Übungsblatt 04 – Routing & Traffic Analysis

Im Moodle-Kurs liegt eine Zip-Datei `network_packets.zip`. Diese enthält verschiedene Dateien die sie auf verschiedene Arten in Wireshark öffnen können. Sie sollen diese Pakete analysieren. Teilweise sind in diesen Paketen Passwörter und Zugangsdaten zu finden, in einigen Fällen können ganze Nachrichten oder Geräteinformationen gefunden werden.

Aufgabe A – Link Layer & Ethernet Frames

Das OSI-Modell ordnet verschiedene Funktionalitäten der Netzwerkkommunikation den Schichten des Modells zu. In der untersten Schicht werden physikalische Signale über ein Medium übertragen (bspw. Lichtquanten oder Elektronen). D.h. die Schicht 1 interpretiert direkt die Signale und ermöglicht es Signale in Daten umzuwandeln. Direkt darüber können diese Daten bereits „höherwertig“ verarbeitet werden. Auf dem Link-Layer werden die codierten Daten in Rahmen zusammengefasst. Eigentlich sind die hier transportierten Rahmen nur aneinanderreihungen von Einsen und Nullen.

1. Starten sie Wireshark und stellen sie als Adapter *em0* mit Ethernet als Protokoll ein. Erzeugen sie beliebigen Netzwerkverkehr (bspw. Ping auf die eigene IP-Adresse).

2. Analysieren sie ein Ethernet-Frame unter folgenden Aspekten (Sie können Abb. 1 als Hilfe nutzen). Skizzieren/notieren sie sich wo und welche Informationen ihres Ethernet-Frames zu finden sind.
   a) Welche Größe haben:
      i. Wie groß ist ein *IEEE Packet?*
      ii. Wie groß ein Ethernet-Frame?
      iii. Wie groß ist die eigentliche Nutzlast (Payload/ MAC Client Data)?
   b) Welchen Zweck hat die Preamble und das *SFD*-Feld?
   c) Wie viele und welche Adressen sind in einem Ethernet-Frame vermerkt?
   d) In Abb. 1 gibt es innerhalb der Payload ein Feld namens Pad. Wozu dient dies?
   e) Wozu dient die Prüfsumme eines Ethernet-Frames? Wo ist diese zu finden?

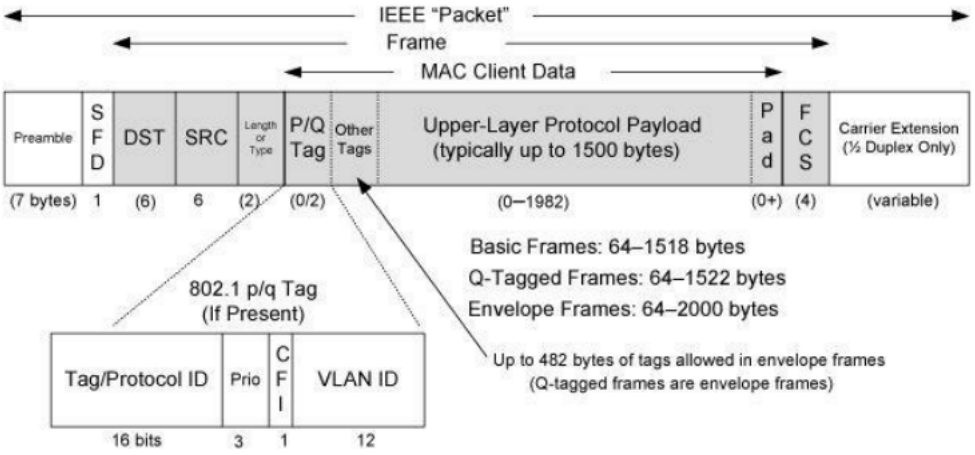

Abbildung 1: Aufbau eines Ethernet-Pakets.

3. Wenn ein Ethernet-Frame mitgeschnitten wird, erfolgt dies im Betriebssystem häufig als Hexadezimalzeichen. Diese Datei ist im ZIP-Archiv als `raw_ethernet_frame` hinterlegt. Importieren sie die Datei als Hex-Dump in Wireshark.

```
0000 00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00
0010 00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00
0020 00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
0030 00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
0040 d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
0050 69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
0060 2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
0070 69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
0080 6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0090 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
00A0 61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
00B0 3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
00C0 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
00D0 0a
```

a) Wie lauten Quell- & Zieladresse des Frames? Können sie den Hersteller des Layer-2 Geräte ausmachen?

b) Ist die Prüfsumme korrekt? Diese müssen sie nicht selbst berechnen, Wireshark teil ihnen mit, ob ein Datum defekte hat.

c) Welcher Layer-3 Protokoll ist im Ethernet-Frame enthalten? Woran erkennen sie dies?

d) Welche IP-Adressen sind vermerkt?

e) Welches Layer-4 Protokoll ist im IP-Paket enthalten?

f) Ist auch ein Layer-5 Protokoll vorhanden? Enthält dies eine Nachricht, die sie direkt interpretieren können?

Aufgabe B – IP

Das IP-Protokoll haben sie schon detaillierten kennengelernt.

1. Nehmen sie ihr oben genutztes Ethernet-Frame. Wo finden sie folgenden Informationen?
   - Welche Adressen sind im Paket enthalten? Wie viele sind dies?
   - Ethernet hat eine Prüfsumme, TCP ebenfalls. Hat IP eine Prüfsumme?
   - Ist IP ein verbindungsorientiertes Protokoll? Begründen sie ihre Antwort anhand der eben vorgenommen Analysen.
   - Ein IP-Paket besteht aus Header und Payload. Wo wird die Trennung festgelegt?
   - Wo ist die Information der nächst höheren Protokollebene zu finden?

Aufgabe C – 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 *netstat* 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
#or.
netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.178.1 0.0.0.0 UG 0 0 0 nm-bridge
192.168.100.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr1
```

5. Ping auf meine eigene IP-Adresse.
6. Ping auf die Loopback-Adresse.
7. Nehmen sie nun eine ihrer Ping-Anfragen und analysieren sie diese mithilfe Wiresharks genauer.
   a) Auf welcher Ebene des OSI-Modells ist das ICMP-Protokoll einzuordnen? Begründen sie ihre Antwort!
   b) Analysieren sie mithilfe Wiresharks den Aufbau eines ICMP-Pakets. Wie ist der generische Aufbau? Skizzieren sie den Aufbau mithilfe der in Abb. 2.

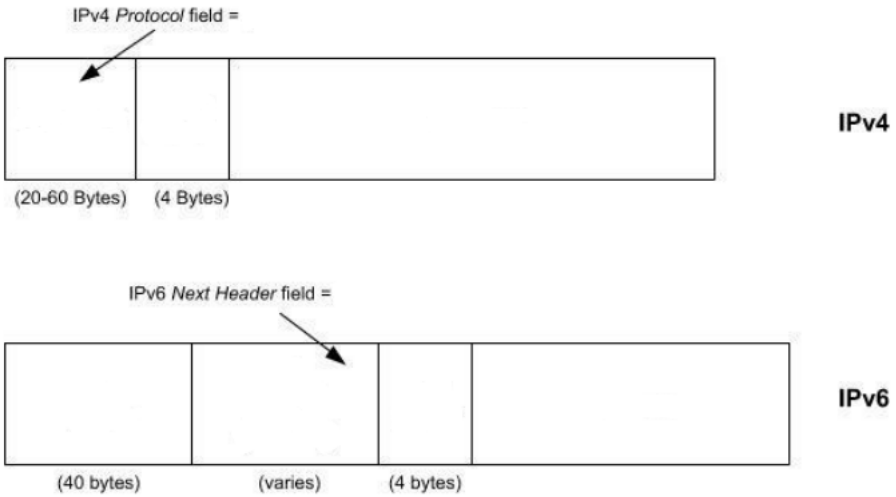

Abbildung 2: Generischer Aufbau eines ICMP-Pakets für IPv4 und IPv6.

   c) Welche Nachrichtentypen werden für den Ping-Messages genutzt? Wo sind die Nachrichtentypen zu finden?
   d) Skizzieren sie mithilfe von Abb.3 die ICMP-Nachricht und welche Informationen Wireshark ihnen liefert.

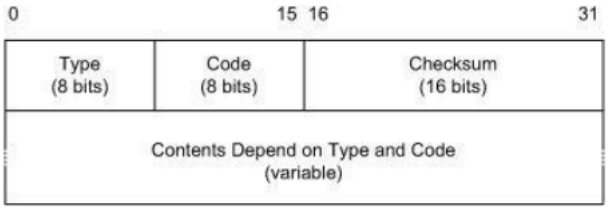

Abbildung 3: Nutzlast eines ICMP-Pakets.

8. Starten sie eine Routenverfolgung via *traceroute* auf eine beliebige Adresse. Verfolgen sie dabei die Ausgabe auf der Konsole und Wireshark (Filtern sie in Wireshark entsprechend). Spiegeln sich die Einträge in Wireshark mit denen auf der Kommandozeile?

9. Welche ICMP-Nachrichten wurden hier verwendet?

10. Erläutern sie die genaue Routenverfolgung mithilfe der ICMP-Nachrichten. Welches Feld wird hier genutzt um jeden Hop „verfolgen“ zu können?

11. Überlegen sie sich zunächst anhand Ihrer Recherche was *traceroute* in etwa ausgeben müsste, wenn sie auf der VM eine Route von einem Rechner A zu einem Rechner B verfolgen würden. Wobei beide Rechner zu unterschiedlichen LANs gehören.

12. Nutzen Sie anschließend *traceroute* um sich die Router zwischen zwei VMs anzeigen zu lassen. Stimmen Ihre theoretische Überlegungen mit denen von *traceroute* überein? Falls nicht, sollten Sie analysieren woran dies liegen könnte.

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. Um einen ARP-Request auszulösen können sie das Werkzeug *arp* nutzen. Lesen sie in der *man*-Page:
   - Wie können sie sich ihre MAC-Adresse und Interface anzeigen lassen?
   - Wie können sie sich den ARP-Table ausgeben lassen?
   - Wie leeren sie den ARP-Cache?

2. Finden sie mithilfe Wiresharks heraus, wie die Adressauflösung funktioniert.
   a) Starten sie Wireshark und stellen sie das korrekte Interface ein.
   b) Leeren sie zunächst den ARP-Cache.
   c) Pingen sie nun einen Rechner an, den sie vorhin noch nicht „angepingt“ haben. Die dafür ausgetauschten Pakete werden nun „gesnifft“.
   d) Beenden sie das Mitschneiden des Netzwerksverkehrs und setzen sie als Filtern die MAC-Adresse ihres Adapters.
   e) Versuchen sie über den Mitschnitt herauszufinden, wie die Bestimmung des zugehörigen Netzadapters und die MAC-Adresse erfolgt.

3. 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 – 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, etwa durch ein HTTP-Request!), die sie noch nicht von der VM aus getätigt haben.
2. Starten sie Wireshark, richten sie Interface und Protokolltype 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

Fakultative Aufgabe - Packet Analysis

Im Moodle-Kurs liegt eine Zip-Datei `network_packets.zip`. Diese enthält verschiedene Dateien die sie auf verschiedene Arten in Wireshark öffnen können. Sie sollen diese Pakete analysieren. Teilweise sind in diesen Paketen Passwörter und Zugangsdaten zu finden, in einigen Fällen können ganze Nachrichten oder Geräteinformationen gefunden werden.

1. Die Datei `ftp.pcap` ist eine FTP-Session mit Passwort Authentifizierung. Finden sie das Paket sowie Passwort.

2. Die Datei `telnet.pcap` ist eine Telnet-Session mit Passwort Authentifizierung. Finden sie das Paket sowie Passwort.

3. Die Datei `twitter.pcap` ist eine Twitter-Session welche die Authentifizierung enthält. Finden sie heraus, wie diese umgesetzt wurde und finden sie das Passwort.

4. Die Datei `bt.bin` für die Authentisierung von Bluetooth-Geräten gedacht. Im wesentlichen benötigen sie die MAC-Adresse des Gerätes und den Gerätenamen. Beides ist in der Datei enthalten. Die Authentisierung erfolgt die Hashing mit SHA1 (eine kryptografische Hashfunktion [1]). Finden sie das Tupel aus MAC-Adresse und Gerätenamen heraus und lassen Sie die SHA1 Funktion darüber laufen.

```
1 echo "XXXXXXXXXXXXXXXXXXX" | sha1sum
```

[1] Mehr dazu demnächst. SHA1 gilt seit Jahren als unsicher!