LAPORAN KEAMANAN BASIS DATA
HTTP HTTPS DATABASE CONNECTION

Disusun Oleh :

M. Arghian Taufahena

4332101007

PROGRAM STUDI REKAYASA KEAMANAN SIBER

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

2022

DAFTAR ISI

BAB I
PENDAHULUAN

1. Hypertext Transfer Protocol (HTTP)

HTTP adalah sebuah protocol jaringan yang berfungsi untuk membantu transfer data atau informasi antar komputer melalui yang namanya browser atau *application layer*. HTTP biasanya melakukan transfer data berupa file, gambar, audio, video dan dokumen.

Cara kerja HTTP ini adalah dengan komunikasi antar client dan server, contohnya client ingin membuka website dengan domain tertentu, maka protocol HTTP inilah yang akan membantu memenuhi permintaan client tersebut.

2. Hypertext Transfer Protocol Secure (HTTPS)

HTTPS adalah protocol yang lebih aman dari HTTP, cara kerja HTTPS tidak jauh beda dari HTTP, hanya pada protocol HPTTS ini menggunakan metode enkripsi pada saat melakukan transfer data.

Banyak website yang menggunakan protocol HTTPS karena keamanan transfer data yang diberikan, contohnya seperti facebook, google, dan lainya. Enkripsi pada saat transfer data ini dilakukan untuk menjaga keamanan data yang akan dikirim dan diterima poleh client.

HTTPS biasa juga disebut sebagai protocol TLS atau Transport Layer Security, yang sebelumnya dikenal dengan Secure Sockets Layer atau SSL. Protokol ini menggunakan infrastruktur kriptografi dengan kunci pulbik asimetris, menggunakan public key dan private key.

BAB II

IMPLEMENTASI

1. MySQL Database

Pada Server Database, kita menggunakan MySQL sebagai basic database untuk penerapan SSL (Secure Socket Layer) untuk https. Disini saya menggunakan 2 server virtual Ubuntu dengan masing –masing menggnakan adapter bridged dan Host-Only. untuk kebutuhan remote user MySQL.

- Database Server Ip : 192.168.20.18 (Host Only)
- Remote Server Ip : 192.168.20.20 (Host Only)

Pada Database Server, kita buat 1 user dengan privileges *.*, untuk dapat mudah mendapat akses kesemua database. Disini user yang akan saya pakai adalah 'taufahena'@'192.168.20.20'

```
mysql> select user, host, account_locked from mysql.user;
+------------------+---------------+----------------+
| user             | host          | account_locked |
+------------------+---------------+----------------+
| eghi             | %             | N              |
| ghian            | 192.168.20.1  | N              |
| taufahena        | 192.168.20.20 | N              |
| debian-sys-maint | localhost     | N              |
| gamma            | localhost     | N              |
| mysql.infoschema | localhost     | Y              |
| mysql.session    | localhost     | Y              |
| mysql.sys        | localhost     | Y              |
| root             | localhost     | N              |
+------------------+---------------+----------------+
9 rows in set (0.00 sec)
```

Tidak lupa pada konfigurasi bind address kita ubah ip nya menjadi 0.0.0.0 agar database server dapat menerima ip dari mana saja.

```
root@sucxsz: /var/lib/mysql
 GNU nano 6.2      /etc/mysql/mysql.conf.d/mysqld.cnf *
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
mysqlx-bind-address     = 127.0.0.1
#
# * Fine Tuning
#
```

Sebelum mengaktifkan SSL pada MySQL. Pastikan untuk cek versi dari MySQL, pastikan versinya sudah sesuai, yaitu versi 8.0, karena beberapa perintah seperti membuat sertifikat ssl tidak tersedia pada versi lain, seperti MariaDB.

```
root@sucxsz:/home/sucxsz# mysql --version
mysql  Ver 8.0.31-0ubuntu0.22.04.1 for Linux
root@sucxsz:/home/sucxsz#
```

Setelah membuat user dan privileges nya, selanjutnya kita membuat sertifikat dan kunci SSL pada MySQL dengan perintah **mysql_ssl_rsa_setup ~uid=mysql ,** Selanjutnya kita dapat mengecek hasil sertifikatnya pada direktori **/var/lib/mysql**, yaitu file dengan format .pem.

```
mysql> exit;
Bye
root@sucxsz:/home/sucxsz# mysql_ssl_rsa_setup --uid=mysql
root@sucxsz:/home/sucxsz# cd /var/lib/mysql
root@sucxsz:/var/lib/mysql# ls
 auto.cnf          client-key.pem      '#innodb_redo'        server-key.pem
 binlog.000001     db_https            '#innodb_temp'        sucxsz.pid
 binlog.000002     debian-5.7.flag      mysql                sys
 binlog.000003    '#ib_16384_0.dblwr'   mysql.ibd            undo_001
 binlog.index     '#ib_16384_1.dblwr'   performance_schema   undo_002
 ca-key.pem        ib_buffer_pool       private_key.pem
 ca.pem            ibdata1              public_key.pem
 client-cert.pem   ibtmp1               server-cert.pem
root@sucxsz:/var/lib/mysql# find -name '*.pem' -ls
   527113      4 -rw-------   1 mysql    mysql        1705 Nov 24 15:05 ./private_key.pem
   527110      4 -rw-r--r--   1 mysql    mysql        1112 Nov 24 15:05 ./server-cert.pem
   527105      4 -rw-------   1 mysql    mysql        1701 Nov 24 15:05 ./ca-key.pem
   527112      4 -rw-r--r--   1 mysql    mysql        1112 Nov 24 15:05 ./client-cert.pem
   527111      4 -rw-------   1 mysql    mysql        1705 Nov 24 15:05 ./client-key.pem
   527109      4 -rw-------   1 mysql    mysql        1705 Nov 24 15:05 ./server-key.pem
   527114      4 -rw-r--r--   1 mysql    mysql         452 Nov 24 15:05 ./public_key.pem
   527108      4 -rw-r--r--   1 mysql    mysql        1112 Nov 24 15:05 ./ca.pem
root@sucxsz:/var/lib/mysql#
```

2. MySQL Remote

Pada Server remote kita akan melakukan login serta mengaktifkan mode SSL dengan perintah **mysql –u user –h host –p –ssl-mode=required**

```
root@sucxsz:/var/www/html# mysql -u taufahena -h 192.168.20.18 -p --ssl-mode=required
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 8.0.31-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.
```

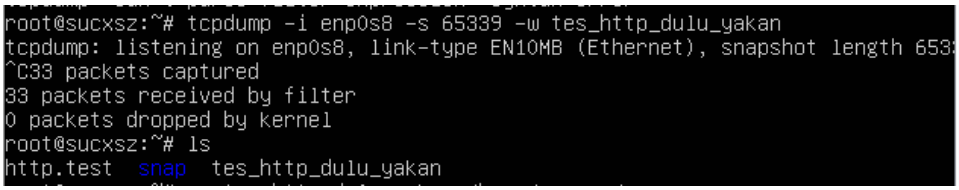
Dan jalankan perintah \s untuk melihat apakah sertifikat ssl nya sudah diterapkan. Pada bagian SSL, dapat dilihat jenis kriptografi dari sertifikat yang digunakan.

```
mysql> \s
--------------
mysql  Ver 8.0.31-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))

Connection id:          2234
Current database:
Current user:           taufahena@192.168.20.20
SSL:                    Cipher in use is TLS_AES_256_GCM_SHA384
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.31-0ubuntu0.22.04.1 (Ubuntu)
Protocol version:       10
Connection:             192.168.20.18 via TCP/IP
Server characterset:    utf8mb4
Db     characterset:    utf8mb4
Client characterset:    utf8mb4
Conn.  characterset:    utf8mb4
TCP port:               3306
Binary data as:         Hexadecimal
Uptime:                 11 hours 32 min 39 sec

Threads: 2  Questions: 253796  Slow queries: 1  Opens: 4531  Flush
ies per second avg: 6.106
--------------
```

3. TCPDUMP

Disini tcpdump digunakan untuk mengcapture dengan tujuan hasil capture nanti akan memperlihatkan perbedaan dari MySQL menggunakan SSL dan tanpa SSL.

Langsung saja kita implementasikan pada MySQL Remote dengan menggunakan perintah **tcpdump –I network-interface –s 65539 –w nama_file.** untuk pertama, boleh kita capture http terlebih dahulu, setelah itu kita lakukan hal yang sama untuk https.



- **HTTP Capture**

  Pada saat capture dimulai, kita dapat melakukan login remote lagi dengan bantuan terminal lain, bisa dengan menggunakan metode SSH. Dan caranya sama seperti diatas, login remote seperti MySQL biasa, tapi tidak dengan menggunakan **--ssl-mode=required,**

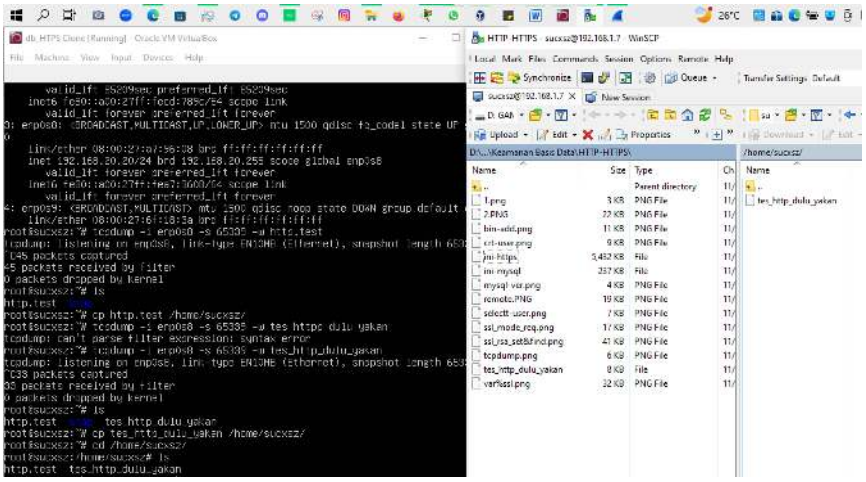
- **HTTPS Capture**

  Sama halnya seperti http capture, pada capture HTTPS kita juga melakukan login remote lagi dengan bantuan terminal lain, bisa dengan menggunakan metode SSH. Dan caranya sama seperti diatas, login remote seperti MySQL biasa, **TAPI** dengan menggunakan **--ssl-mode=required.**

Capture TCPDUMP dapat dihentikan jika dirasa sudah selesai (sudah melakukan login remote MySQL) dengan cara ketik ctrl + c pada Server Remote yang sebelumnya di jalankan tcpdump.

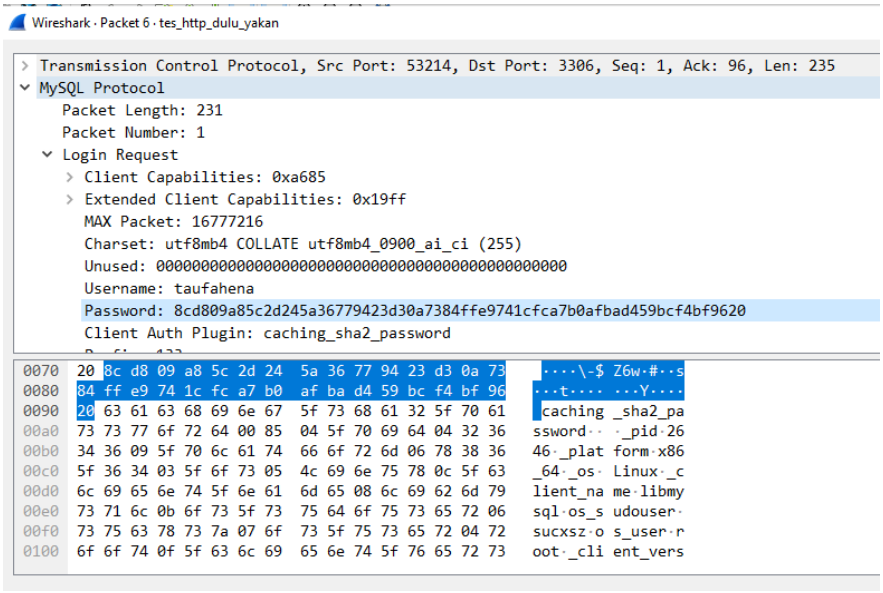
4. WINSCP & WIRESHARK

WinScp adalah platform atau software file transfer protocol (FTP) yang digunakan untuk mentransfer file hasil capture yang ada pada Server Remote MySql tadi ke Desktop Windows saya .

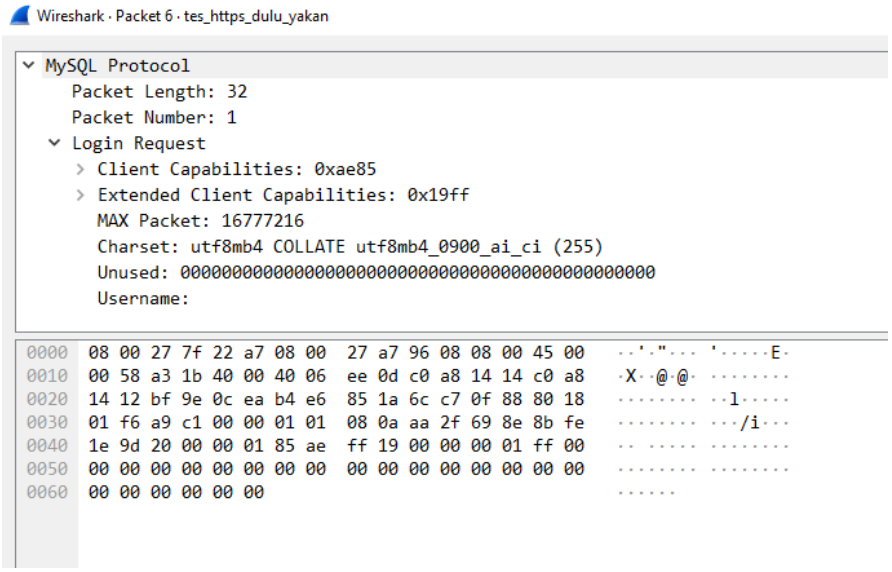


Selanjutnya setelah menempatkan kedua hasil capture tadi di windows, kita dapat menggunakan wireshark untuk melihat kembali isi dari capture file tersebut. Dengan cara buka file tersebut pada wireshark, dan filter packet dengan nama MySQL.

- Hasil capture HTTP



- Hasil capture HTTPS

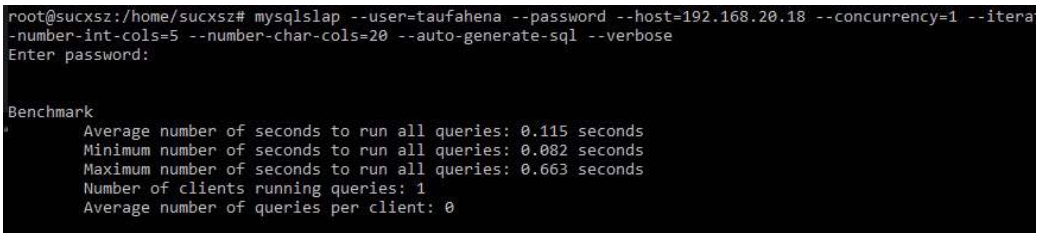


5. Hit 1000 DATABASE

Untuk melakukan tes koneksi hit ke database kita dapat menggunakan perintah **msyqlslap,** mysqlslap sendiri digunakan untuk menguji beban dari database MySQL itu sendiri.

- HTTP

Untuk hit HTTP dapat dilakukan dengan perintah **mysqlslap –user=taufahena ~password –host=192.168.20.18 ~concurrency-1 ~iterations=1000 –number-int-cols=5 ~number-char-cols=20 ~auto-generate-sql –verbose**



- HTTPS

Sama seperti saat menjalankan TCPDUMP yang sembari melakukan login remote, untuk HTTPS ditambahkan dengan peritnah ~ssl-mode=required

mysqlslap –user=taufahena ~password –host=192.168.20.18 ~concurrency-1 ~ iterations=1000 –number-int-cols=5 ~number-char-cols=20 ~auto-generate-sql – verbose ~ssl-mode=required

```
root@sucxsz:/var/www/html# cd
root@sucxsz:~# mysqlslap --user=taufahena --password --host=192.168.20.18 --concurrency=1 --iterations=1000 --number-int
-cols=5 --number-char-cols=20 --auto-generate-sql --verbose --ssl-mode=required
Enter password:


Benchmark
        Average number of seconds to run all queries: 0.189 seconds
        Minimum number of seconds to run all queries: 0.081 seconds
        Maximum number of seconds to run all queries: 10.106 seconds
        Number of clients running queries: 1
        Average number of queries per client: 0
```

BAB II
KESIMPULAN

1. Performa Penggunaan SSL pada MySQL

Penggunaan SSL pada database atau bisa dibilang penggunaan HTTPS pertama dapat kita ketahui di file capture hasil tcpdump, yang dimana penggunaan HTTPS membatasi credential login pada database, yaitu hanya nama user saja beserta jenis kriptografi hasil pembuatan sertifikat SSL.

Sedangkan penggunaan database tanpa SSL atau hanya HTTP bisa dibilang tidak cukup aman jika dilihat dari hasil capture tcpdump.

2. Penjelasan singkat penggunaan pengukuran MYSQLSLAP

Mysqlsap disini yang digunakan untuk pengukuran beban server yang akan memaksa server untuk menjalankan setiap perintah query yang akan di lakukan nantinya.

Dari mysqlslap yang saya jalankan, saya menjalankan pengukuran dengan cara membuat tabel dengan 5 numeric kolom, 20 karakter setiap kolom, mensimulasikan 1 koneksi klien, dengan 1000 kali test.

DAFTAR PUSTAKA

Web cloudraya.com, Penjelasan mengenai HTTP

https://cloudraya.com/blog/pengertian-http/

Web cloudflare.com, Penjelasan mengenai HTTPS

https://www.cloudflare.com/learning/ssl/what-is-https/

arctype.com, Penjelasan mengenai penggunaaan SSL pada MySQL

https://arctype.com/blog/mysql-ssl/

mariadb.com, Penjelasan mengenai penggunaan mysqlslap
https://mariadb.com/kb/en/mysqlslap/#:~:text=mysqlslap%20is%20a%20tool%20for,set%20of%20queries%20multiple%20times.

lms.onnocenter.or.id, Penjelasan mengenai pengukuran mysqlslap
https://lms.onnocenter.or.id/wiki/index.php/Mysqlslap:_cara_melakukan_pengukuran