Server absichern mit lynis

https://nissel.it/index.php/2021/01/01/server-absichern-mit-lynis/

Mithilfe von lynis können einige Sicherheitstests durchgeführt werden die dann auch erläutert werden.

```
wget -qO- https://downloads.cisofy.com/lynis/lynis-3.0.2.tar.gz | tar xvz
```

```
cd lynis && ./lynis update check && ./lynis audit system
```

```
[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to comple

  - Plugins enabled                                           [ NONE ]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB                                    [ OK ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ NONE ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 42 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 72 enabled services
  - Check startup files (permissions)                         [ OK ]

[+] Kernel
------------------------------------
  - Checking default run level                                [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported               [ FOUND ]
  - Checking kernel version and release                       [ DONE ]
  - Checking kernel type                                      [ DONE ]
  - Checking loaded kernel modules                            [ DONE ]
      Found 80 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration
    - configuration in systemd conf files                     [ DEFAULT ]
    - configuration in etc/profile                            [ DEFAULT ]
    - 'hard' configuration in security/limits.conf            [ DEFAULT ]
    - 'soft' configuration in security/limits.conf            [ DEFAULT ]
    - Checking setuid core dumps configuration                [ PROTECTED ]
  - Check if reboot is needed                                 [ NO ]
```

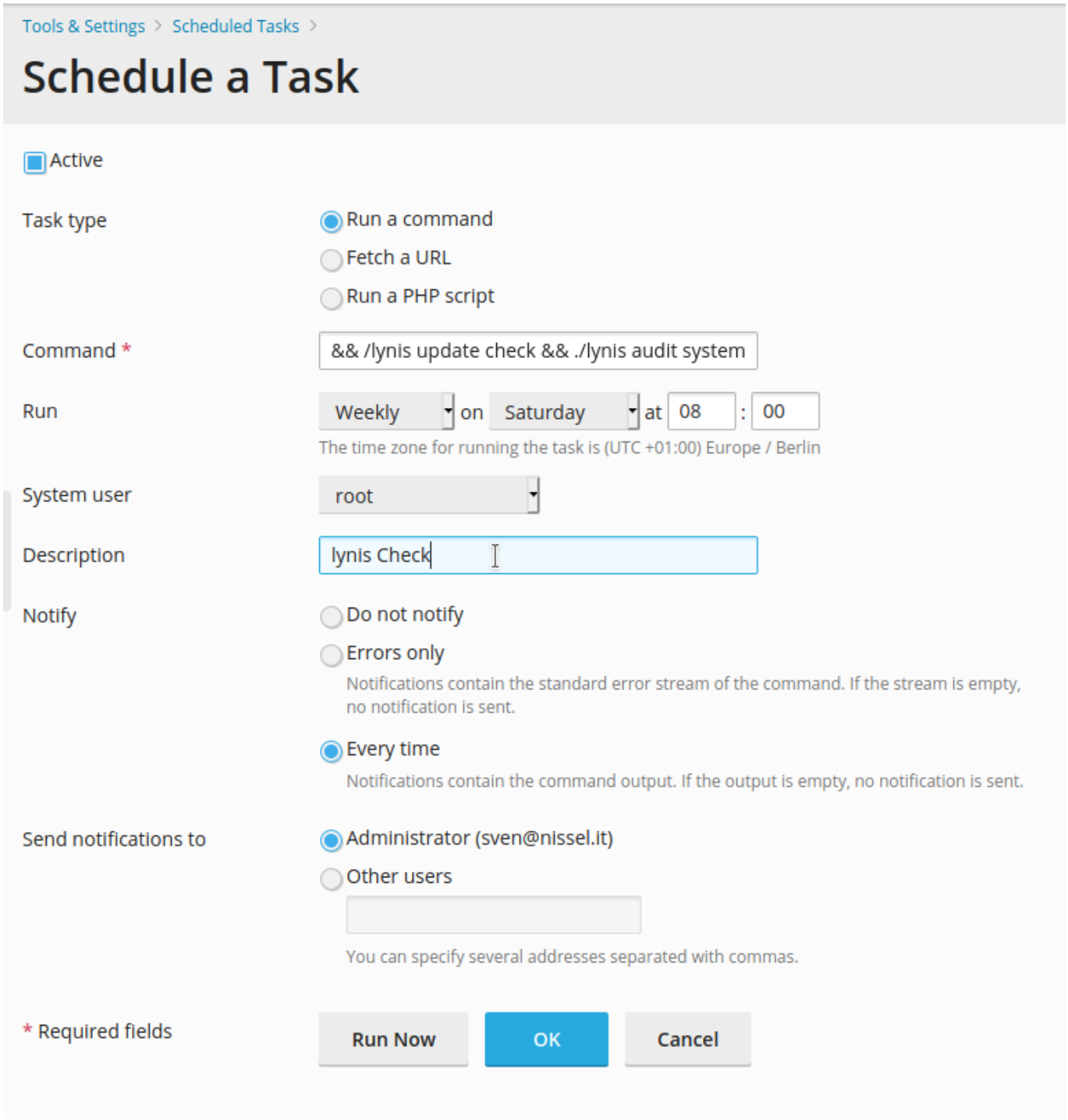
lynis Ausgabe

Jede Warnung und Hinweis muss natürlich bewertet werden. z.B: legt Plesk für weitere FTP Benutzer einen Benutzer mit identischer UID an. Darauf weißt lynis z.B: hin.

lynis regelmäßig ausführen

Die Ausführung kann als cronjob eingerichtet werden.

```
cd /root/lynis && ./lynis update check --cronjob --no-
log && ./lynis audit system --no-log --cronjob --warnings-only
```



SMTP Banner anpassen

Das Programm aus der SMTP "Begrüßung" heraus zu nehmen macht es evtl. ein paar scripten auf der Suche nach Sicherheitslücken etwas schwerer. Dazu muss die /etc/postfix/main.cf angepasst werden.

```
smtpd_banner = $myhostname ESMTP
```

Und postfix neu gestartet werden.

```
service postfix restart
```

Alte Zertifikate entfernen

In der Kostenlosen Variante gibt lynis nicht preis wo veraltete Zertifikate liegen. Ein möglicher Ort ist /opt/psa/var/certificates. Mit folgenden skript wird geprüft ob ein Zertifikat gelöscht werden kann:

```
#!/bin/bash

for filename in /opt/psa/var/certificates/*; do
    if ! openssl x509 -checkend 0 -noout -in ${filename} &>/dev/null;
then
        if ! grep --quiet -R "${filename}" /etc/nginx/plesk.conf.d/*;
then
            if ! grep --quiet "${filename}" /etc/apache2/plesk.conf.d/
server.conf; then
```

```
                echo "${filename} can be deleted"
            else
                echo "${filename} is expired but still in use by apach
e (default cert)"
            fi
        else
            echo "${filename} is expired but still in use by nginx"
        fi
    fi
done
```

Warnungen ignorieren

Damit nur eine Mail verschickt wird, wenn ein neuer Fehler auftaucht, müssen alle Warnungen die ignoriert werden sollen deaktiviert werden. Dazu muss die default.prf editiert werden.

```
profile-name=Plesk Audit Template
skip-test=TIME-3185
...
```

SSH Konfiguration härten

Es gibt einige Einstellungen die von lynis empfohlen werden. Dazu die /etc/ssh/sshd_config editieren:

```
PermitRootLogin without-password
MaxAuthTries 3
LogLevel VERBOSE
ClientAliveCountMax 2
AllowAgentForwarding no
```

```
AllowTcpForwarding no
X11Forwarding no
```

Kernel

Unterbinden eines core dumps über die /etc/security/limits.conf

```
*               hard    core            0
```

System Passwort Einstellungen

Auf heutiger Hardware können deutlich mehr Runden als der default 5000 für die Generierung von Passwort Hashes verwendet werden. Dazu in der Datei /etc/login.defs folgende Werte anpassen:

```
SHA_CRYPT_MIN_ROUNDS 50000
SHA_CRYPT_MAX_ROUNDS 500000
```

Es sollte dafür gesorgt werden, dass die Passwörter nicht ewig gültig sind:

```
PASS_MAX_DAYS   356
PASS_WARN_AGE   30
```

Mit dem Befehl chage können die Gültigkeitsdauer von bestehenden Benutzern angezeigt und geändert werden.

```
chage -l username
chage -M 365 -m 365 -W 30 username
```

Passend dazu die Plesk Einstellungen für Passwort Stärke

Tools & Settings -> Security Policy

Links

https://cisofy.com/lynis/

https://cisofy.com/lynis/controls/MAIL-8818/

https://support.plesk.com/hc/en-us/articles/115000269754-How-to-change-the-hostname-and-SMTP-banner-in-Postfix-on-a-Plesk-server

https://www.tecmint.com/scan-linux-for-malware-and-rootkits/

https://talk.plesk.com/threads/ssl-certificate-files-location.336076/

https://stackoverflow.com/questions/21297853/how-to-determine-ssl-cert-expiration-date-from-a-pem-encoded-certificate

https://askubuntu.com/questions/449364/what-does-without-password-mean-in-sshd-config-file

https://linux-audit.com/understand-and-configure-core-dumps-work-on-linux/

https://blog.sys4.de/rounds-and-iterations-for-ssh-and-other-keys-en.html

https://www.cyberciti.biz/faq/linux-howto-check-user-password-expiration-date-and-time/