Übungsblatt 6 – Routen & Application Layer

Nachdem Sie nun komplexere Netzwerke aufgesetzt haben und den Verkehr Ihrer Netzwerke analysiert haben, betrachten wir in der kommenden Übung Anwendungen eines Netzwerkes. Viele dieser Applications nutzen Sie bereits, teilweise ohne es bewusst wahrgenommen zu haben. Da Sie als angehende Netzwerkprofis aber nicht nur daran interessiert sind Dinge zu nutzen, sondern deren Aufbau zu verstehen, soll mit der Übung zum Application-Layer diese Lücke ein Stück weit kleiner werden.
Hilfreiche Links:

- `https://en.wikipedia.org/wiki/Traceroute`
- `https://paris-traceroute.net/` Achtung HTTPS ist kaputt!
- `https://en.wikipedia.org/wiki/Domain_Name_System`
- `https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol`
- `https://en.wikipedia.org/wiki/SMTPS`
- `https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol`
- `https://en.wikipedia.org/wiki/HTTPS`
- `https://en.wikipedia.org/wiki/Transport_Layer_Security`

Aufgabe A – Routing & Traceroute

1.) Im wesentlichen gibt es zwei fundamentale Routing-Algorithmen. Dies sind das Distanz-Vektor- und Link-State-Routing. Um den kürzesten Weg durch einen Graphen zu finden (Shortest Path Problem) wird für das Distanz-Vektor-Routing gewöhnlich der Bellman-Ford-Algorithmus verwandt, das Link-State-Routing nutzt den Dijkstra-Algorithmus.

a.) Recherchieren Sie wie das Link-State-Routing unter Nutzung des Dijkstra-Algorithmus funktioniert.

b.) Recherchieren Sie wie das Distanz-Vektor-Routing unter Nutzung des Bellman-Ford-Algorithmus funktioniert.

c.) Erläutern Sie die fundamentalen Unterschiede beider Lösungsansätze.

d.) Diskutieren Sie ob der Bellman-Ford-Algorithmus (bzw. warum nicht) für das Link-State-Routing und der Dijkstra-Algorithmus für das Distanz-Vektor-Routing genutzt werden könnte.

2.) Lesen Sie folgende Artikel:
`https://en.wikipedia.org/wiki/Traceroute`,
`https://linux.die.net/man/8/traceroute`.
Beantworten Sie anschließend folgende Fragen:

a.) Wofür wird Traceroute genutzt?

b.) Wie wird Traceroute umgesetzt, d.h. wie läuft eine „Routen-Verfolgung“ ab?

c.) Welche Limitationen ergeben sich aus der Umsetzung?

d.) Dokumentieren Sie die Syntax, sowie die Bedeutung von Traceroute beispielhaft.

3.) Lesen Sie folgendes Paper zu Paris-Traceroute von der ACM International Measurement Conference 2006:
`http://conferences.sigcomm.org/imc/2006/papers/p15-augustin.pdf`

a.) Warum ist eine „neue“ Traceroute-Applikation notwendig?

b.) Nennen Sie drei Topologie-Anomalien die durch Paris-Traceroute erkannt werden können.

Aufgabe B – Domain Name System (DNS)

Das Domain Name System ist ein dezentrales System (verteilte Datenbank nach der Client-Server-Architektur), dessen primäre Aufgabe die Adressauflösung von Domain Name(n) zu IP-Adresse(n) ist. M.a.W. DNS bietet eine Abbildung von Domainname auf IP-Adresse [1]. Im Laufe der Jahre sind hierzu einige Tools entwickelt worden:

- whois
- host
- dig
- nslookup.

In der vierten Übung wurde das DNS bereits kurz angeschnitten, da Ihre Netzwerke im letzten Schritt einen Uplink in Internet erhalten haben und auch Domain Namen auflösen können sollten. Nun schauen wir uns das DNS und einige Tools, die um DNS „gewachsen“ sind, etwas genauer an.

1.) Rekapitulieren Sie Ihr Wissen zu DNS!

a.) Auf welchem Layer des OSI-Modells arbeitet DNS?

b.) Welches Transportprotokoll nutzt DNS?

c.) Auf welchem Port läuft DNS standardmäßig?

[1] Bzw. als Inverse – die Abbildung von IP-Adresse auf Domainnamen (Reverse-Lookup)

2.) Nennen und Erklären Sie die Komponenten des DNS-Systems.

a.) Was wird unter dem Begriff Resolver verstaden?

b.) Was ist ein DNS-Root-Server, was ist ein TLD-Server und was ein Domain-Server?

c.) Was ist ein Stub im Kontext von DNS?

d.) Was ist ein Bind-Server?

3.) Erläutern Sie die Auflösung einer DNS-Anfrage.

a.) Welche beiden Möglichkeiten einer Namensauflösung gibt es? D.h. welche Variante gibt einen Namen aufzulösen.

b.) Wie erfolgt die jeweilige Auflösung eines DNS-Requests?

c.) Verdeutlichen Sie sich anhand eines Beispiels, wie ein DNS-Request bearbeitet wird.

d.) DNS bietet theoretisch eine rekursive und iterative Namensauflösung, praktisch wird eine Mischung aus beiden Verfahren angewandt. Recherchieren Sie, wie diese Auflösung aussieht.

4.) Recherchieren Sie kurz wie die Tools

- whois
- host
- dig
- nslookup.

zu nutzen sind.

a.) Erläutern Sie kurz was jedes der oben genannten Tools leistet.

b.) Nennen Sie für jedes Tool geeignete Einsatzgebiete/ Szenarien.

c.) Recherchieren Sie die Syntax, sowie Semantik der Tools.

d.) Notieren und kommentieren Sie sich entsprechende Beispiele.

Aufgabe C – HTTP(S) & HTML

Kein anderes Protokoll ist für das World-Wide-Web so wichtig wie HTTP. In diesem Teil sollen Sie recherchieren, wie die bunten Seiten in Ihren Browser kommen.

1.) Recherchieren Sie zunächst was HTTP ist. Eine gute Anlaufstelle wäre Tanenbaums Computer Networks Chapter 7.3 – The World Wide Web.

2.) Erläutern Sie die Funktionswiese von HTTP.

3.) Auf welcher Schicht des OSI-Modells ordnen Sie HTTP ein?

4.) Auf welchen Port laufen meistens Webserver? Auf welchem Port läuft die verschlüsselte Variante HTTPS?

5.) Wie sieht ein typischer HTTP-Header aus?

6.) Nennen Sie alle HTTP-Methoden. Notieren Sie sich was diese machen und wie deren Aufruf aussieht.

7.) Machen Sie sich kurz klar, welche Aufgabe SSL/TLS übernimmt. (Hinweis: An dieser Stelle genügt ein grobes Verständnis)

8.) Recherchieren Sie wie die Tools *telnet*, *netcat* und *openssl s_client* genutzt werden können. D.h. wie sieht die Syntax zum Verbinden auf einen Server aus? Notieren Sie sich entsprechend Beispiele. Sie sollten als Vorbereitung auf die Laborübung sich auch das dazugehörige Arbeitsblatt anschauen, sodass Sie zielgerichtet nach entsprechenden Beispielen suchen können.

9.) Optional: Suchen Sie sich ein Tutorial zu *openssl s_client* heraus. Durchlaufen Sie entsprechendes Tutorial.
Bspw.: `https://tinyurl.com/y9nnaz6a`

10.) Recherchieren Sie was *STARTTLS* bedeutet, warum gibt es diese Möglichkeit der verschlüsselten Kommunikation?

11.) Recherchieren Sie kurz was ein kryptografisches Zertifikat ist. Wozu werden diese im Zusammenhang mit HTTP genutzt?

12.) Erläutern Sie wie Sie sich Zertifikate mit *openssl* anschauen können.

Aufgabe D – E-Mail mit POP3, IMAPv4 & SMTP

Das Simple Mail Transfer Protokoll wird, wie der Name schon sagt, zum Austausch von E-Mails in Computernetzwerken genutzt. Primär wird es zum Weiterleiten von Mails zwischen Server genutzt. Auf Ihren Endgeräten kommt zumeist *IMAP* oder *POP3* zum Einsatz.

1.) Recherchieren Sie zunächst was sich hinter den Akronymen POP3, IMAPv4, sowie SMTP verbirgt.

2.) Erläutern Sie im groben welche Aufgaben die oben genannten Protokolle übernehmen.

3.) Auf welcher Ebene des OSI-Modells arbeiten die Protokolle?

4.) Machen Sie sich im groben klar, wie diese Protokolle arbeiten.

5.) Worin unterscheiden sich POP3 und IMAP?

6.) Auf welchen Ports arbeiten die drei Protokolle?

7.) Auf welchen Ports arbeiten die drei Protokolle mit Verschlüsselung?

8.) Recherchieren Sie wie IMAP, POP3 und SMTP via Kommandozeile genutzt werden können. Notieren Sie sich entsprechende Kommandos, sowie deren Bedeutung!