# git资源兵器库

## Nmap脚本库

<https://github.com/christophetd/nmap-nse-info>

搜索nmap脚本的小工具

<https://github.com/scipag/vulscan>

nmap漏洞扫描脚本

<https://github.com/z0x010/icse-nse>

工控nse脚本合集

<https://github.com/jpalanco/nmap-scada>

nmap的scada脚本合集5个

<https://github.com/peter-hackertarget/nmap-nse-scripts>

nmap的WP扫描脚本

<https://github.com/cldrn/nmap-nse-scripts>

nmap搜集合集之一，挺多的

<https://github.com/nosteve/vnc-auth>

vnc扫描

<https://github.com/k0keoyo/schneider-nse>

施耐德设备发现

<https://github.com/tchoutri/nse-csv-script>

nmap输出CSV格式

<https://github.com/vulnersCom/nmap-vulners>

nmap的vulners的漏洞库

<https://github.com/vicendominguez/http-open-proxy-anon>

查找匿名代理

## Windows提权库

<https://github.com/GDSSecurity/Windows-Exploit-Suggester>

识别Windows补丁版本，对比官方漏洞库发现漏洞，Python

<https://github.com/abatchy17/WindowsExploits>

Windows平台的exploits合集，ms-03-026到ms-17-010（没有标注提权），基于Python

<https://github.com/SecWiki/windows-kernel-exploits>

Windows内核exploit提权漏洞合集

<https://github.com/WindowsExploits/Exploits>

windows的powershell版的exploit

<https://github.com/nixawk/labs>

Vulnerability Labs for security analysis

<https://github.com/XiphosResearch/exploits>

Miscellaneous exploit code

<https://github.com/enddo/awesome-windows-exploitation>

awesome Windows Exploitation resources

## Linux提权库

<https://github.com/PenturaLabs/Linux_Exploit_Suggester>

识别Linux版本号，发现可能存在的操作系统漏洞，Perl

<https://github.com/mzet-/linux-exploit-suggester>

识别Linux版本号，发现可能存在的操作系统漏洞，shell版

<https://github.com/SecWiki/macos-kernel-exploits>

MacOS提权漏洞利用

<https://github.com/nilotpalbiswas/Auto-Root-Exploit>

自动root工具

<https://github.com/0xdea/exploits>

Linux、MySQL、solaris、oracle、misc漏洞利用合集

<https://github.com/SecWiki/linux-kernel-exploits>

Linux内核exploit提权漏洞合集

<https://github.com/Billy-Ellis/Exploit-Challenges>

ARM平台的漏洞利用脚本合集，13个

<https://github.com/xairy/linux-kernel-exploitation>

Linux提权技术文章合集

## Pwn库

<https://github.com/Gallopsled/pwntools>

pwntools是CTFpwn框架和exploit开发库

<https://github.com/jmpews/pwn2exploit>

PWN技术学习基本入门资料

<https://github.com/jmpews/pwn2exploit>

pwn学习

<https://github.com/BuddhaLabs/PacketStorm-Exploits>

packetstorm平台的漏洞利用库

## web渗透库

<https://github.com/rastating/wordpress-exploit-framework>

wordpress渗透框架

<https://github.com/3xp10it/exploit>

类似msf的Web集成平台，cdn真实ip查找模块，旁站获取，子站获取，CMS识别……

<https://github.com/infodox/exploits>

常用的漏洞小工具如nodejsshell/phpcgi基于Python

<https://github.com/XiphosResearch/exploits>

web杂项合集，各种exploit，大约30个

<https://github.com/xl7dev/Exploit>

MySQL、Nginx、wget、Tomcat、WP等常见服务器shell版exploit

<https://github.com/joaomatosf/jexboss>

Jboss漏洞利用

<https://github.com/mattiasgeniar/php-exploit-scripts>

针对国外的CMS的漏洞利用脚本

<https://github.com/nettitude/xss_payloads>

XSS功能脚本工具，利用xss漏洞插入各种功能代码

<https://github.com/PolarisLab/Drupal-Exploit>

drupal7的service模块远程代码执行

## 渗透工具库

<https://github.com/reverse-shell/routersploit>

路由器渗透框架

<https://github.com/PowerShellMafia/PowerSploit>

powersploit

<https://github.com/offensive-security/exploit-database>

exploit-db的shellcode和exploits集合

<https://github.com/rfunix/Pompem>

exploit搜索脚本

<https://github.com/kylekirkby/Python-Exploit-Search-Tool>

基于shodan和exploit-db的搜索工具

<https://github.com/nixawk/labs>

Vulnerability Labs for security analysis CVE-2015-5531---CVE-2017-9791

<https://github.com/enddo/awesome-windows-exploitation>

awesome-windows-exploitation

<https://github.com/SecWiki/office-exploits>

office漏洞利用

<https://github.com/mubix/post-exploitation>

Windows后渗透工具

<https://github.com/EmpireProject/Empire>

基于powershell和Python的后渗透工具

<https://github.com/SecWiki/VulScritp>

内网渗透小工具

<https://github.com/nowsecure/dirtycow>

脏牛漏洞

<https://github.com/CaledoniaProject/jenkins-cli-exploit>

jenkins命令执行

<https://github.com/m4n3dw0lf/pythem>

神似msf的Python版

<https://github.com/dc414/Upnp-Exploiter>

Upnp路由器渗透工具

<https://github.com/torque59/Nosql-Exploitation-Framework>

nosql渗透框架

## 学习知识库

<https://github.com/firmianay/CTF-All-In-One>

<https://github.com/vitalysim/Awesome-Hacking-Resources>

Awesome 黑客和渗透测试资源

<https://github.com/1u4nx/Exploit-Exercises-Nebula>

Linux平台漏洞分析入门全攻略

<https://github.com/hardenedlinux/linux-exploit-development-tutorial>

Linux的exploit开发入门

<https://github.com/clymb3r/KdExploitMe>

内核驱动exploit编写练习

<https://github.com/RKX1209/kernel_exploit_world>

内核exploit编写教程

<https://github.com/RPISEC/MBE>

好像是一个2.2K个星的二进制课程平台，具体是啥我也不知道

## 工控库

## 其他

<https://github.com/SecWiki/svn_git_scanner>

全网扫描git和SVN信息泄露

<https://github.com/longld/peda>

Python的exploit开发助手神器基于GDB

<https://github.com/hugsy/gef>

GDB提升插件，很强大

<https://github.com/mgeeky/expdevBadChars>

exp相关的badchar工具

<https://github.com/ratty3697/HackSpy-Trojan-Exploit>

win木马免杀神器