



Lynis - аудит безопасности системы

Опубликовано muff в Ср, 2012-12-05 22:52

Развивая тему [проверки системы безопасности](#) [1], решил испробовать утилиту **Lynis**. В ходе своей работы она выполняет аудит системы, проверяя и систему и конфигурационные файлы. По завершению проверки выводится отчет, в котором также фигурирует общая оценка системы, предупреждения и советы...

Пора это все проверить на практике. Тестовый стенд - тот же:

```
# uname -v

FreeBSD 7.0-RELEASE-p3 #0: Mon Aug  4 13:49:40 EEST 2008   root [at] arey [dot]
local:/usr/obj/usr/src/sys/AREY
```

Выполним установку **lynis** из системы портов:

```
# cd /usr/ports/security/lynis && make install clean && rehash
```

Возможности утилиты следующие (воспользуемся опцией **-h** для вывода короткой справки):

```
[+] Initializing program----- Valid parameters:  -
-auditor "<name>"           : Auditor name      --check-all (-c)       : Check
system      --check-update       : Check for updates  --no-colors
              : Don't use colors in output  --no-log              : Don't crea
te a log file  --profile <profile>      : Scan the system with the given prof
ile file     --quick (-Q)              : Quick mode, don't wait for user input
--quiet (-q)                : No output, except warnings  --reverse-colors
              : Optimize color display for light backgrounds  --tests "<tests>"
              : Run only tests defined by <tests>  --tests-category "<category>" : Run only
tests defined by <category>  --view-manpage (--man)      : View man page  --v
ersion (-V)                  : Display version number and quit

See man page and documentation for all available options.
```

Для более подробного описания доступных опций - **man lynis**.

Выполним полную проверку системы в "тихом" режиме (иначе после каждого блока проверок придется подтверждать действия вводом с клавиатуры):

```
# lynis -c -Q
```

По завершению сканирования, внимательно изучаем отчет. Желательно в первую очередь исправить все **Warnings** и по мере возможности, выполнить рекомендации секции **Suggestions**. Также порадовал параметр **Hardening index**, который отображает числовое значение уровня защищенности сервера.

В моем случае результат сканирования получился следующий:

```
=====
-----

-[ Lynis 1.2.9 Results ]-

Tests performed: 136
Warnings:
-----
- [00:25:16] Warning: Found one or more zombie processes (38686) [test:PROC-3612] [impact:L]
```



- [00:25:16] Warning: Multiple users with UID 0 found in passwd file [test:AUTH-9204] [impact:H]
- [00:25:16] Warning: Multiple accounts found with same UID [test:AUTH-9208] [impact:H]
- [00:25:16] Warning: Possible harmful shell found (for passwordless account!) [test:AUTH-9218] [impact:H]
- [00:25:16] Warning: Found unprotected console in /etc/ttys [test:SHLL-6202] [impact:M]
- [00:25:33] Warning: PHP option expose_php is possibly turned on, which can reveal useful information for attackers. [test:PHP-2372] [impact:M]
- [00:25:34] Warning: Found one or more stratum 16 peers [test:TIME-3116] [impact:L]

Suggestions:

- ```

```
- [00:25:14] Suggestion: update to the latest stable release.
  - [00:25:16] Suggestion: Check the output of ps for dead or zombie processes [test:PROC-3612]
  - [00:25:16] Suggestion: Use vipw to delete the 'toor' user if not used. [test:AUTH-9204]
  - [00:25:16] Suggestion: Default umask in /etc/profile could be more strict like 027 [test:AUTH-9328]
  - [00:25:16] Suggestion: Change the console line from 'secure' to 'insecure'. [test:SHLL-6202]
  - [00:25:16] Suggestion: To decrease the impact of a full /tmp file system, place /tmp on a separated partition [test:FILE-6310]
  - [00:25:32] Suggestion: Unused distfiles found. Use portsclean to delete these files. For example: portsclean -DD. [test:PKGS-7348]
  - [00:25:32] Suggestion: [test:Install portaudit from the ports collection to query outdated (vulnerable) packages.]
  - [00:25:32] Suggestion: Configure a firewall/packet filter to filter incoming and outgoing traffic [test:FIRE-4590]
  - [00:25:33] Suggestion: Change the expose\_php line to: expose\_php = Off [test:PHP-2372]
  - [00:25:33] Suggestion: Change the enable\_dl line to: enable\_dl = Off, to disable downloads via PHP [test:PHP-2374]
  - [00:25:33] Suggestion: Change the allow\_url\_fopen line to: allow\_url\_fopen = Off, to disable downloads via PHP [test:PHP-2376]
  - [00:25:33] Suggestion: Enable logging to an external logging host for archiving purposes and additional protection [test:LOGG-2154]
  - [00:25:33] Suggestion: Add legal banner to /etc/motd, to warn unauthorized users [test:BANN-7122]
  - [00:25:34] Suggestion: Check ntpq peers output [test:TIME-3116]
  - [00:25:34] Suggestion: Check ntpq peers output for time source candidates [test:TIME-3128]
  - [00:25:34] Suggestion: Harden the system by removing unneeded compilers. This can decrease the chance of customized trojans, backdoors and rootkits to be compiled and installed [test:HRDN-7220]

=====  
=====

Files:

- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====  
=====

Notice: Lynis update available

Current version : 129 Latest version : 130

=====  
=====

Hardening index : [54] [##### ]

=====  
=====

Кажется пора поработать над безопасностью данного сервера...

Как итог, могу отметить, что по своей сути **lynis** оказался полезным и интересным



инструментом. Однозначно стоит взять его на вооружение и использовать повседневно в работе.

**Источник (получено 2026-06-11 02:14):**

<http://muff.kiev.ua/content/lynis-audit-bezopasnosti-sistemy>

**Ссылки:**

[1] <http://muff.kiev.ua/content/chkrootkit-poisk-v-sisteme-rootkit-i-backdoor>