

作为技术宅的我，日常最大的爱好就是逛论坛。某日看到论坛里有一款基于主机的漏洞扫描工具，用来查找主机上公开EXP的CVE。嗯嗯，我想还是叫提权辅助工具可能会更顺口一些。在我印象中，类似的工具其实还蛮多的，比如我们熟知的Linux\_Exploit\_Suggester和Windows-Exploit-Suggester。

我花了一点时间，整理了 9 款提权辅助工具，不敢独享，特整理成文。如果你对提权有那么点想法，我相信这些工具是可以帮助到你的。

---

## 1、Linux提权辅助工具

Linux\_Exploit\_Suggester是一款根据操作系统版本号自动查找相应提权脚本的工具，如果不带任何参数运行该脚本的话，将执行uname -r返回的操作系统发行版本，或者手工输入-k参数查找指定版本号。

github项目地址：[https://github.com/InteliSecureLabs/Linux\\_Exploit\\_Suggester](https://github.com/InteliSecureLabs/Linux_Exploit_Suggester)

用法示例：

```
$ perl ./Linux_Exploit_Suggester.pl -k 2.6.28
```

## 2、Windows-Exploit-Suggester

Windows-Exploit-Suggester是受Linux\_Exploit\_Suggester的启发而开发的一款提权辅助工具，用python开发而成，通过比对systeminfo生成的文件，从而发现系统是否存在未修复漏洞。

github项目地址：<https://github.com/AonCyberLabs/Windows-Exploit-Suggester>

用法示例：

```
#查看系统可能存在的漏洞
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --systeminfo win7sp1-systeminfo.txt

$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --ostext 'windows server 2008 r2'
```

## 3、gtfo

gtfo是一个纯粹用python3编写的工具，用于搜索GTFOBins和LOLBAS上的二进制文件。

github项目地址：

```
https://github.com/mzfr/gtfo
```

很明显，从以上描述里，我们知道这款工具并不是主角，需要重点关注的是GTFOBins和LOLBAS。

GTFOBins：Linux命令提权辅助查询

```
https://gtfobins.github.io/
```

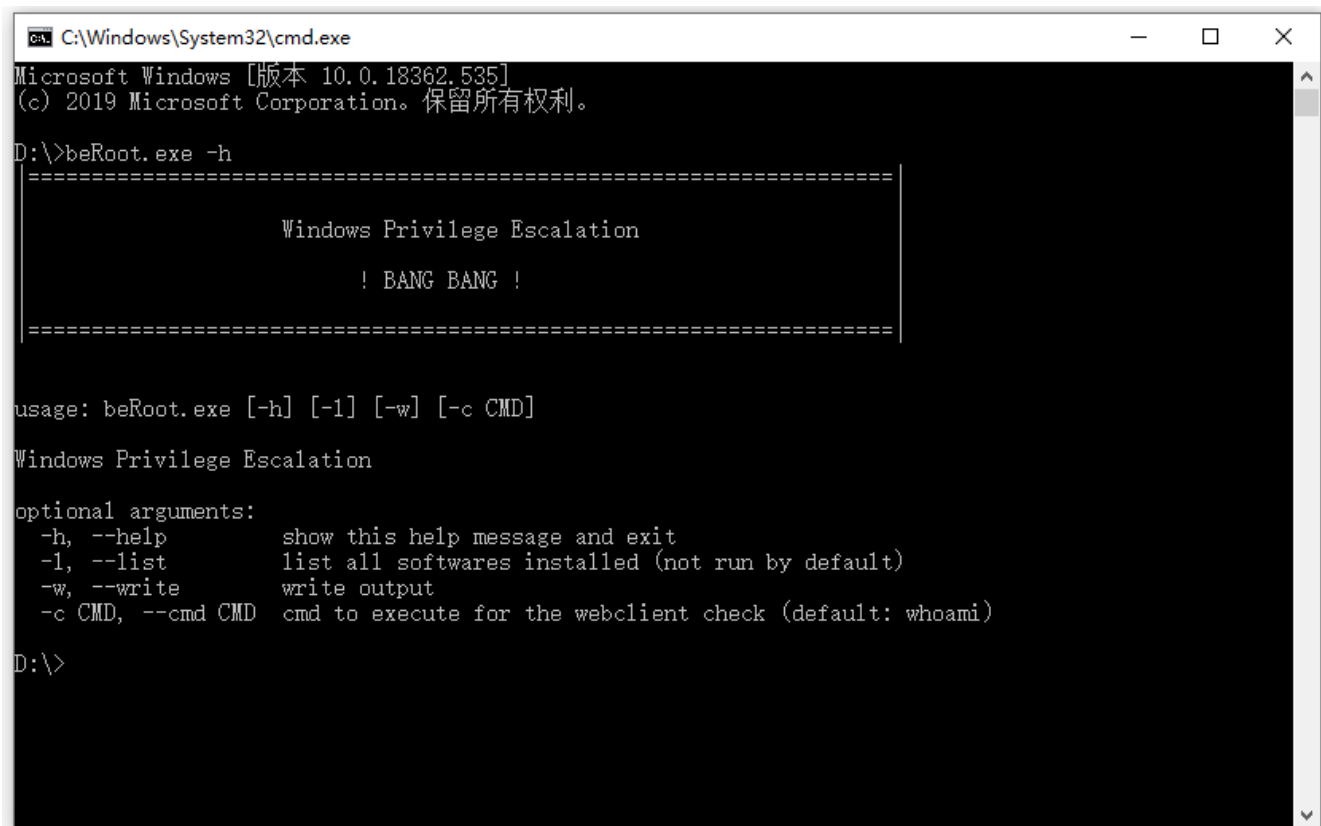
LOLBAS : Windows命令提权辅助查询

<https://lolbas-project.github.io/>

#### 4、BeRoot

BeRoot Project是一个利用后的工具，可以检查常见的错误配置，以找到提升我们特权的方法，该项目可在Windows，Linux和Mac OS上运行。

github项目地址：<https://github.com/AlessandroZ/BeRoot>



```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.535]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\>beRoot.exe -h
=====
                        Windows Privilege Escalation
                        ! BANG BANG !
=====

usage: beRoot.exe [-h] [-l] [-w] [-c CMD]

Windows Privilege Escalation

optional arguments:
  -h, --help            show this help message and exit
  -l, --list            list all softwares installed (not run by default)
  -w, --write          write output
  -c CMD, --cmd CMD    cmd to execute for the webclient check (default: whoami)

D:\>
```

#### 5、Vulmap

Vulmap是一个开源的在线本地漏洞扫描程序项目。它由适用于Windows和Linux操作系统的联机本地漏洞扫描程序组成。

Github项目地址：<https://github.com/vulmon/Vulmap>

```

>_|||||_<
VULMAP
=====
Vulmon Mapper v1.0
www.vulmon.com
=====

[*] Distro Information
[>] DISTRO ID: kali VERSION: 2017.1

[*] Kernel Information
[>] SYSTEM: Linux VERSION: 4.9.0-kali3-amd64 ARCHITECTURE: x86_64

[Info] Default mode. Check vulnerabilities of installed packages...
[*] Vulnerability Found!
[>] Product: bash 4.4.4+b1
[+] CVEID: CVE-2016-9401      Score: 2.1      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2016-9401

[*] Vulnerability Found!
[>] Product: binutils 2.28-3
[+] CVEID: CVE-2005-4808      Score: 7.6      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2005-4808
[+] CVEID: CVE-2005-4807      Score: 7.5      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2005-4807
[+] Available Exploits!!!
[!] Exploit ID: EDB28397 URL: http://vulmon.com/exploitdetails?qid=EDB28397 (GNU BinUtils 2.1x GAS Buffer Overflow Vulnerability)
[+] CVEID: CVE-2006-2362      Score: 7.5      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2006-2362
[+] Available Exploits!!!
[!] Exploit ID: EDB27856 URL: http://vulmon.com/exploitdetails?qid=EDB27856 (GNU BinUtils 2.1x Buffer Overflow Vulnerability)

[*] Vulnerability Found!
[>] Product: busybox 1:1.22.0-19+b2
[+] CVEID: CVE-2017-15873      Score: 4.3      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2017-15873
[+] CVEID: CVE-2006-5050      Score: 5        URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2006-5050
[+] CVEID: CVE-2016-6301      Score: 7.8      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2016-6301
[+] CVEID: CVE-2006-1058      Score: 2.1      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2006-1058
[+] CVEID: CVE-2014-9645      Score: 2.1      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2014-9645
[+] CVEID: CVE-2017-15874      Score: 4.3      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2017-15874
[+] CVEID: CVE-2016-2148      Score: 7.5      URL: http://vulmon.com/vulnerabilitydetails?qid=CVE-2016-2148

```

## 6、WindowsVulnScan

这是一款基于主机的漏洞扫描工具，查看查找主机上具有的CVE和具有公开EXP的CVE。

github项目地址：<https://github.com/chroblert/WindowsVulnScan>

```

PS G:\JC_Tools\01 项目\03 主机漏洞扫描> & D:/Python36/python.exe "G:\JC_Tools\01 项目\03 主机漏洞扫描\cve-check.py" -C -f KB.json

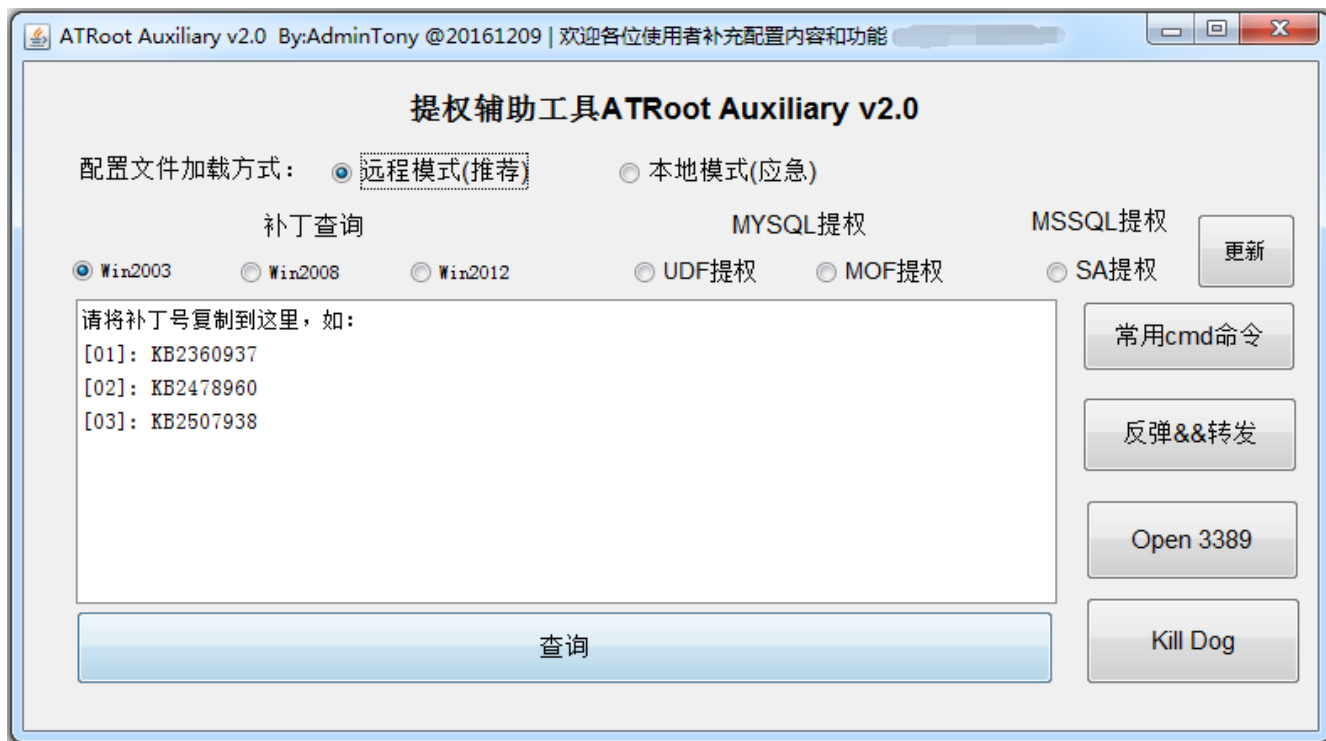
=====CVE-EXP-Check=====
| author:JC0o0l |
| wechat:JC_SecNotes |
| version:1.0 |
=====

系统信息如下:
Windows 10 1909
KB信息如下:
['4534132', '4516115', '4517245', '4521863', '4524569', '4528759', '4537759', '4538674', '4532693']
EXP信息如下:
CVE-2019-1476 has EXP
CVE-2020-0686 has EXP

```

## 7、ATRoot Auxiliary v2.0

基于java开发的提权辅助工具，支持双端加载，本地模式配置文件存放于本地软件目录下的conf目录；远程模式则可以更新配置文件。



## 8、在线提权漏洞检测平台

一款为主流 Linux/Unix 和 Windows 系统提供精准且高效的操作系统脆弱性漏洞检测的专业化平台，基于其强大的安全检测能力，能够给出专业的修复建议，有效验证和加固网络资产漏洞。

在线查询地址：

<https://detect.secwx.com/>



## 9、提权辅助网页

在Windows提权的时候，对比补丁找Exp很烦吧？老是忘记一些提权命令跟工具的语法很苦逼吧？没事，有了这款工具什么问题都解决~

在线查询地址：<http://bugs.hacking8.com/tiquan/>

Windows Exp   CMD探查   端口转发   Kill Dog   打开3389   SQL提权 ▼

补丁号

▼ 查询

Question

在Windows提权的时候，对比补丁找Exp很烦吧？老是忘记一些提权命令跟工具的语法很苦逼吧？没事，有了这款工具什么问题都解决~

本网站数据源每周更新一次，最近更新：20-03-19 05:15:01  
网站作者:小草 && 数据源提供 @SecWiki

Use

请将补丁号或 `systeminfo` 信息复制到文本栏，如：

[01]: KB2360937  
[02]: KB2478960  
[03]: KB2507938

## 10、PEASS-特权升级脚本

在这里，可以找到适用于Windows和Linux / Unix \*的特权升级工具。

github项目地址：<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>

检测清单：<https://book.hacktricks.xyz/>

---

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

