Gary's Cybersecurity Cheat Sheets

This cheat sheet consolidates my notes for teaching and projects. As a Cybersecurity Consultant & Trainer based in Malaysia, I specialize in providing innovative cybersecurity training solutions grounded in the "think red, act blue" philosophy. This approach involves simulating offensive attacks from various perspectives to equip clients with the knowledge and skills to anticipate and counter potential threats.

🥷 OFFENSIVE SECURITY 👨‍💻 GARY'S GITHUB ✍🏻 GARY'S MEDIUM

Content Page

Web Server Hardening - MySQL

MySQL Security

In order to understand the possible attack can be done on MySQL, please read our write up for SQL Injection at http://www.axcelsec.com/2018/02/penetration-testing-with-owasp-top-10.html.

```
SHOW DATABASES;
USE MYSQL;
SELECT * FROM user;
SELECT Host,User,Password FROM user;
```

CIS Benchmark

3. File System Permissions

```
SHOW VARIABLES WHERE
variable_name = 'datadir' OR
variable_name = 'plugin_dir' OR  #Plugin Directory
variable_name LIKE 'log_bin_basename' OR
variable_name LIKE 'log_error' OR
variable_name LIKE 'slow_query_log_file' OR
variable_name LIKE 'relay_log_basename' OR
variable_name LIKE 'general_log_file' OR
variable_name = 'ssl_key'; #SSL Key Files
```

---

4. General

```
SHOW VARIABLES WHERE variable_name LIKE "version";
SHOW VARIABLES LIKE 'have_symlink'; #Ensure the Value returned is DISABLED.
SHOW DATABASES LIKE 'test'; #Ensure that no rows are returned (Ensure the '
SELECT * FROM information_schema.plugins WHERE PLUGIN_NAME='daemon_memcache
SHOW VARIABLES WHERE variable_name = 'secure_file_priv' AND Value<>''; #The
SHOW VARIABLES WHERE variable_name = 'local_infile'; #Ensure the Value fiel
SHOW VARIABLES LIKE 'sql_mode'; #Ensure that STRICT_ALL_TABLES is in the li
```

Ensure the 'test' Database Is Not Installed

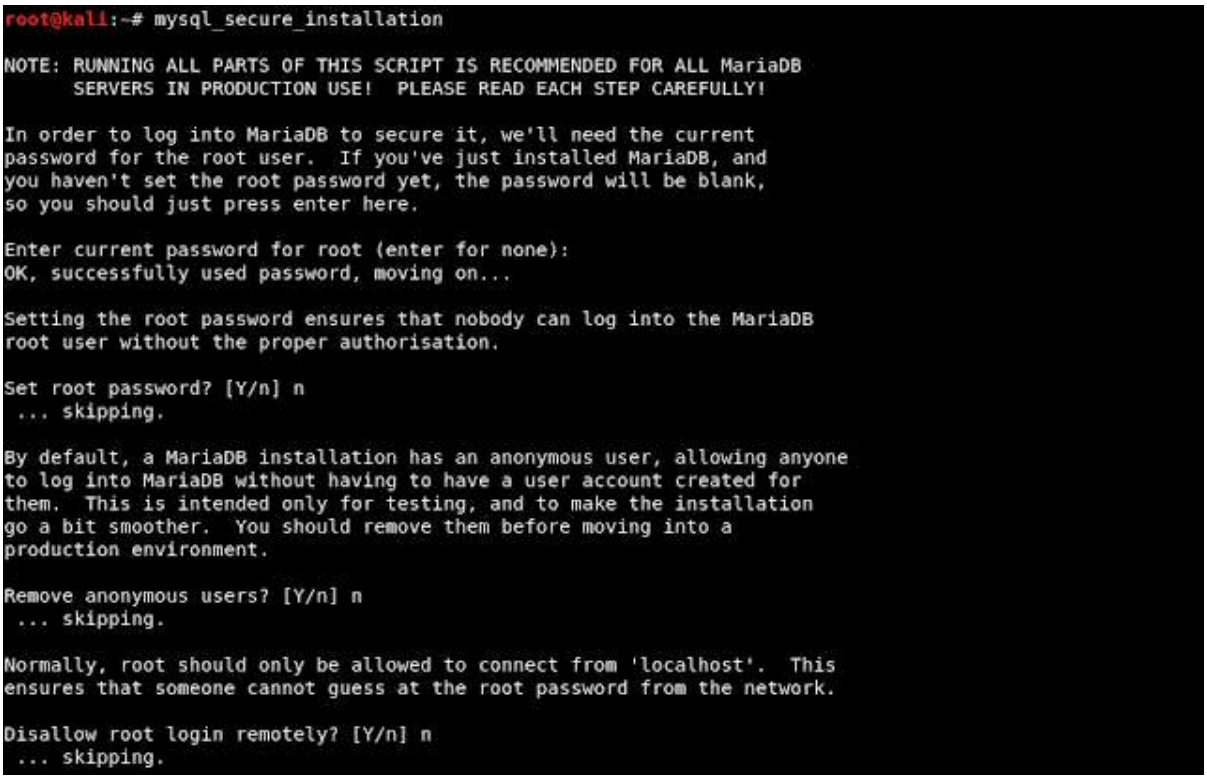
```
SHOW DATABASES LIKE 'test';
DROP DATABASE "test"; #If the above SQL statement is not return zero rows
```

Improve MySQL Installation Security

```
mysql_secure_installation
#/usr/bin/mysql_secure_installation
```

```
#C:\xampp\mysql\bin\mysql_secure_installation.pl
```

- set a password for root accounts
- remove root accounts that are accessible from outside the local host
- remove anonymous-user accounts
- remove the test database



---

5. MySQL Permissions

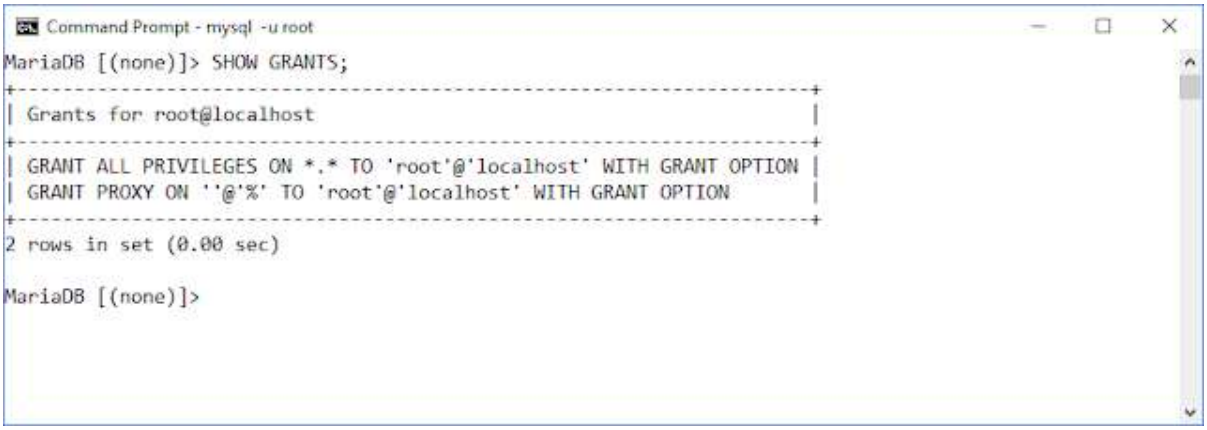
To display the privileges and roles

```
mysql -e "SHOW GRANTS"
mysql -u root -e "SHOW GRANTS"
```

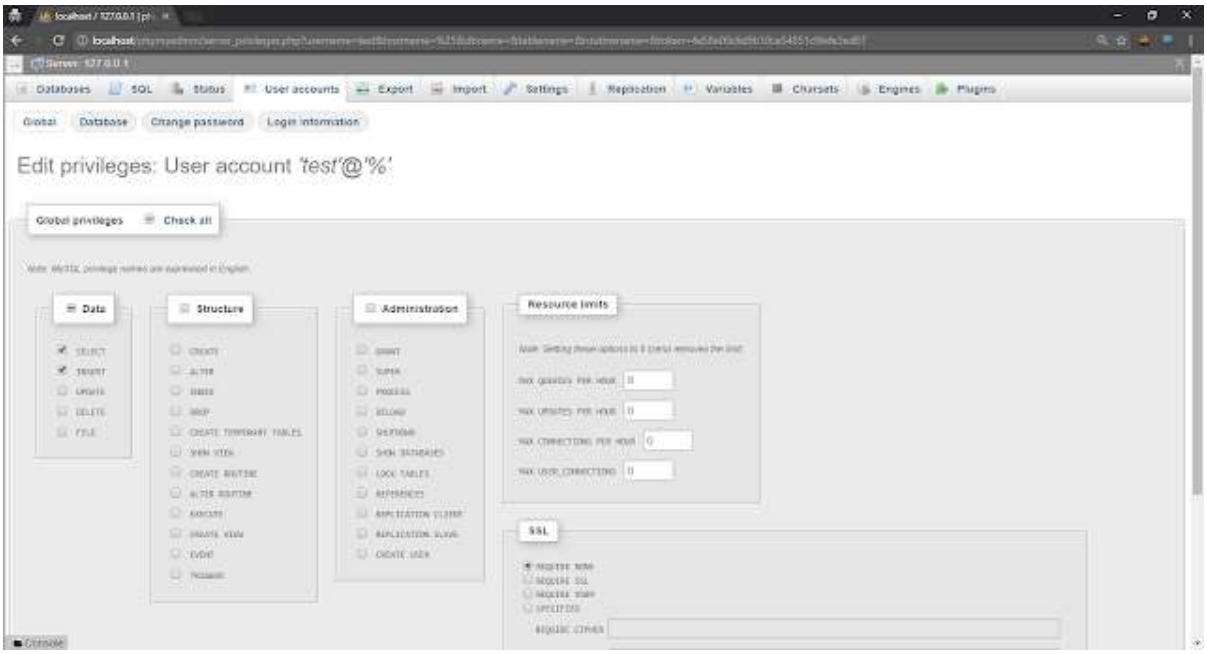
```
C:\>mysql -e "SHOW GRANTS"
+---------------------------------------+
| Grants for @localhost                 |
+---------------------------------------+
| GRANT USAGE ON *.* TO ''@'localhost' |
+---------------------------------------+

C:\>mysql -u root -e "SHOW GRANTS"
+-----------------------------------------------------------------------------+
| Grants for root@localhost                                                   |
+-----------------------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION |
| GRANT PROXY ON ''@'%' TO 'root'@'localhost' WITH GRANT OPTION       |
+-----------------------------------------------------------------------------+
```

To check which accounts have access to what

```
SHOW GRANTS;
SHOW PRIVILEGES;
```



```
MariaDB [(none)]> SHOW PRIVILEGES;
+-------------------------+---------------------------------------+-------------------------------------------------------+
| Privilege               | Context                               | Comment                                               |
+-------------------------+---------------------------------------+-------------------------------------------------------+
| Alter                   | Tables                                | To alter the table                                    |
| Alter routine           | Functions,Procedures                  | To alter or drop stored functions/procedures          |
| Create                  | Databases,Tables,Indexes              | To create new databases and tables                    |
| Create routine          | Databases                             | To use CREATE FUNCTION/PROCEDURE                      |
| Create temporary tables | Databases                             | To use CREATE TEMPORARY TABLE                         |
| Create view             | Tables                                | To create new views                                   |
| Create user             | Server Admin                          | To create new users                                   |
| Delete                  | Tables                                | To delete existing rows                               |
| Drop                    | Databases,Tables                      | To drop databases, tables, and views                  |
| Event                   | Server Admin                          | To create, alter, drop and execute events             |
| Execute                 | Functions,Procedures                  | To execute stored routines                            |
| File                    | File access on server                 | To read and write files on the server                 |
| Grant option            | Databases,Tables,Functions,Procedures | To give to other users those privileges you possess   |
| Index                   | Tables                                | To create or drop indexes                             |
| Insert                  | Tables                                | To insert data into tables                            |
| Lock tables             | Databases                             | To use LOCK TABLES (together with SELECT privilege)   |
| Process                 | Server Admin                          | To view the plain text of currently executing queries |
| Proxy                   | Server Admin                          | To make proxy user possible                           |
| References              | Databases,Tables                      | To have references on tables                          |
| Reload                  | Server Admin                          | To reload or refresh tables, logs and privileges      |
| Replication client      | Server Admin                          | To ask where the slave or master servers are          |
| Replication slave       | Server Admin                          | To read binary log events from the master             |
| Select                  | Tables                                | To retrieve rows from table                           |
| Show databases          | Server Admin                          | To see all databases with SHOW DATABASES              |
| Show view               | Tables                                | To see views with SHOW CREATE VIEW                    |
| Shutdown                | Server Admin                          | To shut down the server                               |
| Super                   | Server Admin                          | To use KILL thread, SET GLOBAL, CHANGE MASTER, etc.   |
| Trigger                 | Tables                                | To use triggers                                       |
| Create tablespace       | Server Admin                          | To create/alter/drop tablespaces                      |
| Update                  | Tables                                | To update existing rows                               |
| Usage                   | Server Admin                          | No privileges - allow connect only                    |
+-------------------------+---------------------------------------+-------------------------------------------------------+
31 rows in set (0.00 sec)
```



Ensure Only Administrative Users Have Full Database Access

```
SELECT user, host
FROM mysql.user
WHERE (Select_priv = 'Y')
OR (Insert_priv = 'Y')
OR (Update_priv = 'Y')
OR (Delete_priv = 'Y')
OR (Create_priv = 'Y')
```

```
OR (Drop_priv = 'Y');

SELECT user, host
FROM mysql.db
WHERE db = 'mysql'
AND ((Select_priv = 'Y')
OR (Insert_priv = 'Y')
OR (Update_priv = 'Y')
OR (Delete_priv = 'Y')
OR (Create_priv = 'Y')
OR (Drop_priv = 'Y'));
```

Ensure Privileges Is Not Give To Non-Administrative Users

```
SELECT user, host, File_priv, Process_priv, Super_priv, Shutdown_priv, Crea
from mysql.user
where File_priv = 'Y'
OR Process_priv = 'Y'
OR Super_priv = 'Y'
OR Shutdown_priv = 'Y'
OR Create_user_priv = 'Y'
OR Grant_priv = 'Y';

SELECT user, host FROM mysql.db WHERE Grant_priv = 'Y';
```

Ensure Privileges Is Not Give To Non-Slave Users

```
SELECT user, host FROM mysql.user WHERE Repl_slave_priv = 'Y';
```

Ensure DML/DDL Grants Are Limited to Specific Databases and Users

```
SELECT User, Host, Db, Select_priv, Insert_priv, Update_priv, Delete_priv,
FROM mysql.db
WHERE Select_priv='Y'
OR Insert_priv='Y'
OR Update_priv='Y'
OR Delete_priv='Y'
OR Create_priv='Y'
```

```
OR Drop_priv='Y'
OR Alter_priv='Y';
```

MySQL Permissions Hardening

```
REVOKE FILE ON *.* FROM '<user>';  #Disallow from reading and writing files
REVOKE PROCESS ON *.* FROM '<user>'; #Disable the ability view currently ex
REVOKE SUPER ON *.* FROM '<user>'; #Disable the ability to perform many act
REVOKE SHUTDOWN ON *.* FROM '<user>'; #Disable the ability to shut down the
REVOKE CREATE USER ON *.* FROM '<user>'; #Disable the ability to add/drop u
REVOKE GRANT OPTION ON *.* FROM '<user>'; #Disable the ability to grant oth

#Deny request updates that have been made on the master server
REVOKE REPLICATION SLAVE ON *.* FROM <user>;

#Limiting the users with the rights to modify or create data structures
REVOKE SELECT ON <host>.<database> FROM <user>;
REVOKE INSERT ON <host>.<database> FROM <user>;
REVOKE UPDATE ON <host>.<database> FROM <user>;
REVOKE DELETE ON <host>.<database> FROM <user>;
REVOKE CREATE ON <host>.<database> FROM <user>;
REVOKE DROP ON <host>.<database> FROM <user>;
REVOKE ALTER ON <host>.<database> FROM <user>;
```

Reference: https://dev.mysql.com/doc/refman/8.0/en/privileges-provided.html

---

6. Auditing and Logging

```
SHOW VARIABLES WHERE
variable_name LIKE 'log_bin_basename' OR   #Ensure the value returned does
variable_name LIKE 'log_error' OR   #Ensure the Value returned is not empty
variable_name LIKE 'log_error_verbosity';   #A value of 2 enables logging o
```

Auditing and Logging Hardening using my.ini (C:\xampp\mysql\bin\my.ini)

```
log_error = "mysql_error.log"  #Enabling error logging
log-raw = OFF  #To prevent password written to log files in plain text
```

User Statistics

```
set global userstat=ON;
SELECT user,total_connections,denied_connections,total_ssl_connections FROM
SHOW USER_STATISTICS;
```

```
MariaDB [(none)]> SELECT user,total_connections,denied_connections,total_ssl_connections FROM information_schema.user_statistics;
+------+-------------------+-------------------+----------------------+
| user | total_connections | denied_connections | total_ssl_connections |
+------+-------------------+-------------------+----------------------+
| test |                 1 |                 0 |                    0 |
| root |                 2 |                 0 |                    0 |
+------+-------------------+-------------------+----------------------+
2 rows in set (0.00 sec)
```

User Connection Errors

---

7. Authentication

```
SELECT @@global.sql_mode;  #Ensure result contains NO_AUTO_CREATE_USER
SELECT @@session.sql_mode; #Ensure result contains NO_AUTO_CREATE_USER

SELECT User,host FROM mysql.user WHERE authentication_string=''; #No rows w
SELECT user, host FROM mysql.user WHERE host = '%';  #Ensure no rows are re
SELECT user,host FROM mysql.user WHERE user = ''; #Ensure no rows are retur

#SHOW VARIABLES LIKE 'default_password_lifetime'; #default_password_lifetim
#SHOW VARIABLES LIKE 'validate_password%';
## validate_password_length should be 14 or more
## validate_password_mixed_case_count should be 1 or more
## validate_password_number_count should be 1 or more
## validate_password_special_char_count should be 1 or more
## validate_password_policy should be MEDIUM or STRONG
```

MySQL Native Password Hashing

```
SELECT PASSWORD('test');
SELECT CONCAT('*', UPPER(SHA1(UNHEX(SHA1('test')))));
```

```
MariaDB [(none)]> SELECT PASSWORD('test');
+-------------------------------------------+
| PASSWORD('test')                          |
+-------------------------------------------+
| *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29 |
+-------------------------------------------+
1 row in set (0.00 sec)

MariaDB [(none)]> SELECT CONCAT('*', UPPER(SHA1(UNHEX(SHA1('test')))));
+-------------------------------------------+
| CONCAT('*', UPPER(SHA1(UNHEX(SHA1('test'))))) |
+-------------------------------------------+
| *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29  |
+-------------------------------------------+
1 row in set (0.00 sec)
```

```
echo -n "test" | sha1sum | cut -c1-40 | xxd -p -r | sha1sum | cut -c1-40 |
```

```
root@kali:~# echo -n "test" | sha1sum | cut -c1-40 | xxd -p -r | sha1sum |
cut -c1-40 | tr '[a-z]' '[A-Z]'
94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
```

Anonymous Account

```
mysql -e "SELECT version(),user(),current_user()"
```

```
C:\>mysql -e "SELECT version(),user(),current_user()"
+-----------------+---------------------+----------------+
| version()       | user()              | current_user() |
+-----------------+---------------------+----------------+
| 10.1.21-MariaDB | Gary Kong@localhost | @localhost     |
+-----------------+---------------------+----------------+
```

```
#Exploitation by Anonymous Account
SHOW SCHEMAS;
SELECT table_schema, table_name FROM information_schema.tables;

USE test;
CREATE TABLE t1(i1 INT NOT NULL AUTO_INCREMENT PRIMARY KEY, v1 VARCHAR(100)
```

```
INSERT INTO t1(i1, v1) VALUES (1, REPEAT('abcde',20)); #abcdeabcdeabcdeabcc
INSERT INTO t1(i1, v1) SELECT NULL, a.v1 FROM t1 a, t1 b, t1 c;
```

```
MariaDB [(none)]> USE test;
Database changed
MariaDB [test]> SHOW TABLES;
Empty set (0.00 sec)

MariaDB [test]> CREATE TABLE t1(i1 INT NOT NULL AUTO_INCREMENT PRIMARY KEY, v1 VARCHAR(100) NOT NULL);
Query OK, 0 rows affected (0.37 sec)

MariaDB [test]> INSERT INTO t1(i1, v1) VALUES (1, REPEAT('abcde',20));
Query OK, 1 row affected (0.05 sec)

MariaDB [test]> INSERT INTO t1(i1, v1) SELECT NULL, a.v1 FROM t1 a, t1 b, t1 c;
Query OK, 1 row affected (0.15 sec)
Records: 1  Duplicates: 0  Warnings: 0

MariaDB [test]> INSERT INTO t1(i1, v1) SELECT NULL, a.v1 FROM t1 a, t1 b, t1 c;
Query OK, 8 rows affected (0.13 sec)
Records: 8  Duplicates: 0  Warnings: 0

MariaDB [test]> INSERT INTO t1(i1, v1) SELECT NULL, a.v1 FROM t1 a, t1 b, t1 c;
Query OK, 1000 rows affected (0.35 sec)
Records: 1000  Duplicates: 0  Warnings: 0

MariaDB [test]> INSERT INTO t1(i1, v1) SELECT NULL, a.v1 FROM t1 a, t1 b, t1 c;
```

+ Options

	i1	v1
Edit Copy Delete	1	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	2	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	3	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	4	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	5	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	6	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	7	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	8	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	9	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...
Edit Copy Delete	10	abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde...

Query OK, 8 rows affected (0.13 sec)

Brute-Force Login

```
msf > use auxiliary/scanner/mysql/mysql_login
msf > use auxiliary/admin/mysql/mysql_enum
mysqldump --single-transaction --host=192.168.24.2 -u test -p dvwa > dvwa.s
```

```
msf auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.24.2:3306     - 192.168.24.2:3306 - Success: 'test:test'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf auxiliary(admin/mysql/mysql_enum) > exploit

[*] 192.168.24.2:3306 - Running MySQL Enumerator...
[*] 192.168.24.2:3306 - Enumerating Parameters
[*] 192.168.24.2:3306 -         MySQL Version: 10.1.21-MariaDB
[*] 192.168.24.2:3306 -         Compiled for the following OS: Win32
[*] 192.168.24.2:3306 -         Architecture: 32
[*] 192.168.24.2:3306 -         Server Hostname: ADMINRG-5ADM31U
[*] 192.168.24.2:3306 -         Data Directory: C:\xampp\mysql\data\
[*] 192.168.24.2:3306 -         Logging of queries and logins: ON
[*] 192.168.24.2:3306 -         Log Files Location: OFF
[*] 192.168.24.2:3306 -         Old Password Hashing Algorithm OFF
[*] 192.168.24.2:3306 -         Loading of local files: OFF
[*] 192.168.24.2:3306 -         Deny logins with old Pre-4.1 Passwords: ON
[*] 192.168.24.2:3306 -         Allow Use of symlinks for Database Files: NO
[*] 192.168.24.2:3306 -         Allow Table Merge:
[*] 192.168.24.2:3306 -         SSL Connection: NO
[*] 192.168.24.2:3306 - Enumerating Accounts:
[*] 192.168.24.2:3306 -         List of Accounts with Password Hashes:
[+] 192.168.24.2:3306 -                 User: root Host: localhost Password Hash:
[+] 192.168.24.2:3306 -                 User: root Host: 127.0.0.1 Password Hash:
[+] 192.168.24.2:3306 -                 User: root Host: ::1 Password Hash:
[+] 192.168.24.2:3306 -                 User:  Host: localhost Password Hash:
[+] 192.168.24.2:3306 -                 User: pma Host: localhost Password Hash:
[+] 192.168.24.2:3306 -                 User: test Host: % Password Hash:
[+] 192.168.24.2:3306 -                 User: admin Host: % Password Hash: *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[+] 192.168.24.2:3306 -                 User: sha256user Host: localhost Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
```

```
root@kali:~# mysqldump --single-transaction --host=192.168.24.2 -u test -p dvwa  > dvwa.sql
Enter password:
root@kali:~# cat dvwa.sql
-- MySQL dump 10.16  Distrib 10.1.29-MariaDB, for debian-linux-gnu (x86_64)
--
-- Host: 192.168.24.2    Database: dvwa
-- ------------------------------------------------------
-- Server version       10.1.21-MariaDB

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `guestbook`
--

DROP TABLE IF EXISTS `guestbook`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `guestbook` (
  `comment_id` smallint(5) unsigned NOT NULL AUTO_INCREMENT,
  `comment` varchar(300) DEFAULT NULL,
  `name` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`comment_id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
```

Authentication Hardening

```
#To assign a password to a MySQL user account
SET PASSWORD FOR '<user>'@'<host>' = '<clear password>' #'
GRANT USAGE ON *.* TO '<user>'@'<host>' IDENTIFIED BY '<clear password>';#]

DELETE FROM mysql.user WHERE user=''; #Removing anonymous accounts
DROP USER '<user>'@'<host>' #removes one or more MySQL accounts and their p
```

```
SET GLOBAL default_password_lifetime=90
```

Pluggable Authentication

```
SHOW PLUGINS;
SELECT PLUGIN_NAME FROM PLUGINS WHERE PLUGIN_TYPE='AUTHENTICATION';

# Maria DB
# https://mariadb.com/kb/en/library/password-authentication-and-encryption-
```

To specify how the server should listen for TCP/IP connections

```
bind-address="127.0.0.1" #Uncomment the statement in my.ini
```

---

8. Network

CIS Assessment

```
SHOW variables WHERE variable_name = 'have_ssl';  #Ensure the Value returne
SELECT user, host, ssl_type FROM mysql.user WHERE NOT HOST IN ('::1', '127.
```

SSL System Variables

```
SHOW VARIABLES LIKE '%ssl%';
SHOW SESSION STATUS LIKE 'Ssl_version';
SHOW SESSION STATUS LIKE 'Ssl_cipher';
```

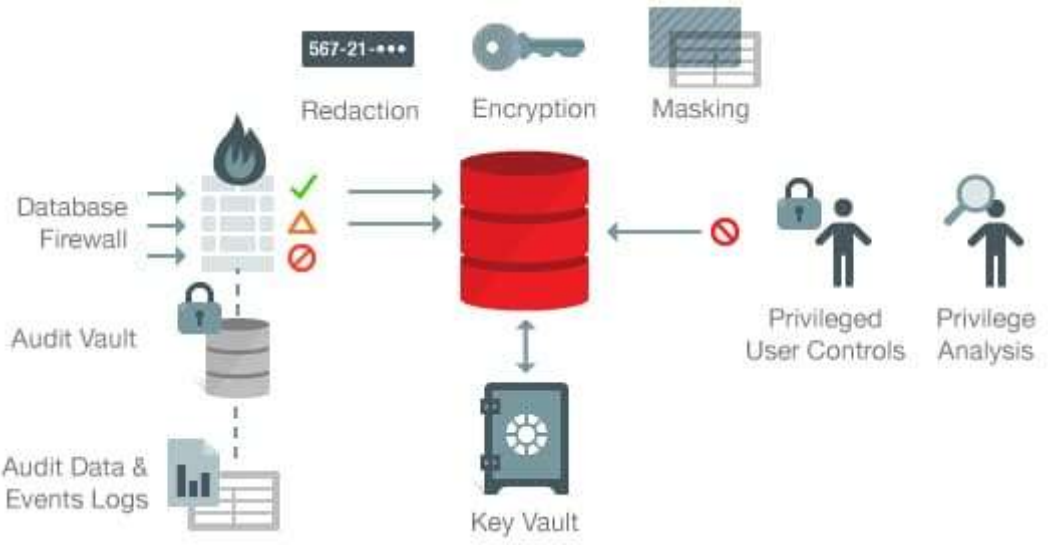
Network Hardening

```
GRANT USAGE ON *.* TO 'my_user'@'app1.example.com' REQUIRE SSL;
```

9. Replication

CIS Assessment

```
select ssl_verify_server_cert from mysql.slave_master_info; #Verify the val
SHOW GLOBAL VARIABLES LIKE 'master_info_repository'; #The result should be
select user, host from mysql.user where user='repl' and Super_priv = 'Y'; #
SELECT user, host FROM mysql.user WHERE user='repl' AND host = '%'; # Ensur
```



Security News

2018

Hacker Fail: IoT botnet command and control server accessible via default credentials

2018 National Exposure Index Research Report (Rapid 7)

2017

Ransomware attacks targeted hundreds of MySQL databases

Reference

Implementing MySQL Security Features (Ronald Bradford, Colin Charles)

Popular posts from this blog

Remote Desktop Protocol (RDP) Security

Common Remote Desktop Protocol (RDP) Vulnerabilities Terminal Services Encryption Level is Medium or Low Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness Terminal Service ...

READ MORE

Penetration Testing - Network

Manual Vulnerability Assessment TCP/21: FTP Anonymous FTP Enabled anonymous guest TCP/22: SSH nmap -p 22 --script ssh2-enum-algos <ip_address> SSH Weak Algorithms Supported SSH Server CB ...

READ MORE

Damn Vulnerable Web Services (DVWS) - Walkthrough

Installation Damn Vulnerable Web Services (DVWS) is an insecure web application with multiple vulnerable web service components that can be used to learn real world web service vulnerabilities. ...

READ MORE

Server Message Block (SMB) Security

Common SMB related vulnerabilities Microsoft Windows SMBv1 Multiple Vulnerabilities SMB Signing Disabled Microsoft Windows SMB NULL Session Authentication Microsoft Windows SMB Shares Unpri ...

READ MORE

Host Configuration Assessment - Windows

OS Information Gathering systeminfo wmic computersystem get domainrole 0 - Standalone workstation 1 - Member workstation 2 - Standalone server 3 - Member server 4 - Domain controller secedit /export /cfg cfg. ...

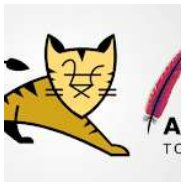
READ MORE

Offensive Security Testing Guide

This cheat sheet compiles the commands we learned to exploit vulnerable machines. However, these commands alone may not be sufficient to obtain your Offensive Security Certified Professional (OSCP) certification. So... ...

READ MORE

Web Server Hardening - Apache Tomcat



Reference: https://tomcat.apache.org/tomcat-8.0-doc/security-howto.html 1. Remove Extraneous Resources Removing sample resources C:\xampp\Tomcat\webapps\docs C:\xampp\Tomcat\webapp ...

READ MORE

Content Page

The Cheat Sheets offer a variety of information security cheat sheets on various security assessments and provides code to simplify testing and verification processes. Penetration Testing Network CMS - WordPress Mobile - Android Mobile - iOS Web Service (AI ...

READ MORE

Mobile Penetration Testing - Android

Testing Environment Android Emulator Geny Motion: https://www.genymotion.com/fun-zone/ Android Debug Bridge (ADB) C:\Users\<User>\AppData\Local\Android\Sdk\platform-tools ...

READ MORE

Penetration Testing with OWASP Top 10 - 2017 A7 Cross-Site Scripting (XSS)

XSS flaws ...

READ MORE

Powered by Blogger

Total Pageviews

160641

Labels