

AAB06: LinuxUserRechte

Fabio Plunser
Betreuer : Walter Mueller

April 3, 2020

Inhaltsverzeichnis

| | | |
|-----------|---|-----------|
| 1 | Arbeite mit Eurem Ubuntu Mint in der VMWare weiter. | 1 |
| 2 | Startet den virtuellen Rechner, meldet Euch an und startet dort ein Terminalfenster. | 1 |
| 3 | Gebt mit cat /etc/passwd die Benutzerdatenbank aus. Was erkennt ihr? | 2 |
| 4 | Legt einen weiteren Benutzer mit eurem Vornamen an: | 3 |
| 4.1 | Wie bekommst Du Hilfe zum useradd-Kommando? | 3 |
| 4.2 | Was versteht man unter Optionen eines Kommandos? | 3 |
| 5 | Vergebt für den Nutzer ein Passwort: | 3 |
| 6 | Zeigt die entsprechenden Teile der Benutzerdatenbank an. | 4 |
| 6.1 | Recherchiert im Internet was ein HASH-Wert ist und was das mit der Datei /etc/shadow zu tun hat. | 4 |
| 6.2 | Shadowfile-Erklärung | 5 |
| 7 | Meldet Euch vom PC aus erneut mit putty (IP Adresse im VMWare-Fenster mit ip addr show ermitteln) aber dieses Mal als Benutzer walter an! | 6 |
| 7.1 | Könnt ihr als walter auch root werden? | 6 |
| 8 | Gebt dem neuen Benutzer zusätzliche Rechte in dem ihr den account zur sudo Gruppe hinzugefügt. Das müsst Ihr natürlich im root Fenster machen! | 7 |
| 8.1 | Prüft das, indem Ihr den Benutzer walter mit grep in der Gruppendatei /etc/group sucht. | 7 |
| 9 | Meldet euch erneut mit putty am Server als walter an und prüft mit dem Kommando groups, zu welchen Gruppen Ihr nun gehört. | 8 |
| 9.1 | Könnt ihr nun als walter mit sudo root werden? | 8 |
| 10 | Gebt mit ls -ld/tmp /bin die Rechte auf den Verzeichnissen /tmp und bin aus. | 9 |
| 10.1 | Interpretiert die Ausgabe und vergleicht diese mit der Ausgabe des grafischen Dateiexplorers im Tab Permissions | 9 |
| 11 | Legt als Benutzer walter mit mkdir ein Verzeichnis unter /tmp an und überprüft die Eigenschaften dieses Verzeichnisses. | 9 |
| 11.1 | Legt im Verzeichnis die Datei an: | 9 |
| 12 | Könnt ihr die Datei im grafischen explorer öffnen, könnt ihr dies ändern/überschreiben? | 10 |
| 13 | Ändert als walter (in putty) die Rechte des Verzeichnisses mit | 10 |
| 13.1 | Wie wirkt sich das auf die Sichtbarkeit im explorer aus? | 10 |
| 14 | Gebt den ursprünglichen Benutzer eures Linux-Rechners zusätzlich die Gruppe walter. | 11 |
| 14.1 | Meldet Euch mit "Logout" ab und erneut an. | 11 |
| 14.2 | Was bewirkt das und was gilt nun für die Zugriffsrechte des ursprünglichen Nutzers? | 11 |

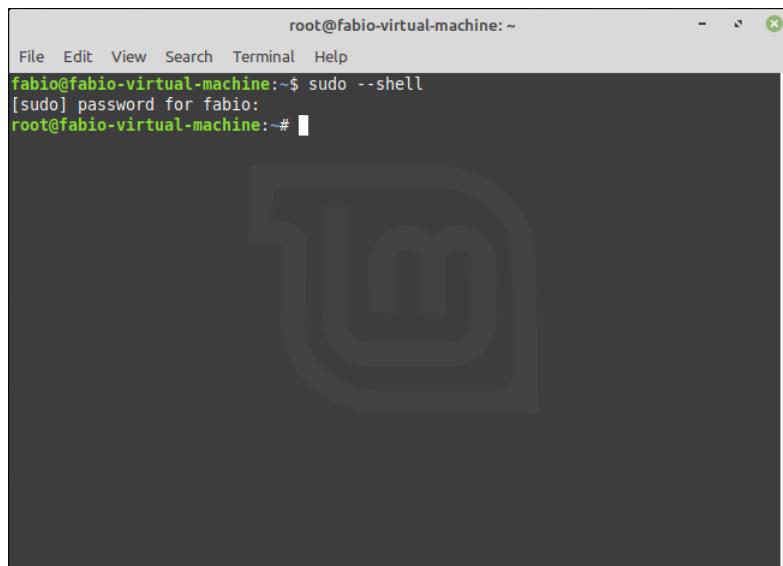
Abbildungsverzeichnis

| | | |
|----------|---|----------|
| 1 | Root-Rechte | 1 |
| 2 | User-Datenbank | 2 |
| 3 | User-hinzufügen | 3 |
| 4 | User-hinzufügen-passwort | 3 |
| 5 | Grep-Walter | 4 |

| | | |
|----|-----------------------------------|----|
| 6 | Shadow-Hash | 4 |
| 7 | Shadow-File-Erklärung | 5 |
| 8 | SSH-Verbindung | 6 |
| 9 | Sudo-Benutzer | 7 |
| 10 | Sudo-Benutzer | 7 |
| 11 | SSH-Groups | 8 |
| 12 | SSH-Root | 8 |
| 13 | ls-ld/temp /bin | 9 |
| 14 | SSH-mkdir | 9 |
| 15 | SSH-echo "Hallo Walter" | 9 |
| 16 | Erstellte-Datие | 10 |
| 17 | SSH-chmod 770 | 10 |
| 18 | Chmod 770 | 10 |
| 19 | Gruppe-Walter | 11 |
| 20 | Gruppe-Walter | 11 |

- 1 Arbeite mit Eurem Ubuntu Mint in der VMWare weiter.**
- 2 Startet den virtuellen Rechner, meldet Euch an und startet dort ein Terminalfenster.**

Gebt dort das Kommando `sudo --shell` ein. Ihr bekommt einen Promt (=Eingabeaufforderung) mit einem # → Ihr habt nun root-(=Administrator) Rechte. (Screenshot)



The screenshot shows a terminal window titled "root@fabio-virtual-machine: ~". The window has a standard Linux terminal interface with a dark background and light-colored text. At the top, there is a menu bar with options: File, Edit, View, Search, Terminal, and Help. Below the menu bar, the prompt "root@fabio-virtual-machine: ~" is displayed in green. The user then types the command "sudo --shell", followed by "[sudo] password for fabio:", both in green. After entering the password, the prompt changes to "#", which is also in green, indicating that the user now has root privileges. The terminal window is set against a background featuring a large, semi-transparent watermark of the HTL logo.

Figure 1: Root-Rechte

3 Gebt mit cat /etc/passwd die Benutzerdatenbank aus. Was erkennt ihr?

```
root@fabio-virtual-machine:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
cups-pk-helper:x:106:112:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
kernoops:x:107:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
rtkit:x:108:113:RealtimeKit,,,:/proc:/usr/sbin/nologin
avahi-autoipd:x:109:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:111:117:systemd core dump processing,,,:/run/systemd:/usr/sbin/nologin
ntp:x:112:118::/nonexistent:/usr/sbin/nologin
lightdm:x:113:119:Light Display Manager:/var/lib/lightdm:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
saned:x:115:122::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:116:123:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:118:125:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:120:126:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
hplip:x:121:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:122:128::/var/lib/geoclue:/usr/sbin/nologin
fabio:x:1000:1000:Fabio,,,:/home/fabio:/bin/bash
root@fabio-virtual-machine:~#
```

Figure 2: User-Datenbank

4 Legt einen weiteren Benutzer mit eurem Vornamen an:

useradd –create-home –comment 'dein Name' –shell /bin/bash walter
(Screenshot)

```
root@fabio-virtual-machine:~# useradd --create-home --comment 'Plunser' --shell /bin/bash walter
```

Figure 3: User-hinzufügen

4.1 Wie bekommst Du Hilfe zum useradd-Kommando?

useradd -h

4.2 Was versteht man unter Optionen eines Kommandos?

alle –”befehle”

5 Vergebt für den Nutzer ein Passwort:

passwd walter

```
root@fabio-virtual-machine:~# passwd walter
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@fabio-virtual-machine:~# █
```

Figure 4: User-hinzufügen-passwort

6 Zeigt die entsprechenden Teile der Benutzerdatenbank an.

Erklärung: grep durchsucht Textdateien nach Zeichenketten.
grep walter /etc/passwd /etc/shadow
(Screenshot)

```
root@fabio-virtual-machine:~# grep walter /etc/passwd /etc/shadow
/etc/passwd:walter:x:1004:1004:Plunser:/home/walter:/bin/bash
/etc/shadow:walter:$6$UhDQLNO.$n2P1umqXPYMsQSJTQZL9eKhGalCCm8bU9eChw59/frX5GewkVMc4mkPI6EPEhD8/.ZFqHm00EKLGrfB.In/EF/:18355:0:99999:7:::
```

Figure 5: Grep-Walter

Walter hat UID: 1004 und GID: 1004.

Da ich vorher schon einen User erstellt habe aber nicht nach Vorgabe. Diesen habe ich wieder gelöscht daher besitzt dieser User nicht wie üblich die IDs 1001 sondern 1004. Warum es nicht 1002 oder 1003 ist kann mir nicht erklären.

6.1 Recherchiert im Internet was ein HASH-Wert ist und was das mit der Datei /etc/shadow zu tun hat.

```
/etc/shadow:walter:$6$UhDQLNO.$n2P1umqXPYMsQSJTQZL9eKhGalCCm8bU9eChw59/frX5GewkVMc4mkPI6EPEhD8/.ZFqHm00EKLGrfB.In/EF/:18355:0:99999:7:::
```

Figure 6: Shadow-Hash

Die Hash ist eine Einwegfunktion die aus dem normalen Passwort Text, eine Lange Zahl erstellt. Diese Zahl wird jedes mal beim einloggen neu berechnet. Vor der Hash Zahl gibt es eine Zufallszahl für Sicherheit und um Benutzer mit dem gleichen Passwort zu unterscheiden.

6.2 Shadowfile-Erklärung



(Fig.01: /etc/shadow file fields)

1. **Username**: It is your login name.
2. **Password**: It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to \$id\$salt\$hashed, The \$id is the algorithm used On GNU/Linux as follows:
 1. **\$1\$** is MD5
 2. **\$2a\$** is Blowfish
 3. **\$2y\$** is Blowfish
 4. **\$5\$** is SHA-256
 5. **\$6\$** is SHA-512
3. **Last password change (lastchanged)**: Days since Jan 1, 1970 that password was last changed
4. **Minimum**: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum**: The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn**: The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive**: The number of days after password expires that account is disabled
8. **Expire**: days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

Figure 7: Shadow-File-Erklärung

Quelle: <https://www.cyberciti.biz/faq/understanding-etcshadow-file/>

7 Meldet Euch vom PC aus erneut mit putty (IP Adresse im VMWare-Fenster mit ip addr show ermitteln) aber dieses Mal als Benutzer walter an!

7.1 Könnt ihr als walter auch root werden?

Es muss dafür mit:

apt-get install openssh-server ssh installiert werden.

um ssh zu aktivieren: systemctl restart ssh.

```
• MobaXterm 10.9 •  
(SSH client, X-server and networking tools)  
► SSH session to walter@192.168.198.128  
• SSH compression : ✓  
• SSH-browser : ✓  
• X11-forwarding : ✓ (remote display is forwarded through SSH)  
• DISPLAY : ✓ (automatically set on remote server)  
► For more info, ctrl+click on help or visit our website  
usr/bin/xauth: timeout in locking authority file /home/walter/.Xauthority  
walter@fabio-virtual-machine:~$
```

Figure 8: SSH-Verbindung

- 8 Gebt dem neuen Benutzer zusätzliche Rechte in dem ihr den account zur sudo Gruppe hinzugefügt. Das müsst Ihr natürlich im root Fenster machen!

```
sudo:x:27:fabio
```

Figure 9: Sudo-Benutzer

mit less /etc/group: walter ist noch nicht in der sudo Gruppe

mit: usermod -groups sudo walter zu sudo gruppe hinzufügen

- 8.1 Prüft das, indem Ihr den Benutzer walter mit grep in der Gruppendatei /etc/group sucht.

```
root@fabio-virtual-machine:~# grep walter /etc/group
sudo:x:27:fabio,walter
walter:x:1004:
```

Figure 10: Sudo-Benutzer

9 Meldet euch erneut mit putty am Server als walter an und prüft mit dem Kommando groups, zu welchen Gruppen Ihr nun gehört.

```
walter@fabio-virtual-machine:~$ groups  
walter sudo  
walter@fabio-virtual-machine:~$ █
```

Figure 11: SSH-Groups

Gruppe: walter und Gruppe: Sudo

9.1 Könnt ihr nun als walter mit sudo root werden?

Ja

```
walter@fabio-virtual-machine:~$ sudo -i  
[sudo] password for walter:  
root@fabio-virtual-machine:~# █
```

Figure 12: SSH-Root

10 Gebt mit ls -ld /tmp /bin die Rechte auf den Verzeichnissen /tmp und bin aus.

10.1 Interpretiert die Ausgabe und vergleicht diese mit der Ausgabe des grafischen Dateiexplorers im Tab Permissions

```
root@fabio-virtual-machine:~# ls -ld /tmp /bin
drwxr-xr-x 2 root root 4096 Mar 23 21:05 /bin
drwxrwxrwt 15 root root 4096 Apr  3 08:58 /tmp
```

Figure 13: ls-ld/temp /bin

drwxr -xr -x:

dr = directory → zeigt dass ein Ordner ist

wxr = write, execution/changedir, read für Besitzer der Datei

-xr = User in der Gruppe root dürfen executen/changedir und lesen

-x = execution/changedir für alle User die nicht in der root Gruppe sind

3 Blöcke rwx für Besitzer der Datei, für alle in der Gruppe root, für den Rest

drwxrwxrwt: 3er Blöcke wxr wxr wt

11 Legt als Benutzer walter mit mkdir ein Verzeichnis unter /tmp an und überprüft die Eigenschaften dieses Verzeichnisses.

```
walter@fabio-virtual-machine:~$ mkdir /tmp/walter
```

Figure 14: SSH-mkdir

11.1 Legt im Verzeichnis die Datei an:

```
echo "Hallo walter" > /tmp/xxx/WalterDatei
```

```
walter@fabio-virtual-machine:~$ echo "Hallo Walter" >/tmp/walter/WalterDatei
```

Figure 15: SSH-echo "Hallo Walter"

12 Könnt ihr die Datei im grafischen explorer öffnen, könnt ihr dies ändern/überschreiben?

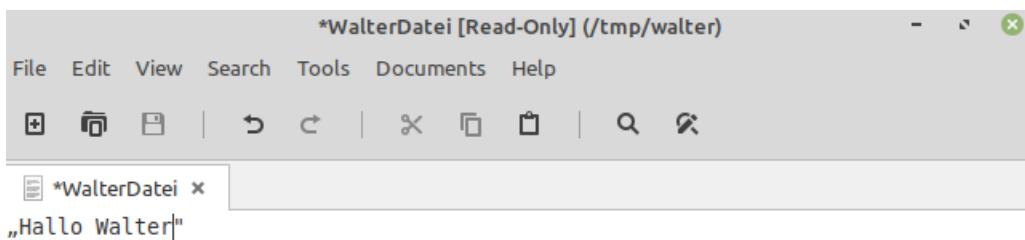


Figure 16: Erstellte-Datие

Wie es auf dem Bild zu erkennen ist, darf jeder andere Benutzer die Datei zwar lesen aber nicht verändern. Nur Root und Benutzer Walter dürfen die Datei ändern und User mit sudo rechten in der cmd line.

13 Ändert als walter (in putty) die Rechte des Verzeichnisses mit

```
chmod 770 /temp/xxx bzw chmod o-rwx /tmp/xxx
```

```
root@fabio-virtual-machine:~# chmod 770 /tmp/walter
```

Figure 17: SSH-chmod 770

13.1 Wie wirkt sich das auf die Sichtbarkeit im explorer aus?

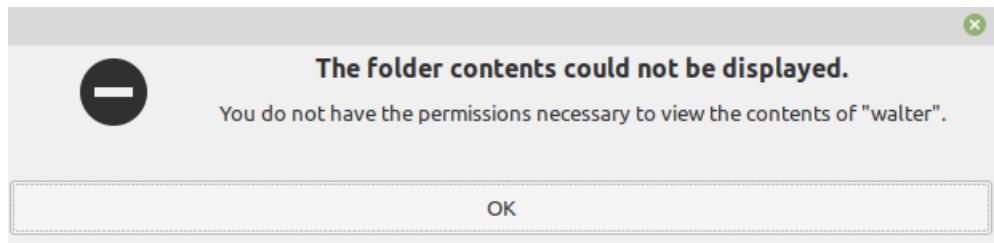


Figure 18: Chmod 770

Ich darf nicht mehr auf den Ordner zugreifen bzw, ich darf nicht mehr sehen was im Ordner drinnen ist.

14 Gebt den ursprünglichen Benutzer eures Linux-Rechners zusätzlich die Gruppe walter.

```
root@fabio-virtual-machine:~# usermod --groups walter fabio
```

Figure 19: Gruppe-Walter

```
root@fabio-virtual-machine:~# grep walter /etc/group
sudo:x:27:walter
walter:x:1004:fabio
```

Figure 20: Gruppe-Walter

Benutzer Fabio ist jetzt in der Gruppe Walter.

14.1 Meldet Euch mit "Logout" ab und erneut an.

14.2 Was bewirkt das und was gilt nun für die Zugriffsrechte des ursprünglichen Nutzers?

Ich darf wieder die Datei anschauen und habe keine Einschränkungen auf die erstellte Datei.