Übungsblatt 03 – Netzwerkinfrastruktur Teil 1

Aufgabe A - Setup

Bevor es richtig losgeht müssen sie folgende Vorbereitungen treffen.

1. Sie benötigen drei VMs. Hierfür sollten sie ein minimales *freeBSD*, ein minimales *Linux* [1] und das *freeBSD* mit grafischer Oberfläche (GUI) bereithalten.
   Importieren Sie die VMs. Hierfür habe ich ein kurzes Video vorbereitet: https://mediathek.htw-berlin.de/video/Virtualbox-Network-Preperations-amp-Cloning/276fab5dbd663d7589d12a30234da003 [2]

2. Ändern sie die Hostname der VMs! Jede VM sollte einen individuellen Namen bekommen. Später empfiehlt es sich die Namen den Funktionalitäten zuzuordnen oder ein festes Namensschema zu nutzen.

3. Für *freeBSD*: https://www.cyberciti.biz/faq/howot-freebsd-change-hostname-without-rebo

4. Für Linux: https://www.cyberciti.biz/faq/linux-change-hostname/

Aufgabe B - Anzeige der bestehenden Netzwerkkonfiguration

Bevor sie ein eigenes kleines Netzwerk einrichten, sollen sie sich mit den dafür Notwendigen Tools vertraut machen. Daher soll zunächst die bestehende Netzwerkkonfiguration untersucht werden.
Eine aktive Netzwerkverbindung ist Voraussetzung für die Kommunikation zwischen Rechnern in einem Netzwerk. Jeder Rechner muss hierfür eine passende IP-Adresse haben, mit der er andere Rechner bzw. Zwischenknoten im Netz erreichen kann. Wenn Sie dem Tutorial gefolgt sind, haben die VMs jeweils drei Interfaces. Eines davon hat Zugang zu einem DHCP-Netzwerk. Somit auch eine automatisch zugeordnete IP-Adresse.

1. Starten sie eine *freeBSD* und Linux VM.

2. Nutzen Sie für die nachfolgende Aufgabe beide Tools (ip addr (Linux) als auch ifconfig (*freeBSD*))

3. Lassen Sie sich die aktuelle IP-Adresskonfiguration anzeigen.

4. Wo finden Sie in der Ausgabe die folgenden Informationen:
   a) *MAC*-Adresse der Netzwerkkarte
   b) Aktuelle IP-Adresse des Systems
   c) Subnetzmaske

[1] Minimal heißt hier: ohne grafische Oberfläche/Headless
[2] Anmeldung in der Mediathek nicht vergessen!

   d) Besteht eine aktive Verbindung mit dem Netzwerk?
   e) Anzahl fehlerhafter Pakete?
   f) Übertragene und empfangene Datenmenge?

5. Überprüfen Sie, ob ein Netzwerkverbindung besteht. Zum Prüfen können Sie folgende Aktionen durchführen:
   a) Auf der Kommandozeile einen Rechner mit seinem Namen anpingen (bspw.: `mi.fu-berlin.de`).
   b) Ping auf eine IP-Adresse (bspw.: 160.45.117.199).
   c) Ping auf die IP-Adresse in Ihrem Netzwerk. Bspw. lokale Router (oft IP: 192.168.172.1 oder192.168.0.1) – funktioniert die Kommunikation im lokalen Netz (LAN)?
   d) Ping auf die eigene IP-Adresse – wurde der lokale Netzwerkstack richtig gestartet?

Aufgabe C – Umsetzung des statischen Netzwerkes

Setzen Sie das aus der Planung hervorgegangene Netzwerk um. Drei VMs befinden sich im sleben *LAN* und sollen miteinander kommunizieren.

1. Schalten sie auf allen VMs für die *DHCP*-Netzwerke, falls eingeschaltet, die automatische Adressvergabe aus.
2. Auf jeder VM:
   a) Legen sie eine *IPv4*-Adresse fest.
   b) Ordnen sie der *IPv4*-Adresse einer Subnetzmaske zu. Diese sollte minimal sein, d.h. nur so groß, dass zumindest drei Rechner Platz finden.
   c) Konfigurieren sie das Netzwerkgerät mit den oben genannten Werten. Achten sie darauf, dass sie das korrekte Gerät konfiguriert wird. Nutzen sie hierfür die üblichen Tools: *ifconfig* und *ip addr*
3. Testen sie, ob ihr Netzwerk funktioniert. Nutzen sie *ping* oder *netcat* um dies zu testen.
4. Haben ihre VMs einen Zugang zu anderen Rechnern? Können diese Maschinen außerhalb des LANs oder gar Rechner im Internet erreichen? Erläutern sie ihre Befunde!

Aufgabe D - Fakultativ: Here be Dragons... Network-Discovery

Nachdem sie ihr erstes Netzwerk umgesetzt haben, könne sie schauen, ob noch andere Rechner in ihrem virtualBox LAN oder ihrem physischen LAN erreichbar sind. Frei nach dem Motto „Here be dragons“ [3].

1. Ein Tool um Informationen über Geräte im LAN zu sammeln sind *arping* und *arp-scan*. Schauen sie in der *Manpage* oder in der Hilfe nach, wie diese Tools zu nutzen sind, wenn sie alle lokal erreichbaren Rechner ermitteln wollen

2. Erstellen sie sich eine kurze Übersicht über die aktiven Maschinen im Netzwerk.

3. Sie könmnen noch mehr über die dubiosen Maschinen in Erfahrung bringen. Mit dem Tool *nmap* können Sie einen Port-Scan starten. Dies ermöglicht Ihnen herauszufinden, welche Dienste auf den jeweiligen Maschinen laufen. **Achtung:** Nutzen sie *nmap* nur innerhalb ihres eigenen Netzwerkes. Port-Scanning kann bei fremden Geräten und Netzen zu rechtlichen Schwierigkeiten führen: s. https://de.wikipedia.org/wiki/Portscanner#Rechtliche_Aspekte
   Starten sie einen Port-Scan auf gefundene Maschinen. Die Ausgabe liefert Ihnen einige Informationen – offene Ports sind Dienste die das System im Netzwerk für andere Teilnehmer anbietet. Manche können auch direkt im Webbrowser aufgerufen werden, beispielsweise die Ports 80 und 443 (viele andere auch, diese beiden sind jedoch die Standardports für HTTP(s)-Websites).

[3] https://en.wikipedia.org/wiki/Here_be_dragons