Bypassing AV with Python Shells

Bypassing Antivirus

Why?

It is safer to bypass AV than it is to disable it. It is also fun to show a client how useless AV is.

How?

If you have a binary that is being caught by You can bypass AV by editing the binary to remove the signature, encoding or packing the binary, modifying the source code and/or recompiling the source code, and my personal favorite using a custom program*.

When?

Anytime your shell is written to disk?

* http://compsec.org/security/index.php/anti-virus/283-anti-virus-central-methods-of-bypassing-anti-virus-av-detection.html

Why Python?

Python is an easy language to learn, has a number of useful libraries, and runs on Linux, Mac, and Windows. For operating systems like Mac and Linux, Python shells can be run natively. For Windows, you will typically need to compile the Python script into an executable.

There are a number of free resources for learning Python:

http://docs.python.org/tutorial/

http://www.makeuseof.com/tag/5-websites-learn-python-programming/

http://www.readwriteweb.com/hack/2011/03/python-is-an-increasingly-popu.php

Python Basics

In the Python language **white space matters**. Indention is used to determine blocks of code. You can use tabs or spaces but you cannot mix them. The standard is to convert tabs to 4 spaces.

Single and double quotes are the same in Python. You can use escape characters such as `\n` and `\t` in ether one. Triple quotes “”” denote a multi-line string.

Use raw strings `r’   ‘` in regular expressions. Raw strings do not require you to escape back slashes, which makes the regex look cleaner.

Classes can be declared inline or placed in another file and `import`ed

Python Basics

```
if a == b:
    print “They’re equal.\n”
else:
    print “They’re not equal.\n”

for i in range(1, 100, 5):
    print ‘Number {0}\n’.format(i)

def new_function():
    print ‘Inside the function.\n’
```

Python Basics

```
class Adder():
    def __init__(self, value=0):
        self.value = value

    def add(self, val):
        self.value += val

a = Adder()
a.add(5)
print a.value

b = Adder(10)
b.add(10)
print b.value
```

What Is A Shell?

A shell accepts commands over the network, executes the commands, and returns the results over the network.

A shell can listen on a port (bind shell) or call back to a server (reverse shell). Reverse shells are preferred because most firewalls do not block outbound traffic but do block inbound.

Before We Look At Code

You will need to have Python installed. This is already installed on Linux and Mac. On Windows you will need to go to *http://www.python.org/download/* and download the Python 2.7.3 Windows Installer.

You will also need Git, which should be installed on most Linux distros and on the Mac. Windows users will need to install Git for Windows, which is available at *http://msysgit.github.com*

SHELL.PY

Open a terminal or Git bash and type the following:

```
git clone https://github.com/averagesecurityguy/scripts
```

Now, `cd` into the `scripts` directory and open `shell.py` in your favorite editor.

ISHELL.PY

Make sure you are in the `scripts` directory and open `ishell.py` in your favorite editor.

MICKEY.PY

Open a terminal or Git bash and type the following:

```
git clone https://github.com/averagesecurityguy/mickey
```

Now, `cd` into the `mickey` directory and open `mickey.py` in your favorite editor.

Compiling with PyInstaller

Download and Unzip PyInstaller

https://github.com/downloads/pyinstaller/pyinstaller/pyinstaller-1.5.1.zip

Download and Install Pywin32

http://sourceforge.net/projects/pywin32/files/pywin32/Build%20217/

Create an Executable

```
pyinstaller.py -F /path/to/script.py
```

The executable will be created in $scriptname/dist folder in the PyInstaller folder.

Let's Try It Out

If you have Metasploit installed then you can follow along. Otherwise, sit back and watch.

First, we are going to attempt to run meterpreter on the machine and we should see it get caught by the AV (Microsoft Security Essentials).

Next, we are going to use our custom Python shell and we should have no problems running our code.

Resources

Learning Python:

http://docs.python.org/tutorial/

http://www.makeuseof.com/tag/5-websites-learn-python-programming/

http://www.readwriteweb.com/hack/2011/03/python-is-an-increasingly-popu.php

Other Python Shells:

https://www.trustedsec.com/files/simple_py_shell.py

https://www.trustedsec.com/files/encrypted_http_shell.zip

Questions?

Bypassing AV with Python Shells