
ATTACK
DEFENSE
by PentesterAcademy

Name	Memcache: Pickled Data
URL	https://www.attackdefense.com/challengedetails?cid=220
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 password of user named "john"?

Answer: password@123

Command: echo -e "get user1\r\nquit\r\n" | nc 127.0.0.1 11211 > user1
python -c 'import pickle;print pickle.load(open("user1"));'

```
student@attackdefense:~$ echo -e "get user1\r\nquit\r\n" | nc 127.0.0.1 11211 > user1
student@attackdefense:~$ cat user1
VALUE user1 0 64
(dp0
S'password'
p1
S'password@123'
p2
sS'Name'
p3
S'john'
p4
s.
END
student@attackdefense:~$ python -c 'import pickle;print pickle.load(open("user1"));'
{'password': 'password@123', 'Name': 'john'}
student@attackdefense:~$
```

Q2. What type of object is obtained after deserializing data present in key “user2” ?

Answer: dict

Command: echo -e "get user2\r\nquit\r\n" | nc 127.0.0.1 11211 > user2
python -c 'import pickle;obj= pickle.load(open("user2"));print type(obj)'

```
student@attackdefense:~$ echo -e "get user2\r\nquit\r\n" | nc 127.0.0.1 11211 > user2
student@attackdefense:~$ cat user2
VALUE user2 0 69
(dp0
S'password'
p1
S'thomas@12011997'
p2
sS'Name'
p3
S'thomas'
p4
s.
END
student@attackdefense:~$
student@attackdefense:~$ python -c 'import pickle;obj= pickle.load(open("user2"));print type(obj)'
<type 'dict'>
```

Q3. What is the flag obtained from the memcache key value pairs?

Answer: th1s_1s_p1ckl3d_fl4gs

Command: echo -e "get flag\r\nquit\r\n" | nc 127.0.0.1 11211 > flag
python -c 'import pickle;print pickle.load(open("flag"));'

```
student@attackdefense:~$ echo -e "get flag\r\nquit\r\n" | nc 127.0.0.1 11211 > flag
student@attackdefense:~$ cat flag
VALUE flag 0 66
cbase64
b64decode
p0
(S'dGgxc18xc19wMWNrbDNkX2ZsNGdz'
p1
tp2
Rp3
.
END
student@attackdefense:~$ python -c 'import pickle;print pickle.load(open("flag"));'
th1s_1s_p1ckl3d_fl4gs
student@attackdefense:~$
```

Q4. What is the value of complex number stored in data of key “complex”?

Answer: 4+5j

Command: echo -e "get complex\r\nquit\r\n" | nc 127.0.0.1 11211 > complex
python -c 'import pickle;print pickle.load(open("complex"));'

```
student@attackdefense:~$ echo -e "get complex\r\nquit\r\n" | nc 127.0.0.1 11211 > complex
student@attackdefense:~$ cat complex
VALUE complex 0 64
(dp0
S'complex'
p1
c__builtin__
complex
p2
(F4.0
F5.0
tp3
Rp4
s.
END
student@attackdefense:~$ python -c 'import pickle;print pickle.load(open("complex"));'
{'complex': (4+5j)}
student@attackdefense:~$
```

Q5. What is the sum of complex numbers stored in data of key “sum”?

Answer: 15+13j

Command: echo -e "get sum\r\nquit\r\n" | nc 127.0.0.1 11211 > sum
python -c 'import pickle;print pickle.load(open("sum"));'

```
student@attackdefense:~$ echo -e "get sum\r\nquit\r\n" | nc 127.0.0.1 11211 > su
student@attackdefense:~$ cat sum
VALUE sum 0 157
(dp0
S'a'
p1
c__builtin__
complex
p2
(F4.0
F5.0
tp3
Rp4
sS'c'
p5
g2
```

```
student@attackdefense:~$ python -c 'import pickle;print pickle.load(open("sum"));'
{'a': (4+5j), 'c': (9+10j), 'b': (1-3j), 'd': (1+1j)}
student@attackdefense:~$
```

(4+5j)+ (9+10j)+ (1-3j)+ (1+1j) =15+13j

References:

1. Memcached (https://memcached.org/)
2. Memcached Cheat Sheet (https://lzone.de/cheat-sheet/memcached)