Python For Security

Hello reader,

Chances are you have wondered how some programming languages are implemented for security. C languages running behind the scenes on many heuristics based systems are becoming antiquated and scripting languages can perform so many tasks now that it almost becomes easier to have snippets for security tasks instead of whole programs.

Python Snippets

Python is a scripting language not unlike bash or php in that it doesn't really require a compiler but rather just an interpreter to function. A snippet can be executed from within a shell, as a process by a daemon, or even from within the IDE itself.

Example of a python port scanner, I found this example some time back - I didn't write it but I know it works fairly well in geany, ninja, and various other IDE. If you do attempt to copy this script remember to save with the extension .py as in scanner.py or it will simply not function.

```
#!/usr/bin/env python
import socket
import subprocess
import sys
from datetime import datetime

# Clear the screen
subprocess.call('clear', shell=True)

# Ask for input
remoteServer = raw_input("Enter a remote host to scan: ")
remoteServerIP = socket.gethostbyname(remoteServer)

# Print a nice banner with information on which host we are about to scan
print "-" * 60
print "Please wait, scanning remote host", remoteServerIP
print "-" * 60

# Check what time the scan started
t1 = datetime.now()

# Using the range function to specify ports (here it will scans all ports between 1 and 1024)

# We also put in some error handling for catching errors

try:
for port in range(1,1025):
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
result = sock.connect_ex((remoteServerIP, port))
if result == 0:
print "Port {}: Open".format(port)
sock.close()

except KeyboardInterrupt:
print "You pressed Ctrl+C"
sys.exit()

except socket.gaierror:
print 'Hostname could not be resolved. Exiting'
sys.exit()

except socket.error:
print "Couldn't connect to server"
sys.exit()

# Checking the time again
t2 = datetime.now()

# Calculates the difference of time, to see how long it took to run the script
total = t2 - t1

# Printing the information to screen
print 'Scanning Completed in: ', total
```

To date I've found at least 35-40 snippets that can act as replacements for whole programs when it comes to security. I'm learning to implement quick changes to them for specific needs and incorporating php snippets as well.

A quick tip for output - much like in bash you can output to a text file at need by using the > symbol. Example output > python.txt