Das System härten mit Hilfe von Lynis

Tobias Brandl

08.05.2017

Index

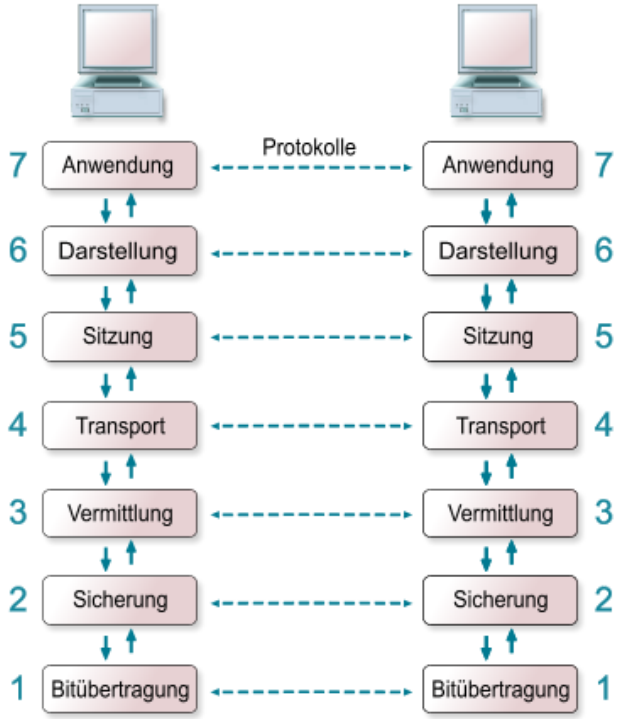
Grundlagen

- Wie werde ich angegriffen?
- Wie schütze ich mich?

Wie werde ich angegriffen?

Über das Internet oder das Lokale Netzwerk.

OSI-Schichtenmodell



[1]

Und wo?

- Anwendungen, e.g. Browser
- Dienste (offene Ports)
- Kernel

[1] Bildquelle: http://www.selflinux.org/

Wie schütze ich mich?

- So wenig Pakete wie möglich installieren
- System aktuell halten (Updates)
- Unnötige Dienste deaktivieren (Ports schließen)
- Gesunder Menschenverstand
- Systemschutz verstärken (härten)

Das System härten mit Lynis

Lynis ist ein Programm, welches diverse Systemsettings und das Vorhandensein von Sicherheitssoftware prüft.

Lynis hat keine Schutzfunktion, es gibt nur Verbesserungsvorschläge.

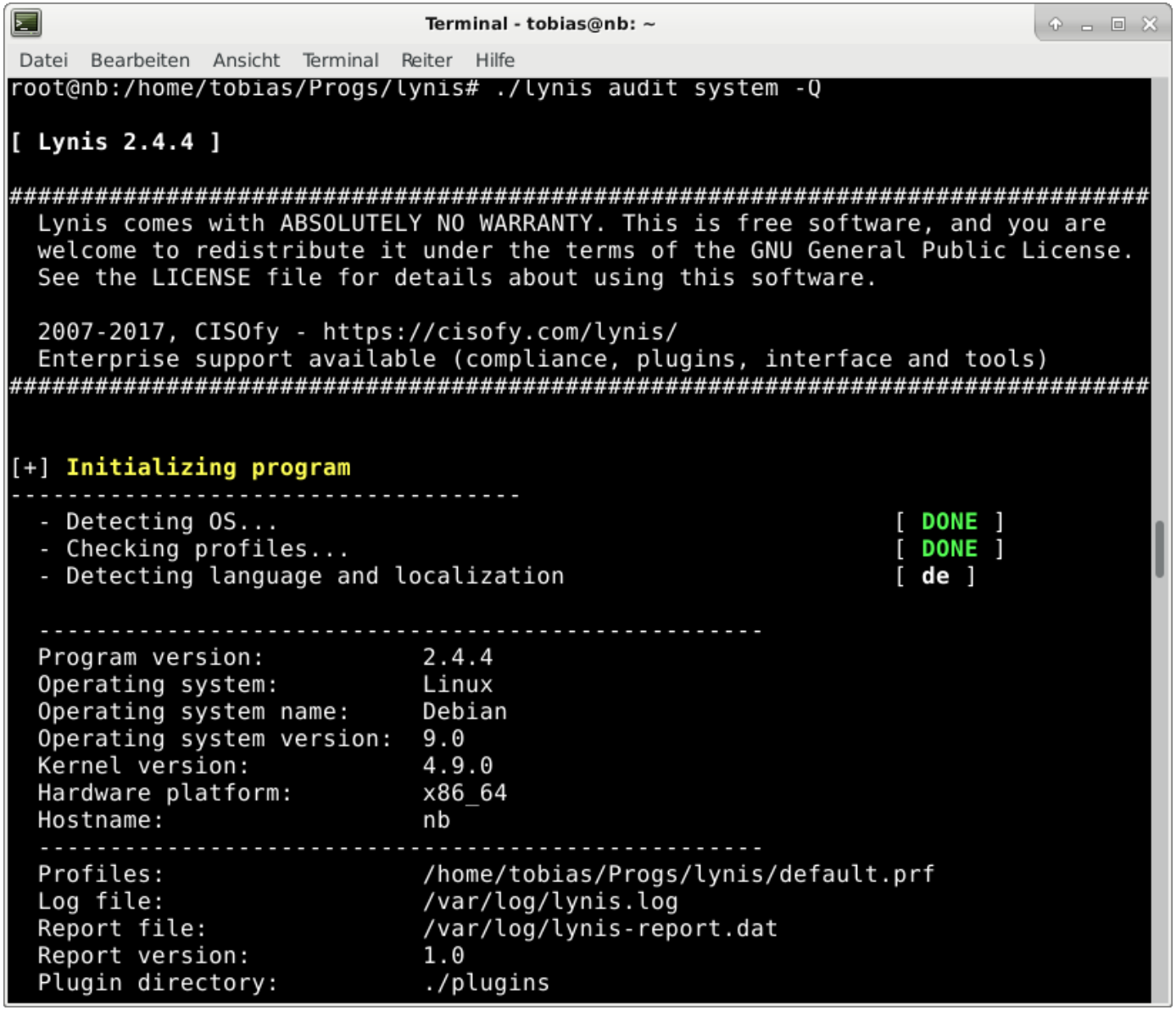
Im Endeffekt muss dann jeder für sich selbst entscheiden, welcher Vorschlag einem selbst mehr Sicherheit bringt.

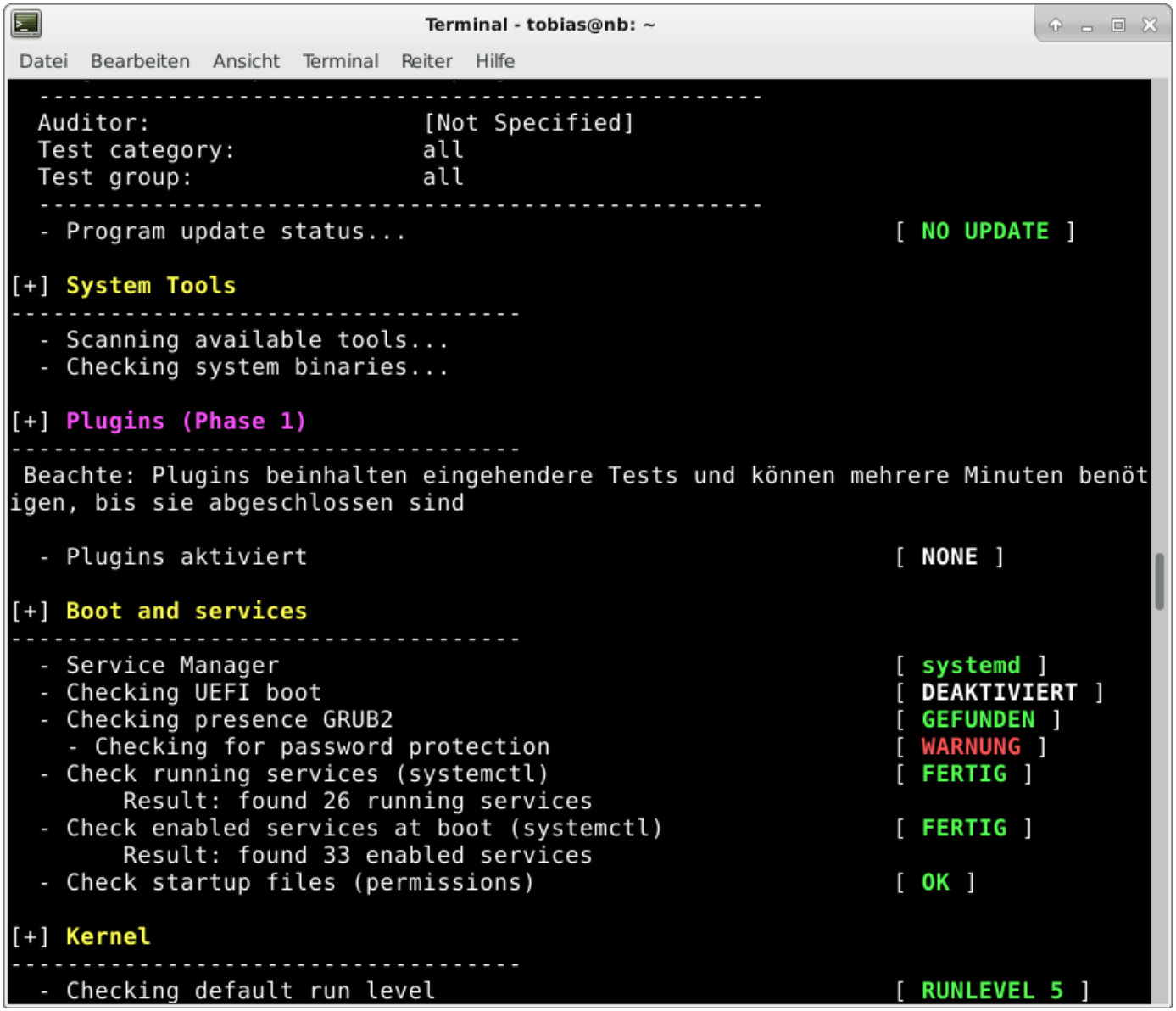
Die Ergebnis-Prozentzahl ist am Ende nur ein grober Ansatz. Am Ende ist es egal, welcher Wert dort Stand, wenn das System kompromittiert wurde.

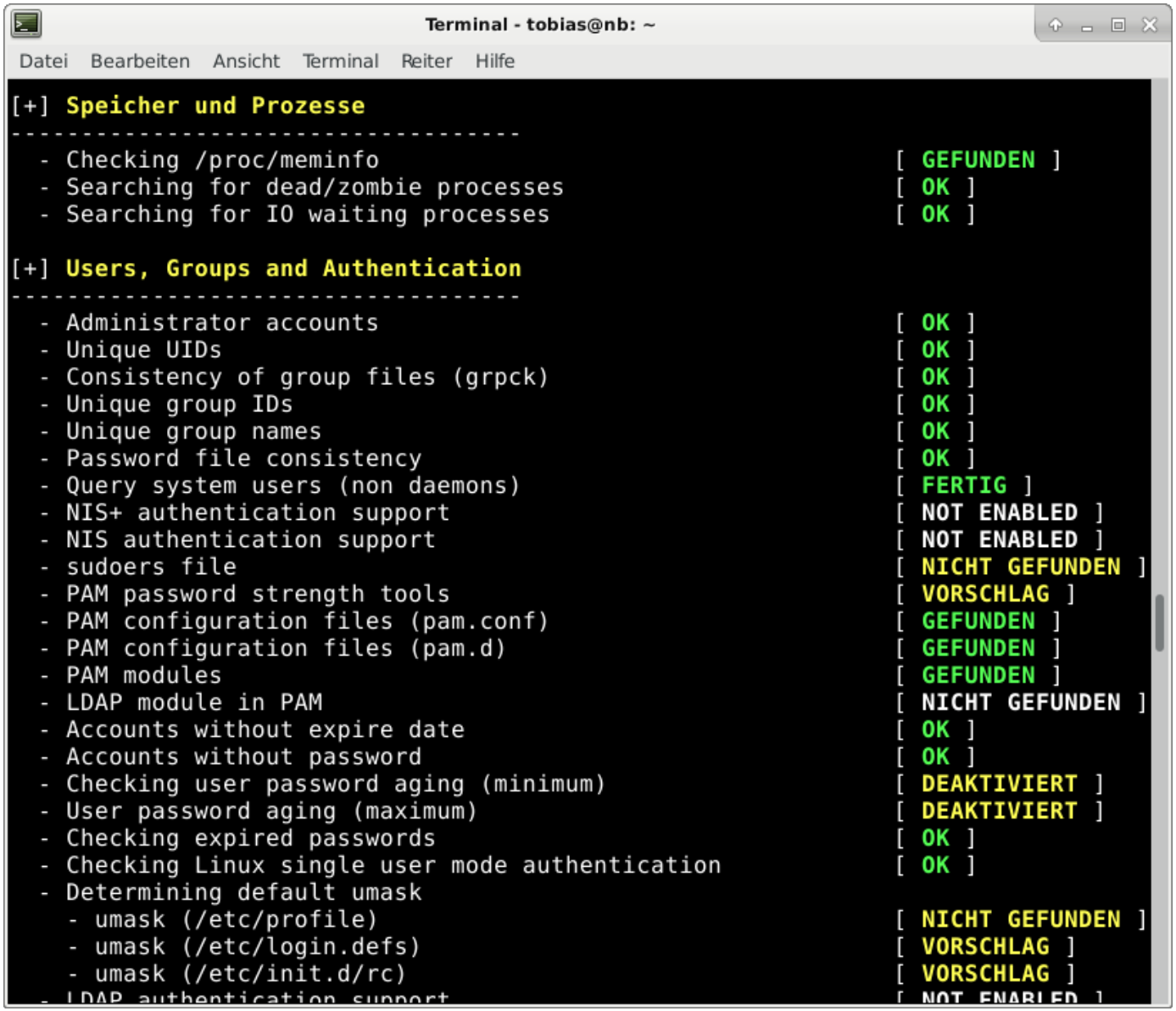
Installation

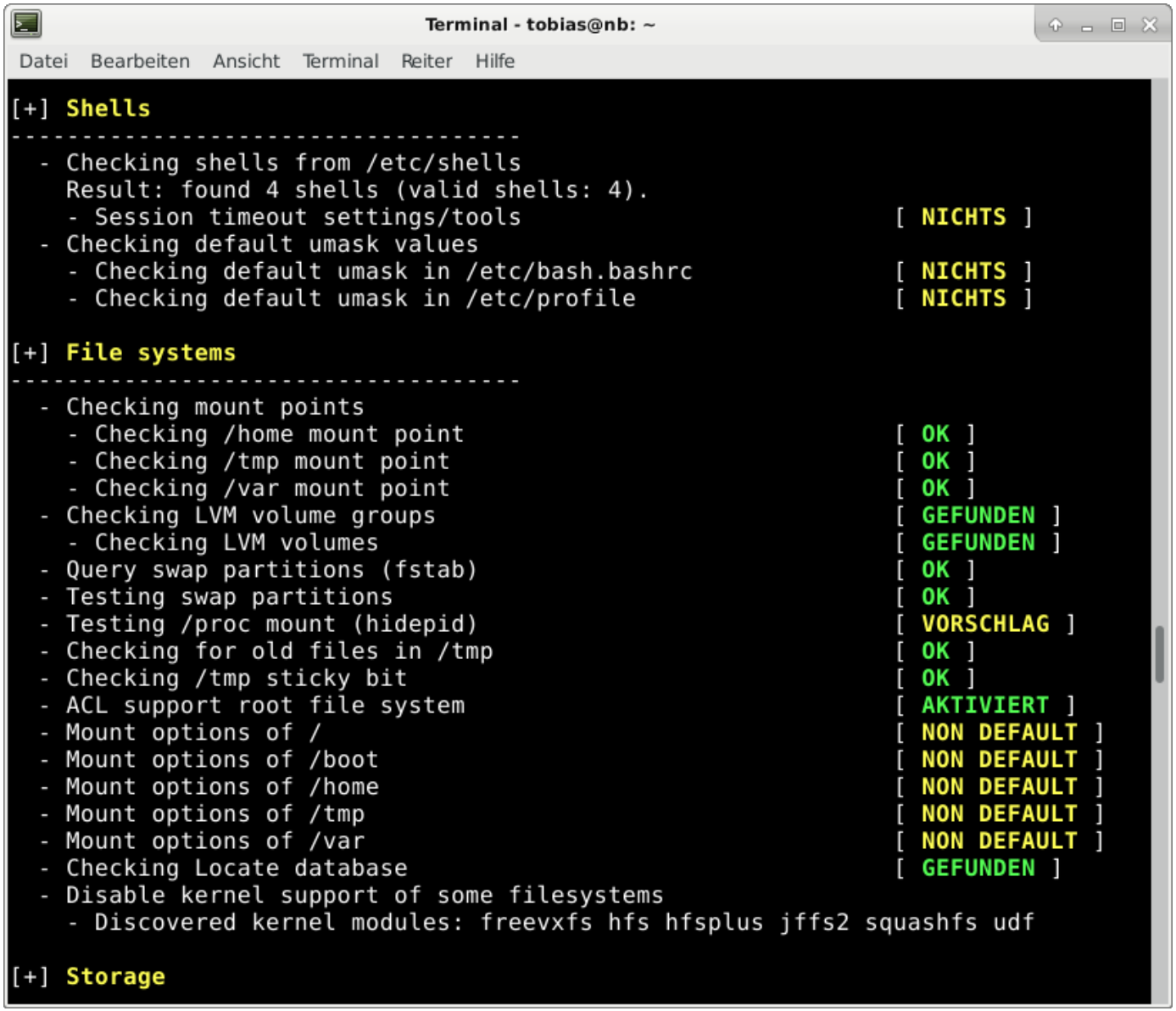
- Manuelle Installation
  - Downloaden unter https://cisofy.com/download/lynis/
  - ggf. Herkunft prüfen
  - entpacken: tar -xf lynis-2.4.7.tar.gz
  - chown -R 0:0 lynis (Root zuweisen)
- Paketmanager
  z.B. apt-get install lynis
- Offizielles Cisofy Repository

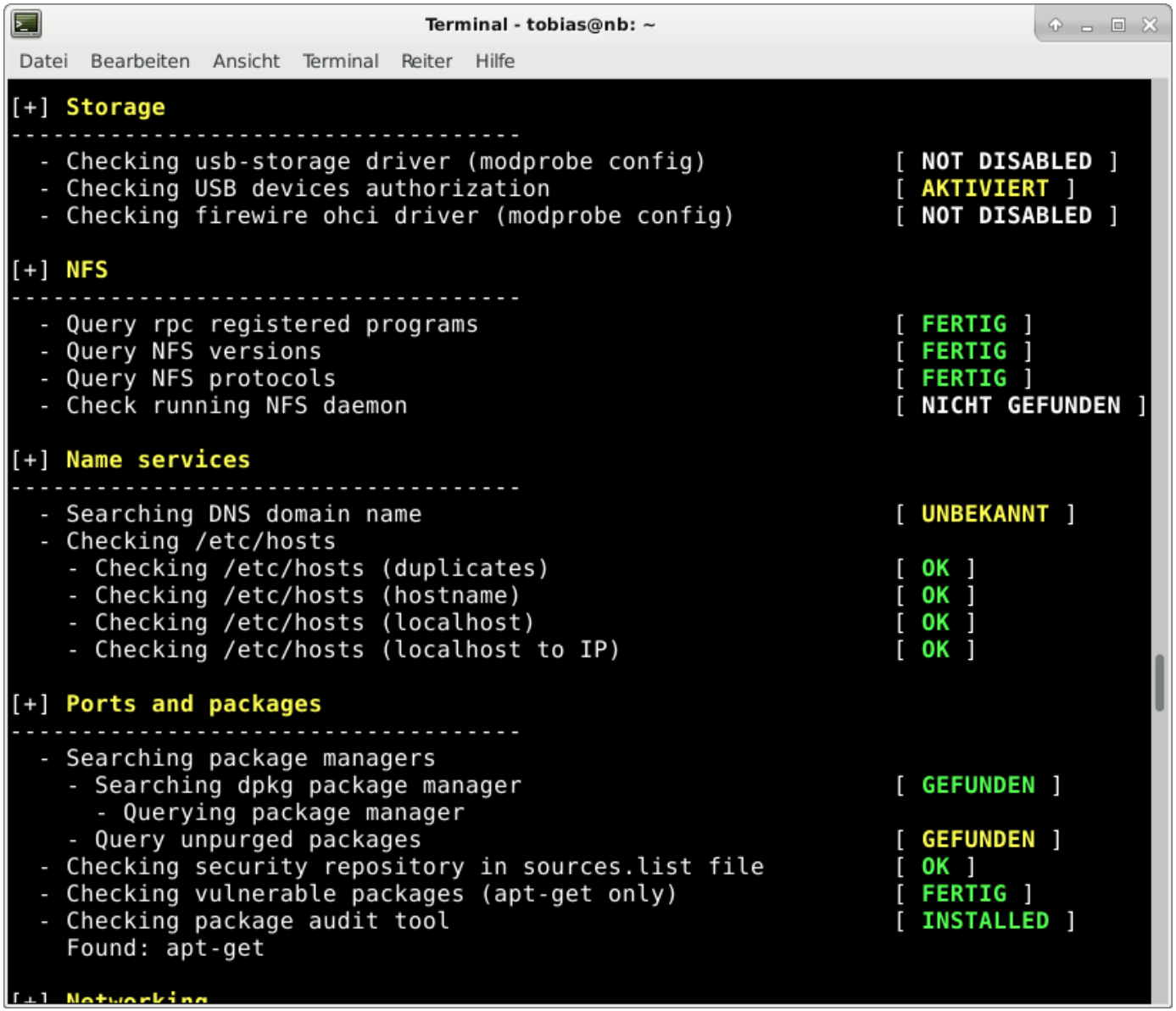
Mein initialer Lauf

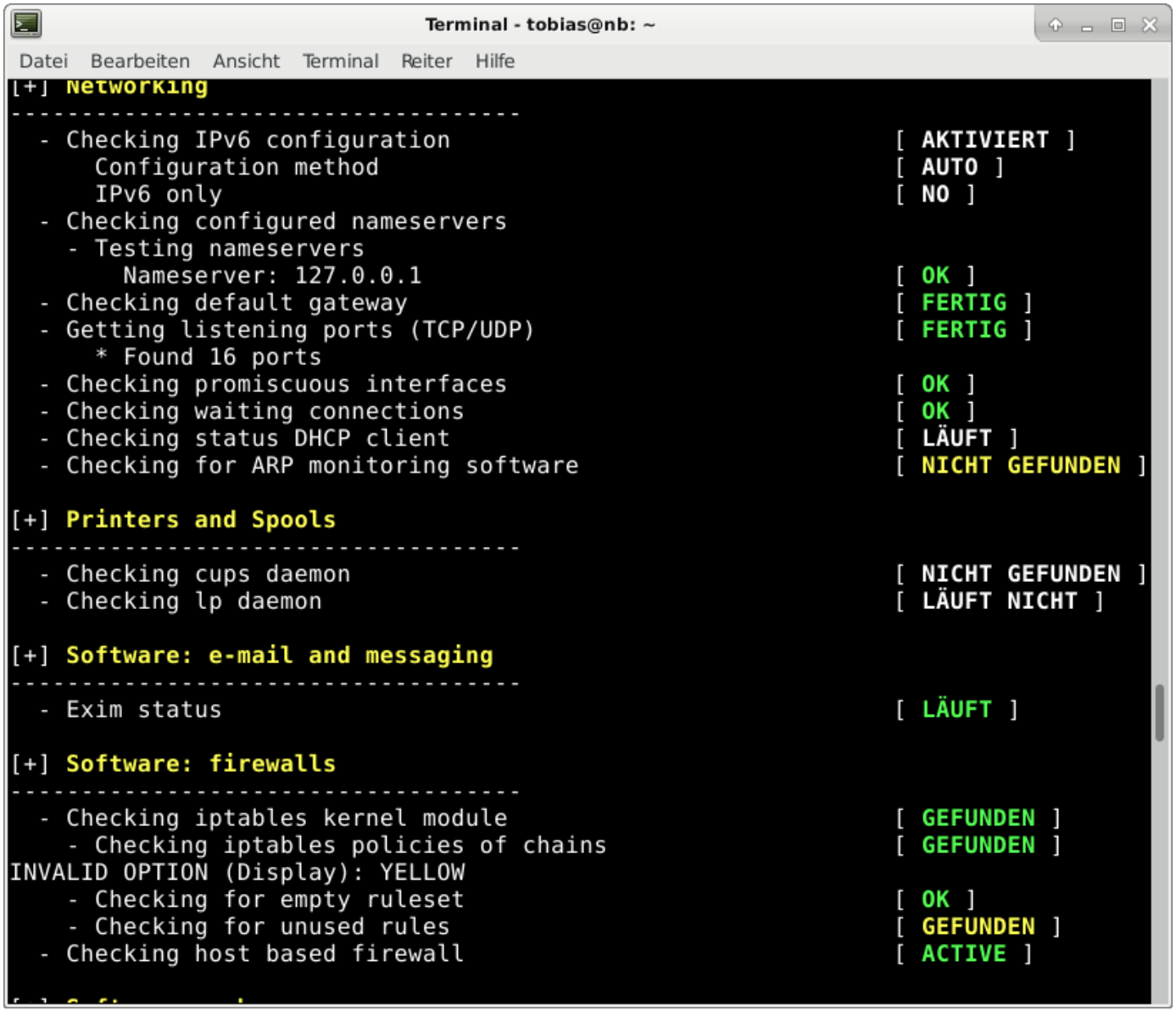


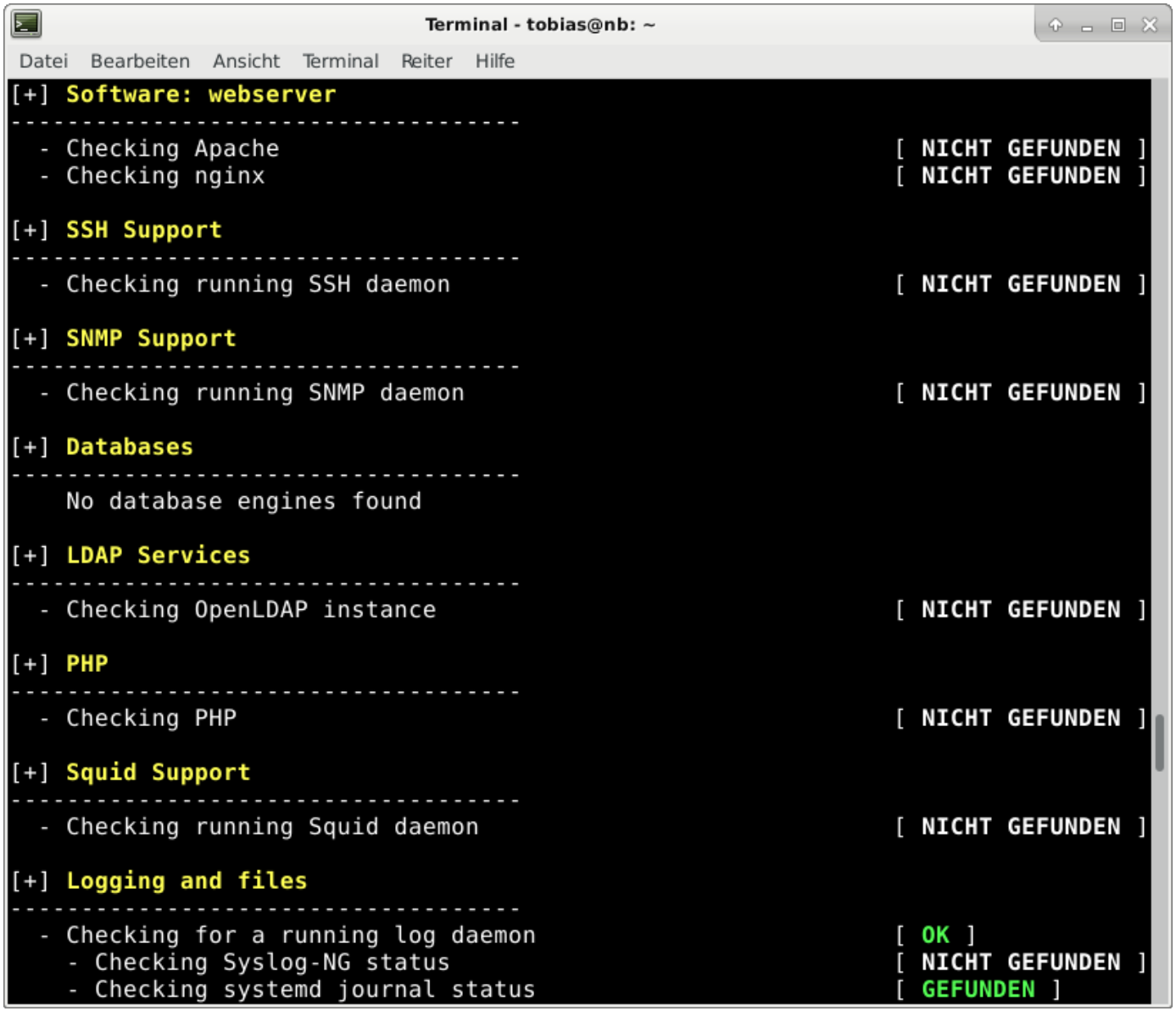

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
Auditor: [Not Specified]
Test category: all
Test group: all
- Program update status... [NO UPDATE]
[+] System Tools
- Scanning available tools...
- Checking system binaries...
[+] Plugins (Phase 1)
Beachte: Plugins beinhalten eingehendere Tests und können mehrere Minuten benöt
igen, bis sie abgeschlossen sind
- Plugins aktiviert [NONE]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DEAKTIVIERT]
- Checking presence GRUB2 [GEFUNDEN]
- Checking for password protection [WARNUNG]
- Check running services (systemctl) [FERTIG]
Result: found 26 running services
- Check enabled services at boot (systemctl) [FERTIG]
Result: found 33 enabled services
- Check startup files (permissions) [OK]
[+] Kernel
- Checking default run level [RUNLEVEL 5]

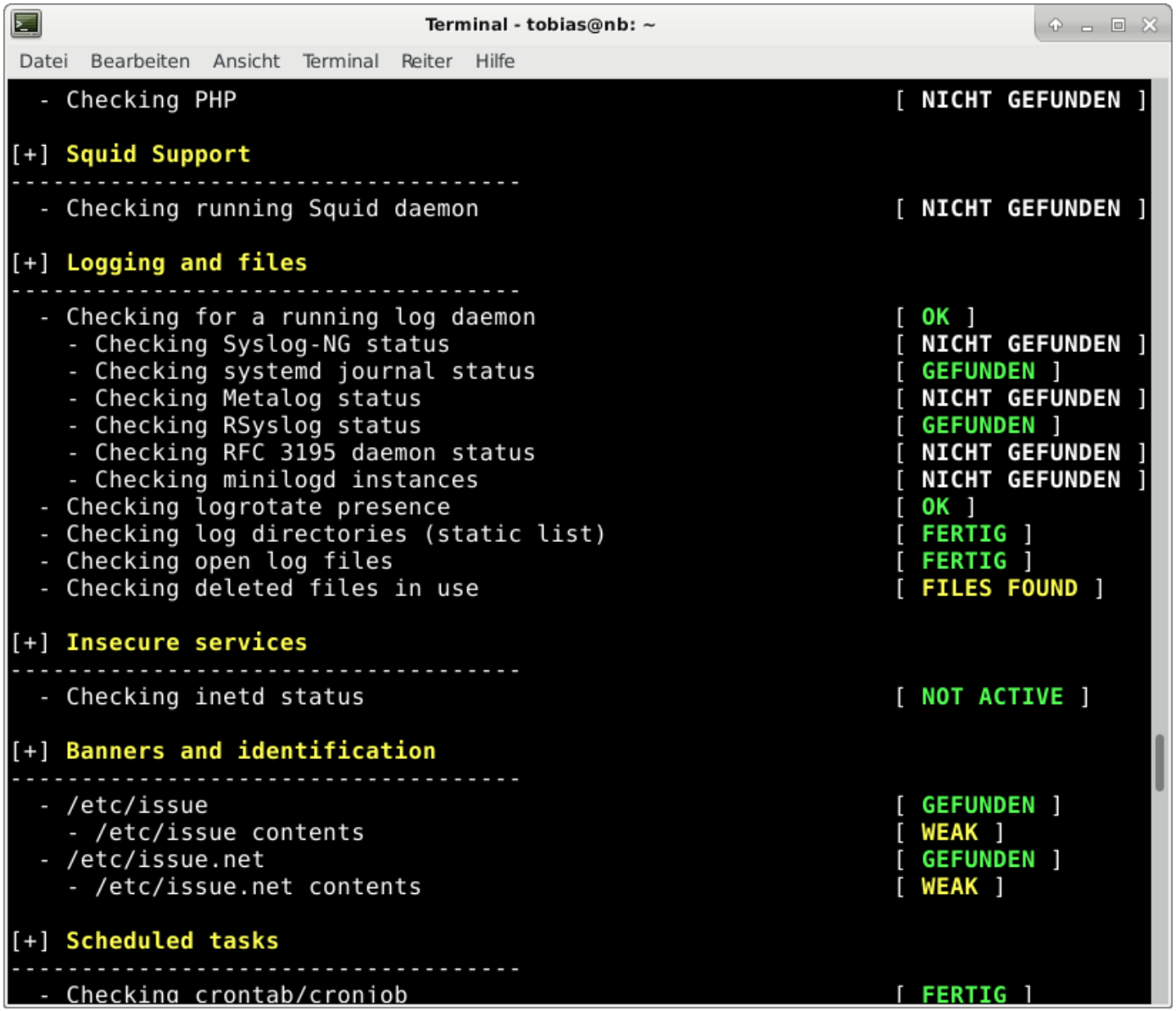

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
[+] Speicher und Prozesse
- Checking /proc/meminfo [GEFUNDEN]
- Searching for dead/zombie processes [OK]
- Searching for IO waiting processes [OK]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Query system users (non daemons) [FERTIG]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- sudoers file [NICHT GEFUNDEN]
- PAM password strength tools [VORSCHLAG]
- PAM configuration files (pam.conf) [GEFUNDEN]
- PAM configuration files (pam.d) [GEFUNDEN]
- PAM modules [GEFUNDEN]
- LDAP module in PAM [NICHT GEFUNDEN]
- Accounts without expire date [OK]
- Accounts without password [OK]
- Checking user password aging (minimum) [DEAKTIVIERT]
- User password aging (maximum) [DEAKTIVIERT]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NICHT GEFUNDEN]
- umask (/etc/login.defs) [VORSCHLAG]
- umask (/etc/init.d/rc) [VORSCHLAG]
- LDAP authentication support [NOT ENABLED]

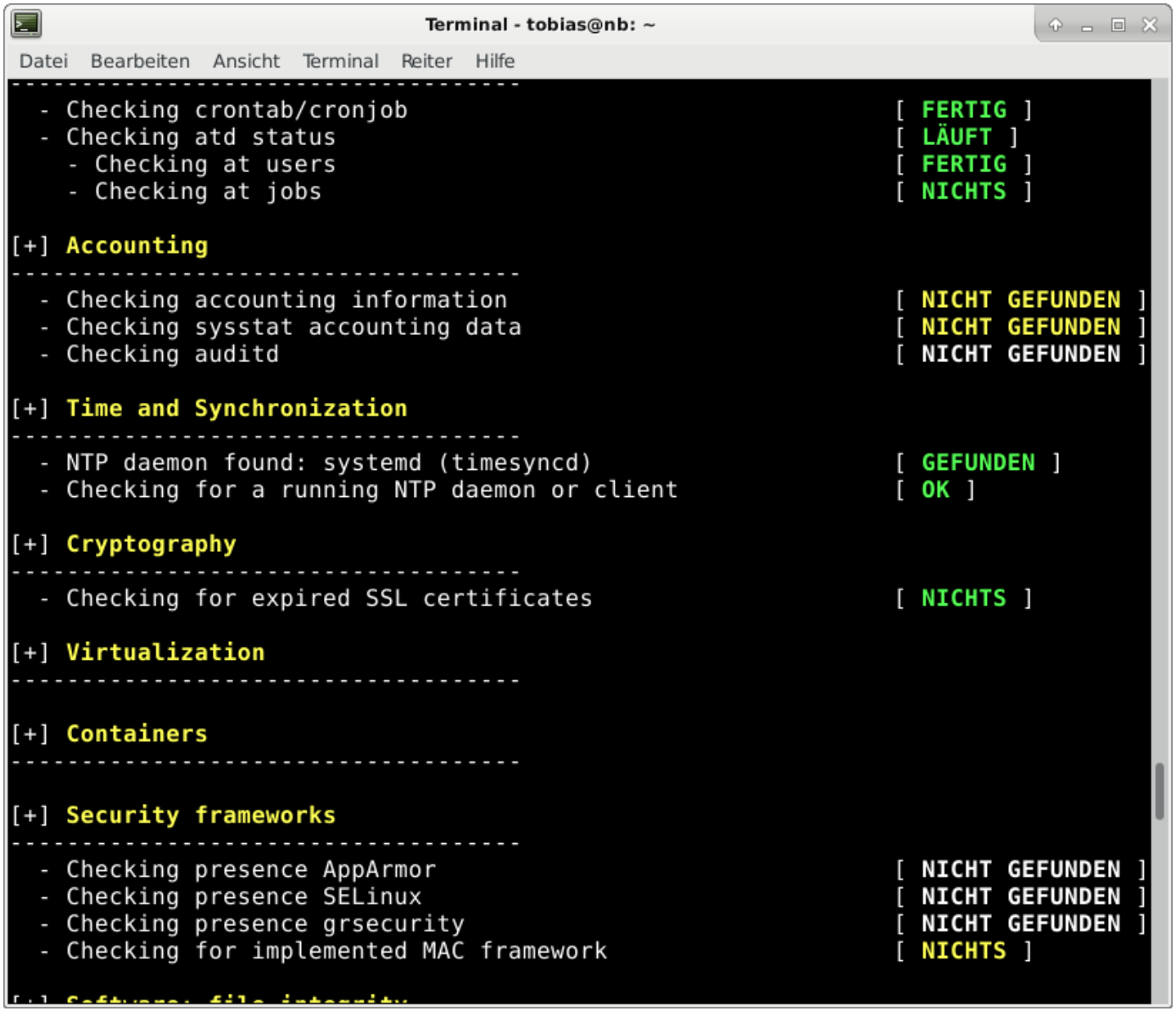

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
[+] Shells
- Checking shells from /etc/shells
Result: found 4 shells (valid shells: 4).
- Session timeout settings/tools [NICHTS]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NICHTS]
- Checking default umask in /etc/profile [NICHTS]
[+] File systems
- Checking mount points
- Checking /home mount point [OK]
- Checking /tmp mount point [OK]
- Checking /var mount point [OK]
- Checking LVM volume groups [GEFUNDEN]
- Checking LVM volumes [GEFUNDEN]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [VORSCHLAG]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- ACL support root file system [AKTIVIERT]
- Mount options of / [NON DEFAULT]
- Mount options of /boot [NON DEFAULT]
- Mount options of /home [NON DEFAULT]
- Mount options of /tmp [NON DEFAULT]
- Mount options of /var [NON DEFAULT]
- Checking Locate database [GEFUNDEN]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] Storage

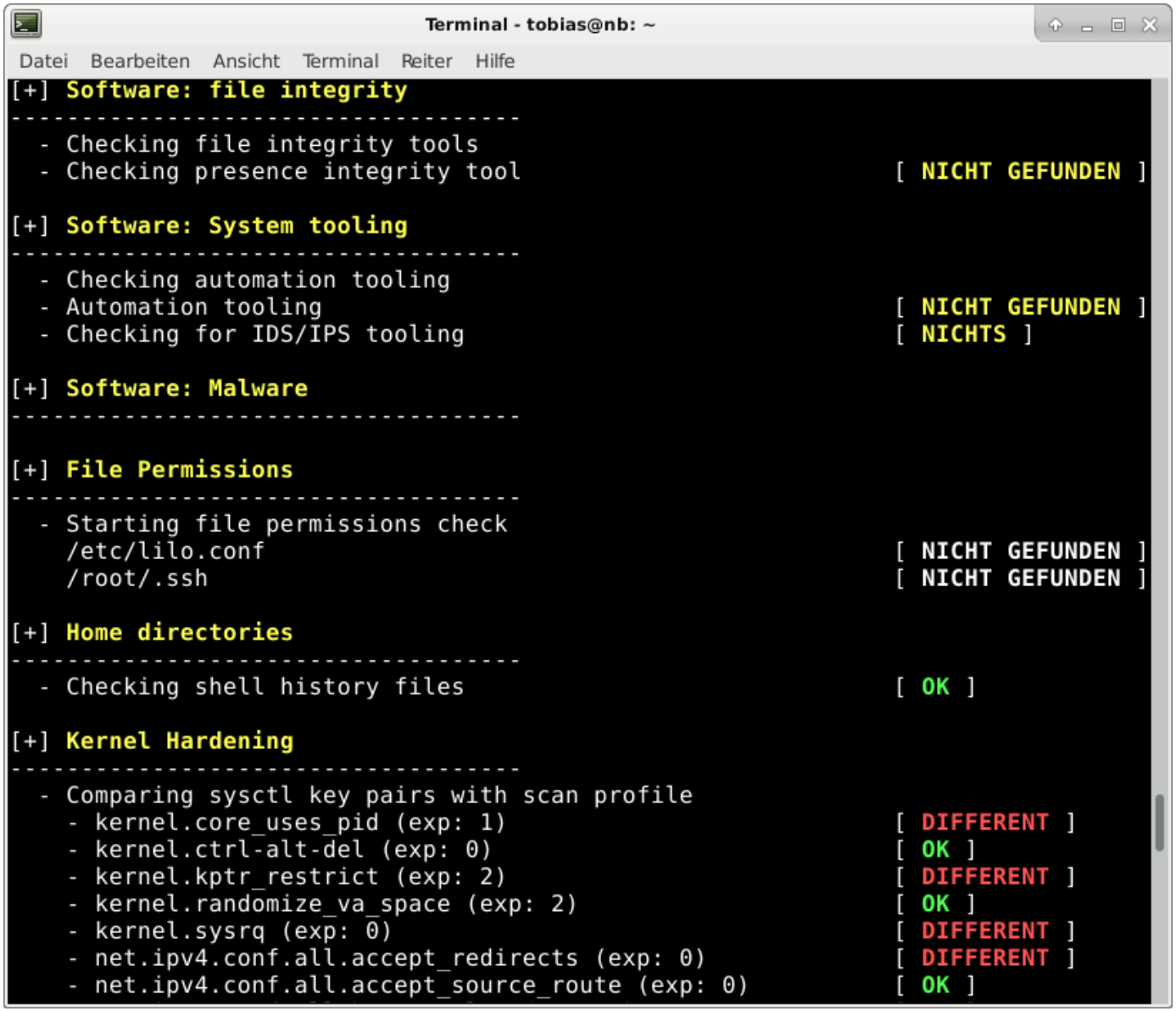


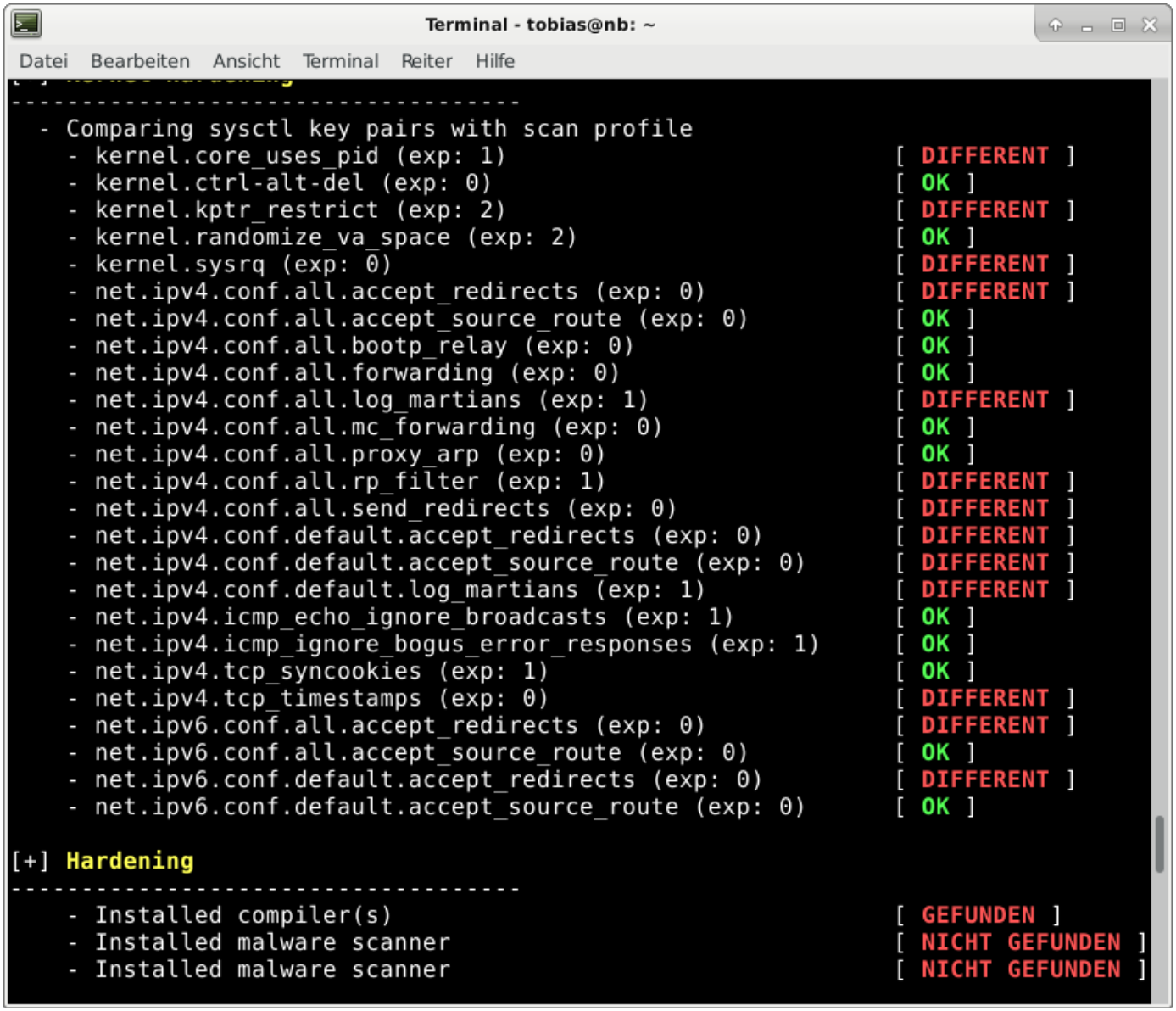

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
[+] Networking
- Checking IPv6 configuration [AKTIVIERT]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 127.0.0.1 [OK]
- Checking default gateway [FERTIG]
- Getting listening ports (TCP/UDP) [FERTIG]
* Found 16 ports
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client [LÄUFT]
- Checking for ARP monitoring software [NICHT GEFUNDEN]
[+] Printers and Spools
- Checking cups daemon [NICHT GEFUNDEN]
- Checking lp daemon [LÄUFT NICHT]
[+] Software: e-mail and messaging
- Exim status [LÄUFT]
[+] Software: firewalls
- Checking iptables kernel module [GEFUNDEN]
- Checking iptables policies of chains [GEFUNDEN]
INVALID OPTION (Display): YELLOW
- Checking for empty ruleset [OK]
- Checking for unused rules [GEFUNDEN]
- Checking host based firewall [ACTIVE]

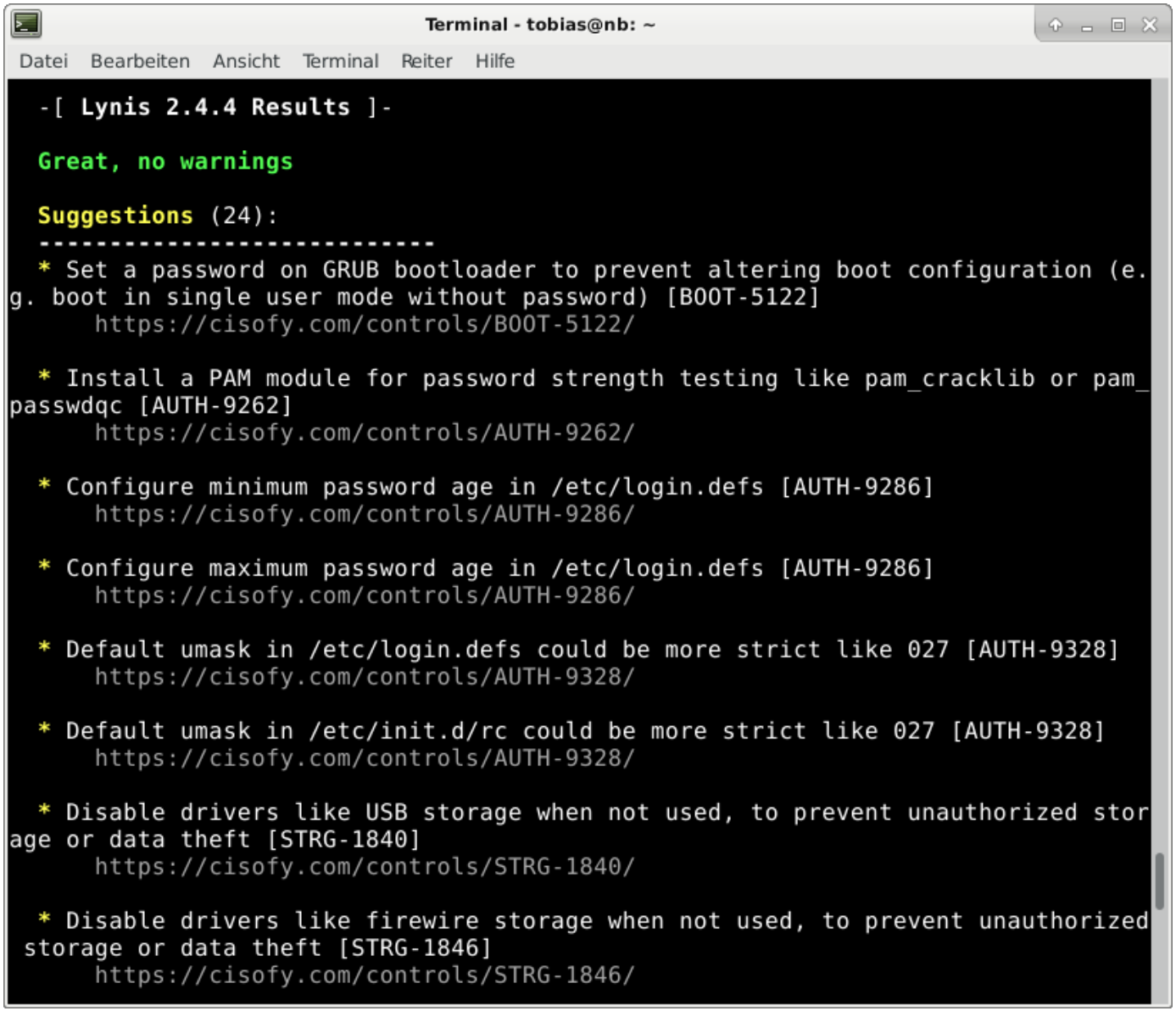


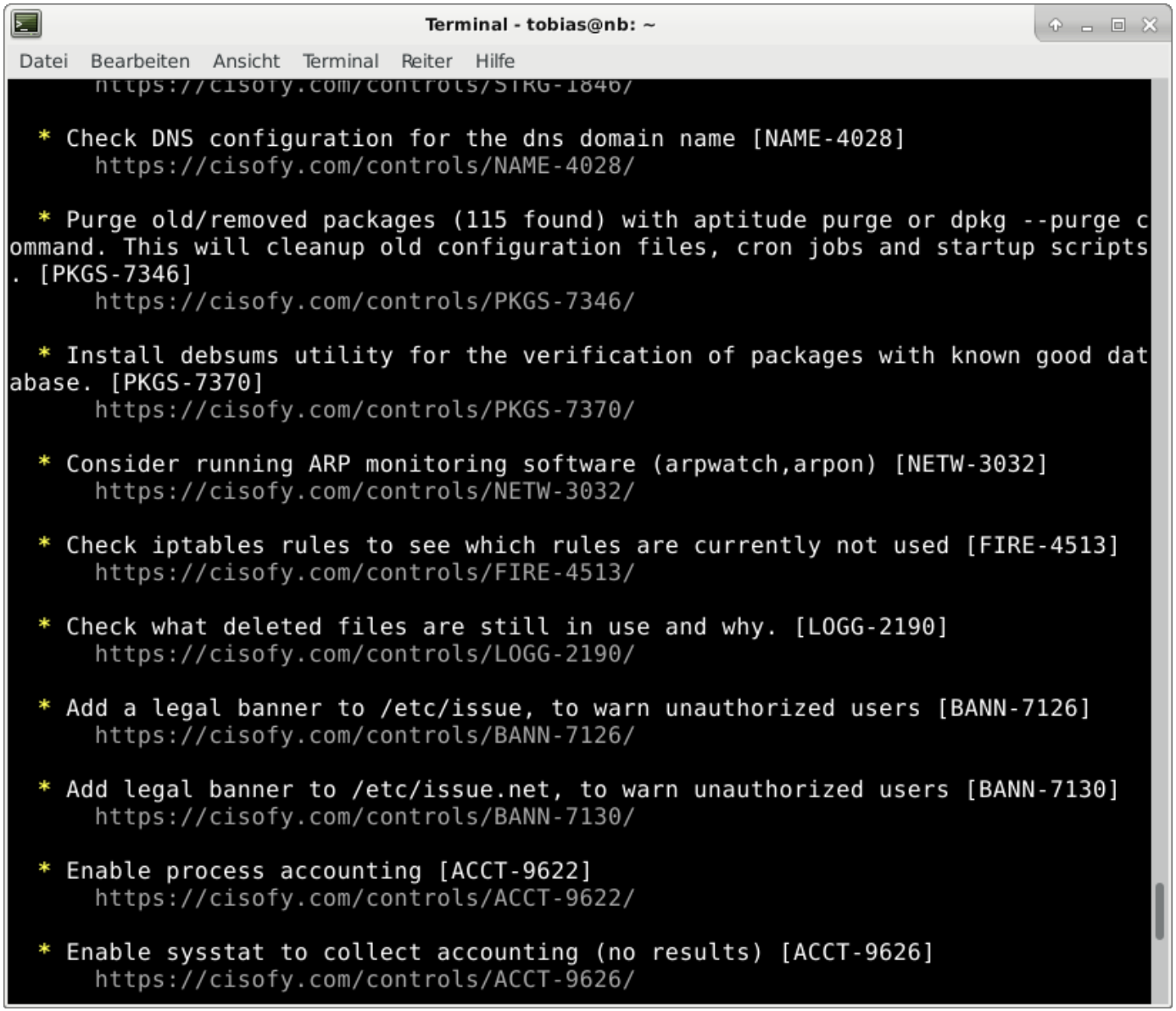


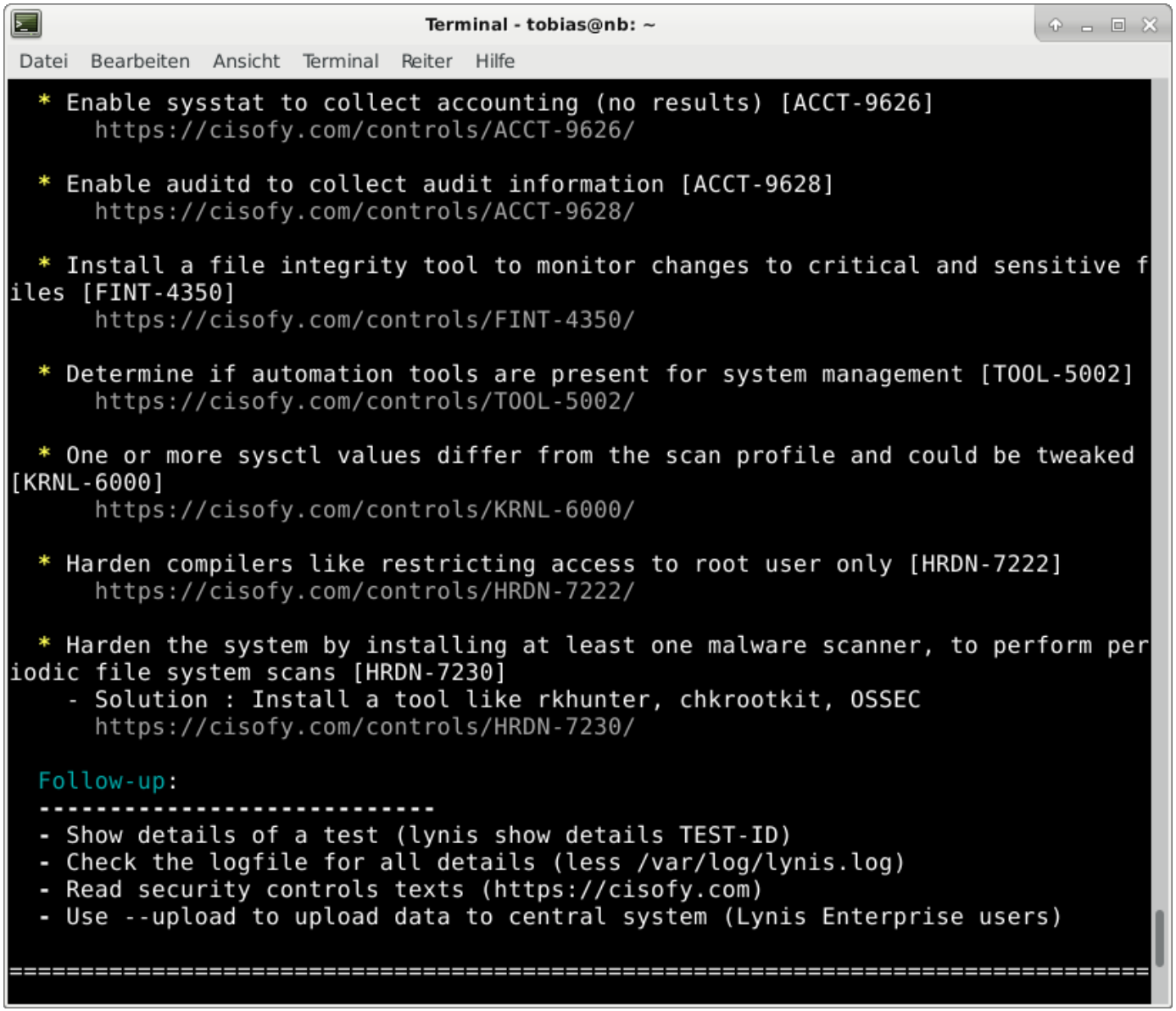

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
- Checking crontab/cronjob [FERTIG]
- Checking atd status [LÄUFT]
- Checking at users [FERTIG]
- Checking at jobs [NICHTS]
[+] Accounting
- Checking accounting information [NICHT GEFUNDEN]
- Checking sysstat accounting data [NICHT GEFUNDEN]
- Checking auditd [NICHT GEFUNDEN]
[+] Time and Synchronization
- NTP daemon found: systemd (timesyncd) [GEFUNDEN]
- Checking for a running NTP daemon or client [OK]
[+] Cryptography
- Checking for expired SSL certificates [NICHTS]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [NICHT GEFUNDEN]
- Checking presence SELinux [NICHT GEFUNDEN]
- Checking presence grsecurity [NICHT GEFUNDEN]
- Checking for implemented MAC framework [NICHTS]

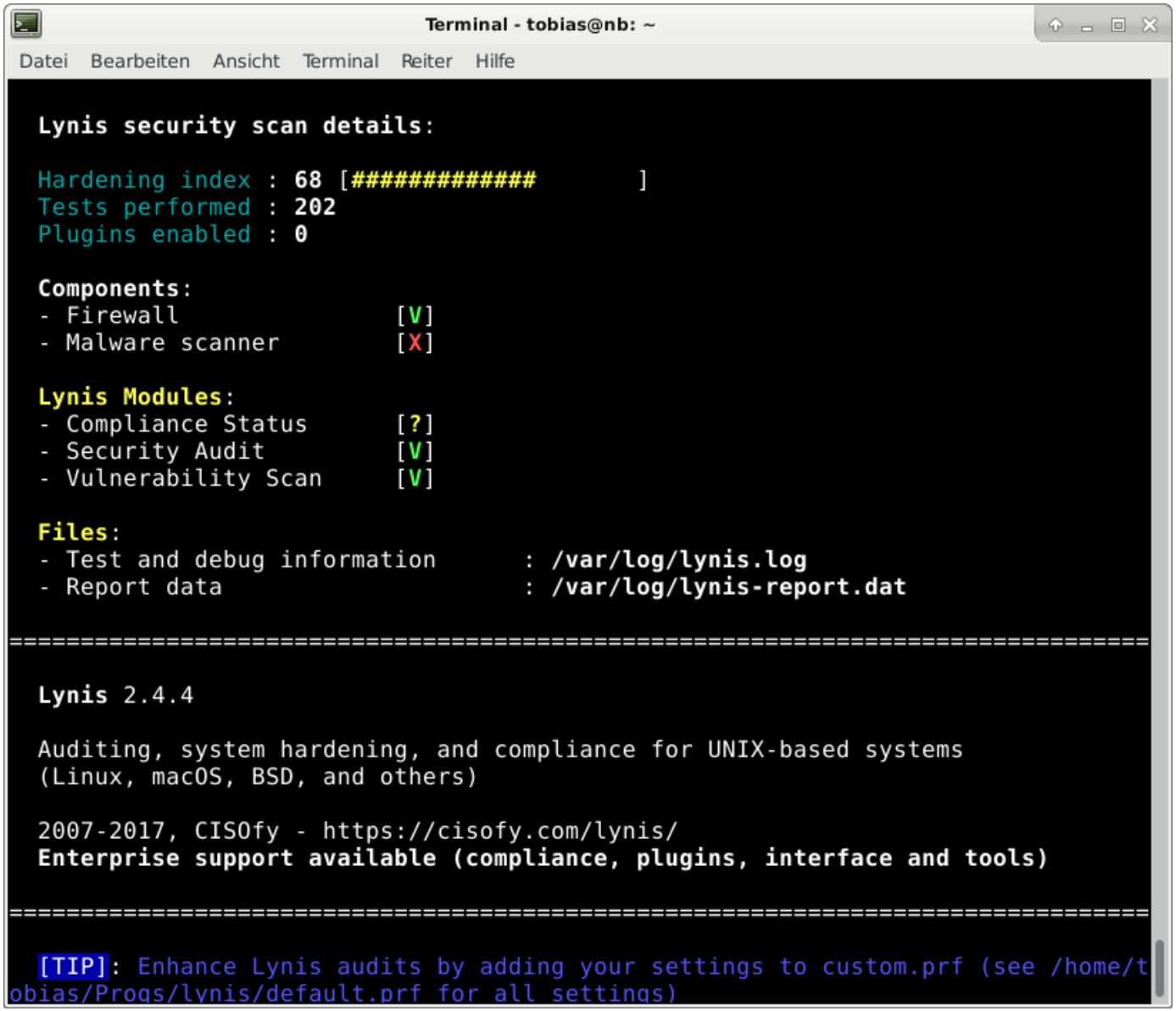

Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
[+] Software: file integrity
- Checking file integrity tools
- Checking presence integrity tool [NICHT GEFUNDEN]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NICHT GEFUNDEN]
- Checking for IDS/IPS tooling [NICHTS]
[+] Software: Malware
[+] File Permissions
- Starting file permissions check
/etc/lilo.conf [NICHT GEFUNDEN]
/root/.ssh [NICHT GEFUNDEN]
[+] Home directories
- Checking shell history files [OK]
[+] Kernel Hardening
- Comparing sysctl key pairs with scan profile
- kernel.core_uses_pid (exp: 1) [DIFFERENT]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]








Terminal - tobias@nb: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
* Enable sysstat to collect accounting (no results) [ACCT-9626]
https://cisofy.com/controls/ACCT-9626/
* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/controls/ACCT-9628/
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/controls/FINT-4350/
* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/controls/TOOL-5002/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
https://cisofy.com/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/controls/HRDN-7222/
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)



Ein paar Einzelfälle

- Mount von /tmp
- Kernel sysctl Werte
- Gelöschte Dateien in Verwendung
- Aufräumen von Paketen (purge)
- umask
- Kernel Treiber deaktivieren
- iptables
- Compiler

Mount von /tmp

Sofern Angreifer einen Angriffspunkt auf den Computer haben, versuchen Sie oft auf /tmp mit vorgefertigten Scripten etwas auszuführen.
Ist /tmp nicht ausführbar gemountet, so werden diese nicht funktionieren.
Absichern kann man /tmp in der /etc/fstab mit den zusätzlichen optionen nosuid,nodev,noexec.

```
/dev/mapper/nb--vg-tmp /tmp           ext4    defaults,nosuid,nodev,noexec
   0       2
```

Zusätzlich habe ich auch var/tmp auf /tmp gemountet.

```
/tmp /var/tmp   none    rw,noexec,nosuid,nodev,bind      0       0
```

Ergebnis:

```
- Mount options of /tmp                                    [ HARDENED ]
- Mount options of /var                                    [ NON DEFAULT ]
- Mount options of /var/tmp                                [ HARDENED ]
- /var/tmp is bound to /tmp                                [ OK ]
```

Befehle:

#/var/tmp auf /tmp mounten:

```
mount -o rw,noexec,nosuid,nodev,bind /tmp/ /var/tmp/
```

#/tmp sicherer mounten

```
mount -o remount,noexec,nosuid,nodev /tmp
```

#/etc/fstab neu einlesen

```
mount -a
```

noexec	nicht ausführbar
nosuid	auch Dateien mit SetUID oder SetGID können nicht ausgeführt werden
nodev	keine Gerätedateien auf dieser Partition

Problem:

Der Befehl apt-get upgrade benötigt ein ausführbares /tmp.

Lösung:

In /etc/apt/apt.conf.d/ habe ich eine Datei 99user erstellt und die folgenden Befehle dort hinterlegt.

```
Dpkg::Pre-Invoke {“mount -o remount,exec /tmp”;};
Dpkg::Post-Invoke {“mount -o remount /tmp”;};
```

Kernel sysctl Werte

Prüfen was die Werte eigentlich tun, welche lynis hier vorschlägt.

Beispiel: kernel.core_uses_pid im Kernel-Manual nachschauen.

Bedeutung: Core dumps enthalten die Prozess ID

Fazit: Sicherlich nicht verkehrt $\rightarrow$ Meinetwegen.

Einmaliges ändern mit

```
sysctl kernel.core_uses_pid=1
```

Dauerhaft:
In /etc gibt es die sysctl.conf
Dort kann man die Werte anfügen.
Diese werden beim nächsten Start automatisch gesetzt.

Gelöschte Dateien in Verwendung

Wie finde ich heraus welche das sind?

```
lsof | grep deleted
```

Ist das jetzt ein Problem?
Laut meinen Recherchen nicht. Bei einem frisch gebooteten System auf dem noch nichts aktiv läuft sollte jedoch auch nichts erscheinen.

Erscheint doch etwas könnte das ein Hinweis auf aktive Malware sein.

Aufräumen von Paketen (purge)

Wie finde ich heraus welche Pakete das sind?

```
dpkg -l | grep ^rc | awk '{print $2}'
```

Und wie kann ich diese nun einfach direkt entfernen?

```
apt-get purge $(dpkg -l | grep ^rc | awk '{print $2}')
```

Aber warum das ganze?
Im Falle einer Re-Installation könnten alte Konfigurationsdateien verwendet werden und somit ggf. neue Sicherheitsrelevante Änderungen an diesen fehlen.

Zudem ist das System einfach sauberer und damit übersichtlicher.

umask

Was ist das eigentlich?
umask regelt die Rechte für neu angelegte Dateien.

In Wikipedia gibt es eine gut detaillierte Beschreibung. Es geht um die Rechte für Eigentümer, Gruppe und Andere. Die Werte sind Oktal und je höher der Wert desto weniger Rechte gibt es. 027 ist also sicherer als 022, da es für Andere alle Rechte entzieht.
Im Gegensatz zu chmod heißt 0 hier "alle Rechte".

```
umask 0027
```

oder die von lynis genannten Konfigurationsdateien

Kernel Treiber deaktivieren

Warum eigentlich?
Falls der Rechner stationär ist und keine USB-Sticks oder Firewire zugelassen werden soll.
Ein Kernelmodul weniger ist ein Modul weniger, welches angegriffen werden kann.

Beispiel: firewire
Auf meinem System nicht geladen.

```
lsmod | grep firewire
```

Aber falls, wie deaktiviere ich es dauerhaft?
In /etc/modprobe.d/ eine Datei anlegen mit

```
blacklist firewire_core
```

iptables

Auf einem Rechner, der entweder direkt im Internet erreichbar ist, oder sich in einem unsicheren Netzwerk befindet ist das für mich immer sinnvoll.

Grundsätzlich gilt hierbei, dass **alles verboten** ist was nicht ausdrücklich erlaubt wird.
Aus meiner Sicht sollten hierbei auch die Verbindungen von innen nach außen explizit geregelt werden.

Und mein Desktop Rechner daheim? Das muss jeder für sich selbst entscheiden. Der Desktop-Rechner hätte eine Sicherheitsbarriere mehr.

Damit die iptables beim nächsten Systemstart erhalten bleiben muss man entweder ein Script schreiben und an geeigneter Stelle im System platzieren oder das Paket **iptables-persistent** verwenden.

Compiler

Nicht benötigte Compiler sollten deinstalliert werden, sofern benötigt (z.B. Arch Linux), jedoch nicht für das programmieren selbst, sollten Compiler-Programme nur als root ausgeführt werden können.

Lynis-Beschreibung:
`https://cisofy.com/controls/HRDN-7222/`

Kurzfassung:
Hat ein Angreifer es geschafft sich in meinem System einzuloggen (als ein normaler User) so hat er mit Compilern wohl erweiterte Möglichkeiten Sicherheitsmechanismen des Kernels auszuhebeln.

Und woher weiß ich, was ein Compiler ist?

```
dpkg -l | grep compiler
```

OK und wo ist nun die Datei bei der ich die Rechte anpassen soll?

```
dpkg -L paketname
```

-L steht hier für Listfiles.

Sonstiges

Weitere interessante Punkte, die man sich ggf. anschauen möchte, sind aus meiner Sicht:

- Logfiles
- File Integrity Check
- Security Frameworks
- Chroot
- Host Intrusion Detection Systems
- Rootkits

chroot → firejail

Aktuell prüft Lynis noch nicht, ob Firejail vorhanden ist. Ich kann mir jedoch gut vorstellen, dass dies in Zukunft so sein wird.

Was tut es?
Mit Firejail kann man seine Programme in sog. Sandboxes verfrachten. Wird dieses Programm korrumpiert, so bleibt das restliche System einigermaßen abgeschottet.

Anwendungsgebiete?
Alle Programme, welche direkt mit dem Internet kommunizieren, allen voran der Webbrowser.

Danke für eure Aufmerksamkeit!

Latex-Usetheme:
`http://latex.artikel-namsu.de/english/themes/Marburg.html`