# Mikołaj Piotrowski - raport; Zadanie 3

## Apache

1. Pobrano moduł mod_qos z użyciem dockerfila

```
  GNU nano 6.0                    Apache-Mod *
FROM httpd

RUN apt-get update \
        && apt-get install -y git gcc make
RUN apt-get install -y libapr1 libapr1-dev libaprutil1-dev
RUN apt-get install -y libapache2-mod-qos
```

```
server2:
  build:
    context: .
    dockerfile: Apache-Mod
  image: httpd:latest
```

2. Ponownie uruchomiono dockera

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx]
└─$ sudo docker-compose -f docker-compose.yml down
Removing ssl-docker-nginx_server1_1 ... done
Removing ssl-docker-nginx_server2_1 ... done
Removing network ssl-docker-nginx_default

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx]
└─$ sudo docker-compose -f docker-compose.yml build
server1 uses an image, skipping
Building server2
Step 1/4 : FROM httpd
 ---> c30a46771695
Step 2/4 : RUN apt-get update         && apt-get install -y git gcc make
 ---> Using cache
 ---> 2bade5732c99
Step 3/4 : RUN apt-get install -y libapr1 libapr1-dev libaprutil1-dev
 ---> Using cache
 ---> c21136b85463
Step 4/4 : RUN apt-get install -y libapache2-mod-qos
 ---> Using cache
 ---> 7d8a480715bc
Successfully built 7d8a480715bc
Successfully tagged httpd:latest

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx]
└─$ sudo docker-compose -f docker-compose.yml up
```

3. Skonfigurowano plik httpd.conf

```
#
LoadModule qos_module  /usr/lib/apache2/modules/mod_qos.so
```

4. Skonfigurowano plik httpd-ssl.conf. W celach testowych ustawiono limit 100 żądań na 60 sekund za pomocą QS_EventLimitCount a także limit 10 żądań na ten sam przedział czasu dla konkretnego user-agenta.

```
##
## SSL Virtual Host Context
##

SetEnvIf Request_URI ^/limit-a Limit_a

QS_EventLimitCount Limit_a 100 60

SetEnvIf User-Agent curl QS_COND=curl
QS_CondClientEventLimitCount 10 60 Limit_a curl

<VirtualHost _default_:443>
```

# NGINX

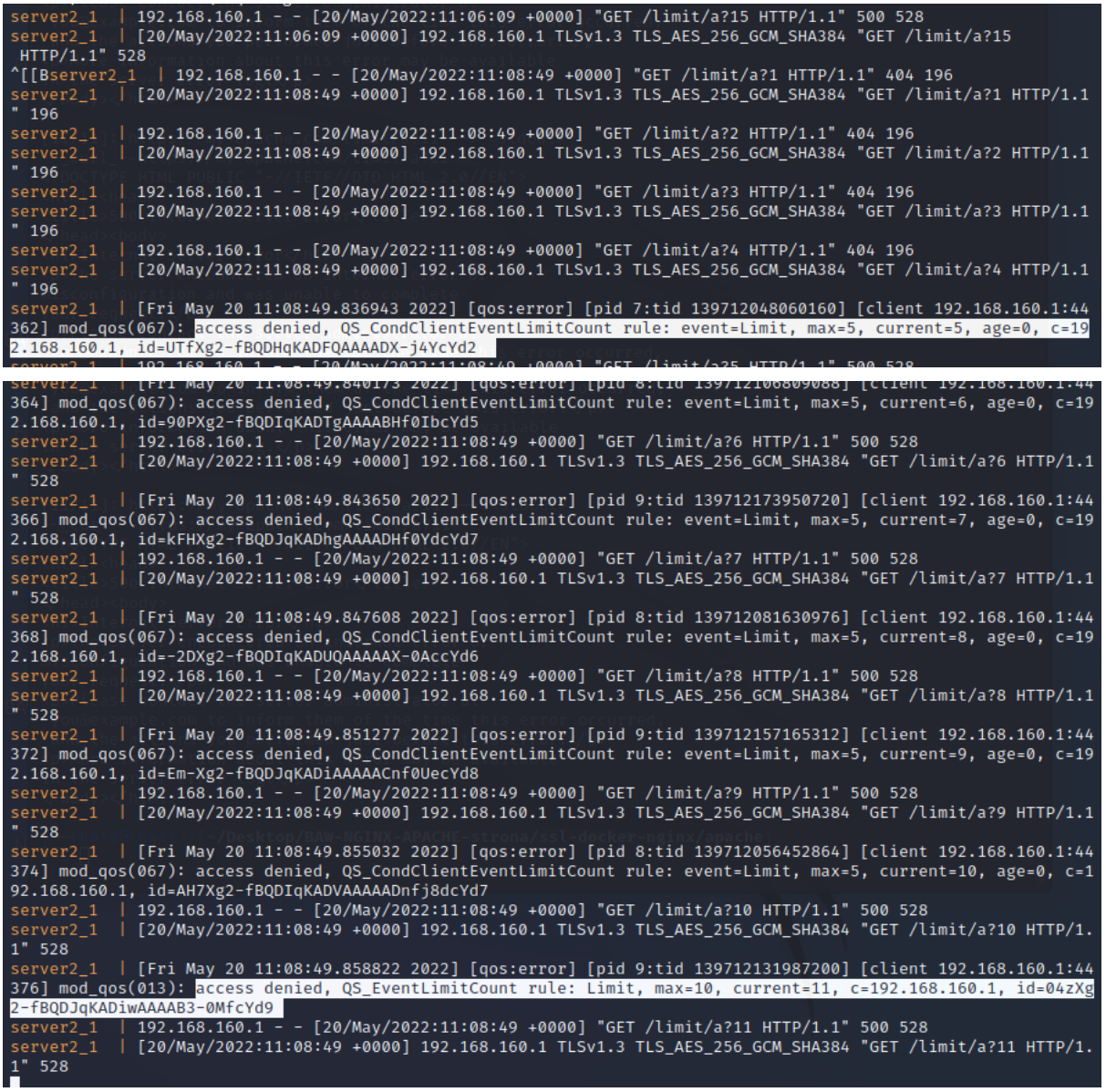
5. Skonfigurowano plik nginx.conf na podstawie https://urlund.com/blog/rate-limit-nginx-by-user-agent/

```
ssl_verify_client optional;


limit_req_zone $binary_remote_addr zone=default:1m rate=25r/m;

events {
  worker_connections  4096;  ## Default: 1024
}
```

```
http {
    server {
        listen 80;
        server_name my-nginx.com:8080;
        root         /usr/share/nginx/html/;

        location /https-only {
            deny all;
            return 403;
        }
        location ^(?:(?!\/http-https\/|\/http-only\/).)*$ {
            return 301 https://my-nginx.com$request_uri;
        }
        location /limit-a {
    # apply  rules
            limit_req zone=default nodelay;
            limit_req_status 418;
        }
    }
```

# TESTY

6. Wykonano zapytania na testową ścieżkę “limit” (zamiast 100 i 10 ma 10 i 5) w celu pokazania działania obu zabezpieczeń przed atakami dos.


server2_1 | 192.168.160.1 - - [20/May/2022:11:06:09 +0000] "GET /limit/a?15 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:06:09 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?15 HTTP/1.1" 528
^[[Bserver2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?1 HTTP/1.1" 404 196
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?1 HTTP/1.1" 196
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?2 HTTP/1.1" 404 196
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?2 HTTP/1.1" 196
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?3 HTTP/1.1" 404 196
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?3 HTTP/1.1" 196
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?4 HTTP/1.1" 404 196
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?4 HTTP/1.1" 196
server2_1 | [Fri May 20 11:08:49.836943 2022] [qos:error] [pid 7:tid 139712048060160] [client 192.168.160.1:44362] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=5, age=0, c=192.168.160.1, id=UTfXg2-fBQDHqKADFQAAAADX-j4YcYd2
server2_1 | [Fri May 20 11:08:49.840173 2022] [qos:error] [pid 8:tid 139712068090088] [client 192.168.160.1:44364] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=6, age=0, c=192.168.160.1, id=90PXg2-fBQDIqKADTgAAAABHf0IbcYd5
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?6 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?6 HTTP/1.1" 528
server2_1 | [Fri May 20 11:08:49.843650 2022] [qos:error] [pid 9:tid 139712173950720] [client 192.168.160.1:44366] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=7, age=0, c=192.168.160.1, id=kFHXg2-fBQDJqKADhgAAAADHf0YdcYd7
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?7 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?7 HTTP/1.1" 528
server2_1 | [Fri May 20 11:08:49.847608 2022] [qos:error] [pid 8:tid 139712081630976] [client 192.168.160.1:44368] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=8, age=0, c=192.168.160.1, id=-2DXg2-fBQDIqKADUQAAAAAX-0AccYd6
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?8 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?8 HTTP/1.1" 528
server2_1 | [Fri May 20 11:08:49.851277 2022] [qos:error] [pid 9:tid 139712157165312] [client 192.168.160.1:44372] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=9, age=0, c=192.168.160.1, id=Em-Xg2-fBQDJqKADiAAAAACnf0UecYd8
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?9 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?9 HTTP/1.1" 528
server2_1 | [Fri May 20 11:08:49.855032 2022] [qos:error] [pid 8:tid 139712056452864] [client 192.168.160.1:44374] mod_qos(067): access denied, QS_CondClientEventLimitCount rule: event=Limit, max=5, current=10, age=0, c=192.168.160.1, id=AH7Xg2-fBQDIqKADVAAAAADnfj8dcYd7
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?10 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?10 HTTP/1.1" 528
server2_1 | [Fri May 20 11:08:49.858822 2022] [qos:error] [pid 9:tid 139712131987200] [client 192.168.160.1:44376] mod_qos(013): access denied, QS_EventLimitCount rule: Limit, max=10, current=11, c=192.168.160.1, id=04zXg2-fBQDJqKADiwAAAAB3-0MfcYd9
server2_1 | 192.168.160.1 - - [20/May/2022:11:08:49 +0000] "GET /limit/a?11 HTTP/1.1" 500 528
server2_1 | [20/May/2022:11:08:49 +0000] 192.168.160.1 TLSv1.3 TLS_AES_256_GCM_SHA384 "GET /limit/a?11 HTTP/1.1" 528