Linux 開機啟動持久化方法 & 偵測手冊

1. 概述
攻擊者在取得 Linux 系統權限後，常會利用開機啟動機制達到持久化目的。本文件整理常見的持久化方法及對應的檢測方式，方便在藍隊防禦或實驗室測試中使用。

2. systemd enable 持久化
透過建立 systemd 服務並啟用開機自啟，惡意程式會在每次系統開機時自動執行。
檢測方式：
```
# 列出所有已啟用的服務
systemctl list-unit-files --type=service --state=enabled

# 查看服務檔案內容
systemctl cat <服務名>

# 尋找非系統路徑的啟動服務
systemctl list-unit-files --type=service --state=enabled | awk '{print $1}' | xargs -I {} systemctl cat {} | grep ExecStart= | grep -vE '/(usr|bin|sbin|lib|li
```

3. cron job 持久化
透過 cron 排程在開機時或固定時間執行惡意程式，例如在 /etc/crontab 或使用者 crontab 中加入惡意命令。
檢測方式：
```
# 查看系統 crontab
cat /etc/crontab

# 查看所有使用者的 crontab
for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l 2>/dev/null; done
```

4. rc.local 持久化
部分系統仍支援 /etc/rc.local 在開機時自動執行腳本，攻擊者可在其中加入惡意命令。
檢測方式：
```
cat /etc/rc.local
```

5. Shell 啟動檔 Hook
在 ~/.bashrc、~/.bash_profile、~/.zshrc 等檔案中加入惡意命令，當使用者登入 Shell 時自動執行。
檢測方式：
```
grep -E "bash|sh|nc|curl|wget" ~/.bashrc ~/.bash_profile ~/.zshrc 2>/dev/null
```

6. 防禦建議
- 嚴格限制誰可以修改 systemd 服務檔與啟用服務 - 定期比對服務設定與基準配置 - 建立檔案完整性監控（如 AIDE、Tripwire） - 設定日誌監控 systemctl enable、crontab 修改等行為