Header analysieren mit Protocol Analyzer 5-1-2

Ziel
Sie verstehen, wozu ein Protokoll Analyzer dient und wie man ihn einsetzt.
Sie können mit einem Protokoll Analyzer Daten aufzeichnen, die verschiedenen Header in den aufgezeichneten Daten erkennen und den OSI-Layer und Protokollen zuordnen.
Sie können die Filter eines Protokoll Analyzers so konfigurieren, dass nur Pakete, die den Vorgaben entsprechen, aufgezeichnet werden.

Einführung

Der Protokoll Analyzer / Paket Sniffer ist eines der wichtigsten Tools eines Netzwerktechnikers und zwar nicht, um in den Daten anderer rum zu schnüffeln, sondern um bei Problemen die Pakete und die Vorgänge im Netz bis in letzte Details analysieren zu können.
Der Analyzer kennt alle verschiedenen Header und Headerfelder der unterstützen Protokolle und stellt diese möglichst leicht lesbar dar.
Die Interpretation dieser Werte bleibt jedoch dem Menschen überlassen, das heisst zur Fehlerbehebung müssen Sie selber die korrekten Werte kennen!
Durch einen speziellen Modus der Netzwerkkarte (**Promiscuous Mode**) zeichnet der Protokoll Analyzer nicht nur die Datenübertragung des eigenen PCs auf, sondern sämtliche Pakete, die er auf dem Kabel 'sieht'. Da in einem produktiven Netz oft sehr viele Daten übertragen werden, sind Filter ein **wichtiges** Feature von Analyzern. Damit definieren Sie, welche Daten für Sie interessant sind und aufgezeichnet werden (z.B. nur bestimmten Protokolle oder Adressen).

Voraussetzungen

Sie kennen den Aufbau und die Schichten des OSI-Schichtmodells

Benötigte Infrastruktur

`vmLF1` und `vmWP1` mit installiertem Protocol-Analyzer Wireshark auf dem `vmWP1` (*Firewall Einstellungen beachten, dass die ICMP/eingehende Echoanforderung zulassen aktiv ist!*).

Aufgabenstellung

1) Starten Sie Wireshark auf dem `vmWP1`
2) Lesen Sie zuerst die Einführung `Marktplatz\Module\129\Wireshark\129-Wire-Shark Workshop` (Kapitel 1+2) durch.
3) Starten Sie jetzt einen neuen Capture-Vorgang (Aufzeichnung). Stoppen Sie, nachdem Sie einige Pakete aufgezeichnet haben und lassen Sie sich die aufgezeichneten Daten anzeigen. Was stellt der Analyzer in den drei verschiedenen Teilen des Fensters dar? Beschreiben Sie kurz!

.....

.....

.....

.....

4) Produzieren Sie nun selbst einen definierten Datenverkehr und schauen Sie diesen in Wireshark an: a) ein Ping-Paket, b) ein HTTP-Paket. Wie produzieren Sie ein HTTP-Paket?

.....

Header analysieren mit Protocol Analyzer 5-1

5) Untersuchen Sie ein HTTP-Paket genauer. Notieren Sie alle Header, die Sie in diesem Paket entdecken und die zugehörige OSI-Schicht.

.....

.....

.....

6) Sie können die einzelnen Header in Wireshark auf- und zuklappen. Schauen Sie sich die Headerfelder aller Header an. Was sehen Sie beim Layer 4 für Headerfelder? Notieren Sie die ersten fünf Felder (Wir werden diese dann später genauer kennenlernen)!

.....

.....

.....

7) Lesen Sie die genaue Definition des Headerfeldes „Window Size“ in der entsprechenden Norm nach. Welche Norm ist das? .....
Beschreiben Sie dieses Feld kurz auf Deutsch!

.....

.....

.....

Mit dem Programm TCP Optimizer können wir aktiv die „Window Size“ beeinflussen.
https://www.speedguide.net/downloads.php

8) Konfigurieren Sie nun den „Capture Filter“ des Network Analyzers so, dass Sie nur noch ***ping*** **Pakete, die von oder zu Ihrem PC gehen,** speichern. Sie können den nötigen Filterausdruck direkt bei „Capture Filter“ eintippen. Für Wireshark finden Sie Erklärungen zu den Filtern im Tutorial 2. Wie lautet der Filterausdruck?

.....

9) Beschreiben Sie stichwortartig die zwei Tests, die nötig sind, um Ihren Filter zu überprüfen (ob er durchlässt, was er durchlassen soll, und ob er den Rest herausfiltert)

.....

.....

Zeitbedarf

45 - 60 min + 30 min Einführung