Übungsblatt 2 – Application Layer

Zunächst beginnen wir mit der Anwendungsschicht. Dies hat den Vorteil, dass Sie die meisten der vorliegenden Anwendungen bzw. deren Protokolle bereits kennen. Wir können natürlich nicht alle Anwendungsprotokolle betrachten, daher geht dieses Blatt auf die Folgenden Protokolle ein:

- Wireshark – als Analysewerkzeug
- E-Mail via IMAP (POP3) & SMTP
- HTTP/HTTPs – Protokoll des Webs
- DNS: Namensauflösung – Abbildung von Namen auf IP-Adresse

Eine gute Einführung finden Sie im Kurose et al. [1, S. 83] (Kapitel 2).

Vorbereitung

Um die Übung effizienter zu gestalten habe ich in den Weiten des Internets folgendes gefunden:

- Fakultativ: Schauen Sie als Einführung die Videos 1.1 bis 1.6. Diese Videos dienen nur der Rekapitulation.
  https://www.youtube.com/watch?v=5D67Qy1tPLY&list=PLLFIgriuZPAcCkmSTfcq7oaHcVy3rzEtc
- Falls Sie trotz der Vorlesung noch nicht komplett sicher in der Anwendungsschicht sind, schauen Sie folgendes Video: https://youtu.be/xJ9JTT2fXWk
- Folgende Konzepte sind für die Übung von Interesse:

  a.) Aufbau und Nutzen des ISO-OSI-Schichtenmodells.

  b.) Das Akronym *API*: Was ist mit Schnittstelle gemeint und welchen Nutzen bringt diese.

  c.) Konzept eines Ports – als Eintrittspunkt im Betriebssystem.

  d.) Konzept der Sockets – als Adressierungsschema für Anwendungen.

  Diese Aufgaben müssen Sie nicht notwendigerweise als erste Aufgabe lösen! Sollten Konzepte nach dem Bearbeiten unklar bleiben, notieren Sie entsprechende Fragen im Moodle-Plenum.

Aufgabe A – Wireshark

Da Sie nicht nur Netzwerkanwendungen nutzen können sollen, müssen Sie verstehen wie Anwendungen realisiert werden. Hierzu müssen Sie hinter die Kulissen schauen. Im Fall von Netzwerken wird die Kommunikation via Protokolle umgesetzt. Das heißt, beide Seiten haben sich auf ein Art und Weise verständigt, wie kommuniziert wird. Daher gibt es Standards, die befolgt werden (RFCs, ISOs, etc.). Aufgrund der Nutzung von standardisierter Protokolle ist es ebenfalls relativ leicht möglich Programme zu bauen, die diese Protokolle verstehen und mitschneiden können. Das Mitschneiden und Analysieren kann mittels eines sogenannten Sniffers realisiert werden.
Wir nutzen den Netzwerk-Sniffer *Wireshark*. Wireshark ist eine Open-Source-Software mithilfe dessen Analysen, Fehlerbehebungen, Software- und Protokollkommunikation untersucht werden können.
Hilfreiche Links:

- https://www.lifewire.com/wireshark-tutorial-4143298
- https://www.wireshark.org/download/docs/user-guide.pdf
- https://wiki.wireshark.org/

1.) Finden Sie heraus was das OSI-Modell ist. Sie brauchen zunächst nur ein grobes Verständnis!

2.) Erläutern Sie was in Netzwerken unter Datenkapselung verstanden wird. (Sollte in der Erklärung des OSI-Modells enthalten sein.)

3.) Lesen Sie folgendes Tutorial in Hinblick auf die Fragen in Aufgabe A 4.): https://tinyurl.com/yby2kukf [1]

4.) Nachdem Sie die Tutorials abgearbeitet haben:

a.) Was ist ein *Network-Sniffer*?

b.) Wozu kann ein Netzwerk-Sniffer genutzt werden?

c.) Verschaffen Sie sich einen Überblick, sodass Sie einen Überblick haben wo was zu finden ist, bzw. wo Sie Hilfe finden können.

d.) Recherchieren Sie wozu Filter in *Wireshark* eingesetzt werden.

e.) Bringen Sie in Erfahrung wie Filter genutzt werden.

f.) Welche beiden unterschiedlichen Mitschnitt-Modi (Caputre Modes) bietet *Wireshark*? Worin unterscheiden sich diese?

5.) Erläutern Sie anhand von Beispielen den grundlegende Umgang mit *Wireshark*.

[1] Lohnenswert ist das Wireshark 101 Buch im PDF Format – erhältlich bei der Suchmaschine Ihres Vertrauens.

a.) Erläutern Sie was ein Netzwerkinterface ist.

b.) Wie stellen Sie Netzwerkinterfaces ein – auf welchem Interface soll der Mitschnitt laufen.

c.) Wie filtern Sie nach Protokollen? (TCP, UDP, DNS...)

d.) Wie filtern Sie *MAC*-Adressen?
Die *MAC*-Adresse ist eine Link-Layer-Adresse und sorgt für die Punkt-zu-Punkt-Verbindung innerhalb eines Netzsegmentes (Bspw.: LAN).

e.) Wie filtern Sie *IP*-Adressen?
Analog zur *MAC*-Adresse – jedoch auf dem Network-Layer. *IP* sorgt für eine Ende-zu-Ende-Verbindung über die Grenzen eines Netzsegmentes von zwei Kommunikationsparteien. (Zwei Rechner die über das Hochschulnetz kommunizieren.)

6.) **Fakultativ:** Wenn Sie mögen, können Sie *Wireshark* auf Ihre(n) Gerät(en) installieren oder in der virtuellen Maschine laufen lassen und ihren Netzwerkverkehr ein wenig analysieren.

- https://www.wireshark.org/download.html
- https://www.wireshark.org/docs/wsug_html_chunked/ChapterBuildInstall.html

Aufgabe B – HTTP(S)

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 [1, S. 98ff].

2.) Alternativ: unter https://youtu.be/oXUgqWSvH6k finden Sie eine Einführung zu HTTP.

3.) Skizzieren Sie grob die Funktionalitäten von HTTP.

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

5.) Recherchieren Sie was unter einem Port verstanden wird! Ein grobes Verständnis genügt.

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

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

8.) HTTP ist ein zustandsloses Protokoll. Erläutern Sie diese Aussage!

9.) HTTP arbeitet mithilfe von Methoden: Nennen Sie alle HTTP-Methoden. Notieren Sie sich was diese machen und wie deren Aufruf aussieht.

10.) Machen Sie sich kurz klar, welche Aufgabe SSL/TLS übernimmt. (Hinweis: An dieser Stelle genügt es, wenn Sie wissen was SSL/TLS macht.)

11.) Auf welcher Schicht arbeitet SSL/TLS? Wenn Sie das Akronym auflösen, sollte die Lösung Ihnen entgegen fallen.

12.) HTTP ist ein textbasiertes Protokoll, entsprechend kann dies auch über die Kommandozeile bedient werden.
Mithilfe der Tools *telnet*, *netcat* und *openssl s_client* können Sie Anfragen an den Webserver absetzen.
Durchlaufen Sie folgende Tutorials und notieren Sie sich wie vorgegangen wird:

- https://www.thomas-krenn.com/de/wiki/TCP_Port_80_(http)_Zugriff_mit_telnet_%C3%BCberpr%C3%BCfen
- https://administrator.de/wissen/netcat-tcp-ip-swiss-army-knife-40641.html#toc-4
- https://tinyurl.com/y9nnaz6a oder https://www.feistyduck.com/library/openssl-cookbook/online/ch-testing-with-openssl.html

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

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

15.) Erläutern Sie wie Zertifikate mithilfe *openssl*s geprüft werden können.

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

Das Simple Mail Transfer Protokoll (SMTP) 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.) Wie in den vorigen Aufgaben: https://youtu.be/TntfISdGwO8 gibt eine Einführung zu E-Mail.

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

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

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

5.) Machen Sie sich im Groben klar, wie diese Protokolle arbeiten.

6.) Worin unterscheiden sich POP3 und IMAP?

7.) Auf welchen Ports arbeiten die drei Protokolle?

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

9.) Durchlaufen Sie folgende Tutorials:

- https://www.unixwitch.de/de/sysadmin/tools/imap-mit-ssl-testen
- https://www.atmail.com/blog/imap-101-manual-imap-sessions/
- https://tecadmin.net/send-email-smtp-server-linux-command-line-ssmtp/

Aufgabe D – 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.
Sie nutzen das DNS sicherlich täglich! Bei jedem Aufruf von Websites, lesen Ihrer E-Mails etc. nutzen Sie sicherlich keine *IP*-Adressen, sondern Namen – genauer gesagt Domain-Names, wie etwa htw-berlin.de statt 141.45.66.214. Diese Übersetzung von Domainname auf *IP*-Adresse ist rein kosmetischer Natur, da Menschen i.A. sich Namen besser merken können, als lange Zahlenkolonnen.

1.) DNS 101 – Grundsätzliches zu DNS
Schauen Sie folgendes Video: https://youtu.be/XondVs0hJ8U

a.) Beschreiben Sie mit eigenen Worten, was das DNS leistet.

b.) Recherchieren Sie, was eine Client-Server-Architektur ist. Sie müssen lediglich verstehen, wie diese Aufgebaut ist.

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

a.) Was wird unter dem Begriff Resolver verstanden?

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

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

d.) Was ist ein Bind-Server?

3.) Rechner können die unterschiedlichsten Dienste bereitstellen, auf einem Rechner laufen zumeist mehrere Dienste. Entsprechend gibt es diverse DNS-Record-Types die dies realisieren.
Recherchieren Sie welche Typen von Records es gibt.

4.) 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.) In der Praxis wird eine Mischung aus den beiden obrigen Verfahren angewandt. Recherchieren Sie, wie diese Auflösung „in the wild“ aussieht.

5.) Durchlaufen Sie folgende Tutorials:

- https://www.madboa.com/geek/dig/
- https://www.poftut.com/nslookup-commands-tutorial-with-examples/

Notieren Sie sich wie vorgegangen wird! Diese Tools nutzen Sie in der nächsten Laborübung.

6.) Namensauflösung am praktischen Beispiel.

Tabelle 1: Adressen für DNS-Auflösung.

	Bob	Alice
IP address:	192.45.56.127	208.115.92.45
Local name server:	192.47.56.2	208.115.92.2
SMTP server:	mail.server.org	mail.server.org
Email Address:	bob@realword.org	alice@wonderland.org

a.) Nehmen Sie an Bob möchte eine E-Mail an Alice senden. Um eine Verbindung mit dem SMTP-Server aufzubauen, muss der Name des Servers via DNS in eine IP-Adresse aufgelöst werden. Erläutern Sie welche Nachrichten ausgetauscht werden müssen und zwischen welchen Hosts. Die Auflösung des Domainnamen ist rein rekursive.
Nehmen Sie weiter an, dass nur der Nameserver der für die Domäne server.org zuständig ist, die Anfrage beantworten kann. (Alle Adressen sind in Tabelle 1 zu sehen!) Skizzieren Sie den Ablauf der Namensauflösung!

b.) Nun ist Alice am Zug um Bob zu antworten. Erläutern Sie den Nachrichtenaustausch, wenn eine rein iterative Namensauflösung genutzt wird. Nehmen Sie wie in der vorigen Aufgabe an, dass das nur der Namensserver der zuständig für die Domäne server.org die Anfrage beantworten kann. Skizzieren Sie den Ablauf der Namensauflösung!

c.) Erläutern Sie, wie Bobs SMTP-Server den für Alice verantwortlichen Mail-Transfer-Agent (MTA) findet.

Literatur

[1] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*. Pearson, 6th edition, 2012.