



-

&

&



#

1.

2.

3.



-Win

LogonTracer-

- Mysql&Mssql&Oracle -

- -

- ir-rescue -

1-Win LogonTracer-
<https://github.com/JPCERTCC/LogonTracer/wiki/>

linux

1. neo4j tar -zxvf neo4j-community-4.2.1-unix.tar

2. java11 sudo yum install java-11-openjdk -y

3. neo4j

dbms.connector.bolt.listen_address=0.0.0.0:7687

dbms.connector.http.listen_address=0.0.0.0:7474

./bin/neo4j console &

4. LogonTracer

git clone <https://github.com/JPCERTCC/LogonTracer.git>

pip3 install -r requirements.txt

5. LogonTracer

python3 logontracer.py -r -o [PORT] -u [USERNAME] -p [PASSWORD] -s [IP]

python3 logontracer.py -r -o 8080 -u neo4j -p xiaodi -s 47.98.99.126

python3 logontracer.py -e [EVTX] -z [] -u [] -p [] -s [IP]

python3 logontracer.py -e Security.evtx -z -13 -u neo4j -p xiaodi -s 127.0.0.1

6. LogonTracer-web_gui

2- Mysql&Mssql&Oracle -
SQL

Mysql SQL

show variables like '%general%';

SET GLOBAL general_log = 'On';

SET GLOBAL general_log_file = '/var/lib/mysql/mysql.log';

Mssql

3- -

1.

2.

1.windows linux :

WindowsVulnScan,linux-exploit-suggester

D:\Myproject\venv\Scripts\python.exe cve-check.py -C -f KB.json

./linux-exploit-suggester.sh

2.windows linux :

windows Get-WmiObject -class Win32_Product

linux LinEnum.sh

searchsploit weblogic

searchsploit

3.windows linux - -snetcraker

4- ir-rescue -

<https://github.com/diogo-fernan/ir-rescue>



<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/1tQS1mUelmEh3l68AL7yXGg> xiao
