Übungsblatt 04 – Wireshark

Aufgabe A – TCP: 3-Way-Handshake

Nachdem Sie sich bereits theoretisch mit dem 3-Way-Handshake auseinandergesetzt haben, sollen Sie nun schauen, ob der TCP-Handshake tatsächlich wie theoretisch beschrieben arbeitet.

1. Überlegen Sie sich eine Anfragen an eine Website (dies sollte TCP nutzen, wie HTTP!), die Sie noch nicht von der VM aus getätigt haben. Da ansonsten bestimmte Inhalte bereits gecacht vorliegen könnten oder über andere Verfahren eine TCP-Handshake vereiteln könnten.
2. Starten Sie Wireshark, richten Sie Interface und Protokoll-Type ein. Filtern Sie nur auf eine speziellen Request!
3. Lösen Sie den Handshake durch aufrufen der Website (oder Ressource) aus, während Wireshark den Netzverkehr mitschneidet.
4. Analysieren Sie den 3-Way-Handshake!
5. Zum Vergleich: Analysieren Sie ihren Mitschnitt mit folgender Aufzeichnung: https://wiki.wireshark.org/TCP_3_way_handshaking?action=AttachFile&do=view&target=3-way+handshake.pcap

Aufgabe B – ICMP

Da die Befehle *ping* und *traceroute ICMP* nutzen, sollen Sie mit Wireshark solche Request mitverfolgen.

1. Setzen Sie alle notwendigen Parameter um Wireshark mitlaufen zu lassen, sodass Sie die ICMP-Nachrichten mitverfolgen können.
2. Pingen Sie einen Rechner mit seinem Namen an (bspw.: `mi.fu-berlin.de`).
3. Ping auf eine IP-Adresse (bspw.: 160.45.117.199).
4. Ping auf die IP-Adresse Ihres Routers.
   Hinweis: Sie können diese durch *ip r* oder *route* in Erfahrung bringen.

```
ip r
default via XXX.XXX.XXX dev DEVICE proto dhcp src YOU.RIP.ADD metric VALUE
#or
route -n
Destination  Gateway  Genmask  Flags  Metric  Ref  Use  Iface
0.0.0.0  XXX.XXX.XXX  0.0.0.0  UG  VALUE  0  0  DEVICE
```

5. Ping auf meine eigene IP-Adresse.
6. Ping auf die Loopback-Adresse.
7. Starten Sie eine Routenverfolgung via *traceroute* auf eine beliebige Adresse. Verfolgen Sie dabei den Ausgabe auf der Konsole als auch in Wireshark (Filtern Sie in Wireshark entsprechend). Spiegeln sich die Einträge in Wireshark mit denen auf der Kommandozeile?
8. Erläutern Sie die Ergebnisse Ihrer vorigen Aufgabe. Wie funktioniert *traceroute* und wie hängt dies mit *ICMP* zusammen?

Aufgabe C – Routing & Traceroute

Nachdem Sie recherchiert haben, wie *traceroute* arbeitet, welche Kritik an Traceroute geäußert wurde und wie diese mit dem Tool Paris-Traceroute abgestellt wurden, sollen beide Tools hier kurz erprobt werden.

1. Überlegen Sie sich zunächst anhand Ihrer Recherche was *traceroute* in etwa ausgeben müsste, wenn Sie im Labor eine Route von einem Rechner A zu einem Rechner B verfolgen würden. Wobei beide Rechner zu unterschiedlichen Netzwerken gehören (d.h. unterschiedlichen Tischreihen).
2. Nutzen Sie anschließend *traceroute* um sich die Router zwischen zwei Laborrechnern anzeigen zu lassen. Stimmen Ihre theoretische Überlegungen mit denen von *traceroute* überein? Falls nicht, sollten Sie analysieren woran dies liegen könnte.
3. Vergleichen Sie die Ausgaben von *traceroute* und *paris-traceroute* für folgende IP-Adressen:
   a) 41.231.21.44
   b) 91.198.174.192
   c) 37.220.21.130
   d) 80.239.142.229

   Hinweis: Für *paris-traceroute* sollten Sie den „exhaustive algorithm“ Nutzen (in machen Versionen als Parameter: `-na exhaustive`)
4. Analysieren Sie anschließend die Ausgabe beider Tools.
5. Warum wurde Ihnen eine Liste von IP-Adressen genannt anstelle von Domainnamen? Nennen Sie mindestens zwei Gründe!