Institut für Informatik
Dr. Andreas Paul

Technische Universität München
WiSe 2017 / 2018

# Praktikum Systemadministration

Aufgabenblatt 2

## 1. Einrichten eines Netzwerkes

In dieser Aufgabe gilt es ein Netzwerk einzurichten, über das die von Ihnen im Rahmen des ersten Aufgabenblattes installierten Systeme miteinander kommunizieren können.

### Verbindung zwischen virtuellen Maschinen

Auf dem Praktikumsserver (`psa.in.tum.de`) wurden die virtuellen Maschinen so konfiguriert, daß sie prinzipiell über ihren zweiten Netzwerk–Adapter untereinander kommunizieren können. Je nach installiertem Betriebssystem kann die Reihenfolge der Netzwerk–Adapter bei der Nummerierung bzw. Anzeige variieren. Gemeint ist der Adapter, der nicht bereits mit einer IP–Adresse (10.0.2.15) durch die DHCP Funktion der Virtualisierungsumgebung vorkonfiguriert ist.

Diese zweiten Adapter sollen in den virtuellen Maschinen eines Teams nun mit IP–Adressen konfiguriert werden, die im selben Subnetz liegen. Dafür sind den Teams die Subnetze

`192.168.<`*TeamNr*`>.0/24`

zugeordnet. Alle Maschinen eines Teams sollen daraufhin untereinander `ping`bar sein, d.h. sie sehen und antworten auf die ICMP–Echo Pakete der anderen Maschinen im selben Subnetz.

Verwenden Sie für die Konfiguration der Netzwerk–Adapter das Kommando `ifconfig` oder `ip` und dokumentieren Sie wo Sie welche Kommandos (inklusive Aufrufparameter) ausgeführt haben.

### Verbindung zwischen Subnetzen

Damit die virtuellen Maschinen zweier Teams untereinander kommunizieren können soll zwischen genau einer VM des einen Teams und einer VM des anderen Teams ein Netzwerk konfiguriert werden. Die dafür zu verwendenden Verbindungs–Subnetze ergeben sich aus den Nummern der beteiligten Teams:

`192.168.<`*1.TeamNr*`><`*2.TeamNr*`>.0/24`

Damit die Zuordnung eindeutig ist soll **immer**

<*1.TeamNr*> > <*2.TeamNr*>

gelten. Falls die so gewonnene Nummer des Subnetzes vierstellig wird, ersetzen Sie die beiden mittleren Ziffern durch deren Summe (aus 1210, dem Verbindungs–Subnetz der Teams 10 und 12 wird so zum Beispiel das Subnetz 130).

Vereinbaren Sie mit einem anderen Team die Verbindung Ihrer jeweiligen Subnetze. Wählen Sie jeweils eine Ihrer Team–VMs aus und konfigurieren Sie deren zweiten Adapter mit einer zusätzlichen, IP–Adresse aus dem Verbindungs–Subnetz (`ifconfig` bzw. `ip`). Ergänzen Sie die Routing–Tabelle der anderen VM(s) Ihres Teams um einen Eintrag, der es Ihnen erlaubt über das Verbindungs–Subnetz mit allen VMs des anderen Teams zu kommunizieren.

Verwenden Sie die Kommandos `ifconfig`, `route` bzw. `ip` und dokumentieren Sie, so wie im letzten Schritt, wo welche Kommandos ausgeführt wurden.

Schaffen Sie so lange weitere Verbindungen zu den Subnetzen der anderen Teams, bis alle VMs aller Teams mit allen anderen VMs kommunizieren können.

## 2. Firewall

Richten Sie auf Ihrer virtuellen Maschine eine lokale Firewall ein (z.B. `iptables`). Achten Sie darauf, daß die dadurch realisierten Einschränkungen für die Benutzer Ihres Systems möglichst transparent sind und ein *normales* arbeiten nicht behindert wird. Das heißt zum Beispiel, daß DNS und *normales* surfen im Web möglich sein sollte. Das *normale* surfen im Netz ist dabei in der Regel nur über einen Proxy–Server möglich. Verwenden sie ggf. `proxy.in.tum.de` (Port 8080) als systemweiten Proxy–Server.

### TCP Verbindungen von außen zur VM (incoming)

Konfigurieren Sie Ihre Firewall so, daß eingehende Verbindungen zu Ihrer VM auf Port 22 (Secure Shell) möglich sind.

Ebenso sollen Port 80 (http) und Port 443 (https) erreichbar sein (auch wenn zu diesem Zeitpunkt darauf noch keine Dienste laufen). Achten Sie darauf, daß die Firewall bei diesen beiden Ports keine Informationen über die Verbindungen speichert (*stateless*).

Abgesehen von den genannten Ausnahmen (Ports 22, 80 und 443) sollen alle anderen Netzwerk–Ports von außen **nicht** erreichbar sein.

Versichern Sie sich, daß Ihre Firewall korrekt funktioniert.

### TCP Verbindungen von der VM nach außen (outgoing)

Von der VM ausgehende Netzwerkverbindungen sollen ebenfalls beschränkt sein.

Innerhalb des Haus–Netzes der Fakultät für Informatik (131.159.0.0/16 Class B) sowie der im ersten Teil dieser Aufgabe eingerichteten Subnetze sollen alle Adressen für beliebige Verbindungen erreichbar sein (insbesondere ssh Verbindungen müssen möglich sein). Darüber hinaus sollen nur ganz bestimmte externe Adressen erreichbar sein (z.B. die Update–Server ihres Betriebssystems). Konfigurieren Sie dementsprechend mindestens eine externe Adresse in Ihrer Firewall.

### Internet Control Message Protocol (ICMP)

Richten Sie die Firewall so ein, daß ICMP uneingeschränkt möglich ist.

## 3. Testen der Konfiguration

Schreiben Sie ein Shell–Skript `test_PSA_02.sh`, das die wesentlichen Einstellungen und Aspekte der Konfiguration testet bzw. anzeigt. Legen Sie dieses Shell–Skript im HOME-Verzeichnis der `root`–Kennung auf den jeweiligen VMs ab.

## 4. Dokumentation

Dokumentieren Sie Ihre Lösung nachvollziehbar im Wiki unter
https://psa.in.tum.de/index.php/PSA2017WiSeDokumentationDerAufgaben