Übungsblatt 04 – Netzwerkgrundlagen

Zusammenfassung:
Sie lernen die Rechner kennen und bauen ein eigenes Netzwerk auf. Hierfür untersuchen Sie zunächst einen bereits vorkonfigurierten Netzwerkadapter, anschließend nehmen Sie die Konfiguration des Netzwerkes auf Grundlage Ihrer Hausaufgaben händisch vor.

Aufgabe A - Setup

1.) Lassen Sie sich den Status des DHCP und Networking-Service anzeigen.

2.) Lassen Sie sich den Status des Networking-Mangers anzeigen.

3.) Falls der DHCP-Service ausgeschaltet sein sollte, können Sie diesen mithilfe von Systemd wieder einschalten.

4.) Lassen Sie sich mit den Kommandos:

```
uname -or
```

und

```
cat /etc/os-release
```

anzeigen, welcher Betriebssystemkern (Kernel) und welche Distribution als VM läuft.

5.) Nutzen Sie diese Information um im Falle von Fehlern/Fehlkonfigurationen nach möglichen Lösungen für das Betriebssystem zu recherchieren. Es ist schlau in einer Suche den Namen des Betriebssystems vorkommen zu lassen. Sie wollen keine Lösungen für Windows finden.

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.

1.) Lassen Sie sich die aktuelle IP-Adresskonfiguration anzeigen.

2.) Wo finden Sie in der Ausgabe die folgenden Informationen:

a.) MAC-Adresse der Netzwerkkarte

b.) Aktuelle IP-Adresse des Systems

c.) Subnetzmaske

d.) Besteht eine aktive Verbindung mit dem Netzwerk (also Kabel mit dem Switch verbunden)?

e.) Qualität der Verbindung? (Anzahl fehlerhafter Pakete)

f.) Übertragene Datenmenge?

3.) Überprüfen Sie, ob ein Netzwerkverbindung besteht. Zum Prüfen können Sie folgende Aktionen durchführen:

a.) Webbrowser öffnen und versuchen eine Seite anzuzeigen (dazu muss der Rechner eine IP-Adresse haben, sein Gateway kennen und das DNS richtig konfiguriert sein, der Webserver muss aktiv sein, keine Firewall darf die Pakete blocken).

b.) Auf der Kommandozeile einen Rechner mit seinem Namen anpingen (bspw.: `mi.fu-berlin.de`).

c.) Ping auf eine IP-Adresse (bspw.: 160.45.117.199).

d.) Ping auf die IP-Adresse des Laborrouters (IP: 10.10.10.254) – funktioniert die Kommunikation im lokalen Netz (LAN)?

e.) Ping auf meine eigene IP-Adresse – wurde der lokale Netzwerkstack richtig gestartet?

4.) Schalten Sie den Netwrok-Manger via Systemd permanent aus!

5.) Löschen Sie alle von DHCP gesetzten Einträge, d.h. alle IP-Adressen, Default-Routen sollen verworfen werden.

Aufgabe C - Switched LAN

In der Hausaufgabe haben Sie ein kleines Netzwerk geplant, dies soll in Vierergruppen mit der vorhandenen Hardware umgesetzt werden.

1.) Beschriften Sie die Skizze aus der Planungsphase mit Gerätename und evtl. den Namen der Gruppenmitglieder.

2.) Legen Sie für die Gruppe eine Netzwerkadresse samt Subnetzmaske fest.
Das Netzwerk sollte der IP-Range 10.0.X.Y genügen. D.h. X ist durch ihre Bankreihe bestimmt und Y entspricht dem Host in dieser Reihe. Die Subnetzmaske sollte der Anzahl Ihrer verwendeten Hosts genügen.
Beispielsweise: 10.0.3.4 – dritte Reihe, vierter Rechner.
Die IP-Adressen 10.0.0.0 und 10.255.255.255 können nicht belegt werden. Ebenso ist die Adresse 10.10.10.254 bereits vergeben.

3.) Vergeben Sie für jede VM eine *IPv4*-Adresse, tragen Sie diese auf Ihrer Skizze ein.

4.) Umsetzen der Konfiguration:

a.) Lassen Sie sich im Terminal die aktuelle Netzwerkkonfiguration mit *ifconfig* und *ip addr* anzeigen. Haben Sie eine IP-Adresse (*inet*) und Subnetzmaske (*netmask*)?

b.) Richten Sie die VMs mit den Ihnen bekannten Befehlen ein. D.h. Sie müssen nun manuell *IPv4*-Adressen vergeben, sodass Ihre VMs miteinander kommunizieren können. Nutzen Sie hierfür Werkzeuge aus beiden Werkzeugkästen (*iproute2*, *net-tools*).

c.) Lassen Sie sich im Terminal die neue Netzwerkkonfiguration mit *ifconfig* oder *ip addr* anzeigen.

d.) Überprüfen Sie ob Ihr Netzwerkinterface tatsächlich aktiv ist! Dies ist unter *ip addr* direkt einsehbar, bei *ifconfig* nur indirekt.

5.) Testen des Netzes

a.) Testen Sie, ob sich Ihre VMs gegenseitig mit dem Befehl *ping* „anpingen“ können. Lassen Sie dabei einen der drei anderen VMs außen vor und merken Sie sich welcher das war.

b.) Starten Sie Ihre VM per Kommandozeile neu. Pingen Sie einen der beiden bereits „angepingten“ VMs erneut an. Funktioniert es immer noch?

c.) Lassen Sie sich die Netzwerkkonfiguration erneut anzeigen.

6.) Setzen Sie eine persistente Netzwerkkonfiguration mittels Dateien um. Gehen Sie beim Testen ebenso vor, wie in der vorigen Aufgabe.

Aufgabe D - Bestimmung des physischen Rechners zu einer IP-Adresse – ARP

Sie haben bereits theoretisch recherchiert wie die Zuordnung von physischer Adresse zu einer IP-Adresse vonstatten geht. Im Folgenden sollen Sie herausfinden, ob die Auflösung von IP-Adresse auf physische Adresse wirklich analog zu Ihren theoretischen Recherchen abläuft.

1.) Finden Sie mithilfe Wiresharks heraus, wie die Adressauflösung funktioniert.

a.) Leeren Sie zunächst den ARP-Cache.

b.) Pingen Sie nun einen Rechner an, den Sie vorhin noch nicht „angepingt“ haben. Die dafür ausgetauschten Pakete (und wahrscheinlich einige mehr) werden „gesnifft“.

c.) Beenden sie das Mitschneiden des Netzwerksverkehrs und setzen Sie als Filtern die MAC-Adresse ihres Adapters.

d.) Versuchen Sie über den Mitschnitt herauszufinden, wie die Bestimmung des zugehörigen Netzadapters und die MAC-Adresse erfolgt.

2.) Damit Ihr Rechner nicht jedes mal eine Auflösung veranlassen muss, werden die ARP-Informationen lokal in einem Cache zwischengespeichert („cached“).

a.) Lassen Sie sich Ihren aktuellen ARP-Cache anzeigen. Welche Informationen können Sie diesem entnehmen?

b.) Schauen Sie kurz nach wie lange der ARP-Cache Einträge vorhält.

c.) Lassen Sie zwei VMs die IP-Adressen tauschen. Dies sollte möglichst schnell umgesetzt werden!

d.) Versuchen Sie nun durch eine dritte VM eine „alte“ IP-Adresse zu erreichen. Werden die Daten an den richtigen Knoten übermittelt?

e.) Verfolgen Sie die Datenübermittlung per Wireshark mit.

Aufgabe E - ARP-Cache-Poisoning

Wie in den Hausaufgaben bereits zu erahnen war, dürfen Sie nun ein wenig Unruhe in Ihren Netzwerken stiften!
Sie sollen in diesem Teil der Laborübung ein ARP-Spoofing vornehmen. Um dies zu erreichen, sollen Sie den ARP-Cache so manipulieren das sämtlicher Verkehr zwischen Ihren LANs A und B nicht mehr über den Router geleitet wird, sondern über den Angreifenden Host.

1.) Ziel ist es sämtlichen Netzwerkverkehr statt direkt über das Labor-Gateway über den Angreifen laufen zu lassen.

2.) Setzen Sie alle vorgenommenen Konfigurationen zurück. D.h. Sie müssen veränderte Systemdateien in den ursprünglichen Zustand zurücksetzen. Es stehen einige Shell-Skripte bereit. Diese laufen mit root-Rechten und müssen daher mit dem Schlüsselwort *sudo* ausgeführt werden.

3.) Setzen Sie Ihr System wieder in die Ausgangslage zurück. D.h. Sie sollen wieder eine IP-Adresse und Default-Route vom DHCP-Server beziehen.

4.) Zunächst beginnen Sie mit der sogenannten Reconnaissance-Phase (Aufklärung). Sie müssen Angreifer und Opfer in Ihren Netzwerk auswählen. Bringen Sie hierfür alle notwendige Informationen in Erfahrung (IP-Adressen, Adapter).

5.) Analysieren Sie den ARP-Cache des anzugreifenden Systems.

6.) Da der angreifende Host als „MITM-Router“ fungiert, muss das Forwarding aktiviert sein und eine Default-Route zum Backbone angelegt werden, sodass der Abgefangene Traffic auch beim Ziel ankommt. Mit Folgendem Befehl aktivieren Sie das Forwarding:

```
1 sudo sysctl -w net.ipv4.ip_forward=1
```

Die Default-Route sollte durch den DHCP bereits korrekt gesetzt sein! Schauen Sie trotzdem im Routing-Table nach.

7.) Im Ordner `~/arp_poison/` liegt ein Python-Skript (wie auch ein Perl-Skript und eine C-Datei), welche für den Angriff genutzt werden kann. Bevor Sie dies einsetzen: Schauen Sie sich das Skript erneut an. Wie muss dieses Skript ausgeführt werden? Haben Sie die entsprechenden Rechte? Haben Sie alle benötigten Parameter?

8.) Führen Sie das ARP-Cache-Poisoning durch.

9.) Lassen Sie sowohl auf dem angreifenden als auch angegriffenen System Wireshark mitlaufen.

10.) Erzeugen Sie ein wenig Netzwerkverkehr, am besten unverschlüsselt!

11.) Betrachten Sie den ARP-Cache während des Angriffs, sowie einige Zeit nachdem Angriff.

12.) Ziehen Sie ein Fazit aus dem eben durchgeführten Angriff!

Here be Dragons... Network-Discovery

Nachdem Sie Ihr System wieder in die Ausgangslage versetzt haben, sollen Sie im nächsten Schritt das Labornetzwerk erkunden. Frei nach dem Motto "Here be dragons"[1] sind im Labor neben den VMs auch andere Maschinen Online. In späteren Übungen werden Sie diese fragwürdigen Geräte genauer begutachten.

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.

2.) Erstellen Sie sich eine kurze Übersicht über die aktiven Maschinen im Netzwerk. Neben Ihren VMs sollten auch andere Systeme auftauchen. Die Unterscheidung kann mithilfe der Adressen als auch anhand der Hostnamen erfolgen.

3.) Sie sollen noch ein wenig 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.
Starten Sie einen Port-Scan!

4.) Welche Ports sind geöffnet? Und welche Services verstecken sich dort? Gibt es vielleicht interessante Dienste, die Sie näher erkunden wollen?

5.) Falls eine Maschine die Web-Ports offen hat: Rufen Sie die Maschinen mit den Ports 80 oder 443 via Browser auf.[2]

[1] https://en.wikipedia.org/wiki/Here_be_dragons
[2] Sie könne auch andere Tools hierfür verwenden.