Python Extension

Meterpreter's **python** extension was added to the Metasploit Framework in November of 2015. This addition is a perfect example how the community can expand, and contribute to an already versatile framework that is Metasploit.

At the time of this writing the extension is still under active development, however this add-on shows much promise as it gives users the ability to run Python code natively on a target machine, without having the interpreter installed. The in memory implementation of various Python modules, such as cTypes, can greatly expand Meterpreter's hold on a compromised Windows target.

With an active meterpreter shell running on our target machine, typing **load python** will load the extension giving us access to new commands.

```
meterpreter > load python
Loading extension python...success.
```

Once loaded, we can issue the **help** command in order to see the Python commands.

```
meterpreter > help
...
Python Commands
===============

    Command         Description
    -------         -----------
    python_execute  Execute a python command string
    python_import   Import/run a python file or module
    python_reset    Resets/restarts the Python interpreter
```

The **python_execute** command runs the given python string on the target. If a result is required, it should be stored in a python variable, and that variable should passed using the **-r** parameter.

```
meterpreter > python_execute -h
Usage: python_execute  [-r result var name]

Runs the given python string on the target. If a result is required, it
should be stored in a python variable,
and that variable should passed using the -r parameter.

OPTIONS:

    -h        Help banner
    -r   Name of the variable containing the result (optional)
```

Loads a python code file or module from disk into memory on the target. The module loader requires a path to a folder that contains the module, and the folder name will be used as the module name. Only .py files will work with modules.

```
meterpreter > python_import -h
Usage: python_import  [-n mod name] [-r result var name]

Loads a python code file or module from disk into memory on the target.
The module loader requires a path to a folder that contains the module,
and the folder name will be used as the module name. Only .py files will
work with modules.

OPTIONS:

    -f   Path to the file (.py, .pyc), or module directory to import
    -h        Help banner
    -n   Name of the module (optional, for single files only)
    -r   Name of the variable containing the result (optional, single files
only)
```

This one is rather self-explanatory.

```
meterpreter > python_reset -h
[+] Python interpreter successfully reset
```