# LINUX 資訊安全檢測與漏洞分析

## LINUX INFORMATION SECURITY AUDITING AND EXPLOITATION ANALYSIS

AUTHOR：張呈顥
ADVISOR：盧東華助理教授

## 研究動機

- 伺服器長久失修
- 多項資安項目缺失
- 存有不少 CVE 漏洞
- 伺服器提供服務眾多
- 資安威脅只會增加不會減少

## 研究目的

資安健全 | 安全意識 | 資安普及

## AUDITING

Nessus | Qualys

Chkrootkit | Lynis

ClamAV | LMD

## PWNKIT CVE-2021-4034

CVSS v. 3.x: 7.8 HIGH

keyword: Local Privilege Escalation, out-of-bounds read/write, Memory corruption, SUID-root program

- PwnKit 未檢查 argument count
- argument pointer可以被越界讀寫
- 可重新引入已被清除的不安全環境變數
- 取得 root 權限

```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

## LOONEY TUNABLES CVE-2023-4911

CVSS v. 3.x: 7.8 HIGH

keyword: keywords: glibc, buffer overflow, SUID permission

- 未檢查 GLIBC_TUNABLES 格式
- tunestr 賦值時未檢查邊界及剩餘空間
- 執行任意code 如 root

## 研究報告詳細內容

HackMD | GitHub

## 參考連結

https://hackmd.io/@takedaTW/LinuxStudy
https://github.com/windware1203/InfoSec_study
https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
https://www.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-escalation-glibc-ld-so.txt

奈武々田