Day75 应急响应-数据库&漏洞口令检索&应急取证箱

75.1 知识点

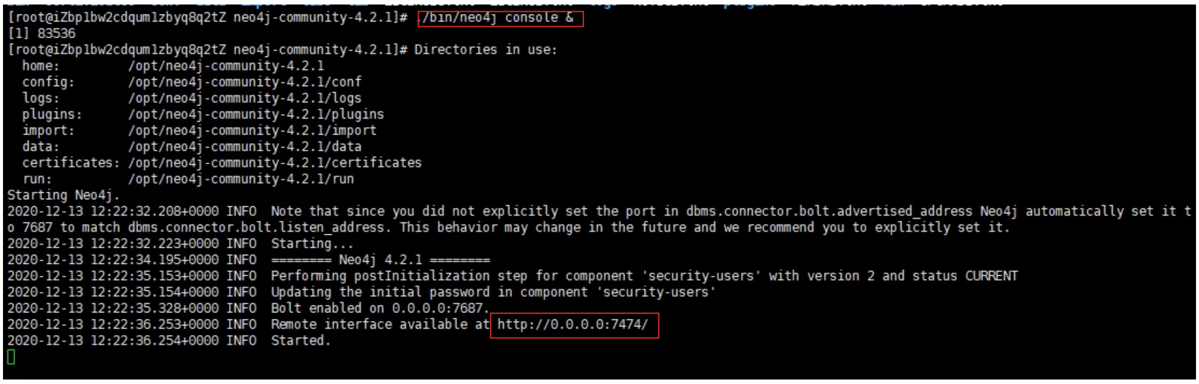
1.第三方应用由于是选择性安装，如何做好信息收集和漏洞探针也是获取攻击者思路的重要操作，除去本身漏洞外，提前预知或口令相关攻击也要进行筛选。
2.排除三方应用攻击行为，自查漏洞分析攻击者思路，人工配合工具脚本
3.由于工具或脚本更新迭代快，分类复杂，打造自己的工具箱迫在眉睫

75.2 案例 1-Win 日志自动神器 LogonTracer-外网内网

```
如何安装使用：https://github.com/JPCERTCC/LogonTracer/wiki/

linux 安装使用笔记：阿里云主机记得开放端口及关闭防火墙

1.下载并解压 neo4j：tar -zvxf neo4j-community-4.2.1-unix.tar

2.安装 java11 环境：sudo yum install java-11-openjdk -y

3.修改 neo4j 配置保证外部访问：
dbms.connector.bolt.listen_address=0.0.0.0:7687
dbms.connector.http.listen_address=0.0.0.0:7474
```

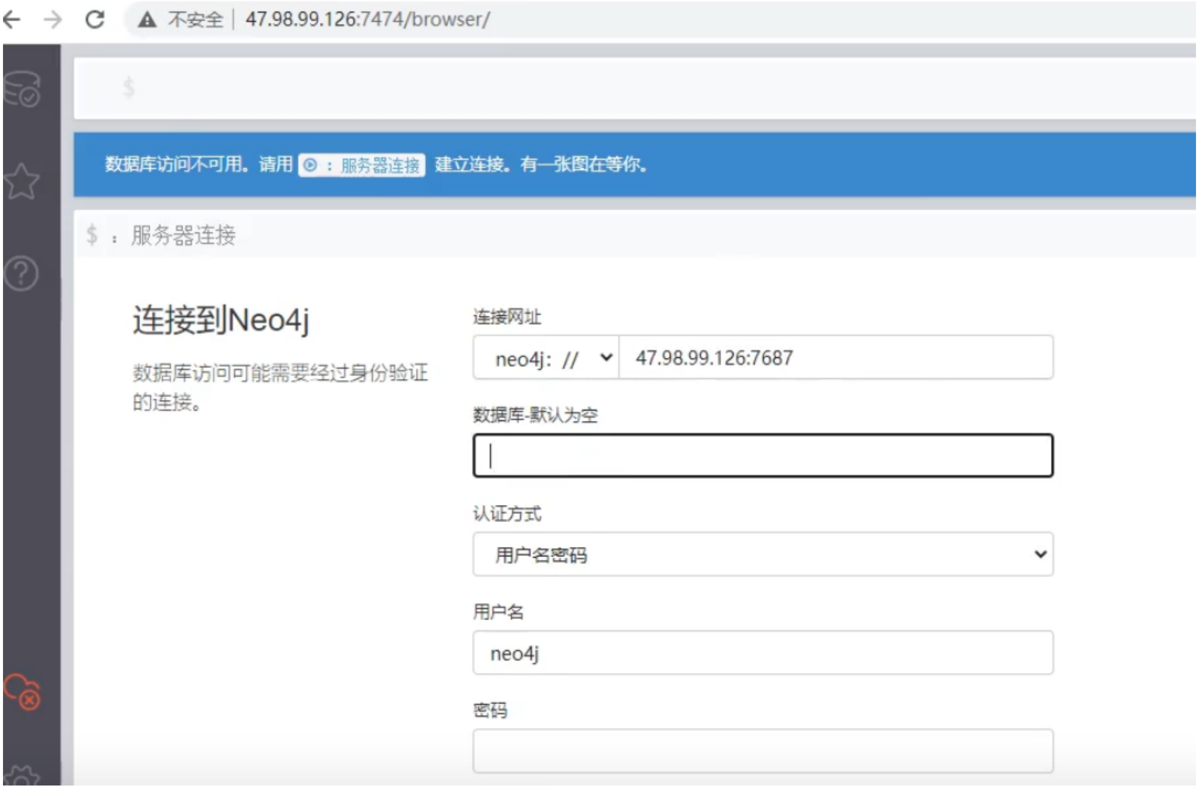
```

./bin/neo4j console &

4.下载 LogonTracer 并安装库：
git clone
https://github.com/JPCERTCC/LogonTracer.git
pip3 install -r requirements.txt

5.启动 LogonTracer 并导入日志文件分析
python3 logontracer.py -r -o [PORT] -u
[USERNAME] -p [PASSWORD] -s [IP 地址]
python3 logontracer.py -r -o 8080 -u neo4j -p
xiaodi -s 47.98.99.126
python3 logontracer.py -e [EVTX 文件] -z [时区] -u
[用户名] -p [密码] -s [IP 地址]
python3 logontracer.py -e Security.evtx -z -13 -
u neo4j -p xiaodi -s 127.0.0.1

6.刷新访问 LogonTracer-web_gui 查看分析结果
```

配置完neo4j后，启动即可



```
[root@iZbp1bw2cdquml zbyq8q2tZ neo4j-community-4.2.1]# ./bin/neo4j console &
[1] 83536
[root@iZbp1bw2cdquml zbyq8q2tZ neo4j-community-4.2.1]# Directories in use:
  home:         /opt/neo4j-community-4.2.1
  config:       /opt/neo4j-community-4.2.1/conf
  logs:         /opt/neo4j-community-4.2.1/logs
  plugins:      /opt/neo4j-community-4.2.1/plugins
  import:       /opt/neo4j-community-4.2.1/import
  data:         /opt/neo4j-community-4.2.1/data
  certificates: /opt/neo4j-community-4.2.1/certificates
  run:          /opt/neo4j-community-4.2.1/run
Starting Neo4j.
2020-12-13 12:22:32.208+0000 INFO  Note that since you did not explicitly set the port in dbms.connector.bolt.advertised_address Neo4j automatically set it t
o 7687 to match dbms.connector.bolt.listen_address. This behavior may change in the future and we recommend you to explicitly set it.
2020-12-13 12:22:32.223+0000 INFO  Starting...
2020-12-13 12:22:34.195+0000 INFO  ======== Neo4j 4.2.1 ========
2020-12-13 12:22:35.153+0000 INFO  Performing postInitialization step for component 'security-users' with version 2 and status CURRENT
2020-12-13 12:22:35.154+0000 INFO  Updating the initial password in component 'security-users'
2020-12-13 12:22:35.328+0000 INFO  Bolt enabled on 0.0.0.0:7687.
2020-12-13 12:22:36.253+0000 INFO  Remote interface available at http://0.0.0.0:7474/
2020-12-13 12:22:36.254+0000 INFO  Started.
```

启动后访问服务器7474端口即可，默认用户名密码是neo4j



不安全 | 47.98.99.126:7474/browser/

$

数据库访问不可用。请用 :服务器连接 建立连接。有一张图在等你。

$: 服务器连接

连接到Neo4j

数据库访问可能需要经过身份验证的连接。

连接网址: neo4j:// 47.98.99.126:7687

数据库-默认为空:

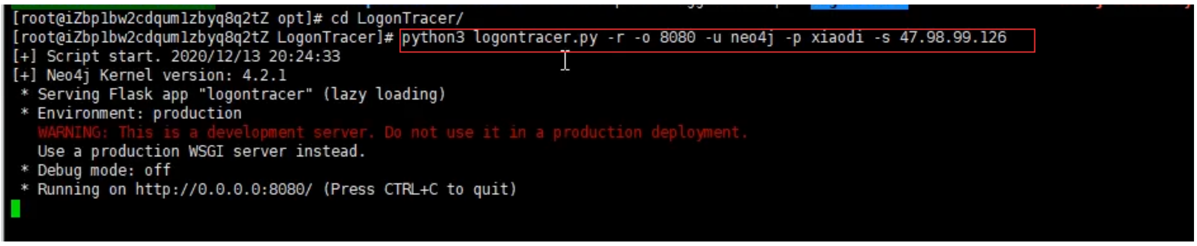
认证方式: 用户名密码

用户名: neo4j

密码:

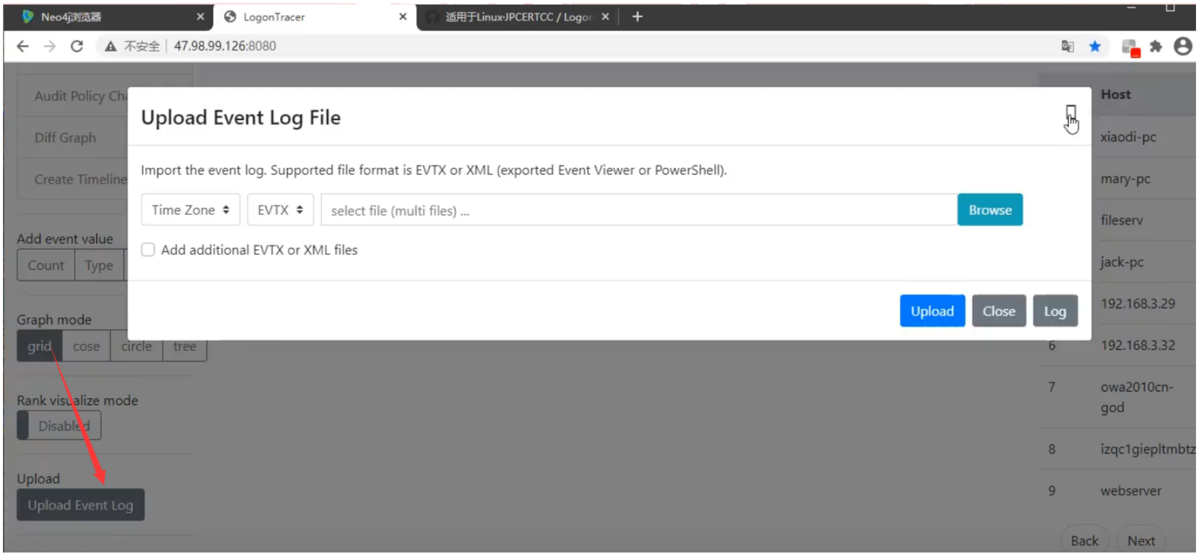
再在服务器上下载LogonTracer并安装

切换到LogonTracer的目录，通过python3启动LogonTracer



```
[root@iZbp1bw2cdqum1zbyq8q2tZ opt]# cd LogonTracer/
[root@iZbp1bw2cdqum1zbyq8q2tZ LogonTracer]# python3 logontracer.py -r -o 8080 -u neo4j -p xiaodi -s 47.98.99.126
[+] Script start. 2020/12/13 20:24:33
[+] Neo4j Kernel version: 4.2.1
 * Serving Flask app "logontracer" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)
```

启动后访问服务器的8080端口
可以在图形化界面将日志上传进行分析



不安全 | 47.98.99.126:8080

Upload Event Log File

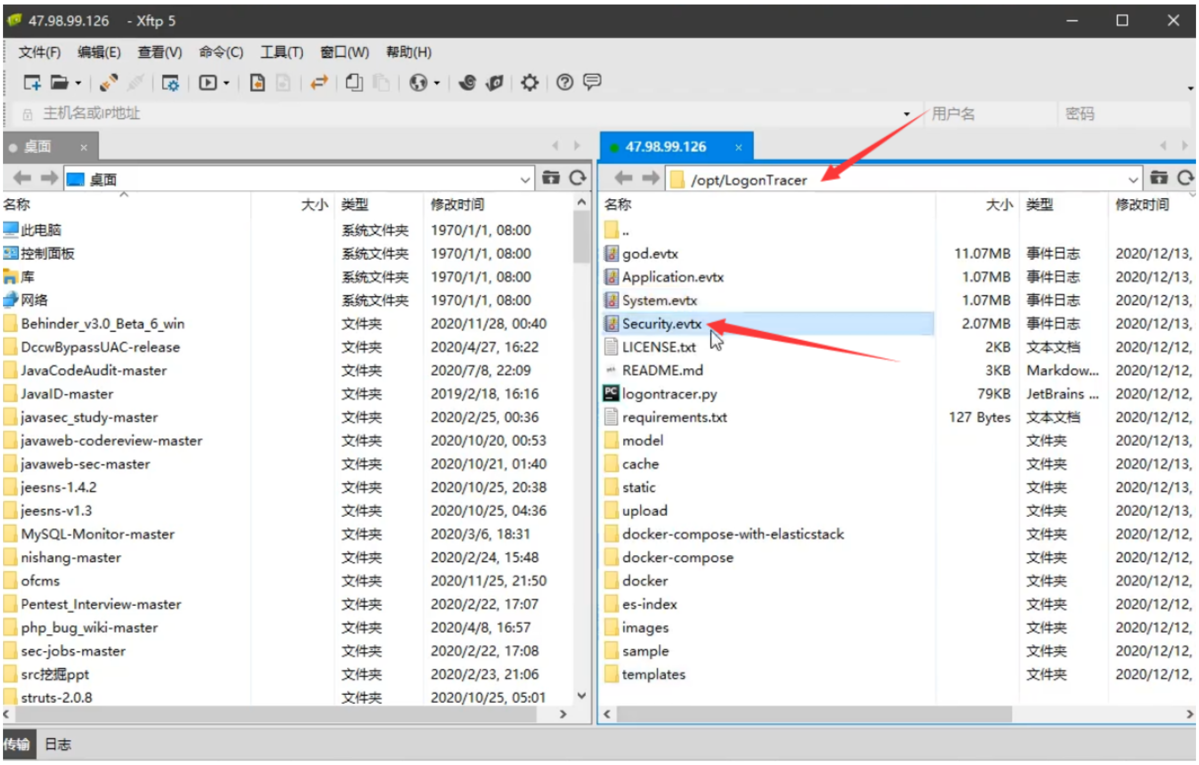
Import the event log. Supported file format is EVTX or XML (exported Event Viewer or PowerShell).

Time Zone | EVTX | select file (multi files) ... | Browse

□ Add additional EVTX or XML files

也可以通过命令行上传日志文件进行分析

将日志文件上传到服务器的LogonTracer的目录



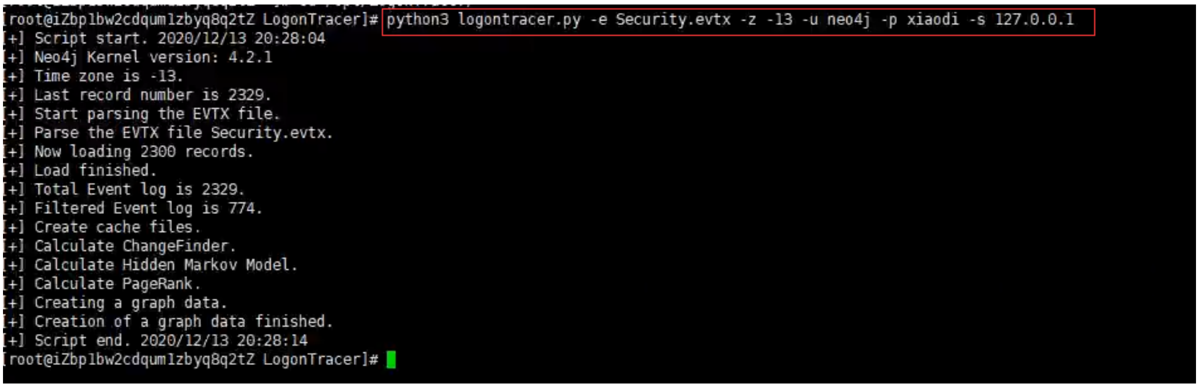
桌面

名称	大小	类型	修改时间
此电脑		系统文件夹	1970/1/1, 08:00
控制面板		系统文件夹	1970/1/1, 08:00
库		系统文件夹	1970/1/1, 08:00
网络		系统文件夹	1970/1/1, 08:00
Behinder_v3.0_Beta_6_win		文件夹	2020/11/28, 00:40
DccwBypassUAC-release		文件夹	2020/4/27, 16:22
JavaCodeAudit-master		文件夹	2020/7/8, 22:09
JavaID-master		文件夹	2019/2/18, 16:16
javasec_study-master		文件夹	2020/2/25, 00:36
javaweb-codereview-master		文件夹	2020/10/20, 00:53
javaweb-sec-master		文件夹	2020/10/21, 01:40
jeesns-1.4.2		文件夹	2020/10/25, 20:38
jeesns-v1.3		文件夹	2020/10/25, 04:36
MySQL-Monitor-master		文件夹	2020/3/6, 18:31
nishang-master		文件夹	2020/2/24, 15:48
ofcms		文件夹	2020/11/25, 21:50
Pentest_Interview-master		文件夹	2020/2/22, 17:07
php_bug_wiki-master		文件夹	2020/4/8, 16:57
sec-jobs-master		文件夹	2020/2/22, 17:08
src挖掘ppt		文件夹	2020/2/23, 21:06
struts-2.0.8		文件夹	2020/10/25, 05:01

/opt/LogonTracer

名称	大小	类型	修改时间
..			
god.evtx	11.07MB	事件日志	2020/12/13,
Application.evtx	1.07MB	事件日志	2020/12/13,
System.evtx	1.07MB	事件日志	2020/12/13,
Security.evtx	2.07MB	事件日志	2020/12/13,
LICENSE.txt	2KB	文本文档	2020/12/12,
README.md	3KB	Markdow...	2020/12/12,
logontracer.py	79KB	JetBrains ...	2020/12/12,
requirements.txt	127 Bytes	文本文档	2020/12/12,
model		文件夹	2020/12/13,
cache		文件夹	2020/12/13,
static		文件夹	2020/12/13,
upload		文件夹	2020/12/13,
docker-compose-with-elasticstack		文件夹	2020/12/12,
docker-compose		文件夹	2020/12/12,
docker		文件夹	2020/12/12,
es-index		文件夹	2020/12/12,
images		文件夹	2020/12/12,
sample		文件夹	2020/12/12,
templates		文件夹	2020/12/12,

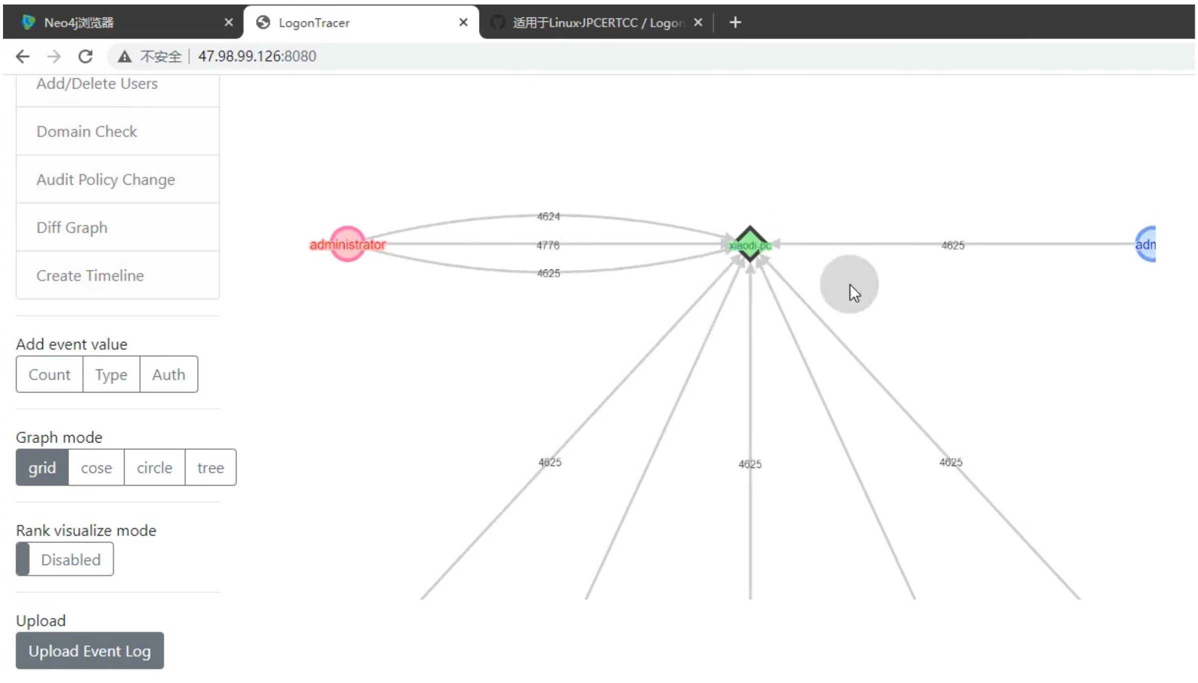
通过python3运行脚本，将日志导入进行分析



```
[root@iZbp1bw2cdqum1zbyq8q2tZ LogonTracer]# python3 logontracer.py -e Security.evtx -z -13 -u neo4j -p xiaodi -s 127.0.0.1
[+] Script start. 2020/12/13 20:28:04
[+] Neo4j Kernel version: 4.2.1
[+] Time zone is -13.
[+] Last record number is 2329.
[+] Start parsing the EVTX file.
[+] Parse the EVTX file Security.evtx.
[+] Now loading 2300 records.
[+] Load finished.
[+] Total Event log is 2329.
[+] Filtered Event log is 774.
[+] Create cache files.
[+] Calculate ChangeFinder.
[+] Calculate Hidden Markov Model.
[+] Calculate PageRank.
[+] Creating a graph data.
[+] Creation of a graph data finished.
[+] Script end. 2020/12/13 20:28:14
[root@iZbp1bw2cdqum1zbyq8q2tZ LogonTracer]#
```

执行后访问服务器的8080端口

LogonTracer会将日志进行分析并以导图的形式展现出来

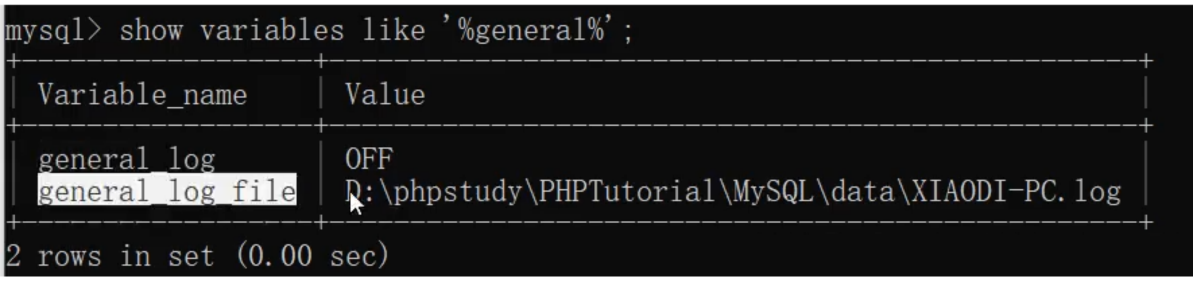


75.3 案例 2-数据库 Mysql&Mssql&Oracle 等日志分析-爆破注入操作

常见的数据库攻击包括弱口令、SQL 注入、提升权限、窃取备份等。对数据库日志进行分析，可以发现攻击行为，进一步还原攻击场景及追溯攻击源。

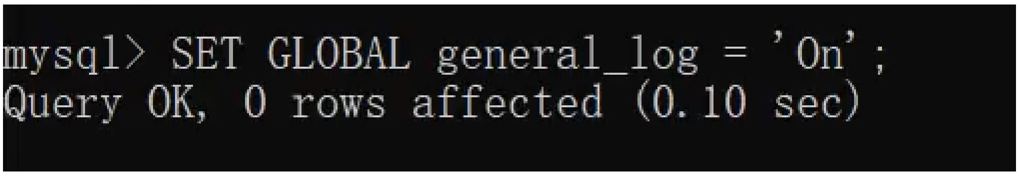
```
Mysql：启用，记录，分析（分析 SQL 注入及口令登录爆破等）
show variables like '%general%';
SET GLOBAL general_log = 'On';
SET GLOBAL general_log_file =
'/var/lib/mysql/mysql.log';
```

`show variables like ’%general%’;`查看数据库状态，数据库配置文件路径



```
mysql> show variables like ’%general%’;
+------------------+----------------------------------------------+
| Variable_name    | Value                                        |
+------------------+----------------------------------------------+
| general_log      | OFF                                          |
| general_log_file | D:\phpstudy\PHPTutorial\MySQL\data\XIAODI-PC.log |
+------------------+----------------------------------------------+
2 rows in set (0.00 sec)
```

`GLOBAL general_log = 'On';`开启数据日志



```
mysql> SET GLOBAL general_log = 'On';
Query OK, 0 rows affected (0.10 sec)
```

```
Mssql：查看，跟踪，分析（配置跟踪可分析操作，查看日志可分析登录等）
```

75.4 案例 3-自查漏洞模拟渗透测试寻找攻击源头-漏洞口令检索

```
1.日志被删除或没价值信息
2.没有思路进行分析可以采用模拟渗透
1.windows，linux 系统漏洞自查:
WindowsVulnScan,linux-exploit-suggester
D:\Myproject\venv\Scripts\python.exe cve-check.py -C -f KB.json
./linux-exploit-suggester.sh
2.windows，linux 服务漏洞自查:
windows：Get-WmiObject -class Win32_Product
linux：LinEnum.sh
searchsploit weblogic
利用前期信息收集配合 searchsploit 进行应用服务协议等漏洞检索
3.windows，linux 协议弱口令自查-工具探针或人工获取判断-snetcraker
```

75.5 案例 4-自动化 ir-rescue 应急响应工具箱-实时为您提供服务

```
https://github.com/diogo-fernan/ir-rescue
分析脚本工具原理，尝试自己进行编写修改，成为自己的工具箱杀器
```

资源：

```
https://github.com/rebootuser/LinEnum
https://github.com/diogo-fernan/ir-rescue
https://github.com/offensive-security/exploitdb
https://github.com/chroblert/WindowsVulnScan
https://github.com/JPCERTCC/LogonTracer.git
https://github.com/mzet-/linux-exploit-suggester
https://pan.baidu.com/s/1tQS1mUelmEh3I68AL7yXGg 提取码：xiao
```