ATTACK DEFENSE

by PentesterAcademy

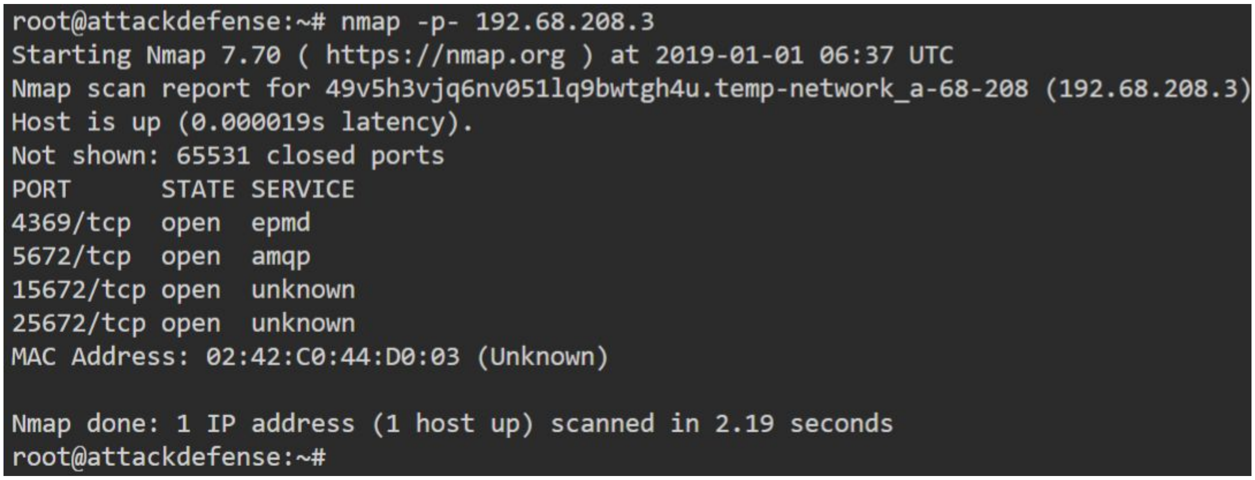
Name	Basic Recon and Interaction
URL	https://www.attackdefense.com/challengedetails?cid=577
Type	IOT : AMQP

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. List the default ports used by RabbitMQ and Erlang.

Answer: 4369, 5672, 15672, 25672

Command: nmap -p- 192.68.208.3

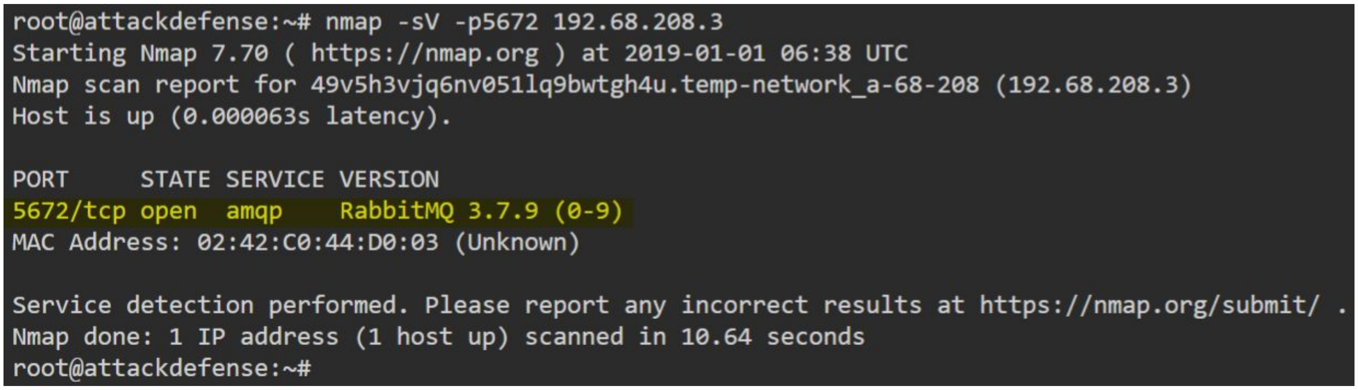


```
root@attackdefense:~# nmap -p- 192.68.208.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 06:37 UTC
Nmap scan report for 49v5h3vjq6nv051lq9bwtgh4u.temp-network_a-68-208 (192.68.208.3)
Host is up (0.000019s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
4369/tcp  open  epmd
5672/tcp  open  amqp
15672/tcp open  unknown
25672/tcp open  unknown
MAC Address: 02:42:C0:44:D0:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
root@attackdefense:~#
```

Q2. Find the version of RabbitMQ server.

Answer: RabbitMQ 3.7.9

Command: nmap -sV -p 5672 192.68.208.3

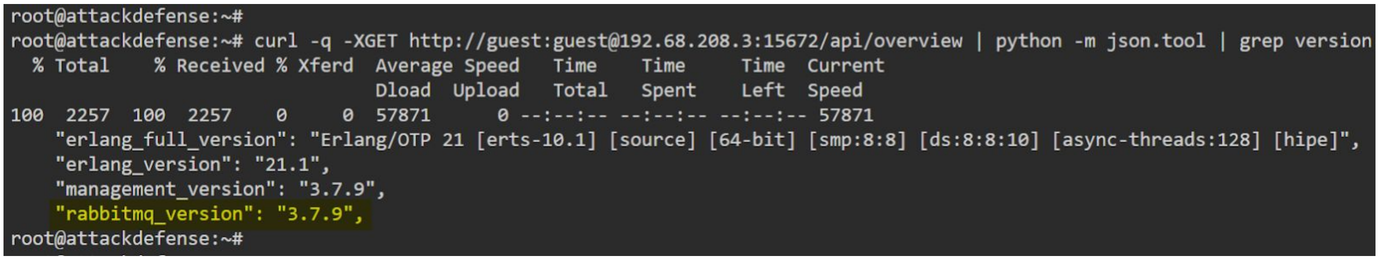


```
root@attackdefense:~# nmap -sV -p5672 192.68.208.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 06:38 UTC
Nmap scan report for 49v5h3vjq6nv051lq9bwtgh4u.temp-network_a-68-208 (192.68.208.3)
Host is up (0.000063s latency).

PORT     STATE SERVICE VERSION
5672/tcp open  amqp    RabbitMQ 3.7.9 (0-9)
MAC Address: 02:42:C0:44:D0:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.64 seconds
root@attackdefense:~#
```

Q3. Find the version information using RabbitMQ http api.

Answer: 3.7.9

Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/overview | python -m json.tool

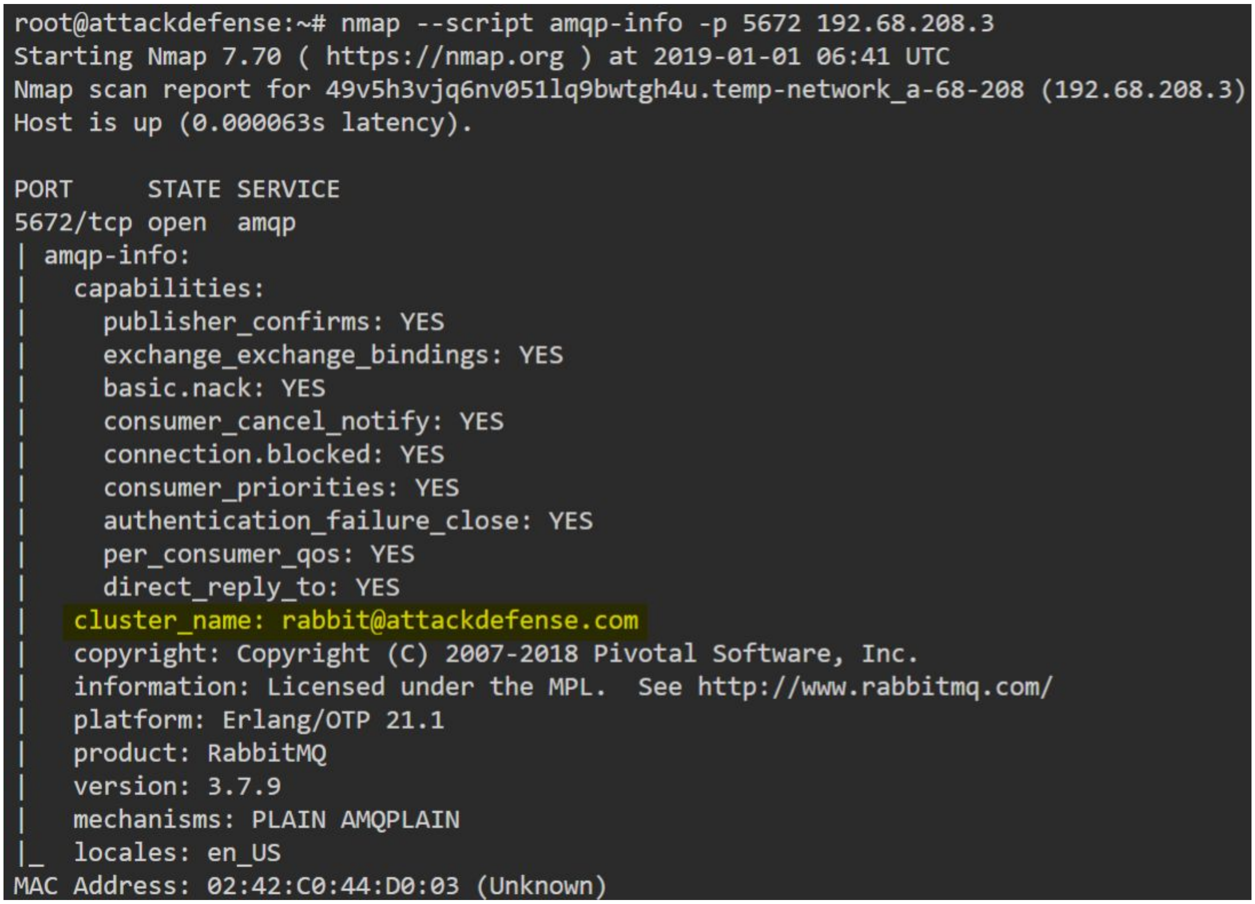


```
root@attackdefense:~#
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/overview | python -m json.tool | grep version
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2257  100  2257    0     0  57871      0 --:--:-- --:--:-- --:--:-- 57871
    "erlang_full_version": "Erlang/OTP 21 [erts-10.1] [source] [64-bit] [smp:8:8] [ds:8:8:10] [async-threads:128] [hipe]",
    "erlang_version": "21.1",
    "management_version": "3.7.9",
    "rabbitmq_version": "3.7.9",
root@attackdefense:~#
```

Q4. Find the name of RabbitMQ cluster using nmap script.

Answer: rabbit@attackdefense.com

Command: nmap --script amqp-info -p 5672 192.68.208.3

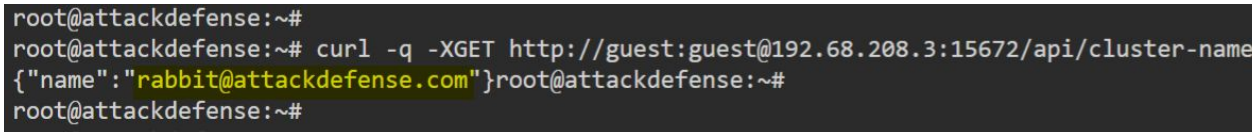


```
root@attackdefense:~# nmap --script amqp-info -p 5672 192.68.208.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 06:41 UTC
Nmap scan report for 49v5h3vjq6nv051lq9bwtgh4u.temp-network_a-68-208 (192.68.208.3)
Host is up (0.000063s latency).

PORT     STATE SERVICE
5672/tcp open  amqp
| amqp-info:
|   capabilities:
|     publisher_confirms: YES
|     exchange_exchange_bindings: YES
|     basic.nack: YES
|     consumer_cancel_notify: YES
|     connection.blocked: YES
|     consumer_priorities: YES
|     authentication_failure_close: YES
|     per_consumer_qos: YES
|     direct_reply_to: YES
|   cluster_name: rabbit@attackdefense.com
|   copyright: Copyright (C) 2007-2018 Pivotal Software, Inc.
|   information: Licensed under the MPL.  See http://www.rabbitmq.com/
|   platform: Erlang/OTP 21.1
|   product: RabbitMQ
|   version: 3.7.9
|   mechanisms: PLAIN AMQPLAIN
|_  locales: en_US
MAC Address: 02:42:C0:44:D0:03 (Unknown)
```

Q5. Find the name of RabbitMQ cluster using RabbitMQ http api.

Answer: rabbit@attackdefense.com

Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/cluster-name

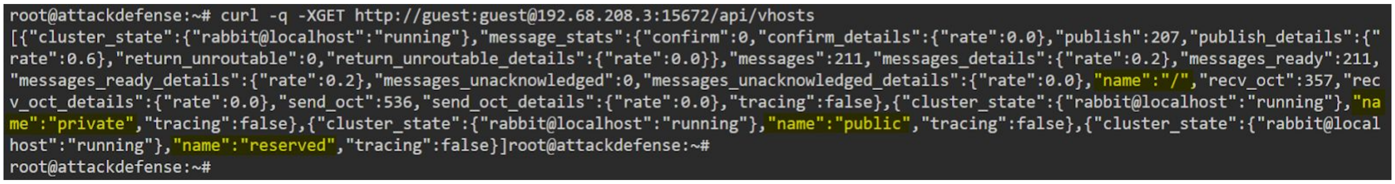


```
root@attackdefense:~#
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/cluster-name
{"name":"rabbit@attackdefense.com"}root@attackdefense:~#
root@attackdefense:~#
```

Q6. List all the virtual hosts on the RabbitMQ server.

Answer: /, reserved, public, private

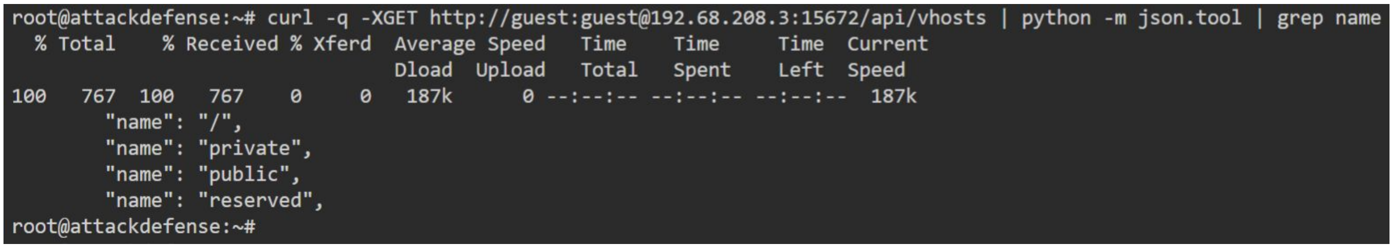
Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/vhosts



```
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/vhosts
[{"cluster_state":{"rabbit@localhost":"running"},"message_stats":{"confirm":0,"confirm_details":{"rate":0.0},"publish":207,"publish_details":{"
rate":0.6},"return_unroutable":0,"return_unroutable_details":{"rate":0.0}},"messages":211,"messages_details":{"rate":0.2},"messages_ready":211,
"messages_ready_details":{"rate":0.2},"messages_unacknowledged":0,"messages_unacknowledged_details":{"rate":0.0},"name":"/","recv_oct":357,"rec
v_oct_details":{"rate":0.0},"send_oct":536,"send_oct_details":{"rate":0.0},"tracing":false},{"cluster_state":{"rabbit@localhost":"running"},"na
me":"private","tracing":false},{"cluster_state":{"rabbit@localhost":"running"},"name":"public","tracing":false},{"cluster_state":{"rabbit@local
host":"running"},"name":"reserved","tracing":false}]root@attackdefense:~#
root@attackdefense:~#
```

OR

Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/vhosts | python -m json.tool | grep name

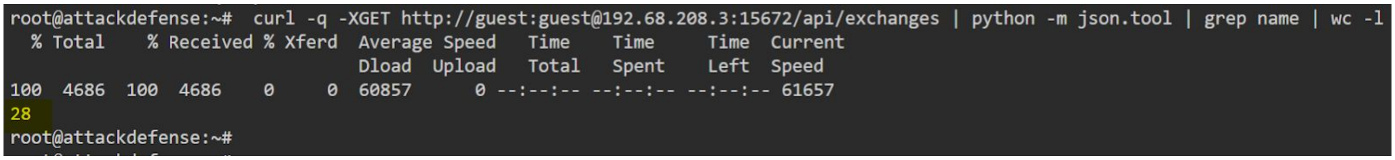


```
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/vhosts | python -m json.tool | grep name
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   767  100   767    0     0   187k      0 --:--:-- --:--:-- --:--:--  187k
        "name": "/",
        "name": "private",
        "name": "public",
        "name": "reserved",
root@attackdefense:~#
```

Q7. How many exchanges are present on the Rabbit MQ server?

Answer: 28

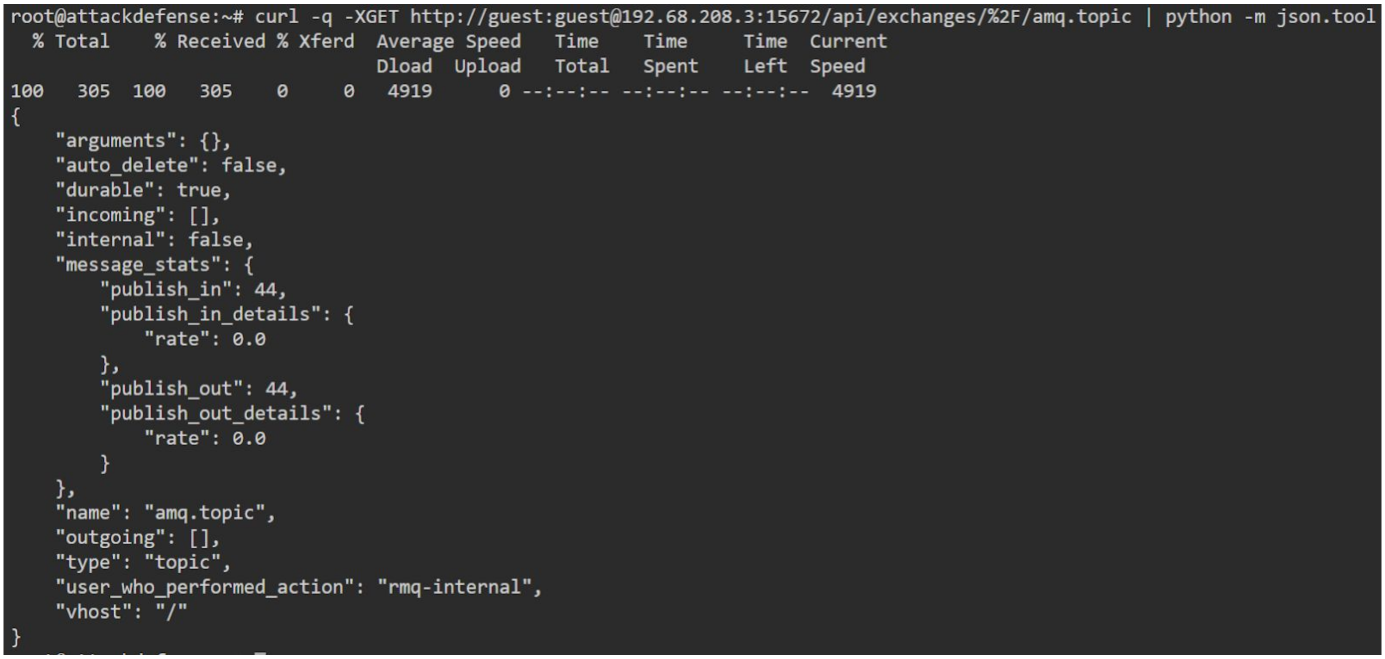
Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/exchanges | python -m json.tool | grep name | wc -l



```
root@attackdefense:~#  curl -q -XGET http://guest:guest@192.68.208.3:15672/api/exchanges | python -m json.tool | grep name | wc -l
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4686  100  4686    0     0  60857      0 --:--:-- --:--:-- --:--:-- 61657
28
root@attackdefense:~#
```

Q8. Fetch more details for exchange “amq.topic” from RabbitMQ server.

Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/exchanges/%2F/amq.topic | python -m json.tool

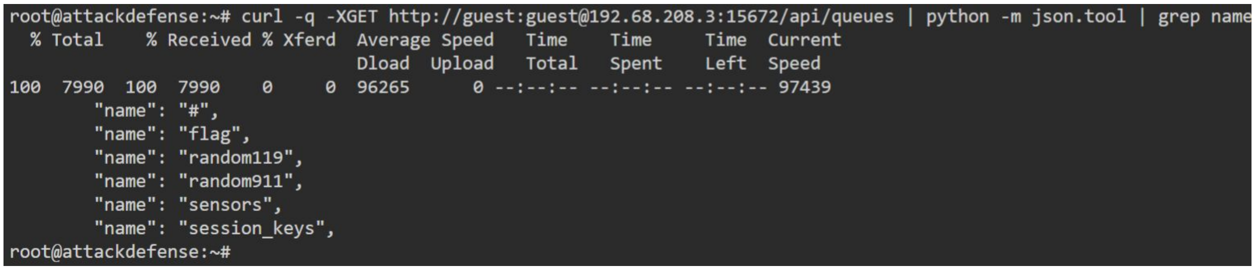


```
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/exchanges/%2F/amq.topic | python -m json.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   305  100   305    0     0   4919      0 --:--:-- --:--:-- --:--:--  4919
{
    "arguments": {},
    "auto_delete": false,
    "durable": true,
    "incoming": [],
    "internal": false,
    "message_stats": {
        "publish_in": 44,
        "publish_in_details": {
            "rate": 0.0
        },
        "publish_out": 44,
        "publish_out_details": {
            "rate": 0.0
        }
    },
    "name": "amq.topic",
    "outgoing": [],
    "type": "topic",
    "user_who_performed_action": "rmq-internal",
    "vhost": "/"
}
```

Q9. How many queues on the on the Rabbit MQ server? Also list their names.

Answer: 6
#, flag, random911, random119, sensors, sessions_keys

Command: curl -q -XGET http://guest:guest@192.68.208.3:15672/api/queues | python -m json.tool | grep name



```
root@attackdefense:~# curl -q -XGET http://guest:guest@192.68.208.3:15672/api/queues | python -m json.tool | grep name
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7990  100  7990    0     0  96265      0 --:--:-- --:--:-- --:--:-- 97439
        "name": "#",
        "name": "flag",
        "name": "random119",
        "name": "random911",
        "name": "sensors",
        "name": "session_keys",
root@attackdefense:~#
```

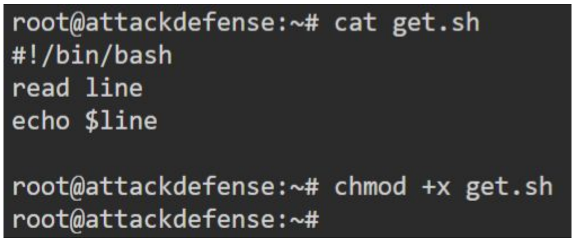
Q10. Connect to “sensors” queue and retrieve the messages.

Solution:

Save the bash script given below as “get.sh”

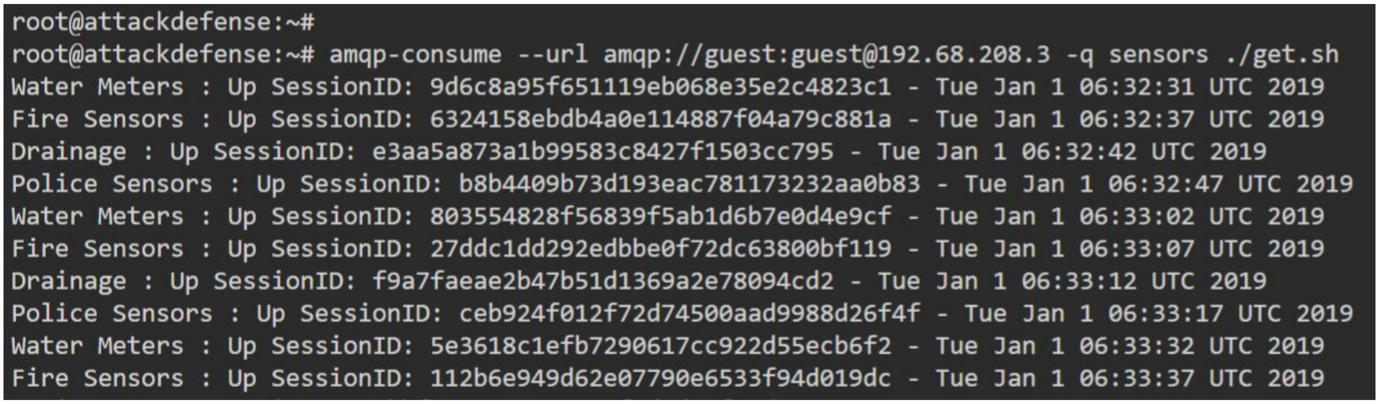
#!/bin/bash
read line
echo $line

Command: chmod +x get.sh



```
root@attackdefense:~# cat get.sh
#!/bin/bash
read line
echo $line

root@attackdefense:~# chmod +x get.sh
root@attackdefense:~#
```

Command: amqp-consume --url amqp://guest:guest@192.68.208.3 -q sensors ./get.sh



```
root@attackdefense:~#
root@attackdefense:~# amqp-consume --url amqp://guest:guest@192.68.208.3 -q sensors ./get.sh
Water Meters : Up SessionID: 9d6c8a95f651119eb068e35e2c4823c1 - Tue Jan 1 06:32:31 UTC 2019
Fire Sensors : Up SessionID: 6324158ebdb4a0e114887f04a79c881a - Tue Jan 1 06:32:37 UTC 2019
Drainage : Up SessionID: e3aa5a873a1b99583c8427f1503cc795 - Tue Jan 1 06:32:42 UTC 2019
Police Sensors : Up SessionID: b8b4409b73d193eac781173232aa0b83 - Tue Jan 1 06:32:47 UTC 2019
Water Meters : Up SessionID: 803554828f56839f5ab1d6b7e0d4e9cf - Tue Jan 1 06:33:02 UTC 2019
Fire Sensors : Up SessionID: 27ddc1dd292edbbe0f72dc63800bf119 - Tue Jan 1 06:33:07 UTC 2019
Drainage : Up SessionID: f9a7faeae2b47b51d1369a2e78094cd2 - Tue Jan 1 06:33:12 UTC 2019
Police Sensors : Up SessionID: ceb924f012f72d74500aad9988d26f4f - Tue Jan 1 06:33:17 UTC 2019
Water Meters : Up SessionID: 5e3618c1efb7290617cc922d55ecb6f2 - Tue Jan 1 06:33:32 UTC 2019
Fire Sensors : Up SessionID: 112b6e949d62e07790e6533f94d019dc - Tue Jan 1 06:33:37 UTC 2019
```

Q11. The messages containing flag are being stored in one of queues. Check the queues and retrieve the flag.

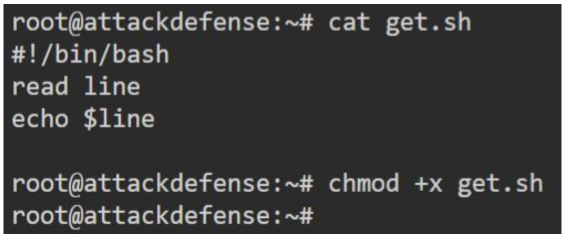
Answer: 7b8ea765a5631ab9b4790e781330af49

Solution:

Save the bash script given below as “get.sh”

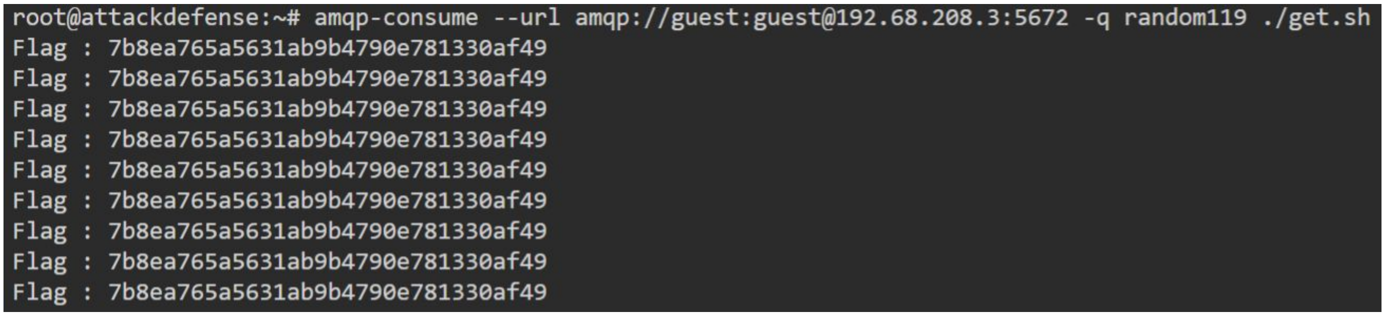
```
#!/bin/bash
read line
echo $line
```

Command: chmod +x get.sh



```
root@attackdefense:~# cat get.sh
#!/bin/bash
read line
echo $line

root@attackdefense:~# chmod +x get.sh
root@attackdefense:~#
```

Command: amqp-consume --url amqp://guest:guest@192.68.208.3:5672 -q random119 ./get.sh



```
root@attackdefense:~# amqp-consume --url amqp://guest:guest@192.68.208.3:5672 -q random119 ./get.sh
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
Flag : 7b8ea765a5631ab9b4790e781330af49
```

References:

1. RabbitMQ (https://www.rabbitmq.com/)
2. RabbitMQ Management HTTP API (https://pulse.mozilla.org/api/)
3. amqp-consume (https://linux.die.net/man/1/amqp-consume)