Aufgabe 1

1. Bootstrap Protocol (BOOTP)
   Discover, Offer, Request, Ack

Port (67->68)

	Src	Dst
Router	192.168.178.1	255.255.255.255
Client	0.0.0.0	255.255.255.255

Die ClientenIP ist zu Begin 0.0.0.0
255.255.255.255 Broadcast

2. Domain Name System (DNS) ermittelt die nötige IP Adresse zu dem Aufruf

Ablauf in unserem Capture

→No12	Zunächst wird das Netzwerk eingestellt mittels NBNS → Gerätenamen und IP werden registriert beim WINS-Server
→No26	DNS ermittelt IP zu „www.google.de“
→No30	TCP erzeugt sichere Verbindung mit GoogleServer
→No33	Anfrage „www.google.de“ wird an GoogleServer versendet
→No35	google sendet Html code zurück
→	Daten werden über TLSv1 Protokoll versendet (gesichertes Transportprotokoll)

3. Die Suchanfrage wurde in unserem Capture verschlüsselt verschickt, mittels TLSv1.
Die Anfrage ist in unverschlüsselter Form ebenfalls HTTP (port 80)

4. Es kann bei einer Beobachtung sämtliche Daten aufgezeichnet werden die sich in Reichweite der Wlan Karte befindet. Dabei wird der gesammte Traffic mitgeschnitten.
Die Nutzung von Protkollen, wie HTTP, FTP, SMTP birgt halt dan Risiken mit sich, wenn persönliche Daten versendet werden.

5. Es gibt kein HTTP Protokoll mehr. Die Daten werden stattdessen komplett mittels TLSv1 und Secure Socket Layer (TLS) verschlüsselt. Die Suchanfrage ist nicht mehr auffindbar.

Aufgabe 3

1	cascada-ubu-eecsit.tu-berlin.de (130.149.245.242)
2	130.149.245.193
3	xr-tub2-te2-4.x-win.dfu.de(188.1.235.117)
4	cr-tub1-te0-0-0-0.x-win.dfu.de(188.1.144.157)
5	te3-1.c101.f.de.plusline.net(80.81.192.132)
6	heise1.f.de.plusline.net(82.98.98.98)
7	www.heisse.de (193.99.144.85)

Aufgabe 1:

1. **Welches Protokoll ist dafür verantwortlich, dass Ihr Rechner eine IP-Adresse bekommt? Welche Pakete dieses Protokolls finden Sie in Ihrem Capture?**

Was ist in diesen Paketen als Source- und Destination IP-Adresse eingetragen und warum?

Aufgabe 2:

1. Wieviele Pakete umfasst der Trace?

Methode: statistics --> summary

62856

2. Wie gross sind die Pakete im Durchschitt?

Methode: statistics --> summary

Durchschnitt 614,574 Bytes

3. Notieren Sie alle im Trace auftauchenen MAC-Adressen.

Methode: statistic--> enpoint lis --> ethernet

"Address","Packets","Bytes","Tx Packets","Tx Bytes","Rx Packets","Rx Bytes"

"D-Link_fc:75:2b","62840","38627670","36098","30320744","26742","8306926"

"DellPcba_c7:76:0e","62855","38629422","26757","8308678","36098","30320744"

"Broadcast","16","1995","0","0","16","1995"

"Ibm_43:ca:fe","1","243","1","243","0","0"

4. Wieviele IP-Adressen tauchen im Trace auf?

Methode: statistic--> enpoint lis --> ipv4

172

5. Einige der auftauchenden MAC-Adressen sind mit IP-Adressen verknüpft.

Notieren sie diese Verknüpfungen.

Methode: filter "arp"

DellPcba_c7:76:0e is 192.168.0.4

D-Link_fc:75:2b is 192.168.0.1

6. Bei welchem Anteil der Pakete wird das Internet Protocol (IP) auf der Netzwerkschicht (ISO/OSI Modell) verwendet?

Frage komisch??? Alle?

7. Bei welchem Anteil der Pakete wird das Transmission Control Protocol (TCP)

auf der Transportschicht verwendet?

Frage komisch???Alle?

8. Notieren Sie alle Protokolle der Applikationsschicht die TCP nutzen.

Methode:Statistics -> Protocol hierarchy

RELOAD

STUNAT

SSH

HTTP

SSL

BiTtorrent

Realtime Streaming Protocol

9. Notieren Sie alle Protokolle der Applikationsschicht die das User Datagram

Protocol (UDP) nutzen.

Methode:Statistics -> Protocol hierarchy

DNS

NetBios Datagram service

Netbios Name Service

Real DAta Transort

10. Notieren sie alle auftauchenden Protokolle der Netzwerkschicht.

tcp

udp

11. Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

arp

12. Wieviele Domain Name System (DNS)-Abfragen fanden statt?

Methode: Filter "dns"

34

13. Wieviele IP-Pakete haben einen ’Time-To-Live’ (TTL) Wert gr ¨ oßer als 200,

mit genau 128 und mit genau 48? Versuchen sie, eine Erkl¨ arung f ¨ ur die gefundene Verteilung zu finden.

Methode: Filter "ip.ttl>200"

ttl > 200 : 23 marked

ttl == 128: 26757

ttl == 48: 105

14. Untersuchen Sie das 16. Paket im Trace genauer:

(a) Wie gross ist der Ethernet-Header?

methode: packet ausgewählt -> Ethernet frame angeklickt-> Markierte Bytes gezählt

000d56c7760e000f3dfc752b0800 =14 Bytes

(b) Wie gross ist der IP-Header?

methode: packet ausgewählt -> ipv4 frame angeklickt-> Markierte Bytes gezählt oder ip.headerlength

450005641fa94000740625d742abb8bcc0a80004=20 Bytes

(c) Wie gross ist das IP-Datagram?

methode: packet ausgewählt -> ipv4 frame angeklickt-> ip.tototallength

1380-20

(d) Wie gross ist der TCP-Header?

methode: packet ausgewählt -> ipv4 frame angeklickt-> tcp.headerlength

20 Bytes

(e) Wie gross ist das TCP-Segment?

methode: packet ausgewählt -> ipv4 frame angeklickt-> data bytes

1340 Bytes

15. Erstellen Sie ein Histogramm ¨ uber die L ¨ ange der IP-Datagramme. Interpretieren Sie das Ergebnis.

Methode: Statistics ->packet lengthfilter "ip"

0-39 0%

40-79 25819

80-159 4411

160-319 1644

320-639 5056

540-1279 4960

1280-2259 20944

>2560 0%

aus Daten histogramm erstellen

16. Zwischen welchen IP-Adressen werden die meisten Bytes ausgetauscht? Erstellen Sie ein Histogramm ¨ uber die L ¨ ange dieser IP-Datagramme. Interpretieren Sie das Ergebnis.

statistics ->conversations ->IP

Zwischen 60.254.20.52 und 192.169.0.4 wurden 10080639 Bytes ausgetauschts

apply filter- > selected A<-> B

0-39 0%

40-79 3891

80-159 3

160-319 769

320-639 115

540-1279 233

1280-2259 6948

>2560 0%

17. Bestand eine SSH-Verbindung? Notieren Sie ggf. die beteiligten Hosts.

192.168.0.4

136.159.5.20

18. Wurde ein Web-Browser benutzt? Wenn ja, welcher?

Ein Brwoser der sich als: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7 ausgibt

19. Wurde ein Medienstream empfangen? Wenn ja, welche Datei?

rtsp://a1651.v87522.c8752.g.vr.akamaistream.net:554/ondemand/7/1651/8752/1137095087000/origin.media.cbc.ca/newsworld/real/clips/rm-newsworld/debate_060110.rm?title=\"Harper%20fends%20off%20attacks%20from%20Duceppe%2c%20Martin%20in%20final%20debate\"&author=\"CBC%20News\"&copyright=\"CBC%20News\"/streamid=1 RTSP/1.0\\r\\n