In Layern DENKEN lernen!

1. Was ist im Internet mit einem „autonomen System(AS)“ gemeint?

Unter einem autonomen System im Internet versteht man ein System mit eigenen Knotenpunkten das sich eigenständig verwaltet.

1. Was war das Besondere an dem IPv4-Adressbereich 169.254.0.0 - 169.254.255.255? (Script!)

Das Besondere an dem IPv4-Adressbereich ist das die IP-Adressen nur für die Kommunikation aller lokalen Rechner innerhalb des Sub-Netzwerkes miteinander kommunizieren.

1. Zeichnet in euer Layer/Sanduhr-Bild aus der Vorbereitungsaufgabe die konkreten IP- Adressen eures Family-Netzwerkes inkl. des Camp-Webservers ein („DM-ASP“).

Layer 3

1. Recherche im Script: Was macht das Protokoll ARP?

ARP – Adress Resolution Protocol

ARP ist ein Protokoll mit dem man die Mac Adresse von Geräten einer IP Adresse zuweist.

2. Zeigt mit Wireshark den Ablauf eines ARP-Requests und den eines ARP-Reply im Family- Netzwerk. Lest den ARP-Cache eures Rechners aus.

Arp Request als Broadcast --> Broadcast sendet an alle Teilnehmer im Netzwerk einen Arp Request

1. Startet einen Traceroute zu www.sony.jp direkt aus einem angebundenen Laptop.

Traceroute zeigt nicht den genauen Weg, an den die Pakete zurücklegen

2. Zeigt mit wireshark die jeweiligen ICMP-Botschaften, die ausgetauscht werden und interpretiert diese.

ICMP Type 8 – Echo Request

Time to live exceeded in transit -> TTL wird vor dem Erreichen des Ziels auf 0 gesetzt und verworfen

TTL hochgesetzt

TTL 4 – Rechenzentrum blockt die ICMP Anfrage

TTL 14 – Rechenzentrum blockt die Anfrage nicht

3. Interpretiert aus der traceroute-Konsolenrückmeldung, welche Route euer Auftrag genommen haben könnte.

Die Route zum Peering Gateway + DNS Resolver to the rest oft the world -> Hochschulserver -> Zeitüberschreitung der Anfrage -> Sony

Routeninterpretation nicht genau möglich, nur Zeit

1. Unbedingt auch einen Blick auf browserbasierte Online-Netzwerktools z.B. unter https://www.heise.de/tools/ werfen.

5. Benutzt ein Web-Geolokalisation-Tool, welche die IP-Route/Ziel auf einer Karte darstellen kann. (z.B. geotraceroute.com, iplocation.net, bigdatacloud.com/ip-geolocation, gEO-IO, DB-IP, etc.). Anm.: Mac-Nutzer sind hier im Vorteil. Sie können sich probeweise die Software little snitch installieren und darin die Geo-IP-Analyse durchführen. Zusätzlich im Dateibereich den Artikel „Unzulaenglichkeiten-bei-der-IP-Lokalisierung ....pdf“ im Dateibereich lesen!

6. Wo ist der Server www.netflix.com? Ist das der Streaming-Server von Netflix?

Der Server von Netflix befindet sich in Frankfurt. Es ist nicht der Streaming Server nur der Presentation Server

Jede Family hat (bis zum Ende des 2. Tages) eine kleine Website zu erstellen, mit der sie ihre Family mit Text, Bildern und AV-Material vorstellt. Die Webseiten werden zentral auf dem Camp-Webserver (DM-ASP) gehostet. Upload über FTP (z.B. Filezilla). Für Videos (ca. 4 min, .mp4) das Smartphone benutzen und über html5-video-tag in die Family-Webseite einbinden.

7. Schneidet mit wireshark den FTP-Upload eures Videos auf den Camp-Webserver mit (inkl. Anmeldevorgang auf dem FTP-Server). Welches Sicherheitsproblem von FTP seht ihr?

-> unverschlüsselt

Aufgaben Tag 2

Layer 3-4

1. Startet den Download einer großen Datei aus dem Internet (>1GB), zeichnet mit Wireshark parallel auf. Interpretiert den Inhalt der vorgelagerten DNS-Anfrage/Antwort gem. Script!

A -> IPv4

AAAA -> IPv6

1. Mit welchem IP-TTL-Startwert beginnt euer Rechner die Download-Anfrage? Mit welchem TTL-Wert kommen die ersten Download-Daten an? Wie sind TTL-Werte zu interpretieren?

IP-TTL Startwert -> 128

Mit dem TTL-Wert 54 kommen die ersten Download Daten an

1. Zeigt den TCP-Slow-Start beim Download (I/O-Durchsatz), die RTT-Werte und die TCP- Window-Skalierung. (Begriffe ggfs. im Script suchen!)

Layer 5-6

1. Schaut euch im Script nochmals das Kapitel „Sockets“ an. Installiert die SysInternal-Suite.

2. Fahrt den Rechner komplett runter, startet ihn neu und meldet euch wie gewohnt an.  
3. Öffnet sofort nach dem Anmelden nur das Sysinternals-Programm TCPView (Browser aus!)

4. Wie ist TCPView zu „lesen“? Versucht die dargestellten Ergebnisse eures „unbenutzten“ Rechners zu interpretieren. Filtermöglichkeiten nutzen! Evtl. helfen hier zusätzlich auch die Tools „Autoruns“ und „Process Explorer“ aus der SysInternal-Suite.

Nach dem Start sind einige Programme im Listen/Established Modus.

Listen -> Programm wartet auf Interaktion

Established -> Programm interagiert bereits

5. Laßt TCP-View offen. Startet einen Browser und erniedrigt ihr in der Webconsole o. Entwicklertools den Downloadspeed auf 50kbit/s und das Delay auf 800ms. Ruft eine typische öffentliche Webseite auf. Versucht die in TCP-View dargestellten Abläufe in Bezug zur Webseite zu interpretieren.

Achtung: Ab hier unbedingt HFU-WLAN am Rechner ausschalten und nur noch family-intern über die Ethernet-Schnittstelle arbeiten - da HFU sonst Netzwerk-Attacke vermutet!!

Tool Nmap

1. Installiert die Software Nmap/Zenmap auf einem Rechner.
2. Siehe Script: Was bedeutet bei IPv4 nochmals die Suffix-Schreibweise „141.28.123.0/24“?

Das Suffix „/y“ gibt die Anzahl der 1ner-Bits in der Netzmaske an. Die übrigen Bits sind folglich der Host-Adressbereich der IP Adresse.

1. Recherchieren & ausprobieren“: Was macht Nmap beim intense scan?

-> scannt UDP Ports macht Akteure sowie Endpunkte sichtbar

4. Scannt das Netzwerk mit Nmap sowohl auf der LAN- wie auf der WAN-Seite (10er-Netz) und schaut mit TCP-View dabei zu. Wie ist der Nmap-Ergebnisbericht inkl. „Netzstruktur“ zu interpretieren? Schneidet einen Scan in wireshark mit. Setzt den Mitschnitt in Bezug zur TCP- View Beobachtung und zum Nmap-Ergebnisbericht.

Nmap WAN Seite -> Hosts + IP-Adresse erkennbar

Layer 7 Achtung: → Browser-Cache deaktivieren oder Force Refresh!

Statische HTML-Seite

1. Zeichnet den Browser-Aufruf eurer Family-HTML-Seite mit Wireshark auf.

2. Erläutert die Abläufe zwischen Webbrowser und Server über alle Netzwerk-Layer (siehe Layer-Bild aus Script/KAP. http!).

Unser Webserver startete seinen http-Prozess, -> TCP-Socket: port80 Status: listen (Webserver erwarten Anfrage)

Der Browser startet nach Tastatureingabe von 10.0.0.81/Streaming-Camp/family3 (keinen dns-Dienst da IP-Abfrage)

Multicast (Nutzergruppen gebucht auf einen Zentralverteiler für Daten) (239...)

TCP baut (mittel 3-Wege-Handshake) eine quittungsbasierte Transportverbindung zum Server auf (SYN).

Als diese steht (SYN\_ACK = established), schreibt der Browser den GET-Befehl für /index.html in den Socket.

Bildung eines TCP-Segments, in welches der GET-Request als Daten eingekapselt wird. Versand als IP-Datagramm.

Das „adressierte“ IP-Datagramm nimmt seinen Weg durch das Streaming Camp Internet.

Entwicklertools

1. Analysiert die Kommunikation mit dem Server in den Browser-Entwicklertools. Erläutert die wesentlichen Features der “Entwicklertools“, insbesondere die Features Netzwerkanalyse, Performance und Lighthouse (Chrome).

2. Schaut euch im Script das Kap. Anwendungsperformance an. Wie sieht in den Entwicklertools das UX-Timing eurer Family-Webseite aus (FCP, LCP, etc.)? Vergleicht mit externen Webseiten!

FCP – First Contentful Paint 2019ms -> 2,02 Sekunden (Zeit bis erster Inhalt geladen wird)

LCP – Largest Contentful Paint 56000ms -> 56 Sekunden (Zeit bis größte Element der Seite geladen wurde)

Amazon

FCP – 1,5 Sekunden

LCP – 46 Sekunden

Dynamische HTML-Seite Erniedrigt ihr in der Webconsole o. Entwicklertools wieder den Downloadspeed auf 50kbit/s und das Delay auf 800ms. Browser-Aufruf einer externen, dynamischen HTML-Seite (Typ: Mashup). Versucht die in TCP-View dargestellten Abläufe in Bezug zur Inhalte der Webseite zu interpretieren.

Aufgaben Tag 3

Vorbereitung

Nehmt einen weiteren Videoclip (max. 4 min) als .mp4 auf und speichert ihn mit einem Namen OHNE ... LEERZEICHEN und OHNE --- BINDESTRICHE lokal ab. Ladet den .mp4 Videoclip über das Webfrontend http://10.0.0.81/abr/uploader zum ASP in den sog. „ABR-Fragmenter“.

Klassisches UDP-Streaming

Im Campnetz läuft auf der IP-Adresse 10.0.0.90 eine Life-CAM mit UDP-Outputstream. Diese kann mit dem VLC über rtsp://10.0.0.90:554/live/ch0 angeschaut werden.

1. Was ist ein Stream-socket, was ist ein Datagram-socket? Dokumentiert die Kommunikation VLC/CAM mit wireshark und erläutert diese.

Stream Poket -> TCP

Datagram -> UDP

In Wireshark sehen wir die Kommunikation zwischen uns und verschiedenen Servern. Streaming Server bietet zwei Control Möglichkeiten Server Sidet Control und Player Control.

Player Control Request -> Response

Realtime Transport Protocol (RTP) -> über quittungsloses, schnelles UDP

Real Time Control Protocol (RTCP) ->

1. Wie soll lt. Script die Kommunikation zwischen einem Player (VLC) und einem Mediaserver (Cam) gemäß Script ablaufen? Ist das in wireshark für die Live-CAM nachvollziehbar.

Achtung bei mehreren Versuchen: → Browser-Cache löschen oder Force Refresh!

Progressiver Filmdownload von der Family-Webseite (DMFLIX)

1. Spielt euer lokales mp.4-Videofile auf der Family-Webseite im Browser ab.
2. Dokumentiert die Kommunikation Browser/Server über die Webconsole/Netzwerk.
3. Dokumentiert die socket-Kommunikation Player/Server mit TCP-View.
4. Dokumentiert die gesamte Netzwerkkommunikation mit Wireshark und erläutert diese

mit Bezug zu 2. und 3.

1. Was passiert beim Drücken von Stop -> Start auf dem Netzwerk? (Achtung

Fortschrittsanzeige/Timeline darf noch nicht am Ende angekommen sein).

Alternative-Abspielmöglichkeit: interner ABR-Videoserver (DMFLIX)

1. Kontrolliert, ob euer Videoclip im Fragmenter zu multiplen ABR-Streamingfiles umkonvertiert wurde: http://10.0.0.81/abr/player
2. Ruft die fragmentierte html-Version eures ABR-Films im Browser ab: .../files/xyz.html
3. Dokumentiert die Kommunikation Browser/Server über die Webconsole/Netzwerk.
4. Dokumentiert die gesamte Netzwerkkommunikation mit TCP-View und Wireshark und

erläutert diese mit Bezug zu 3.

1. Was steht im MPD-Manifest, welches beim ersten Aufruf des Videos übertragen wurde?
2. Probeweise beim Abspielen in den Entwicklertools den Netzwerkdurchsatz drosseln.

Wie verändert sich der Streamablauf.

1. Was passiert bei Stop -> Start und einem zeitl. Skip nach vorne auf dem Netzwerk?

Externer ABR-Videoserver (YouTube)  
Sucht über Google das „University LipDub HFU“-Video auf YouTube und spielt es ab. Im laufenden YouTube-Video einfach mal oben/links mit der rechten Maustaste klicken →“stuff for nerds“. Welche Werte werden angezeigt und wie sind sie zu interpretieren? Gegenüberstellen zu den Wireshark Statistiken-Funktionen TCP-Stream Graphen/RTT und .../Durchsatz. Veränderungen anschauen, wenn in den Entwicklertools Throtteling ein-/ausgeschaltet wird.