PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTING HACKER PENTESTER

TEAM LABSPENTES TO THE PENTESTER

TEAM LABSPENTES TO THE PENTESTER

OF THE PENTESTING HACKER

THE PENTESTING HACKER

TOOL BOX

OF THE PENTESTING

| Name | Memcache: Basics |
|------|--|
| URL | https://www.attackdefense.com/challengedetails?cid=219 |
| 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.

Connect to memcached server using telnet:

Command: telnet 127.0.0.1 11211

```
student@attackdefense:~$ telnet 127.0.0.1 11211
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

Q1. What is the version of memcache server?

Answer: Version 1.5.6 Ubuntu

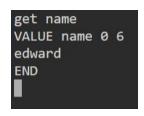
Command: version

version
VERSION 1.5.6 Ubuntu

Q2. What is the value stored in key "name"?

Answer: edward

Command: get name



Q3. What is the length of data stored in key "password"?

Answer: 6

Command: get password



Q4. How many key value pairs are present on the server initially?

Answer: 6

Command: stats items

Items: X: number Y signifies that there are Y number of key-value pairs present in slab X.

```
stats items
STAT items:1:number 5
STAT items:1:number hot 0
STAT items:1:number_warm 0
STAT items:1:number cold 5
STAT items:1:age hot 0
STAT items:1:age_warm 0
STAT items:1:age 831
STAT items:1:evicted 0
STAT items:1:evicted nonzero 0
STAT items:1:evicted time 0
STAT items:1:outofmemory 0
STAT items:1:tailrepairs 0
STAT items:1:reclaimed 0
STAT items:1:expired unfetched 0
STAT items:1:evicted_unfetched 0
STAT items:1:evicted active 0
STAT items:1:crawler reclaimed 0
STAT items:1:crawler_items_checked 16
STAT items:1:lrutail reflocked 0
STAT items:1:moves_to_cold 5
STAT items:1:moves to warm 0
STAT items:1:moves within lru 0
STAT items:1:direct reclaims 0
STAT items:1:hits_to_hot 0
STAT items:1:hits to warm 0
STAT items:1:hits_to_cold 2
STAT items:1:hits to temp 0
STAT items:2:number 1
```

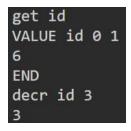
Q5. What command will you use to increment value of key "id" by 1?

Command: incr id 1

get id VALUE id 0 1 5 END incr id 1 6

Q6. What command will you use to decrement value of key "id" by 3?

Command: decr id 3



Q7. What command will you use to add key "phone" with value "123454321"?

Commands:

add phone 0 0 9 123454321

add phone 0 4 9 123454321 STORED

Q8. What command will you use to replace value of key "nick" to "ed"?

Commands:

replace nick 0 0 2 ed

replace nick 0 0 2 ed STORED

Q9. What command will you use to prepend "house" to value of key "address"?

Commands:

prepend address 0 0 6 house

```
get address
VALUE address 0 30
14, 1234 street, Austin, Texas
END
prepend address 0 0 6
house
STORED
get address
VALUE address 0 36
house 14, 1234 street, Austin, Texas
END
```

Q10. What command will you use to append pin code ",73301" to value of key "address" ?

Commands:

append address 0 0 6 ,73301

```
get address
VALUE address 0 36
house 14, 1234 street, Austin, Texas
END
append address 0 0 6
,73301
STORED
get address
VALUE address 0 42
house 14, 1234 street, Austin, Texas,73301
END
```

Q11. What command will you use to delete key "old_address"?

Command: delete old_address

```
get old_address
VALUE old_address 0 30
30, 2002 street, Dallas, Texas
END
delete old_address
DELETED
get old_address
END
```

Q12. What command will you use to invalidate all key values after 30 seconds?

Command: flush_all 30

flush_all 30 OK

References:

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