2019/03/19, Capstone Project

테스트 베드 구축

- 보안 취약점 분석 및 익스플로잇 개발 -

지도교수 : 이종혁

Captain : 201621571 손상진

Sailors : 201621110 권순홍

201621136 서민지

201621173 최서윤

QBQB

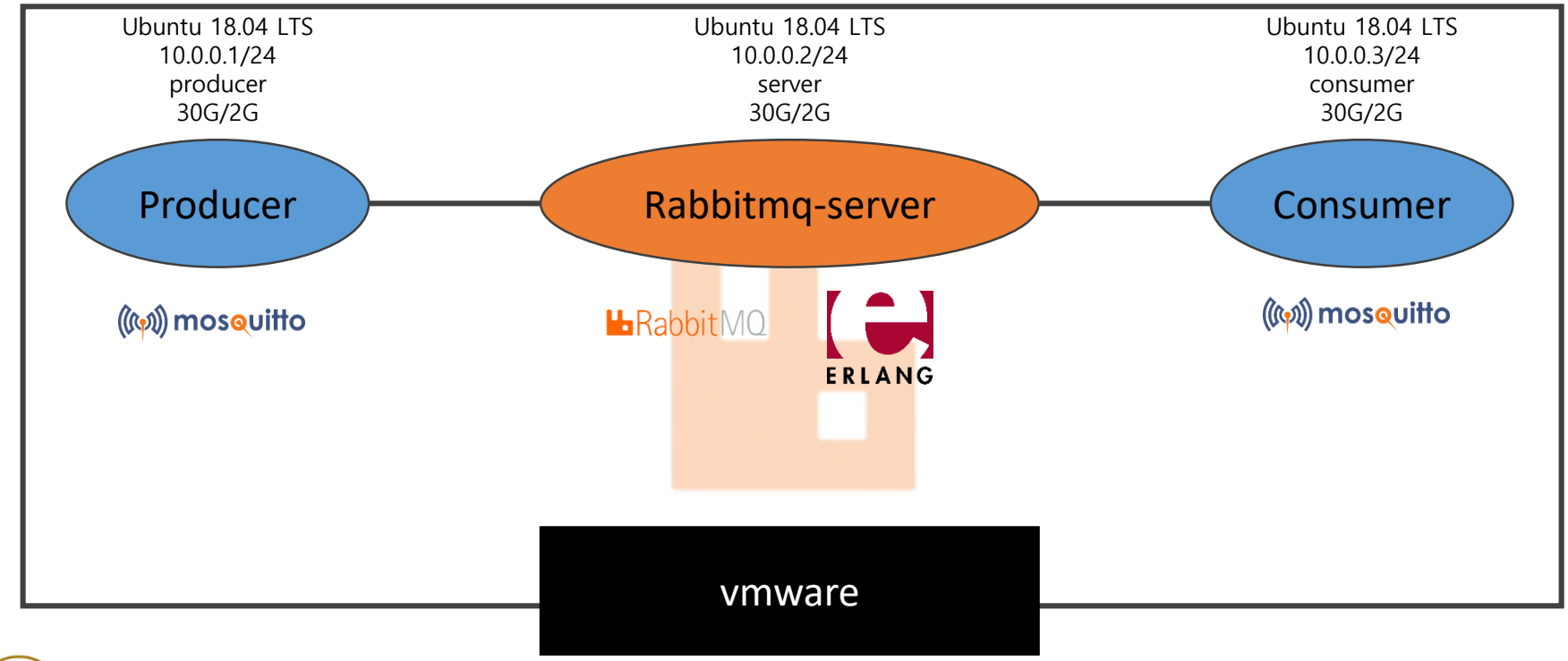
목차

1. 테스트 베드 구축
   - VM 설정
   - 네트워크 설정
   - 테스트

QBQB

1. 테스트 베드 구축

- 테스트 베드 구축



QBQB

https://github.com/F-Secure/mqtt_fuzz

1. 테스트 베드 구축

- VM 세팅
  - 디스크 용량 20GB
  - 메모리 용량 2GB
  - OS : Ubuntu 18.04 LTS
- OS 세팅

```
userm@ubuntu:~$ sudo apt update
[sudo] password for userm:
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
133 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
userm@ubuntu:~$ sudo apt install open-vm-tools open-vm-tools-desktop
Reading package lists... Done
Building dependency tree
Reading state information... Done
open-vm-tools is already the newest version (2:10.3.0-0ubuntu1~18.04.3).
open-vm-tools-desktop is already the newest version (2:10.3.0-0ubuntu1~18.04.3).
0 upgraded, 0 newly installed, 0 to remove and 133 not upgraded.
userm@ubuntu:~$ sudo apt install vim git curl gcc make wget python-pip -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

QBQB

1. 테스트 베드 구축

- Producer
  - 생성된 VM을 복제해 Producer VM을 생성함.
  - Mosquitto-clients 설치

```
userm@ubuntu:~$ sudo apt install mosquitto-clients
[sudo] password for userm:
Reading package lists... Done
```

  - mqtt_fuzz 설치
    - Radamsa 설치(mqtt_fuzz는 Radamsa를 필요로 함.)

```
userm@ubuntu:~$ cd radamsa/
userm@ubuntu:~/radamsa$ rm radamsa.c
rm: remove write-protected regular file 'radamsa.c'? Y
userm@ubuntu:~/radamsa$ make OFLAGS=-O1
```

```
userm@ubuntu:~/radamsa$ sudo make install
[sudo] password for userm:
mkdir -p /usr/bin
cp bin/radamsa /usr/bin
mkdir -p /usr/share/man/man1
cat doc/radamsa.1 | gzip -9 > /usr/share/man/man1/radamsa.1.gz
```

1. 테스트 베드 구축

- Producer
  - mqtt_fuzz 설치

```
userm@ubuntu:~$ pip install Twisted
Collecting Twisted
  Downloading https://files.pythonhosted.org/packages/5d/0e/a72d85a55761c2c3ff1c
b968143a2fd5f360220779ed90e0fadf4106d4f2/Twisted-18.9.0.tar.bz2 (3.1MB)
    100% |████████████████████████████████| 3.1MB 191kB/s
Collecting Automat>=0.3.0 (from Twisted)
```

```
userm@ubuntu:~$ git clone https://github.com/F-Secure/mqtt_fuzz.git
Cloning into 'mqtt_fuzz'...
remote: Enumerating objects: 68, done.
remote: Total 68 (delta 0), reused 0 (delta 0), pack-reused 68
Unpacking objects: 100% (68/68), done.
userm@ubuntu:~$ cd mqtt_fuzz/
userm@ubuntu:~/mqtt_fuzz$ python mqtt_fuzz.py
usage: mqtt_fuzz.py [-h] [-ratio fuzz_ratio] [-delay send_delay]
                    [-validcases validcase_path] [-fuzzer fuzzer_path]
                    target_host target_port
mqtt_fuzz.py: error: too few arguments
```

  - mqtt 메시지 테스트를 위한 스크립트 생성
    - vi test.sh

1. 테스트 베드 구축

- Server
  - 생성된 VM을 복제해 Server VM을 생성함.
  - RabbitMQ 설치

```
userm@ubuntu:~$ sudo apt install rabbitmq-server
[sudo] password for userm:
Reading package lists... Done
Building dependency tree
```

  - 관리용 플러그인, mqtt 플러그인 활성화 및 관리자 계정 설정

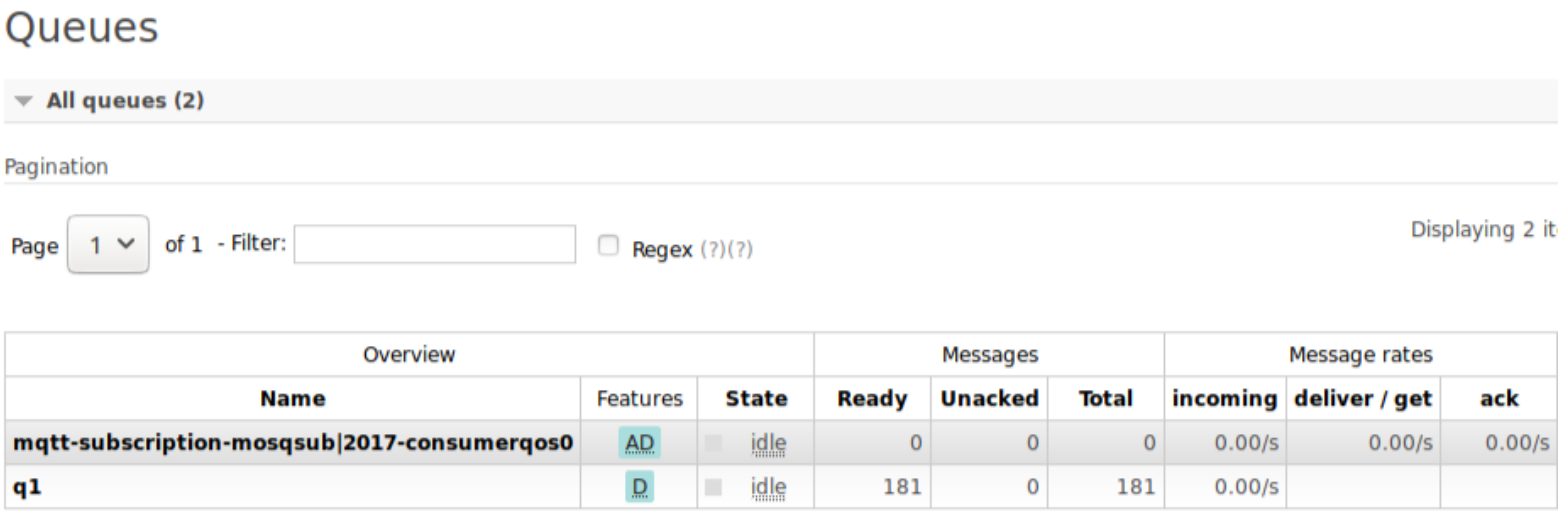
```
userm@ubuntu:~$ sudo rabbitmq-plugins enable rabbitmq_management
The following plugins have been enabled:
  amqp_client
  cowlib
  cowboy
  rabbitmq_web_dispatch
  rabbitmq_management_agent
  rabbitmq_management

Applying plugin configuration to rabbit@ubuntu... started 6 plugins.
userm@ubuntu:~$ sudo rabbitmq-plugins enable rabbitmq_mqtt
The following plugins have been enabled:
  rabbitmq_mqtt
```

```
userm@server:~$ sudo rabbitmqctl add_user testuser jini22
[sudo] password for userm:
Creating user "testuser"
userm@server:~$ sudo rabbitmqctl set_user_tags testuser administrator
Setting tags for user "testuser" to [administrator]
```

1. 테스트 베드 구축

- Server
  - mqtt_fuzz 메시지 테스트를 위한 설정
    - 큐 생성
      - q1이라는 큐를 생성함.



Queues

All queues (2)

Pagination

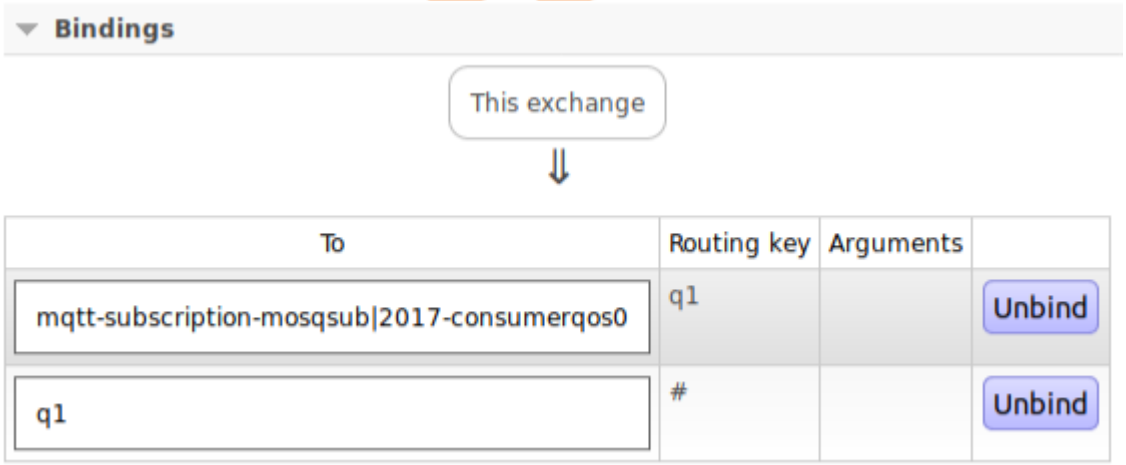
Page 1 of 1 - Filter: Regex (?)(?) Displaying 2 it

Overview			Messages			Message rates		
Name	Features	**State**	**Ready**	**Unacked**	**Total**	**incoming**	**deliver / get**	**ack**
mqtt-subscription-mosqsub|2017-consumerqos0	AD	idle	0	0	0	0.00/s	0.00/s	0.00/s
q1	D	idle	181	0	181	0.00/s		

QBQB

1. 테스트 베드 구축

- Server
  - mqtt_fuzz 메시지 테스트를 위한 설정
    - 교환 설정
      - amq.topic에서 설정
      - Bindings에서 To를 q1으로 설정
      - 라우팅 키 '#'은 모든 요청에 대한 응답
      - 즉, 모든 요청이 큐 q1으로 들어가게 됨.



QBQB

1. 테스트 베드 구축

- Consumer
  - 생성된 VM을 복제해 Consumer VM을 생성함.
  - mosquitto-clients 설치

```
userm@ubuntu:~$ sudo apt install mosquitto-clients
[sudo] password for userm:
Reading package lists... Done
```


QBQB

1. 테스트 베드 구축

- 네트워크 세팅
  - VM 네트워크를 host-only로 변경함.
  - 호스트 네임 설정
    - 호스트 명은 VM 별로 각각 producer, server, consumer로 지정함.
  - hosts 설정
    - IP를 굳이 사용하지 않아도 hostname으로 IP를 알아볼 수 있게 설정함.

```
userm@producer:~$ sudo vi /etc/hosts
userm@producer:~$
```

```
127.0.0.1       localhost
127.0.1.1       ubuntu

10.0.0.1        producer
10.0.0.2        server
10.0.0.3        consumer
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
```

QBQB

1. 테스트 베드 구축

- 네트워크 설정
  - IP 설정
    - 기존 인터넷과 연결된 네트워크 인터페이스인 ens33을 고정 IP로 설정함.
    - IP는 VM 별로 각각 10.0.0.1/24, 10.0.0.2/24, 10.0.0.3/24로 지정함.

```
network:
        ethernets:
                ens33:
                        addresses: [10.0.0.1/24]
                        dhcp4: no
        version: 2
```

```
network:
        ethernets:
                ens33:
                        addresses: [10.0.0.2/24]
                        dhcp4: no
        version: 2
```

```
network:
        ethernets:
                ens33:
                        addresses: [10.0.0.3/24]
                        dhcp4: no
        version: 2
```

QBQB

1. 테스트 베드 구축

- 네트워크 설정
  - Ping 확인

```
root@producer:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) byte
64 bytes from 10.0.0.2: icmp_seq=1
64 bytes from 10.0.0.2: icmp_seq=2
64 bytes from 10.0.0.2: icmp_seq=3
```

```
root@producer:~# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.784 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.633 ms
```

```
root@server:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) byte
64 bytes from 10.0.0.1: icmp_seq=1
64 bytes from 10.0.0.1: icmp_seq=2
64 bytes from 10.0.0.1: icmp_seq=3
```

```
root@server:~# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=0.235 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.767 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.944 ms
```

```
root@consumer:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1
64 bytes from 10.0.0.1: icmp_seq=2
64 bytes from 10.0.0.1: icmp_seq=3
64 bytes from 10.0.0.1: icmp_seq=4
```

```
root@consumer:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.291 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.834 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.965 ms
```

QBQB

1. 테스트 베드 구축

- 테스트
  - 모든 VM이 켜져 있어야 하며 서로 간의 ping 통신이 된 상태여야 함.
  - producer에서 mqtt 메시지를 보내 consumer에서 확인함.
    - Server

```
userm@server:~$ service rabbitmq-server status
● rabbitmq-server.service - RabbitMQ Messaging Server
   Loaded: loaded (/lib/systemd/system/rabbitmq-server.service; enabled; vendor
   Active: active (running) since Tue 2019-03-19 04:46:21 PDT; 2min 35s ago
  Process: 797 ExecStartPost=/usr/lib/rabbitmq/bin/rabbitmq-server-wait (code=ex
 Main PID: 796 (rabbitmq-server)
```

```
userm@server:~$ tail -f /var/log/rabbitmq/rabbit@server.log
```

    - Producer
      - 세팅 과정에서 작성한 스크립트를 실행함.

```
userm@producer:~$ ./test.sh
```

    - Consumer
      - mosquitto_sub를 통해 메시지를 수신함.

```
userm@consumer:~$ mosquitto_sub -h 10.0.0.2 -p 1883 -d -t q1 -u testuser -P jini
22
```

QBQB

1. 테스트 베드 구축

- 테스트
  - 권한 거부

```
userm@producer:~$ ./test.sh
bash: ./test.sh: Permission denied
```

  - 권한 설정
    - chmod 명령어 사용

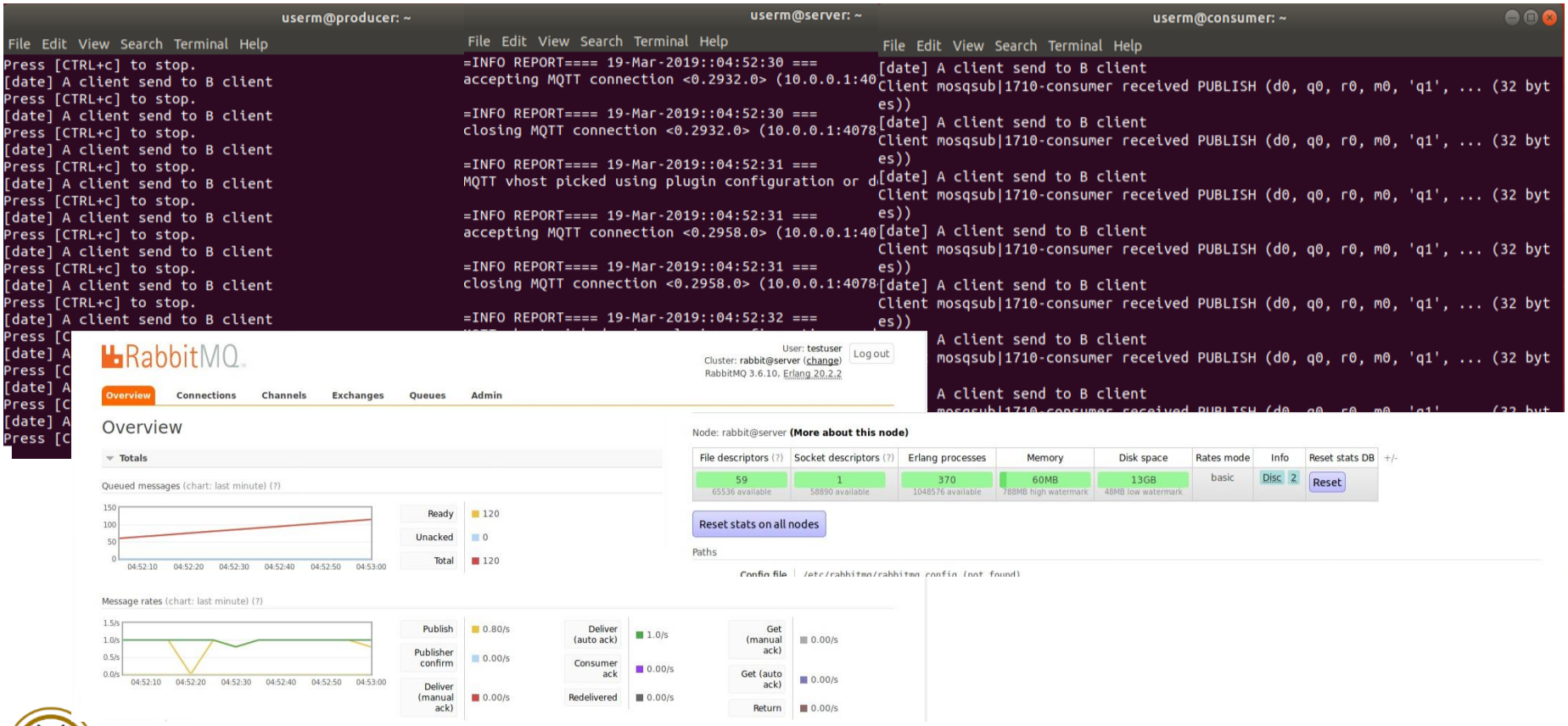
```
-rw-r--r--  1 userm userm    0 Mar 18 10:34 .sudo_as_admin_successful
drwxr-xr-x  2 userm userm 4096 Mar 18 10:32 Templates
-rw-r--r--  1 userm userm  206 Mar 19 00:40 test.sh
drwxr-xr-x  2 userm userm 4096 Mar 18 10:32 Videos
-rw-------  1 root  root   802 Mar 18 19:14 .viminfo
-rw-r--r--  1 root  root   165 Mar 18 10:50 .wget-hsts
userm@producer:~$ sudo chmod -R 777 test.sh
```

```
-rwxrwxrwx  1 userm userm  206 Mar 19 00:40 test.sh
drwxr-xr-x  2 userm userm 4096 Mar 18 10:32 Videos
-rw-------  1 root  root  1034 Mar 19 03:43 .viminfo
-rw-r--r--  1 root  root   165 Mar 18 10:50 .wget-hsts
```

QBQB

1. 테스트 베드 구축

- 테스트



QBQB