Returns list of strings with names of
interfaces (only those that are currently in the "up" state).
```

Definition at line 48 of file ifconfig.py.

2.6.2.5 def long2cidr (*longmask*)

```
Converts specified network mask in long format to CIDR (Classless Inter-Domain Routing)
format. For example if you pass "255.255.255.0" string as an argument, it will return string
"/24"
```

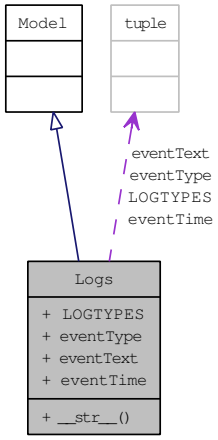
Definition at line 62 of file ifconfig.py.

The documentation for this class was generated from the following file:

- ifconfig.py

2.7 Logs Class Reference

Inheritance diagram for Logs:Collaboration diagram for Logs:



Public Member Functions

- def __str__

Static Public Attributes

- tuple LOGTYPES
- tuple eventType = models.CharField(maxlength=1,choices=LOGTYPES)
- tuple eventText = models.TextField()
- tuple eventTime = models.DateTimeField(auto_now_add=True)

Classes

- class Meta

2.7.1 Detailed Description

```
This model stores RAW results from every operation on
MetaSploit Framework or any other external processess
run through pexpect module
```

Definition at line 3 of file worker/models.py.

2.7.2 Member Function Documentation

2.7.2.1 def __str__ (*self*)

Definition at line 18 of file worker/models.py.

2.7.3 Member Data Documentation

2.7.3.1 tuple LOGTYPES [static]

Initial value:

```
(
        ('S', 'Scanner log'),
        ('E', 'Exploitation log'),
    )
```

Definition at line 9 of file worker/models.py.

2.7.3.2 tuple eventType = models.CharField(maxlength=1,choices=LOGTYPES) [static]

Definition at line 15 of file worker/models.py.

2.7.3.3 tuple eventText = models.TextField() [static]

Definition at line 16 of file worker/models.py.

2.7.3.4 tuple eventTime = models.DateTimeField(auto_now_add=True) [static]

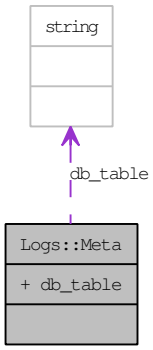
Definition at line 17 of file worker/models.py.

The documentation for this class was generated from the following file:

- worker/models.py

2.8 Logs::Meta Class Reference

Collaboration diagram for Logs::Meta:



Static Public Attributes

- string db_table = "logs"

2.8.1 Detailed Description

Definition at line 13 of file worker/models.py.

2.8.2 Member Data Documentation

2.8.2.1 string db_table = "logs" [static]

Definition at line 14 of file worker/models.py.

The documentation for this class was generated from the following file:

- worker/models.py

2.9 MetaSploit Class Reference

Inheritance diagram for MetaSploit:

Public Member Functions

- def __init__
- def __del__
- def showMatchingExploits
- def exploit
- def listsessions
- def scan
- def loadPlugins

2.9.1 Detailed Description

```
Base class containing methods responsible for communication with Metasploit Framework
```

Definition at line 34 of file metasploit.py.

2.9.2 Member Function Documentation

2.9.2.1 def __init__ (*self*)

```
Default constructor for the Metasploit base class is (abstract) empty.
```

Definition at line 38 of file metasploit.py.

2.9.2.2 def __del__ (*self*)

```
Destructor for MetaSploit class. Kills the child process spawned
by our program. In most cases it is a telnet process or localy running
MetaSploit Framework
```

Definition at line 43 of file metasploit.py.

2.9.2.3 def showMatchingExploits (*self*)

```
Performs matching of available MetaSploit exploits with relation to
services information in the database. Matching is based on IP
destination ports of a particular services and information
provided by authors of MetaSploit exploits.
```

Definition at line 52 of file metasploit.py.

2.9.2.4 def exploit (*self*, *include* = None, *exclude* = None)

```
Starts exploiting of every service and every host existing
in database. Optionally you can specify exclusion or/and inclusion,
by passing particular network ranges as the "include" or "exclude" parameter.
Example:
MetaSploit.exploit(include="172.30.31.0/24")
 or
MetaSploit.exploit(include="10.0.0.1-10.0.0.50")

"exclude" parameter syntax is same as for "include" one.
```

Definition at line 76 of file metasploit.py.

2.9.2.5 def listsessions (*self*)

```
Lists currently connected telnet sessions to the exploited hosts.
   Returns list of string containing raw output from MetaSploit.
```

Definition at line 117 of file metasploit.py.

2.9.2.6 def scan (*self*, *network*)

```
Runs scan for services on specified network. This command spawns
nmap port scanner through MetaSploit framework. Notice that, if you
want to run scan on remote framework, nmap installation on remote
host (running MSF) is required.
```

Definition at line 129 of file metasploit.py.

2.9.2.7 def loadPlugins (*self*, *login*, *password*, *dbname*, *hostname*, *port*)

```
Loads all required framework modules. Currently used to load PostgreSQL backend
module, then make connection to database using credentials passed to the connect() method.
```

Definition at line 146 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.10 MetaSploitLocal Class Reference

Inheritance diagram for MetaSploitLocal:Collaboration diagram for MetaSploitLocal:

Public Member Functions

- def __init__
- def connect

Public Attributes

- path
- port
- host
- connected
- pipe

2.10.1 Detailed Description

```
Class containing code responsible for communication with locally spawned
MetaSploit framework
```

Definition at line 164 of file metasploit.py.

2.10.2 Member Function Documentation

2.10.2.1 def __init__ (*self*, *msfconsolepath*)

Definition at line 169 of file metasploit.py.

2.10.2.2 def connect (*self*, *login*, *password*, *dbname*, *hostname* = "localhost", *port* = "5432")

Definition at line 174 of file metasploit.py.

2.10.3 Member Data Documentation

2.10.3.1 path

Definition at line 170 of file metasploit.py.

2.10.3.2 port

Definition at line 171 of file metasploit.py.

2.10.3.3 host

Definition at line 172 of file metasploit.py.

2.10.3.4 connected

Definition at line 173 of file metasploit.py.

2.10.3.5 pipe

Definition at line 176 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.11 MetaSploitRemote Class Reference

Inheritance diagram for MetaSploitRemote:Collaboration diagram for MetaSploitRemote:

Public Member Functions

- def __init__
- def connect

Public Attributes

- host
- port
- path
- connected
- pipe

2.11.1 Detailed Description

```
Class containing code responsible for communication with MetaSploit framework
running on the remote host. Communication is done via TCP/IP->telnet protocol.
```

Definition at line 183 of file metasploit.py.

2.11.2 Member Function Documentation

2.11.2.1 def __init__ (*self*, *host*, *port*)

Definition at line 188 of file metasploit.py.

2.11.2.2 def connect (*self*, *login*, *password*, *dbname*, *hostname* = "localhost", *port* = "5432")

Definition at line 193 of file metasploit.py.

2.11.3 Member Data Documentation

2.11.3.1 host

Definition at line 189 of file metasploit.py.

2.11.3.2 port

Definition at line 190 of file metasploit.py.

2.11.3.3 path

Definition at line 191 of file metasploit.py.

2.11.3.4 connected

Definition at line 192 of file metasploit.py.

2.11.3.5 pipe

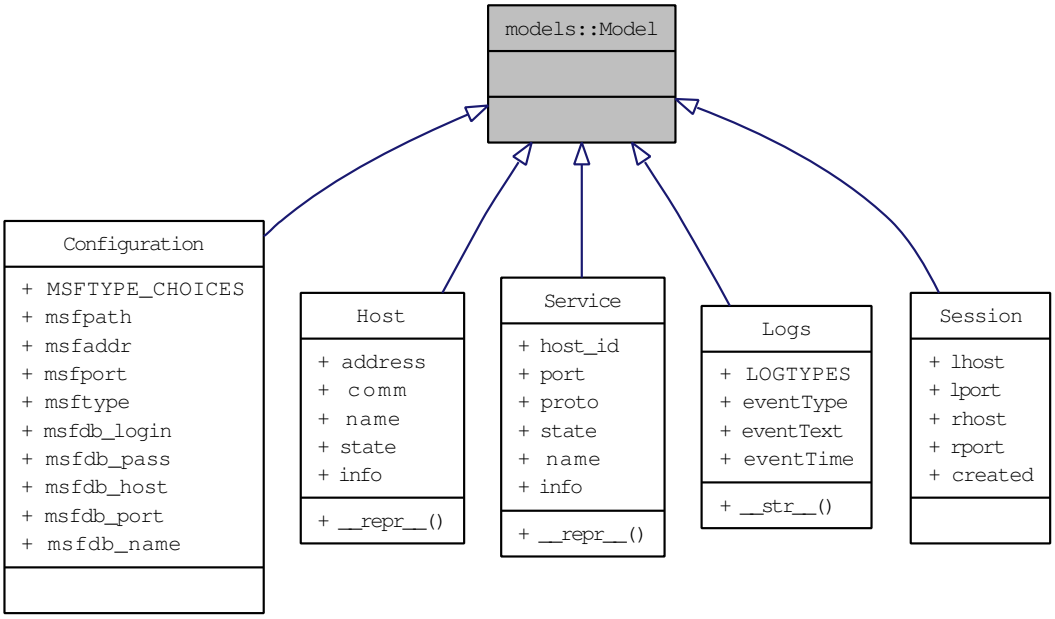
Definition at line 194 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.12 models::Model Class Reference

Inheritance diagram for models::Model:



The documentation for this class was generated from the following files:

- worker/models.py
- hosts/models.py

2.13 MsfExecNotFound Class Reference

Inheritance diagram for MsfExecNotFound:Collaboration diagram for MsfExecNotFound:

Public Member Functions

- def __init__
- def __str__

2.13.1 Detailed Description

Definition at line 28 of file metasploit.py.

2.13.2 Member Function Documentation

2.13.2.1 def __init__ (*self*)

Definition at line 29 of file metasploit.py.

2.13.2.2 def __str__ (*self*)

Definition at line 31 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.14 NetScan Class Reference

Public Member Functions

- def getIfaceData
- def scanNetwork
- def long2cidr
- def parseNmapResults

2.14.1 Detailed Description

Definition at line 4 of file netscan.py.

2.14.2 Member Function Documentation

2.14.2.1 def getIfaceData (*self*, *interfejs*)

```
Metoda pobiera argument interfejs(str) okreslajacy interfejs sieciowy dla ktorego ma sie wykonac.
W przypadku powodzenia zwracana jest krotka (adres_ip, maska_podsieci)
```

Definition at line 5 of file netscan.py.

2.14.2.2 def scanNetwork (*self*, *ip*, *maska*)

```
Metoda pobiera jako argument krotke (adres_ip,maska_podsieci) opisującą sieć IP dla której ma
być wykonane skanowanie.
Zwracana jest lista stringow, w kazdym z nich znajduja sie pojedyńcze linie wykonania programu
NMAP
```

Definition at line 19 of file netscan.py.

2.14.2.3 def long2cidr (*self*, *longmask*)

Definition at line 32 of file netscan.py.

2.14.2.4 def parseNmapResults (*self*, *results*)

Definition at line 37 of file netscan.py.

The documentation for this class was generated from the following file:

- netscan.py

2.15 PluginError Class Reference

Inheritance diagram for PluginError:Collaboration diagram for PluginError:

Public Member Functions

- def __init__
- def __str__

Public Attributes

- value

2.15.1 Detailed Description

Definition at line 18 of file metasploit.py.

2.15.2 Member Function Documentation

2.15.2.1 def __init__ (*self*, *value*)

Definition at line 19 of file metasploit.py.

2.15.2.2 def __str__ (*self*)

Definition at line 21 of file metasploit.py.

2.15.3 Member Data Documentation

2.15.3.1 value

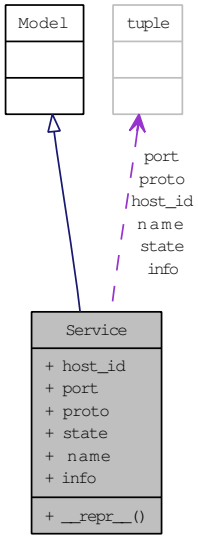
Definition at line 20 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

2.16 Service Class Reference

Inheritance diagram for Service:Collaboration diagram for Service:



Public Member Functions

- def __repr__

Static Public Attributes

- tuple host_id = models.ForeignKey(Host,db_column="host_id")
- tuple port = models.IntegerField(blank=True)
- tuple proto = models.CharField(maxlength=16, blank=True)
- tuple state = models.CharField(maxlength=255, blank=True)
- tuple name = models.CharField(maxlength=255, blank=True)
- tuple info = models.CharField(maxlength=1024, blank=True)

Classes

- class Meta

2.16.1 Detailed Description

Definition at line 14 of file hosts/models.py.

2.16.2 Member Function Documentation

2.16.2.1 def __repr__ (*self*)

Definition at line 24 of file hosts/models.py.

2.16.3 Member Data Documentation

2.16.3.1 tuple host_id = models.ForeignKey(Host,db_column="host_id") [static]

Definition at line 17 of file hosts/models.py.

2.16.3.2 tuple port = models.IntegerField(blank=True) [static]

Definition at line 18 of file hosts/models.py.

2.16.3.3 tuple proto = models.CharField(maxlength=16, blank=True) [static]

Definition at line 19 of file hosts/models.py.

2.16.3.4 tuple state = models.CharField(maxlength=255, blank=True) [static]

Definition at line 20 of file hosts/models.py.

2.16.3.5 tuple name = models.CharField(maxlength=255, blank=True) [static]

Definition at line 21 of file hosts/models.py.

2.16.3.6 tuple info = models.CharField(maxlength=1024, blank=True) [static]

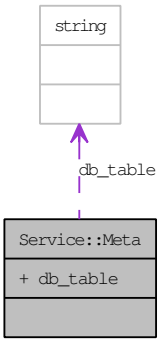
Definition at line 22 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.17 Service::Meta Class Reference

Collaboration diagram for Service::Meta:



Static Public Attributes

- string db_table = 'services'

2.17.1 Detailed Description

Definition at line 15 of file hosts/models.py.

2.17.2 Member Data Documentation

2.17.2.1 string db_table = 'services' [static]

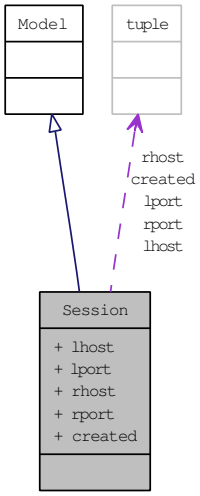
Definition at line 16 of file hosts/models.py.

The documentation for this class was generated from the following file:

- hosts/models.py

2.18 Session Class Reference

Inheritance diagram for Session:Collaboration diagram for Session:



Static Public Attributes

- tuple lhost = models.IPAddressField()
- tuple lport = models.PositiveIntegerField()
- tuple rhost = models.IPAddressField()
- tuple rport = models.PositiveIntegerField()
- tuple created = models.DateTimeField(auto_now_add=True)

Classes

- class Meta

2.18.1 Detailed Description

Definition at line 21 of file worker/models.py.

2.18.2 Member Data Documentation

2.18.2.1 tuple lhost = models.IPAddressField() [static]

Definition at line 24 of file worker/models.py.

2.18.2.2 tuple lport = models.PositiveIntegerField() [static]

Definition at line 25 of file worker/models.py.

2.18.2.3 tuple rhost = models.IPAddressField() [static]

Definition at line 26 of file worker/models.py.

2.18.2.4 tuple rport = models.PositiveIntegerField() [static]

Definition at line 27 of file worker/models.py.

2.18.2.5 tuple created = models.DateTimeField(auto_now_add=True) [static]

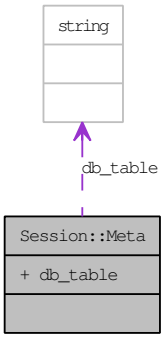
Definition at line 28 of file worker/models.py.

The documentation for this class was generated from the following file:

- worker/models.py

2.19 Session::Meta Class Reference

Collaboration diagram for Session::Meta:



Static Public Attributes

- string db_table = "sessions"

2.19.1 Detailed Description

Definition at line 22 of file worker/models.py.

2.19.2 Member Data Documentation

2.19.2.1 string db_table = "sessions" [static]

Definition at line 23 of file worker/models.py.

The documentation for this class was generated from the following file:

- worker/models.py

2.20 TIMEOUT Class Reference

Inheritance diagram for TIMEOUT:Collaboration diagram for TIMEOUT:

Public Member Functions

- def __init__
- def __str__

2.20.1 Detailed Description

```
TIMEOUT Exception objects are thrown, when metasploit is executing
command for too long. Mainly thrown after catching pexpect.TIMEOUT. Despite
that, it was implemented to clarify source of the errors.
```

Definition at line 7 of file metasploit.py.

2.20.2 Member Function Documentation

2.20.2.1 def __init__ (*self*)

Definition at line 14 of file metasploit.py.

2.20.2.2 def __str__ (*self*)

Definition at line 16 of file metasploit.py.

The documentation for this class was generated from the following file:

- metasploit.py

Chapter 3

File Documentation

3.1 __init__.py File Reference

Namespaces

- namespace pentester

3.2 __init__.py File Reference

Namespaces

- namespace pentester::hosts

3.3 __init__.py File Reference

Namespaces

- namespace pentester::worker

3.4 ifconfig.py File Reference

Namespaces

- namespace pentester::hosts::ifconfig

Classes

- class IFConfig

3.5 manage.py File Reference

Namespaces

- namespace pentester::manage

3.6 metasploit.py File Reference

Namespaces

- namespace pentester::hosts::metasploit

Classes

- class TIMEOUT
- class PluginError
- class ConnectionError
- class MsfExecNotFound
- class MetaSploit
- class MetaSploitLocal
- class MetaSploitRemote

Variables

- int MSFTIMEOUT = 120

3.7 models.py File Reference

Namespaces

- namespace pentester::hosts::models

Classes

- class Host
- class Host::Meta
- class Service
- class Service::Meta
- class Configuration
- class Configuration::Meta

3.8 models.py File Reference

Namespaces

- namespace pentester::worker::models

Classes

- class Logs
- class Logs::Meta
- class Session
- class Session::Meta

3.9 netscan.py File Reference

Namespaces

- namespace pentester::hosts::netscan

Classes

- class NetScan

Variables

- tuple i = ifconfig.IFConfig.get_ifaces_up()

3.10 urls.py File Reference

Namespaces

- namespace pentester::urls

Variables

- dictionary lista_hostow
- dictionary logs_info
- dictionary sessions_info
- tuple urlpatterns

3.11 views.py File Reference

Namespaces

- namespace pentester::hosts::views

Functions

- def ifaces
- def ifaceslist
- def iface_detail
- def index
- def createMenu
- def services
- def servupdate
- def addport
- def configuration
- def deletehost

3.12 views.py File Reference

Namespaces

- namespace pentester::worker::views

Functions

- def getcfgobj
- def scan
- def netscan
- def isValidNetwork
- def exploit
- def clearlogs
- def results

Index

__del__
    pentester::hosts::metasploit::MetaSploit, 31
__init__
    pentester::hosts::ifconfig::IFConfig, 26
    pentester::hosts::metasploit::ConnectionError, 22
    pentester::hosts::metasploit::MetaSploit, 31
    pentester::hosts::metasploit::MetaSploitLocal, 33
    pentester::hosts::metasploit::MetaSploitRemote, 35
    pentester::hosts::metasploit::MsfExecNotFound, 38
    pentester::hosts::metasploit::PluginError, 40
    pentester::hosts::metasploit::TIMEOUT, 47
__init__.py, 49–51
__repr__
    pentester::hosts::models::Host, 23
    pentester::hosts::models::Service, 41
__str__
    pentester::hosts::metasploit::ConnectionError, 22
    pentester::hosts::metasploit::MsfExecNotFound, 38
    pentester::hosts::metasploit::PluginError, 40
    pentester::hosts::metasploit::TIMEOUT, 47
    pentester::worker::models::Logs, 28

addport
    pentester::hosts::views, 7
address
    pentester::hosts::models::Host, 24

clearlogs
    pentester::worker::views, 14
comm
    pentester::hosts::models::Host, 24
configuration
    pentester::hosts::views, 7
connect
    pentester::hosts::metasploit::MetaSploitLocal, 33
    pentester::hosts::metasploit::MetaSploitRemote, 35
connected
    pentester::hosts::metasploit::MetaSploitLocal, 33
    pentester::hosts::metasploit::MetaSploitRemote, 35
created
    pentester::worker::models::Session, 45
createMenu
    pentester::hosts::views, 7

db_table
    pentester::hosts::models::Configuration::Meta, 21
    pentester::hosts::models::Host::Meta, 25
    pentester::hosts::models::Service::Meta, 43
    pentester::worker::models::Logs::Meta, 30
    pentester::worker::models::Session::Meta, 46
deletehost
    pentester::hosts::views, 7

eventText
    pentester::worker::models::Logs, 29
eventTime
    pentester::worker::models::Logs, 29
eventType
    pentester::worker::models::Logs, 29
exploit
    pentester::hosts::metasploit::MetaSploit, 31
    pentester::worker::views, 14

get_ifaces_up
    pentester::hosts::ifconfig::IFConfig, 26
get_ip_address
    pentester::hosts::ifconfig::IFConfig, 26
get_netmask
    pentester::hosts::ifconfig::IFConfig, 26
getcfgobj
    pentester::worker::views, 14
getIfaceData
    pentester::hosts::netscan::NetScan, 39

host
    pentester::hosts::metasploit::MetaSploitLocal, 33
    pentester::hosts::metasploit::MetaSploitRemote, 35
host_id

pentester::hosts::models::Service, 42

i
pentester::hosts::netscan, 6
iface_detail
pentester::hosts::views, 7
ifaces
pentester::hosts::views, 8
ifaceslist
pentester::hosts::views, 8
ifconfig.py, 52
index
pentester::hosts::views, 8
info
pentester::hosts::models::Host, 24
pentester::hosts::models::Service, 42
isValidNetwork
pentester::worker::views, 14

lhost
pentester::worker::models::Session, 44
lista_hostow
pentester::urls, 10
listsessions
pentester::hosts::metasploit::MetaSploit, 32
loadPlugins
pentester::hosts::metasploit::MetaSploit, 32
logs_info
pentester::urls, 10
LOGTYPES
pentester::worker::models::Logs, 29
long2cidr
pentester::hosts::ifconfig::IFConfig, 26
pentester::hosts::netscan::NetScan, 39
lport
pentester::worker::models::Session, 44

manage.py, 53
metasploit.py, 54
models.py, 55, 56
models::Model, 37
msfaddr
pentester::hosts::models::Configuration, 19
msfdb_host
pentester::hosts::models::Configuration, 20
msfdb_login
pentester::hosts::models::Configuration, 20
msfdb_name
pentester::hosts::models::Configuration, 20
msfdb_pass
pentester::hosts::models::Configuration, 20
msfdb_port
pentester::hosts::models::Configuration, 20
msfpath
pentester::hosts::models::Configuration, 19
msfport
pentester::hosts::models::Configuration, 19
MSFTIMEOUT
pentester::hosts::metasploit, 4
msftype
pentester::hosts::models::Configuration, 19
MSFTYPE_CHOICES
pentester::hosts::models::Configuration, 19

name
pentester::hosts::models::Host, 24
pentester::hosts::models::Service, 42
netscan
pentester::worker::views, 14
netscan.py, 57

parseNmapResults
pentester::hosts::netscan::NetScan, 39
path
pentester::hosts::metasploit::MetaSploitLocal, 33
pentester::hosts::metasploit::MetaSploitRemote, 35
pentester, 1
pentester::hosts, 2
pentester::hosts::ifconfig, 3
pentester::hosts::ifconfig::IFConfig, 26
__init__, 26
get_ifaces_up, 26
get_ip_address, 26
get_netmask, 26
long2cidr, 26
pentester::hosts::metasploit, 4
MSFTIMEOUT, 4
pentester::hosts::metasploit::ConnectionError, 22
__init__, 22
__str__, 22
pentester::hosts::metasploit::MetaSploit, 31
__del__, 31
__init__, 31
exploit, 31
listsessions, 32
loadPlugins, 32
scan, 32
showMatchingExploits, 31
pentester::hosts::metasploit::MetaSploitLocal, 33
__init__, 33
connect, 33
connected, 33
host, 33
path, 33
pipe, 34
port, 33

pentester::hosts::metasploit::MetaSploitRemote, 35
__init__, 35
connect, 35
connected, 35
host, 35
path, 35
pipe, 36
port, 35
pentester::hosts::metasploit::MsfExecNotFound, 38
__init__, 38
__str__, 38
pentester::hosts::metasploit::PluginError, 40
__init__, 40
__str__, 40
value, 40
pentester::hosts::metasploit::TIMEOUT, 47
__init__, 47
__str__, 47
pentester::hosts::models, 5
pentester::hosts::models::Configuration, 18
msfaddr, 19
msfdb_host, 20
msfdb_login, 20
msfdb_name, 20
msfdb_pass, 20
msfdb_port, 20
msfpath, 19
msfport, 19
msftype, 19
MSFTYPE_CHOICES, 19
pentester::hosts::models::Configuration::Meta, 21
db_table, 21
pentester::hosts::models::Host, 23
__repr__, 23
address, 24
comm, 24
info, 24
name, 24
state, 24
pentester::hosts::models::Host::Meta, 25
db_table, 25
pentester::hosts::models::Service, 41
__repr__, 41
host_id, 42
info, 42
name, 42
port, 42
proto, 42
state, 42
pentester::hosts::models::Service::Meta, 43
db_table, 43
pentester::hosts::netscan, 6
i, 6
pentester::hosts::netscan::NetScan, 39
getIfaceData, 39
long2cidr, 39
parseNmapResults, 39
scanNetwork, 39
pentester::hosts::views, 7
addport, 7
configuration, 7
createMenu, 7
deletehost, 7
iface_detail, 7
ifaces, 8
ifaceslist, 8
index, 8
services, 8
servupdate, 8
pentester::manage, 9
pentester::urls, 10
lista_hostow, 10
logs_info, 10
sessions_info, 10
urlpatterns, 10
pentester::worker, 12
pentester::worker::models, 13
pentester::worker::models::Logs, 28
__str__, 28
eventText, 29
eventTime, 29
eventType, 29
LOGTYPES, 29
pentester::worker::models::Logs::Meta, 30
db_table, 30
pentester::worker::models::Session, 44
created, 45
lhost, 44
lport, 44
rhost, 44
rport, 45
pentester::worker::models::Session::Meta, 46
db_table, 46
pentester::worker::views, 14
clearlogs, 14
exploit, 14
getcfgobj, 14
isValidNetwork, 14
netscan, 14
results, 14
scan, 15
pipe
pentester::hosts::metasploit::MetaSploitLocal, 34
pentester::hosts::metasploit::MetaSploitRemote, 36
port

pentester::hosts::metasploit::MetaSploitLocal, 33
pentester::hosts::metasploit::MetaSploitRemote, 35
pentester::hosts::models::Service, 42
proto
pentester::hosts::models::Service, 42

results
pentester::worker::views, 14
rhost
pentester::worker::models::Session, 44
rport
pentester::worker::models::Session, 45

scan
pentester::hosts::metasploit::MetaSploit, 32
pentester::worker::views, 15
scanNetwork
pentester::hosts::netscan::NetScan, 39
services
pentester::hosts::views, 8
servupdate
pentester::hosts::views, 8
sessions_info
pentester::urls, 10
showMatchingExploits
pentester::hosts::metasploit::MetaSploit, 31
state
pentester::hosts::models::Host, 24
pentester::hosts::models::Service, 42

urlpatterns
pentester::urls, 10
urls.py, 58

value
pentester::hosts::metasploit::PluginError, 40
views.py, 59, 60