|  |  |  |  |
| --- | --- | --- | --- |
| **Übungsprotokoll**  **ITSI – Informationstechnologie Sicherheit** | | | |
|  | **Übungsdatum:**  02.12.2020 | **Klasse:**  2AHIT | **Name:**  Felix Schneider |
| **Abgabedatum:**  02.12.2020 | **Gruppe:**  ITSI2 | **Note:** |
| **Leitung:**  Jürgen HAUPTMANN | **Mitübende:**  - | | |
| **Übungsbezeichnung**:  Aufsetzung Linux + Übung 1 + 2 + 3 + NFT richtig einstellen | | | |

**Inhaltsverzeichnis:**

[1 Aufgabenstellung 2](#_Toc492801999)

[2 Übungsdurchführung 2](#_Toc492802002)

[3 Ergebnisse 7](#_Toc492802003)

[4 Kommentar 7](#_Toc492802005)

# Aufgabenstellung

Aufsetzung Linux mithilfe der virtuellen Maschine.

Bsp1.:

1. Den PC klonen.
2. Die virtuellen PCs in ein internes Netzwerk geben.
3. Als Root anmelden: su -
4. Netzwerk konfigurieren.
5. Überprüfungen mit dem #ip addr Befehl.
6. Falls eine andere IP drinnen steht diese mit dem #ip addr flush <interface> löschen.
7. Überprüfen der Verbindung mittels ping Befehl.

Bsp2.:

1. Die virtuellen PCs in ein internes Netzwerk geben.
2. PC1 und PC2 ein Gateway zuweisen.
3. Netzwerk konfigurieren.
4. Überprüfungen mit dem #ip addr Befehl.
5. Falls eine andere IP drinnen steht diese mit dem #ip addr flush <interface> löschen.
6. Versuchen sie das Gateway zu pingen.
7. PC3 Wireshark installieren. #apt install wireshark

NFT einstellen:

1. Damit NFT überhaupt funktioniert, muss wireshark installiert sein. (Nr7 von Bsp2)
2. NFT erstellen
3. NFT konfigurieren
4. Überprüfung der richtigen Konfiguration mithilfe des Pingens
5. Mithilfe Wireshark kann man nun PC1 und PC2 überwachen.

# Übungsdurchführung

Benennen Sie Ihre Virtuelle Maschine, wie Sie wollen. Und wählen Sie anschließend den Typ aus, also, ob das ein Linux oder Windows oder … -Betriebssystem werden soll. Bei der Version wählen Sie am besten 64-Bit aus. Die VM benötigt mind. 2048MB RAM Speicher und mind. 8GB – 20GB Hauptspeicher.

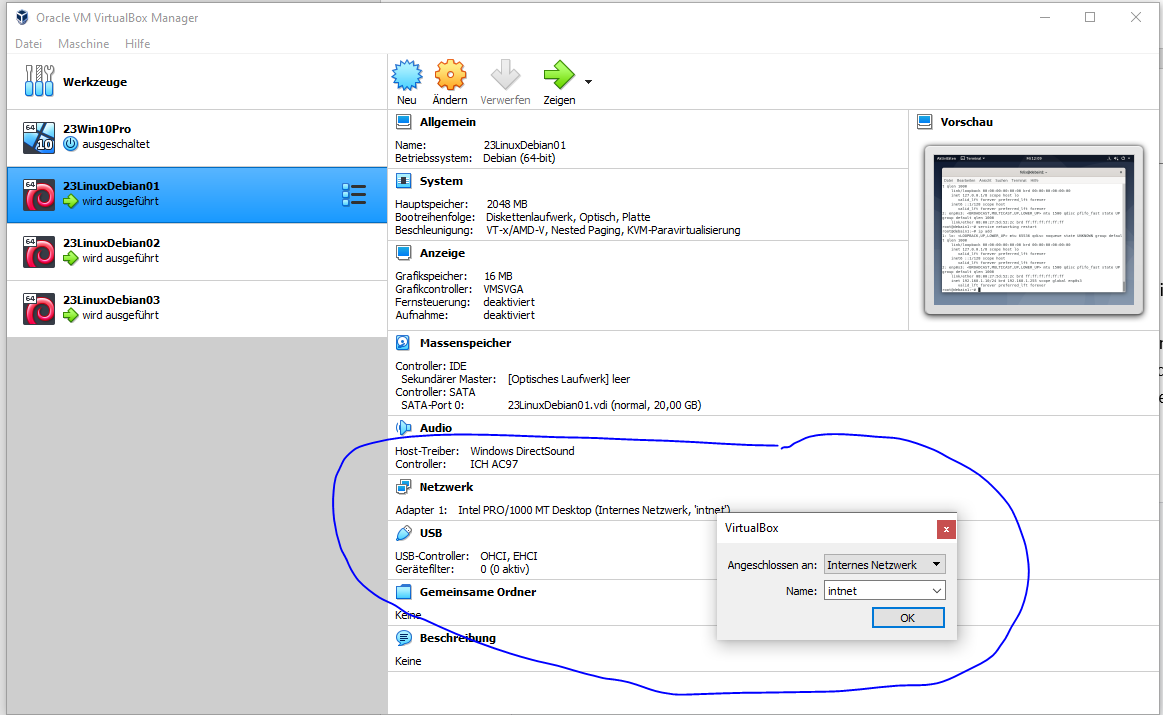
Nachdem die Maschine erstellt wurde, können Sie sie starten. Wenn Sie nach dem Startpfad gefragt werden, wählen Sie die ISO-Datei aus, die Sie auf dem D-Laufwerk gespeichert haben sollten. Die Sprache müssen Sie ebenfalls selbst auswählen. Dann richtet die VM einiges ein und danach werden Sie nach einem Benutzernamen gefragt, Sie brauchen keinen. Anschließend müssen Sie ein root-Passwort, und einen Benutzer erstellen. Bei der Partition wählen Sie 4GB Swap- (das doppelte von RAM-Speicher) und den Rest als Hauptspeicher.

Wenn Sie die VM klonen wollen, schließen Sie vorerst die VM. Anschließend machen Sie einen Rechtsklick auf die VM und klicken auf klonen. Dann können Sie den Namen ändern und

WICHTIG!... Sie müssen eine neue MAC-Adresse erstellen, indem Sie „neue MAC-Adresse erstellen“ auswählen. Anschließend klonen Sie die VM.

**Netzwerk für VMs**

Der erste Schritt, um untereinander pingen zu können, ist in den VM Netzwerk-Einstellungen von NAT auf internes Netzwerk umzustellen.



Diesem können Sie einen beliebigen Namen geben. Anschließend VMs starten. Terminal öffnen. In der Datei /etc/network/interfaces müssen Sie ganz unten folgenden Code hinzufügen. Dabei müssen Sie beachten, dass der Name der Netzwerkinterface Card richtig ist. Diesen können Sie herausfinden, indem Sie den Befehl: **dmesg** in den Terminal eingeben. Vor NIC steht der richtige Name.

auto eth0

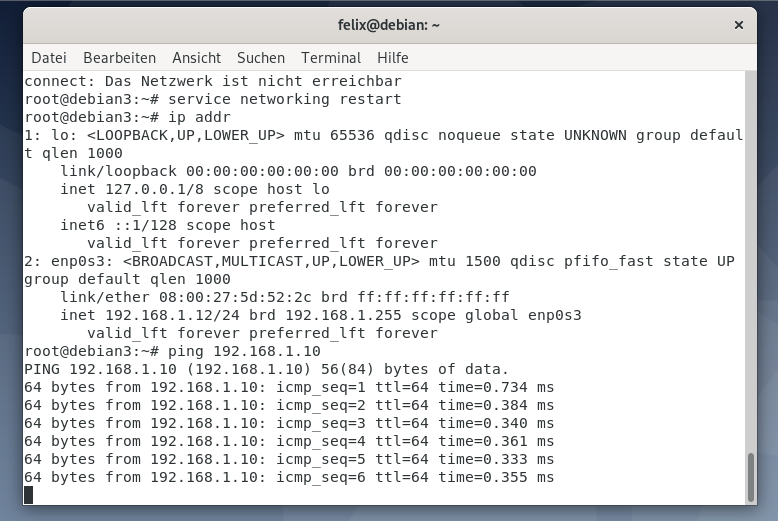
iface eth0 inet static

address 192.168.1.1

netmask 255.255.255.0

Nachdem Sie diesen Code in der Datei **/etc/network/interfaces** hinzugefügt haben, speichern Sie die Datei, gehen Sie zurück in den Terminal und geben Sie den Befehl **service networking restart** ein. Wenn keine Fehler auftreten, haben Sie den Code richtig abgeschrieben und können im besten Fall pingen.

Machen Sie diesen Vorgang bei mind. 2 VM!



**Pingen eines Rechners (wirkt wie Router; ist mit Internet verbunden)**

Als allererstes muss in der VB einer der 3 Computer ausgewählt werden, der den „Router“ spielt. Bei diesem muss unter den Einstellungen 🡪 Netzwerk ein Adapter auf NAT und zwei weitere auf internes Netzwerk gestellt werden (hierbei einen sinnvollen Namen vergeben). Bei Rechner 1 muss dann in den Netzwerkeinstellungen ebenfalls Netzwerk eingestellt sein (der Name sollte mit dem des „Routers“ übereinstimmen). Derselbe Prozess beim 2. PC.

Nun können Sie die VM (alle drei) starten.

Der Terminal muss bei jeder VM Superuserrechte haben (**su -**). Nun müssen Sie in der Datei **/etc/network/interfaces** einiges ändern:

1. Beim „Router“:

Hier müssen die IP-Adressen der Gateway-Adressen auf den beiden PCs mit den IP-Adressen in der Datei übereinstimmen.

auto enp0s3

iface enp0s3 inet dhcp

auto enp0s8

iface enp0s8 inet static

address 192.168.1.10

netmask 255.255.255.0

auto enp0s9

iface enp0s9 inet static

address 192.168.2.10

netmask 255.255.255.0

1. PC1:

auto enp0s3

iface enp0s3 inet static

address 192.168.1.11

netmask 255.255.255.0

gateway 192.168.1.10

1. PC2:

auto enp0s3

iface enp0s3 inet static

address 192.168.2.11

netmask 255.255.255.0

gateway 192.168.2.10

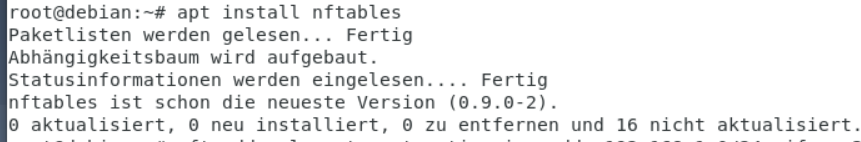
Den Namen des Netzwerkadapters (**enp0s3**) kann man herausfinden, indem man im Terminal **dmesg** eingibt.

Nachdem diese drei Dateien gespeichert wurden, kann das Network restarted werden mit dem Befehl service networking restart eingibt (hierbei ist wichtig, dass man su **-** und nicht nur su geschrieben hat). Anschließend kann man vom PC aus den Router pingen.

Schlussendlich muss noch mit dem Befehl **apt install wireshark** das PC3 Wireshark installiert werden.

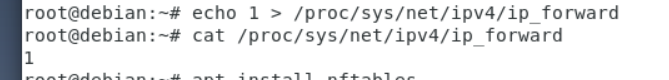
**NFT**

Um NFT zu installieren muss man Superuser am „RouterPC“ sein. Anschließend kann man den Befehl #apt install nftables eingeben, um die Installation durchzuführen.



Ich hatte dies schon installiert.

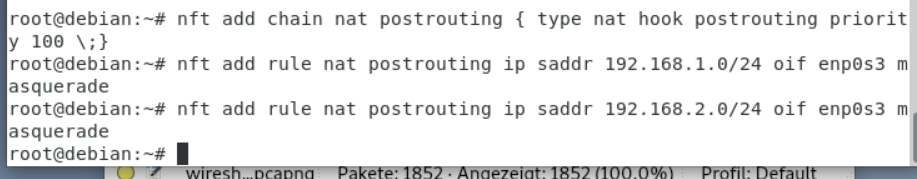
WICHTIG! In der Datei /proc/sys/net/ipv4/ip\_forward muss eine 1 drinnenstehen, damit die PCs Internetzugriff bekommen können. Dieser Befehl muss jedes Mal nach dem Neustart durchgeführt werden. Mithilfe von echo können Sie Dateien sehr schnell umschreiben/ändern.



Um NFT richtig zu konfigurieren gibt man folgende Befehle ein:

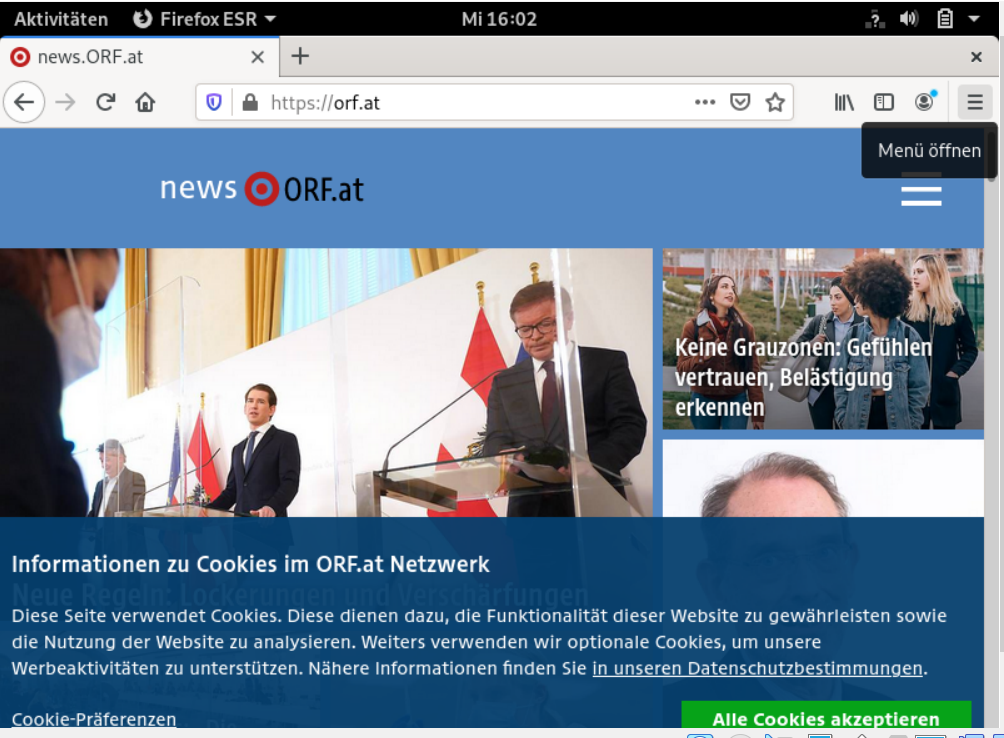
* nft add table nat
* nft add chain nat postrouting { type nat hook postrouting priority 100 \;}
* nft add rule nat postrouting ip saddr 192.168.1.0/24 oif enp0s3 masquerade



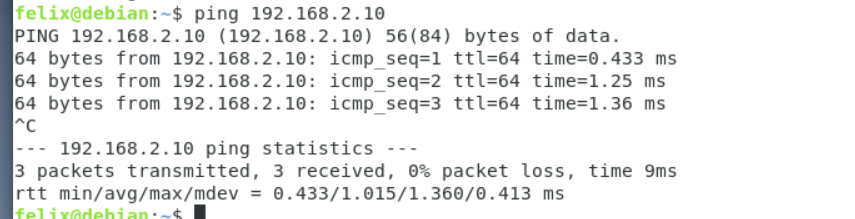


Beachten Sie bitte, dass Sie den letzten Befehl für alle PCs, die im Netzwerk Internetzugriff haben sollen, machen müssen! Außerdem müssen Sie statt „enp0s3“ den richtigen Namen verwenden (dmesg kann unter Sudorechte herausfinden, wie der Name lautet).

Wenn alles richtig funktioniert hat und keine Fehlermeldungen gekommen sind, dann testen Sie NFT, indem Sie auf einem PC ins Internet gehen und auf dem Router in der Wireshark-App mitschauen können, welche IP-Adresse zu anderen IP-Adressen schickt (dies ist in einer Tabelle als „Protokoll“ dargestellt, wenn Sie auf das Shark-Symbol klicken).



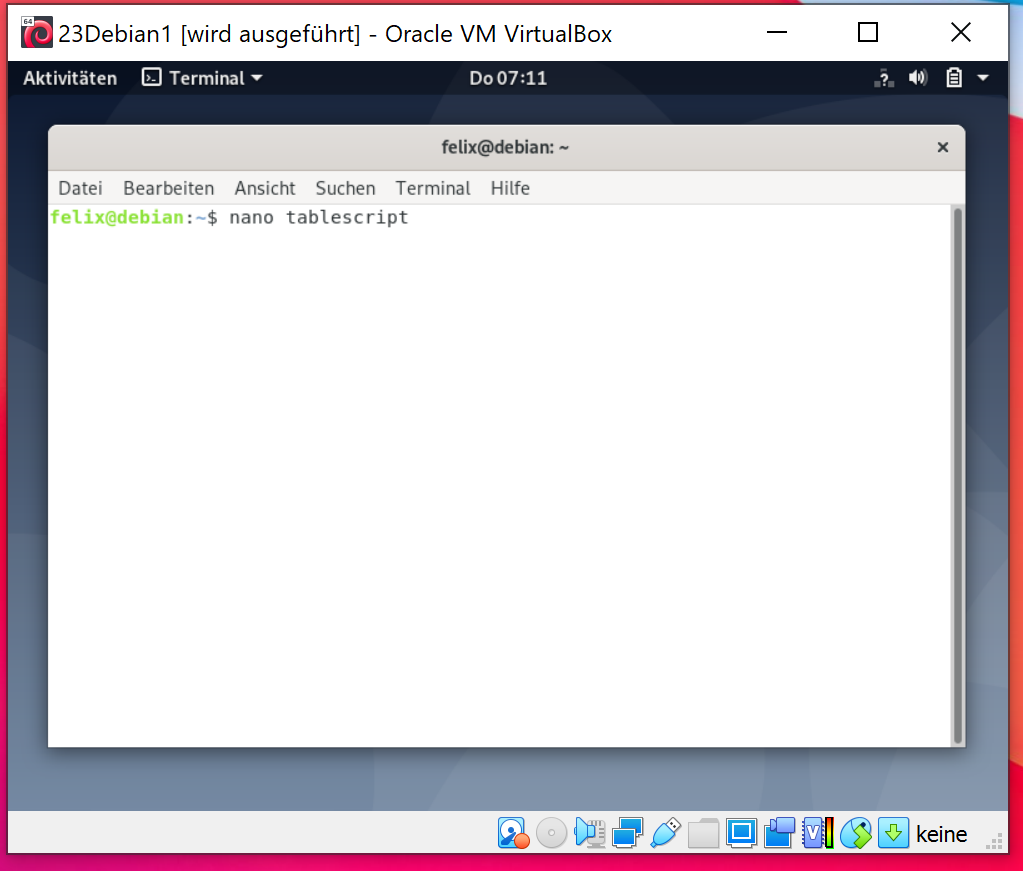
Internetzugriff erfolgreich!



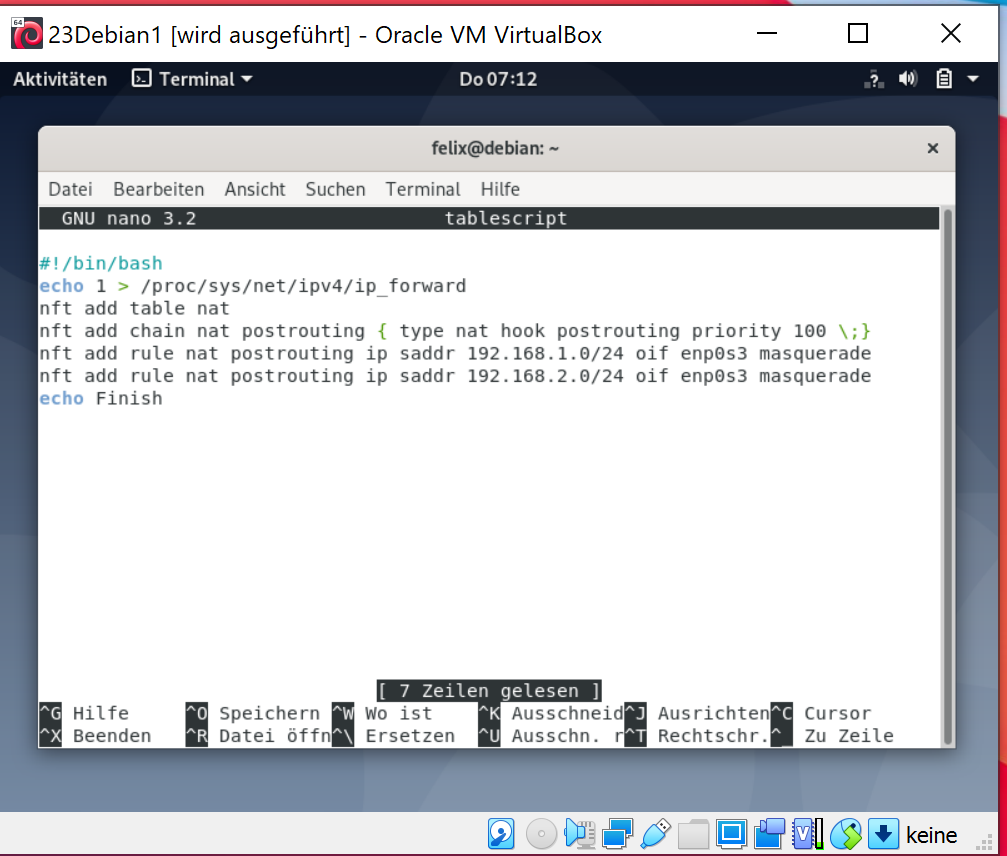
Außerdem ist das Pingen zwischen 2 PCs nun auch möglich.

**Auto-Datei**

Wenn Sie möchten, dass Sie nach dem Neustart der Maschinen nicht all diese Zeilen an Code nochmals schreiben müssen, um Internetzugang an den PCs zu erhalten, dann machen Sie am besten eine txt-Datei in irgendeinem Verzeichnis (Hauptsache Sie wissen noch, wo die Datei liegt).

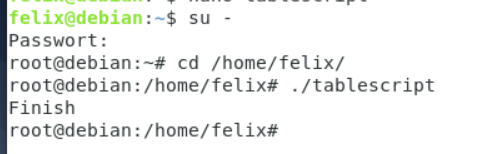


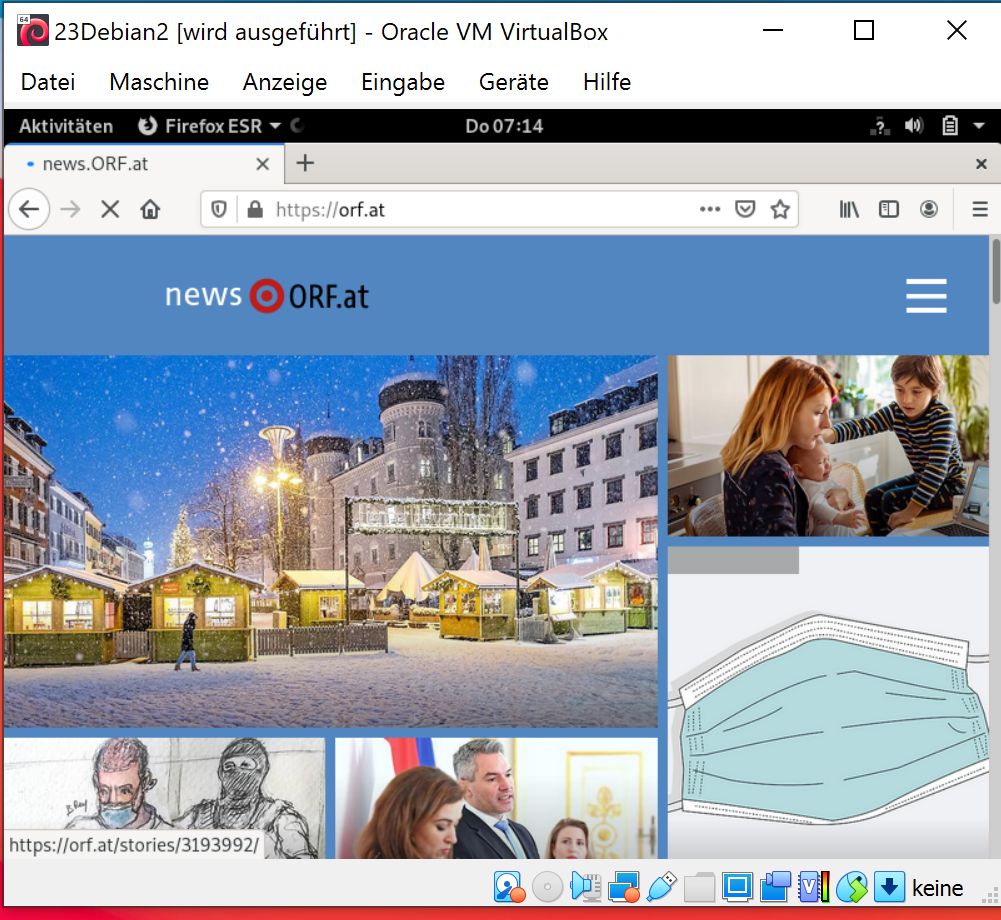
Ich z.B.: habe eine tablescript Datei im /home/felix Ordner erstellt, wo folgendes drinnensteht:



Wenn diese Datei ausgeführt wird (kann nur vom Root ausgeführt werden), dann ist das so, als würde man Zeile für Zeile in das Terminal reinschreiben und nach dem Ende einer Zeile auch ein Enter drücken. Somit werden diese Befehle korrekt ausgeführt und wenn alles funktioniert hat, schreibt die Console am Schluss noch Finish hinzu (eine kleine Überprüfung, ob alles funktioniert hat).

Nun muss man sich im Terminal nur noch als Root anmelden, der auch Programme als Root ausführen kann (su -) und anschließend in das Verzeichnis /home/felix (bei mir zumindest). Wenn man nun die Datei aufzuft mit dem Befehl ./tablescript, dann sollte Finish dastehen und die PCs haben Internet.





# Ergebnisse

Das Pingen war immer erfolgreich.

# Kommentar

Wichtig ist der Inhalt der Dateien /etc/network/interfaces auf jeder VM. Wenn hierbei nämlich ein Rechtschreibfehler oder ähnliches passiert, funktioniert das Pingen nicht.