libnessus Documentation

Release 1.0.0.0

Ronald Bister and Mike Boutillier

Jul 28, 2017

Contents

1 python-libnessus **1**
- 1.1 Code status . . . 1
- 1.2 About . . . 1
- 1.3 Install . . . 1
- 1.4 Model . . . 2
- 1.5 Examples . . . 2

2 Indices and tables **5**

CHAPTER 1

python-libnessus

Code status

Still in dev...

About

libnessue is a python library to manipulate nessus process and data.

libnessus is what you were looking for if you need to implement the following: - manipulate nessus scans results to do reporting - compare and diff nessus scans - store nessus scans in a datastore (mongo and Elasticsearch supported)

In the future we might implement something to discuss with nessus API - automate or schedule nessus scans on a regular basis - batch process scan reports

Install

Dependencies : You might need jsonpickle,elasticsearch,pymongo if you want to use the backend plugins

You can install libnmap via pip:

```
pip install libnessus
```

or via git:

```
$ git clone https://github.com/bmx0r/python-libnessus.git
$ cd python-libnessus
$ python setup.py install
```

Model

NessusReport:

```
In [32]: report = NessusParser.parse_fromfile('/home/vagrant/python-libnessus/
↪libnessus/test/files/nessus_forgedReport_ReportItem.nessus')
In [33]: report?
Type:           NessusReport
String form:    localpci 1 0:00:05
File:           /home/vagrant/python-libnessus/libnessus/objects/report.py
Docstring:
This class represent a Nessus repport, it aims to manipulate
in a easy way the content, and present some metadata
Init docstring:
Description: Constructor of NessusReport
:param name: name of the report
:type name: str
:param hosts: list of NessusReportHost
:type hosts: list
:return: NessusReport
:rtype: NessusReport
```

NessusReportHost:

```
In [34]: host = report.hosts[0]
In [35]: host?
Type:        NessusReportHost
String form: 127.0.0.1 127.0.0.1 {'patch-summary-txt-79ed019e4b6ec5267fd968e511eccdb2
↪': 'CentOS 6 : libtirpc ( <...> 2cda94fbf08': 'CentOS 5 / 6 : libxml2 (CESA-
↪2013:0581): Update the affected libxml2 packages.')'} 5
File:        /home/vagrant/python-libnessus/libnessus/objects/reporthost.py
Docstring:   Description: Represent an object NessusReportHost in a nessus xml
```

NessusReportItem:

```
In [36]: reportitem = host.get_report_items[3]
In [37]: reportitem?
Type:           NessusReportItem
String form:    10544:Linux Multiple statd Packages Remote Format String 4
File:           /home/vagrant/python-libnessus/libnessus/objects/reportitem.py
Docstring:      This class represent a ReportItem in the nessus xml
Init docstring:
Constructor of Vulnerability
:param vuln_info: dict of vulnerabities as generated by
NessusParser.parse_reportitem
:type vuln_info: dict
```

Examples

Here's a basic example:

```
# Parse a nessus report from xml and save it in Elastic search
In [1]: from libnessus.parser import NessusParser
In [3]: from libnessus.plugins.backendplugin import NessusBackendPlugin
In [4]: from libnessus.plugins.backendpluginFactory import BackendPluginFactory
```

```
In [5]: url = {'plugin_name': "es"}
In [6]: backend = BackendPluginFactory.create(\**url)
In [7]: nessus_obj_list = NessusParser.parse_fromfile('/home/vagrant/python-libnessus/
↪libnessus/test/files/nessus_forgedReport_ReportItem.nessus')
In [8]: rc = nessus_obj_list.save(backend)
In [9]: rc
Out[9]: 2275333
In [10]: backend
Out[10]: <libnessus.plugins.es.NessusEsPlugin at 0x1dcc790>
In [11]: nessus_obj_list
Out[11]: localpci 1 0:00:05
#retrieve the report from ES
In [15]: ff = backend.get("2275333")
In [16]: ff
Out[16]: localpci 1 0:00:05
```

Contents:

CHAPTER 2

Indices and tables

- genindex
- modindex
- search