

Lynis 系統安全稽核工具介紹

lynis 是一個 UNIX-based 系統安全稽核程式，它會執行一些常見的基本檢查項目，包含檢查系統設定與軟體安裝是否有常見的缺失，並提供適當的改善建議。目前支援 Linux、FreeBSD、OpenBSD、Mac OS X 與 Solaris 平台。

⚠ 您對 Lynis 檢查後產出的缺失報告與建議，如有明確了解且為必要需求，則可以忽略該建議。

Lynis 檢查項目大致如下：

1. 系統程式是否有被置換或竄改，避免管理者或使用者執行到惡意程式。
2. 開機程式及設定，並檢查目前已啟動的服務。
3. 系統中的帳號資訊 (使用者、群組) 及帳號驗證方式等資訊。
4. 檔案系統相關資訊，如 ACL 權限。
5. 軟體套件管理是否正常，是否存在有弱點的套件。
6. 防火牆設定是否啟用。
7. Web Server、MySQL、PHP、Postfix 設定檢查。
8. NTP 對時是否有啟動。
9. 其他。

安裝方式

- Fedora、CentOS (CentOS 由原始網站提供外部連結，下載 RPM 套件手動安裝)

```
# yum install lynis  
或  
# yum --nogpgcheck localinstall lynis-?.?.?-?.?.noarch.rpm
```

- Debian

```
# apt-get install lynis
```

- 手動安裝

```
# cd /usr/local/src  
# wget http://www.rootkit.nl/files/lynis-?.?.?.tar.gz  
# tar xvfz http://www.rootkit.nl/files/lynis-?.?.?.tar.gz  
# cd lynis-?.?.?  
# sh ./lynis
```

更新資料庫

在使用 Lynis 進行檢查前，不妨先更新資料庫以便獲得較新版本的資訊。

```
# lynis --check--update
```

```
== Lynis ==
Version      : 1.2.7
Release date : 1 November 2009

== Databases ==
-----
Current      Latest      Status
-----
Malware      : 2008062700 2008062700 Up-to-date
File perms   : 2008053000 2008053000 Up-to-date

Copyright 2007-2009 - Michael Boelen, http://www.rootkit.nl/
```

執行方式

首先，您必須獲得 **root** 權限來執行，可以使用 `--help` 了解有哪些參數可以運用：

```
# lynis --help
```

```
--check-all 檢查整個系統
--quick      快速模式，不等待使用者互動確認
--tests      僅執行特定項目的檢查
```

- 執行完整檢查，並逐項確認

```
# lynis --check-all --quick
```

- 執行完整檢查，並產出執行過程的紀錄

```
# lynis --check-all --quick --no-colors > /tmp/lynis.txt
```

- 針對特定項目進行檢查

```
# lynis --quick --tests "HOME-9302"
```

常見問題說明與改善方式

- Warning: klogd is not running, which could lead to missing kernel messages in log files
請檢查您系統上的 **W Syslog** 系統紀錄服務是否正常執行，如下：

```
# ps -ef | grep logd
```

- Warning: Couldn't find 2 responsive nameservers
您的 DNS 名稱解析至少需設定二台以上的名稱解析伺服器，以免其中一台故障時無法解析名稱。

```
# grep nameserver /etc/resolv.conf
```

- Suggestion: You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf)
您的 SMTP 服務的 banner 上透露出部份感興趣的資訊，可以修改 main.cf 檔案中 smtpd_banner 的設定。

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 XXXXXXXXXXXXXXXXXXXX ESMTP Postfix (Debian/GNU)
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

- Warning: PHP option `expose_php` is possibly turned on, which can reveal useful information for attackers.
- Suggestion: Change the `allow_url_fopen` line to: `allow_url_fopen = no`, to disable downloads via PHP

您的網頁伺服器似乎透露出您有使用 PHP，可以修改 `php.ini` 檔案中 `expose_php` 的設定來隱藏。可調整 PHP 當中 `php.ini` 檔案設定：

```
error_reporting = E_ALL & ~E_NOTICE
display_errors = Off
register_globals = Off
expose_php = Off
allow_url_fopen = Off
allow_url_include = Off
file_uploads = Off
enable_dl = Off
```

- 檢查您的 Apache 伺服器是否透露出過多的訊息供有心人士利用，可修改 `httpd.conf` 檔案中如下的設定。

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off
```

Not Found

The requested URL `/test` was not found on this server.

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3 with Suhosin-Patch Server at `deb-server` Port 80

- Suggestion: Use `mysqladmin` to set a MySQL root password (`mysqladmin -u root -p password MYPASSWORD`)
檢查您的 MySQL 中，`root` 帳號是否有設定密碼。
- Suggestion: Harden the system by removing unneeded compilers. This can decrease the chance of customized trojans, backdoors and rootkits to be compiled and installed
如果您的伺服器上沒有編譯程式的需求，可以暫時移除掉編譯器，以避免有心人士在您的系統上編譯或安裝特定的後門程式。

相關連結

- [Lynis](#)
- [Wlynis](#)

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

<https://net.nthu.edu.tw/netsys/security:lynis>

Last update: **2009/11/26 09:22**

