Block 7.2

Gruppe 10 / Tutorium 5

- Sarah Köhler
- Dora Szücs
- Florian Schiller

Aufgabe 6

a) Zuweisung der IP-Adresse

- Über DHCP bekommt der Rechner eine IP-Adresse zugewiesen.
- Im Trace sind eine DHCP Request vom Rechner, worin er eine IP Adresse angibt, und ein DHCP ACK (Acknowledge), womit die IP-Adresse bestätigt wird.
- In der Request ist der Sender als `0.0.0.0` angegeben, weil der Rechner zu diesem Zeitpunkt noch über keine gültige Adresse verfügt. Die Nachricht wurde an `255.255.255.255` gesendet, damit jedes Gerät im Netzwerk die Nachricht empfangen kann, denn der Rechner kennt zu diesem Zeitpunkt den Router noch nicht. In der ACK-Nachricht des Routers identifiziert dieser sich mit seiner Adresse (aus dem lokalen Netzwerk), nämlich `192.168.1.1`. Der Rechner als Empfänger wird bereits mit der neu vergebenen IP-Adresse `192.168.1.109` angesprochen.
- Der Rechner gibt in der DHCP Request die `192.168.1.109` als gewünschte IP-Adresse an.
- Wie man der ACK-Nachricht des Routers sehen kann, bekommt der Rechner die gewünschte Adresse.
- In der ACK-Nachricht des Routers steht als Gültigkeitsdauer der vergebene IP 12 Stunden (Lease Time)
- Als Adresse des DNS-Servers wird die Adresse des Routers angegeben, d.h. DNS-Anfrage werden über den Router geleitet.

b) ARP-Pakete

Die Pakete 1 und 4-7 verwenden das ARP Protokoll und dienen also zur Zuweisung der MAC-Adressen zu IP-Adressen. Router und Rechner teilen sich gegenseitig ihre MAC-Adressen mit.

c) Aufruf einer URL

- Der Rechner fragt über DNS nach der Adresse von www.tkn.tu-berlin.de.
- Als Antwort erhält er die IP-Adresse `130.149.7.204`.

d) HTTP-Request

Die folgenden Antworten können jeweils aus den Headern der HTTP-Request und der Antwort ausgelesen werden: - Der Rechner fragt nach der URL `http://www.tkn.tu-berlin.de/` - Die Anfrage wurde über den (Text-) Browser Lynx gesendet. - Der antwortende Server verwendet Apache. - Die Verbindung ist nicht persistent, weil HTTP in der Regel nicht persistent ist und zudem der Server die Option `Connection: close` in der Antwort sendet.

e) SSH-Verbindung

- Die zweite DNS-Anfrage fragt nach der Adresse von `hyperion.tkn.tu-berlin.de`.
- Der Port des Clients ist `39506` und der Port des Servers `22`.
- Der Port `22` ist für das SSH-Protokoll vorgesehen.
- Aus dem weiteren Austausch zwischen Client und Server kann man keinen sinnvollen Daten mehr entnehmen, da dieser über SSH läuft, also verschlüsselt ist.

f) Sicherheit der Datenübertragung

Alle genannten Protkolle sind standardmäßig nicht verschlüsselt. Alle Daten, auch Login-Daten verschiedener Services und Passwörter (bei HTTP) sowie die Kommunikation (zum Beispiel Emailverkehr über SMTP) und die Inhalte von Datenübertragungen per FTP (zum Beispiel Bilder) können also rekonstruiert werden.

Über den Datenfluss kann ein potentieller Angreifer z.B. auch geöffnete Ports finden (etwa wenn für BitTorrent spezielle Ports freigegeben wurden) um so die Firewall umgehen zu können.