Rechnernetze
Wintersemester 2022/2023

Kai Cikoglu
Sebastian Illges

Wireshark

Aufgabe 3

1. Nennen Sie mindestens 5 Protokolle, die WireShark erkannt hat.
   - ARP
   - MDNS
   - UDP
   - DHCP
   - NBNS

2. Wie lange hat es vom Senden des HTTP Requests (http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html) bis zum Erhalt der HTTP Response gedauert?
   ⇒ `[Time since request: 0.116914000 seconds]`

3. Was ist die Internet-Adresse ihres Rechners? Was ist die Ethernet-Adresse (MAC-Adresse, physikalische Adresse) ihres Rechners? Welches ist die Ziel-MAC-Adresse, zu der ihr Rechner Pakete sendet? Vergleichen Sie die Ziel-MAC-Adresse für verschiedene Ziel-IP-Adressen. Welchem Netzknoten können Sie die Ziel-MAC-Adresse zuordnen?
   - `IP: 172.20.148.115`
   - `MAC source: a4:83:e7:6b:65:23`
   - `MAC destination: 00:a6:ca:f4:9b:4d`
   - `Netzwerkknoten: Destination: Cisco_f4:9b:4d (00:a6:ca:f4:9b:4d)`

4. Betrachten Sie ein HTTP Paket. Welche weiteren Protokolle werden genutzt, um ein http Paket zu übertragen? Welchen Schichten des TCP/IP-Schichtenmodells können Sie die Pakete zuordnen?
   ⇒ `TCP` ⇒ Transportschicht, `IP` ⇒ Netzwerkschicht & `Ethernet` ⇒ Sicherungsschicht
   ⇒ `HTTP` ⇒ Anwendungsschicht

Aufgabe 4

1. Markieren Sie im obigen Paket Ethernet, IP und TCP Header

```
0000  38 22 d6 67 19 00 00 21 cc 63 82 2c 08 00 45 00   8".g...!.c.,..E.
0010  02 9c 02 ed 40 00 80 06 40 66 8d 25 1d 5d 5b c6   ....@...@f.%.][.
0020  ae c0 e2 26 00 50 4f 4c 29 24 72 ce 3c d4 50 18   ...&.POL)$r.<.P.
0030  40 b0 62 e7 00 00 47 45 54 20 2f 77 69 6b 69 2f   @.b...GET /wiki/
0040  53 69 6d 70 6c 65 5f 53 65 72 76 69 63 65 5f 44   Simple_Service_D
0050  69 73 63 6f 76 65 72 79 5f 50 72 6f 74 6f 63 6f   iscovery_Protoco
0060  6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74   l HTTP/1.1..Host
0070  3a 20 64 65 2e 77 69 6b 69 70 65 64 69 61 2e 6f   : de.wikipedia.o
0080  72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20   rg..User-Agent:
0090  4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e   Mozilla/5.0 (Win
00a0  64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57   dows NT 6.1; WOW
00b0  36 34 3b 20 72 76 3a 33 32 2e 30 29 20 47 65 63   64; rv:32.0) Gec
```

2. Was sind die Quell- und Ziel-MAC-Adressen Adressen des dargestellten Pakets?
   - Quell MAC Adresse: `00 21 cc 63 82 2c`

- Ziel MAC Adresse: `38 22 d6 67 19 00`

3. Was sind die Quell- und Ziel-IP-Adressen des dargestellten Pakets?
   - Quell IP Adresse: `8d 25 1d 5d` ⇒ `141.37.29.93`
   - Ziel IP Adresse: `5b c6 ae c0` ⇒ `91.198.174.192`
4. Was sind die verwendeten TCP-Ports des dargestellten Pakets?
   - Quell TCP Port: `e2 26` ⇒ `57894`
   - Ziel TCP Port: `00 50` ⇒ `80`

Aufgabe 5

1. Wie lautet der Filter, mit dem Sie über den TCP Port http Verkehr filtern können?
   ⇒ `tcp.port == 80 && http`
2. Erhalten Sie das gleiche Ergebnis wie bei dem Filter HTTP? Erklären Sie ihre Erkenntnis.
   ⇒ Ja, weil bisher alle HTTP Anfragen diesen TCP Port verwendet haben.
3. Was bewirkt der Filter: `http && !(udp.port==1900)`
   ⇒ Es werden alle http anfragen angezeigt, die nicht über den UDP Port 1900 laufen.
4. Welcher Filter bewirkt, dass nur Pakete angezeigt, werden, die ihre eigene IP-Adresse als Ziel-Adresse haben?
   ⇒ `http && (ip.src == ip.dst)`