
ATTACK
DEFENSE
by PentesterAcademy

Name	Memcache: Pymemcache III
URL	https://www.attackdefense.com/challengedetails?cid=223
Type	Infrastructure Attacks: Memcached

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the value of Flag 1?

Answer: fl4g_f0r_m3mcach3d_g3t_mult1

Solution:

Python code:

```
from pymemcache.client.base import Client
import pickle

def retrieve(key):
  result = client.get_multi(['%s-%s' % (key, i) for i in xrange(32)])
  serialized = ''.join([v for k, v in sorted(result.items()) if v is not None])
  return pickle.loads(serialized)

client = Client(('localhost', 11211))
print retrieve("flag")
```

Save the above python code as “code.py”.

```
from pymemcache.client.base import Client
import pickle

def retrieve(key):
  result = client.get_multi(['%s-%s' % (key, i) for i in xrange(32)])
  serialized = ''.join([v for k, v in sorted(result.items()) if v is not None])
  return pickle.loads(serialized)

client = Client(('localhost', 11211))
print retrieve("flag")
```

Command: python code.py

```
student@attackdefense:~$ python code.py
fl4g_f0r_m3mcach3d_g3t_mult1
student@attackdefense:~$
```

Q2. What is the value of Flag 2?

Answer: fl4g_for_m3mc4ch3d_p1ckl3_b64_enc

Solution:

Python code:

```
from pymemcache.client.base import Client
import pickle
import base64

def retrieve2(key):
  result = client.get_multi(['%s-%s' % (key, i) for i in xrange(32)])
  serialized = ''
  for i in range(11):
      serialized=serialized+result[key+'-'+str(i)]
  return pickle.loads(base64.b64decode(serialized))

client = Client(('localhost', 11211))
print retrieve2("flag2")
```

Save the above python code as “code2.py”.

```
from pymemcache.client.base import Client
import pickle
import base64

def retrieve2(key):
  result = client.get_multi(['%s-%s' % (key, i) for i in xrange(32)])
  serialized = ''
  for i in range(11):
        serialized=serialized+result[key+'-'+str(i)]
  return pickle.loads(base64.b64decode(serialized))

client = Client(('localhost', 11211))
print retrieve2("flag2")
```

Command: python code2.py

```
student@attackdefense:~$ python code2.py
fl4g_for_m3mc4ch3d_p1ckl3_b64_enc
student@attackdefense:~$
```

Q3. What is the sum of complex-4 and complex-5?

Answer: 7+16j

Solution:

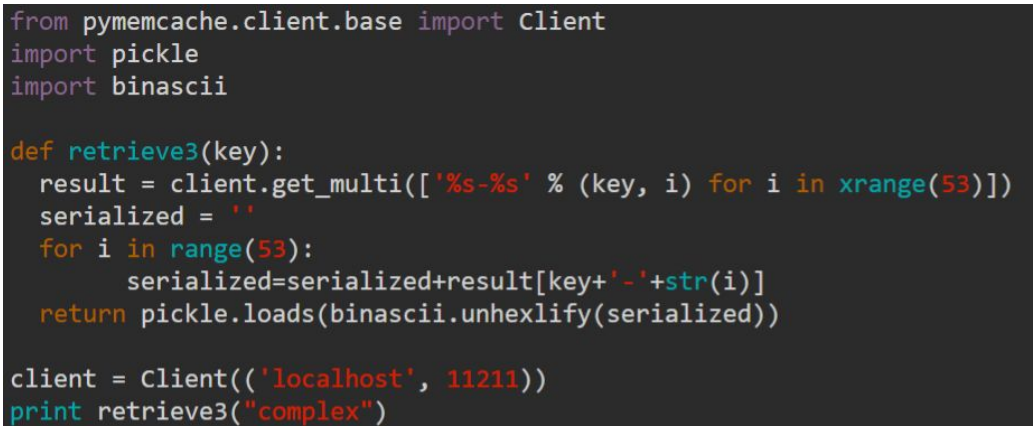
Python code:

```
from pymemcache.client.base import Client
import pickle
import binascii

def retrieve3(key):
  result = client.get_multi(['%s-%s' % (key, i) for i in xrange(53)])
  serialized = ''
  for i in range(53):
        serialized=serialized+result[key+'-'+str(i)]
  return pickle.loads(binascii.unhexlify(serialized))

client = Client(('localhost', 11211))
print retrieve3("complex")
```

Save the above python code as “code3.py”.



Command: python code3.py

```
student@attackdefense:~$ python code3.py
{'complex-2': (5+1j), 'complex-3': (1+1j), 'complex-1': (4+3j), 'complex-6': (8+4j), 'complex-4': (2+7j), 'complex-5': (5+9j)}
student@attackdefense:~$
```

(2+7j) + (5+9j) = 7+16j

References:

1. Memcached (https://memcached.org/)
2. Pymemcache (https://pypi.org/project/pymemcache/)