Labor Netzwerksicherheit 1
Testen von Firmen-Netzwerken

Yanick Eberle
Pascal Schwarz

Inhaltsverzeichnis

1 Aufgabe 1 - Wireshark/ARP

1.1 Protokollaufbau

Die folgende Grafik[1] zeigt den Aufbau des Protokolls.

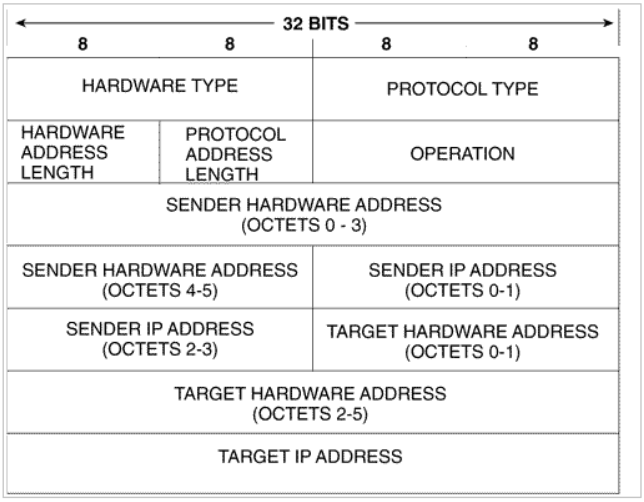


Abbildung 1: Address Resolution Protocol

1.2 Beantwortung der gestellten Fragen zum Protokoll

Wieviele Bytes ist das ARP Opcode-Feld vom Anfang des Ethernet Frames entfernt?
6 Byte
Welcher Wert hat das Opcode-Feld innerhalb des ARP-payload des Ethernet frame, worin eine ARP Anfrage gestellt ist?
ARP request
Enthält die ARP Meldung die IP Adresse des Senders?
Ja
Wo in der ARP-Anfrage erscheint die "Frage": Welche Maschine besitzt diese IP Adresse?
Operation (Opcode)
Geben Sie den Inhalt des ARP-Cache Ihres Laptops an, und erklären Sie, was jede Spalte bedeutet.
arp -n

Address	HWtype	HWaddress	Flags	Mask	Iface
10.196.134.1	ether	ee:ee:ee:01:07:06	C		eth0
10.196.134.127	ether	54:42:49:56:7c:bc	C		eth0

[1]Quelle: http://ipv6.com/images/diagrams/arp1.gif

Address zu welcher IP gehört der Rest der Information in der Zeile?

HWType gibt layer1/2 typ an

HWAddress der IP (Spalte 1) zugeordnete Hardwareadresse (hier MAC-Adresse)

Flags C steht für Complete (ARP Anfrage abgeschlossen), M wäre permanent, P publish

Mask würde zusammen mit publish benutzt

Iface über welches Interface ist die HWAddr erreichbar

2 Aufgabe 2 - Utilities ping, hping3, dig, traceroute

2.1 Perl Script für Host-Discovery im Subnet

```
1  #!/usr/bin/perl -w
2
3  use strict;
4  use Net::IP;
5  print "Scanning...\n";
6
7  #own ip in cidr
8  my $own_ip = `ip -f inet addr show dev eth0 | grep inet | gawk
       '{print \$2}'`;
9  my @own_ip2 = split('/',$own_ip);
10
11 my $hostMin = qx/ipcalc $own_ip2[0] | grep HostMin | gawk \'{print
       \$2}\'/;
12 my $hostMax = qx/ipcalc $own_ip2[0] | grep HostMax | gawk \'{print
       \$2}\'/;
13
14 print "hostMin: $hostMin";
15 print "hostMax: $hostMax";
16
17 my @ip = split('.',$hostMin);
18
19 my $ip = new Net::IP ("$hostMin - $hostMax") || die;
20 my @lines;
21 # Loop
22 do {
23         my $act_ip =$ip->ip();
24         my @line = `hping3 -1   $act_ip -c 1`;
25         my $numlines = @line;
26         print $numlines."\n";
27         if($numlines ==  2){#we have an answer if the hping3 command
               returns more than one row
28                 push(@lines,$act_ip);
29         }
```

```
30  } while (++$ip);
31  foreach(@lines){
32          print $_."\n";
33  }
```

Das Script erzeugt eine Ausgabe ähnlich der Folgenden:

```
10.196.134.1
10.196.134.16
10.196.134.17
10.196.134.19
10.196.134.21
10.196.134.118
10.196.134.120
```

2.2 DNS Protokoll

Viele Informationen in diesem Abschitt stammen von `http://doc-tcpip.org/Dns/named.dns.message.html`.

2.2.1 DNS-Request Packet: Welches Protokoll wird benutzt? Welche Vorteile bietet dies für einen DNS?

Es wird UDP als Transportprotokoll (siehe Grafik 2 auf Seite 5) eingesetzt. Dadurch entsteht weniger Overhead (hauptsächlich weil kein 3-way-Handshake nötig ist), was wiederum die Performance erhöht (geringere Latenz).

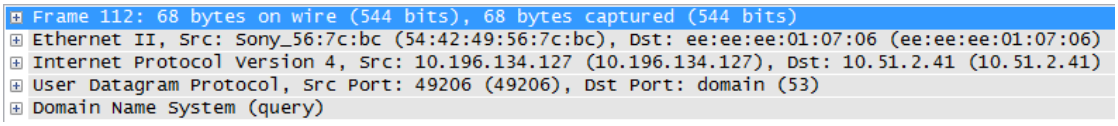


Abbildung 2: DNS Anfrage in Wireshark

2.2.2 DNS-Request Paket: Welcher src und dst port werden definiert? Wie interpretieren Sie das Resultat?

Auf Zielhost wird auf Port 53 abgehört. Da es eine Anfrage ist, ist der Destination Port 53. Siehe hierzu Grafik 3 auf Seite 5.

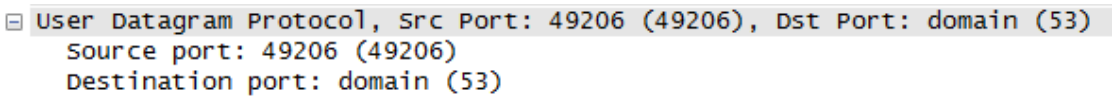


Abbildung 3: DNS Ports in Wireshark

2.2.3 DNS-Response Paket: Welche Felder gibt es? Erklären Sie deren Bedeutung.

Time Antwortzeit

Transaction ID eindeutige Nummer, muss mit Transaction ID des DNS Requests übereinstimmen, ist dies nicht der Fall, muss die Antwort verworfen werden.

Flags Request, Response, Error, no Error, ...

Questions Anzahl Anfragen

Answer RRs Anzahl Antworten

Authority RRs RRs, die auf verantwortliche Server deuten

Additional RRs RRs mit weiteren Informationen/Records

RR steht hier für **Resource Record**, ein Format zur Angabe des Mappings von IP-Adresse zu Name bzw. umgekehrt - oder weitere Information. Resource Records sind die Einträge in den Datenbank-Files des Name Servers.

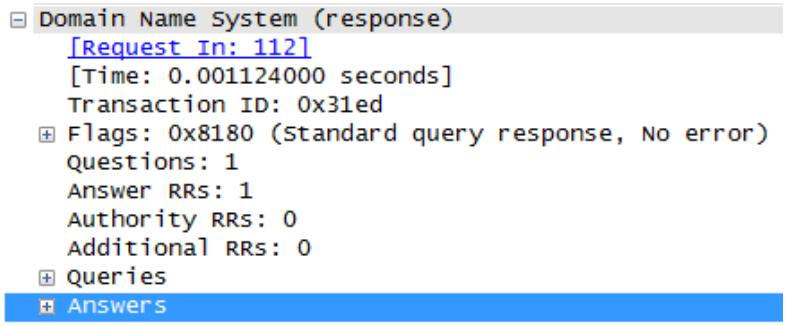


Abbildung 4: Header in DNS Response

2.2.4 DNS-Response Paket: Was enthält das Feld Answer? Erklären Sie jede zusätzliche Information, die Sie in diesem Feld gefunden haben.

NAME Der Domain-Name, zu der dieser RR gehört.

TYPE Der RR-Typ Code. Spezifiziert die Bedeutung des Feldes RDATA. Zwei Oktets.

CLASS RR-Klasse. Spezifiziert die Bedeutung des Feldes RDATA. Zwei Oktets.

TTL Time To Live - eine 32-bittige Zahl, die die Anzahl der Sekunden angibt, für die man diesen Record im Cache behalten darf. Null bedeutet, das dieser RR nur für die aktuelle Transaktion gilt.

RDLENGTH Eine 16-bittige Zahl, die die Anzahl der Oktets im RDATA Feld angibt.

RDATA Ein String variabler Länge (Oktets), der die Resource beschreibt. Das Format hängt von den Setzungen in TYPE und CLASS ab. Bei TYPE = A und CLASS = IN wäre das also eine normale 4 Oktet (32-bittige) ARPA Internet Adresse.

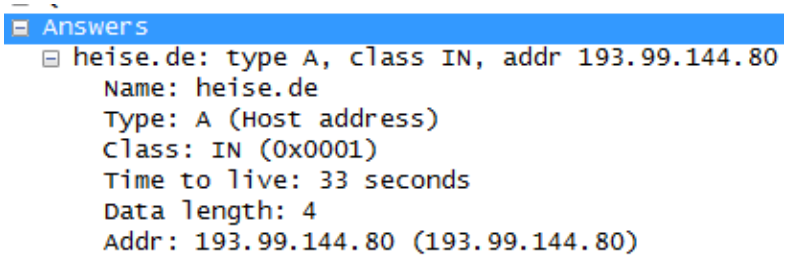


Abbildung 5: Answer-Abschnitt einer Response

2.3 Traceroute apple.com

Die geographische Lage der Router kann insbesondere in diesem Beispiel über die reverse DNS Einträge festgelegt werden. So ist beispielsweise *.zrh1.he.net in Zürich. Der Sprung passiert folglich zwischen Hop 13 und 14, also zwischen Amsterdam und Washington.

Grundsätzlich sollte der Sprung an der Latenzzeit ersichtlich sein. In diesem Fall ist die Latenzzeit der Router in Frankfurt und Amsterdam jedoch schon sehr hoch, was ev. auf eine Überlastung am Übergang zwischen he.net und xo.net in Frankfurt (am DE-CIX) zurückzuführen ist.

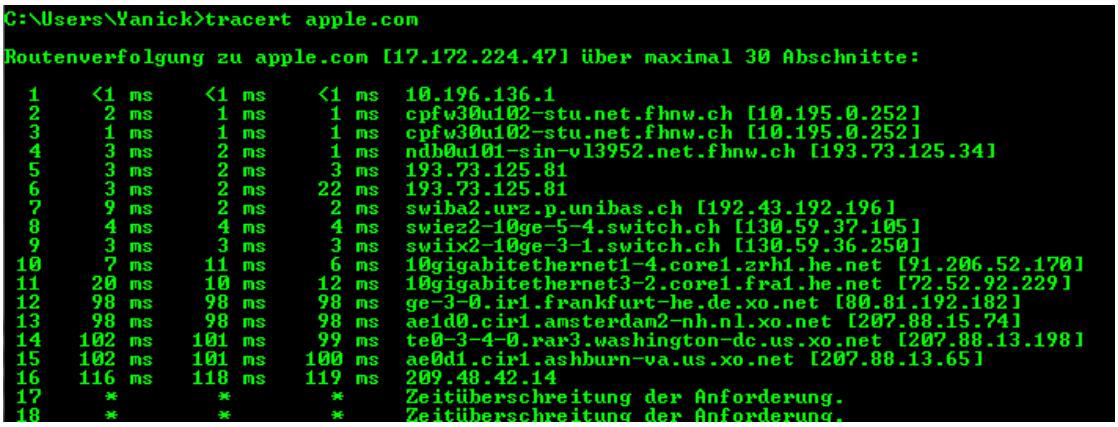


Abbildung 6: Traceroute zu apple.com

3 Aufgabe 3 - Nmap/Wireshark

Wir haben den Aufruf folgendermassen gemacht:

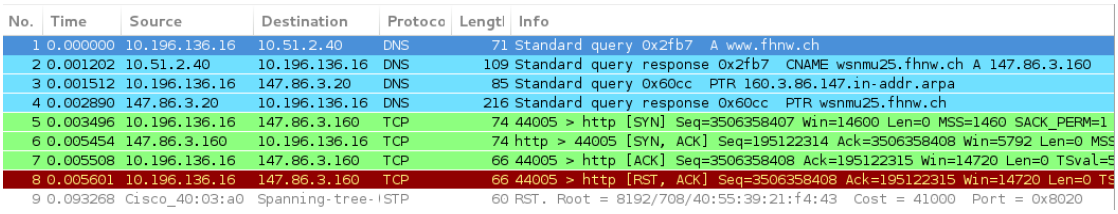
```
nmap -P0 -p80 www.fhnw.ch
```

Wir haben die Option -P0 gesetzt, weil wir wissen, dass unter www.fhnw.ch (mindestens) ein Server erreichbar ist. Der Output des Commands war der folgende:

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-15 08:18 CET
Nmap scan report for www.fhnw.ch (147.86.3.160)
Host is up (0.0021s latency).
rDNS record for 147.86.3.160: wsnmu25.fhnw.ch
PORT   STATE SERVICE
80/tcp open  http
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Mit dem Output können wir praktisch den gesamten aufgezeichneten Verkehr (siehe Grafik 7 auf Seite 8 begründen:

- Der Name muss zu einer IP (hier 147.86.3.160) aufgelöst werden, was mittels DNS geschieht.
- Die IP wird zurück zu einem Namen aufgelöst (reverse DNS Lookup, "rDNS record..."), ebenfalls via DNS.
- Danach wird ein kompletter TCP-3-way-Handshake durchgeführt und die Verbindung danach sofort wieder beendet (Frame 8 mit TCP Flags RST,ACK).
- Da der TCP-Handshake erfolgreich durchgeführt werden konnte zeigt uns nmap an, dass der Port geöffnet ist.



No.	Time	Source	Destination	Protoco	Lengtl	Info
1	0.000000	10.196.136.16	10.51.2.40	DNS	71	Standard query 0x2fb7 A www.fhnw.ch
2	0.001202	10.51.2.40	10.196.136.16	DNS	109	Standard query response 0x2fb7 CNAME wsnmu25.fhnw.ch A 147.86.3.160
3	0.001512	10.196.136.16	147.86.3.20	DNS	85	Standard query 0x60cc PTR 160.3.86.147.in-addr.arpa
4	0.002890	147.86.3.20	10.196.136.16	DNS	216	Standard query response 0x60cc PTR wsnmu25.fhnw.ch
5	0.003496	10.196.136.16	147.86.3.160	TCP	74	44005 > http [SYN] Seq=3506358407 Win=14600 Len=0 MSS=1460 SACK_PERM=1
6	0.005454	147.86.3.160	10.196.136.16	TCP	74	http > 44005 [SYN, ACK] Seq=195122314 Ack=3506358408 Win=5792 Len=0 MSS
7	0.005508	10.196.136.16	147.86.3.160	TCP	66	44005 > http [ACK] Seq=3506358408 Ack=195122315 Win=14720 Len=0 TSval=5
8	0.005601	10.196.136.16	147.86.3.160	TCP	66	44005 > http [RST, ACK] Seq=3506358408 Ack=195122315 Win=14720 Len=0 TS
9	0.093268	Cisco_40:03:a0	Spanning-tree-(STP		60	RST. Root = 8192/708/40:55:39:21:f4:43 Cost = 41000 Port = 0x8020

Abbildung 7: Datenverkehr, der durch den nmap-Aufruf ausgelöst wurde

4 Aufgabe 4 - Installation Metasploit

5 Aufgabe 5 - Footprinting/Scanning

5.1 Footprinting

5.2 Scanning