01 Protokoll-Analyzer

1 Thema des Praktikums

In diesem Praktikum werden Sie die Infrastruktur des Praktikumraums kennenlernen, sowie mit dem Protokoll-Analyzer Wireshark einen einfachen Versuch durchführen.

Die Schwerpunkte des Praktikums sind:

- Kennenlernen der gesamten Laborumgebung (Arbeitsplätze, PC, div. Geräte, Kabel, ...)
- Bedienung und Einsatzmöglichkeiten der Embedded Linux Box (ELB) über die Konsole
- Bedienung und Einsatzmöglichkeiten von Wireshark (Konfiguration, Aufzeichnung starten / stoppen / abspeichern, einzelne Paketinhalte betrachten, einfache Filter setzen, ...)

2 Vorbereitung

Protokoll-Analyzer gehören zu den wichtigsten Werkzeugen, um Protokolle zu untersuchen oder Fehler zu finden. Glücklicherweise gibt es heute ein Open-Source-Produkt (Wireshark), das dank weltweitem Support durch eine grosse Anzahl von Entwicklern praktisch alle bekannten Protokolle unterstützt.
Die Aufzeichnung der Daten erfolgt im einfachsten Fall mit der Standard-Netzwerkkarte des PC und einer ebenfalls freien verfügbaren Software-Library (WinPcap). Die Standard-Netzwerkkarte hat allerdings den Nachteil, dass bei grosser Netzlast nicht alle Pakete aufgezeichnet werden können und nur (Layer 1-) fehlerfreie Pakete angezeigt werden können. Wer mehr braucht, muss in eine Zusatz-Hardware investieren.

- Installieren Sie zuhause Wireshark (https://www.wireshark.org/#download) auf Ihrem persönlichen Laptop bzw. Computer.
- Je nach Vorkenntnissen studieren Sie auf https://www.wireshark.org/docs/ die Einführungsvideos wie „Introduction To Wireshark“. Sie finden dort auch interessante Anwendungsbeispiele, die wesentlich weiter gehen, für die aber noch die Theorie fehlt.
- Starten Sie Wireshark und machen Sie sich mit einigen im Video erklärten Funktionen vertraut.

Vor Beginn des Labors, zeigen Sie die folgenden Vorbereitungen dem Praktikumsbetreuer:

- Demonstrieren Sie den installierten Wireshark auf Ihrem Laptop.
- Was ist die Aufgabe der WinPcap-Library?

WinPcap ermöglicht Anwendungen die Erfassung und Übertragung von Netzwerk-Paketen unter Umgehung des Protokollstapels

---

- Nehmen Sie an, die Aufzeichnung im Wireshark sei gestartet, aber es werden offensichtlich falsche (oder gar keine) Pakete angezeigt. Was könnte der Grund sein?

Ich nehmen an, dass eine mögliche Fehlerquelle eine nicht vorhandene Internverbindung sein könnte. Oder aber WinPcap

---

- Das Wireshark Fenster besteht aus 3 Teilen. Wie werden diese bezeichnet und was ist deren Zweck?

Paket-Liste, Auflistung sämtlicher Pakete (https://www.wireshark.org/docs/wsug_html_chunked/ChUsePacketListPaneSection.html)

Paket-Detailansicht, detailierte Informationen zu einem spezifischen Paket (https://www.wireshark.org/docs/wsug_html_chunked/ChUsePacketDetailsPaneSection.html)

Paket-Bytes, zeigt die Daten des Pakets im hexadezimalen Format an (https://www.wireshark.org/docs/wsug_html_chunked/ChUsePacketBytesPaneSection.html)

- Wozu dienen im Wireshak die Coloring Rules?

Durch die Farbregeln, hat man die Möglichkeit die interessanten Pakete anhand der Farbe zu erkennen. Die Coloring Rules sind standardmässig eingestellt, können aber auch manuell angepasst werden

---

3 Aufbau der Versuchsanordnung

Die Versuchsanordnung soll gemäss Abbildung 1 aufgebaut werden.

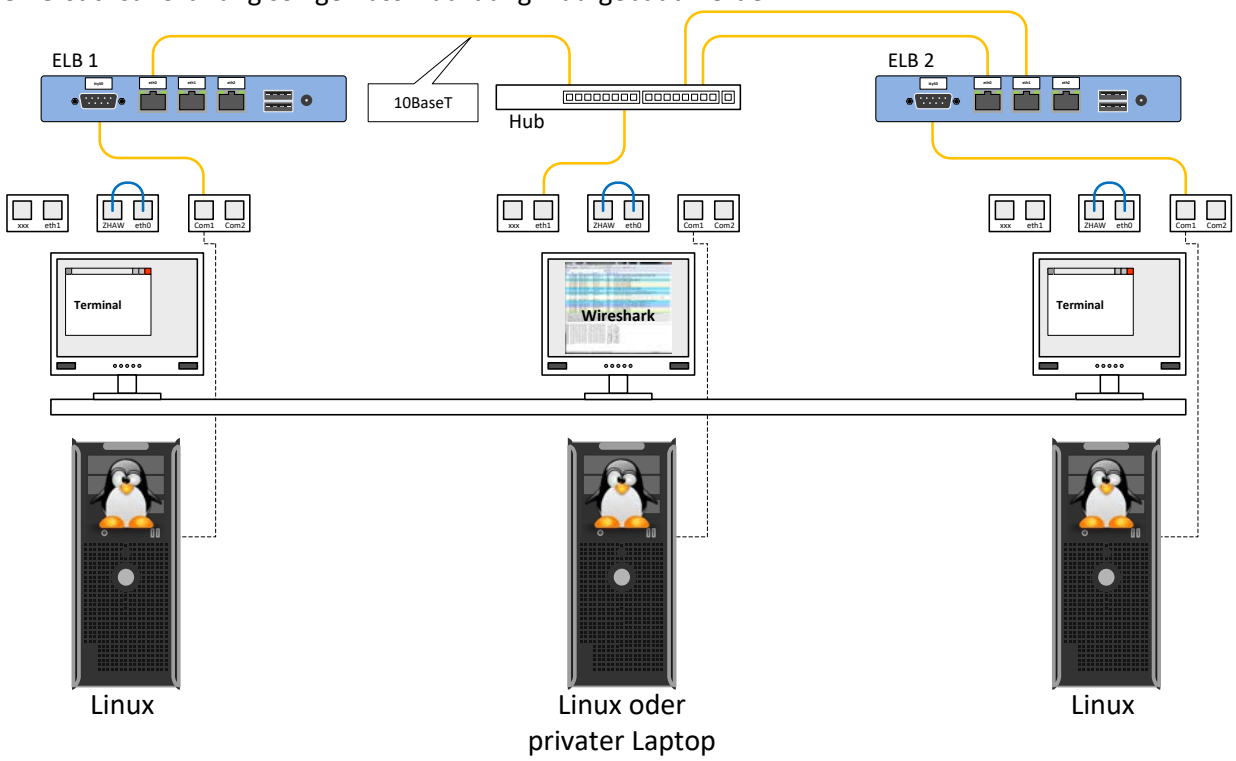

Abbildung 1 - Versuchsaufbau

- Falls nötig, verbinden Sie alle Rechner mit dem ZHAW Netz. Verbinden Sie dazu jeweils an den Arbeitsplätzen die Dosen ZHAW und eth0 miteinander (kurzes blaues 10BaseT Kabel).
- Starten Sie alle Rechner mit Linux

Statt des mittleren Rechners können Sie auch einen oder mehrere private Laptops anschliessen, auf denen Sie Wireshark installiert haben.

Eine **Embedded Linux Box (ELB)** ist ein Kleincomputer mit drei Netzwerkschnittstellen. Darauf ist ein Linux installiert, auf dem nur die notwendigsten Dienste laufen; insbesondere keine grafische Benutzeroberfläche. Die Bedienung muss darum über die serielle Schnittstelle erfolgen. Dazu benötigt man eine Terminal-Emulation wie das Programm **`putty`**. Dieses sendet Tastatureingaben über die serielle Schnittstelle und stellt die von der seriellen Schnittstelle empfangenen Zeichen im Terminal-Window dar.

- Starten Sie die Terminal-Emulation über das Startmenu **`Putty SSH Client`** oder in einem Linux Terminal-Window mit: **`sudo putty`**. Die richtige Schnittstelle laden (**`COM1 oder COM2`**), danach die Verbindung öffnen.
- Nachdem das Linux auf der Embedded Linux Box hochgefahren ist, wechseln Sie in das Verzeichnis von Praktikum eins.

  ```
  cd /ktlabor/prakt_1/
  ```

- Erlangen Sie mit der Eingabe von **`su`** Administratoren Rechte. Das Passwort lautet **`KT-Praktika`**.
- Konfigurieren Sie die beiden Embedded Linux Boxen mit den folgenden Befehlen:

  ELB 1
  ```
  ./config_a
  ```

  ELB 2
  ```
  ./config_b
  ```

Achtung: Wenn Sie die Embedded Linux Boxen am Schluss des Praktikums nicht mehr benötigen, fahren Sie diese unbedingt mit dem folgenden Befehl herunter! Die ELB schaltet sich dann selbst aus.

```
shutdown –h now
```

4 Messungen mit Wireshark durchführen

4.1 Netzwerkverkehr aufzeichnen

- Starten Sie auf dem mittleren Rechner oder dem/den privaten Laptop/s in Wireshark die Aufzeichnung.
- Starten Sie auf der ELB 1 das Programm **`messung1`** (Verzeichnis /ktlabor/prakt_1). Dieses Programm sendet 10´000 Pakete auf Ihr Versuchsnetz.

  `./messung1`
- Schauen Sie sich in den Statistik-Menüs die verschiedenen Informationen an. Nach einiger Zeit stoppen Sie die Aufzeichnung und beantworten Sie die folgenden Fragen:

  Wie gross ist der max. Datendurchsatz im LAN (Bytes/sec)?

Der maximale Datendurchsatz ist 3831 Bytes / sec

Wie gross ist der durchschnittliche Datendurchsatz im LAN (Bytes/sec) ?

Durchschnittlich sind es ca 800 Bytes / sec

Welches Transport-Layer-Protokoll sendet die meisten Daten? TCP

Welches Transport-Layer-Protokoll sendet die meisten Pakete? UDP

Woher kommt der Unterschied zwischen Paketanzahl und Datenmenge?

Nicht jedes Paket hat dieselbe Grösse

4.2 Statistische Auswertungen des Netzwerkverkehrs (*Monitor*)

- Brechen Sie das Programm messung1 auf der ELB 1 ab und beenden Sie die Aufzeichnung im Wireshark.
- Starten Sie auf der ELB 1 das Programm **`messung2`** (2000 Pakete) und zeichnen Sie dieses wieder mit Wireshark auf.

  `./messung2`
- Schauen Sie sich die Informationen in den verschiedenen Windows an.
- Warten Sie bis das Programm **`messung2`** abgeschlossen wurde und stoppen Sie die Aufzeichnung.

  Welche IP-Adresse besitzt der Top User und wie gross ist sein Anteil (in %) ?

160.85.17.10 & nahezu 100%

- Starten Sie eine neue Aufzeichnung und starten Sie auf der ELB 1 das Programm messung2 nochmals. Setzen Sie nach ca. 30 Sekunden auf der ELB 2 den folgenden Befehl ab.

  `ping 160.85.17.10 –f –s 1000`

  Was stellen Sie mit dem Wireshark fest? Welches Protokoll hat am meisten Traffic?

Das Verhältnis hat sich auf 50/50 geändert. Nahezu 100% des Verkehrs laufen über IPv4

- Betrachten Sie die verschiedenen Layer im mittleren Protokoll-Window und die Position der verschiedenen Header im Daten-Window (unten). Zeichnen Sie von einem ICMP-Request-Paket die Header der verschiedenen Layer massstäblich auf.

Zeigen Sie die Resultate dem Laborbetreuer.

5 Such- und Filter-Funktionen

In einem Netzwerk treten sehr grosse Datenmengen auf. Meist sind aber nur einige spezifische Informationen von Interesse. Mit Wireshark können fast alle bekannten Protokolle gefiltert und nach einzelnen Eigenschaften sortiert werden. Unter *Analyze → Enabled Protocols…* können Sie eine Liste abrufen. Um es etwas einfacher zu machen, können Sie in der Toolbar Filter neben dem Eingabefeld mit dem Knopf *Expression …* einen Dialog abrufen, der Ihnen das Zusammenstellen von Filtern vereinfacht.
Sie haben nun die Aufgabe, durch verschiedene Filterfunktionen an Informationen zu gelangen, die in den Paketen versteckt sind. Wenn Sie alle Informationen gefunden haben, können Sie die letzte Aufgabe lösen.

5.1 In der Aufzeichnung Daten suchen

Ein Passwort ist im nächsten Versuch versteckt, finden Sie es!

- Starten Sie eine Aufzeichnung.
- Starten Sie auf der ELB 1 das Programm passwort (2500 Pakete). # ./passwort
- Suchen Sie nach dem Passwort. Unter *Edit -> Find Packet …* (Abbildung 2) können Sie eine Zeichenkette im Paketinhalt suchen; und hier suchen wir offensichtlich nach einem Passwort ☺.

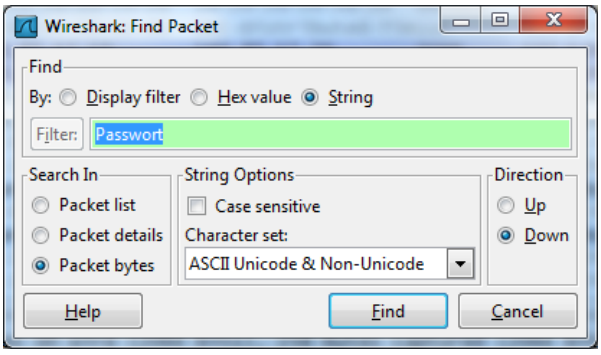

Abbildung 2

5.2 In der Aufzeichnung Daten ausfiltern

- Sie werden nun merken, dass sehr viele Pakete vom Typ udp nur ein leeres Passwort beinhalten, filtern Sie diese mit aus. Die Anweisung „Ich will nur Pakete, die kein udp enthalten!“ müsste eigentlich mit dem folgenden Filter ausgedrückt werden: „**`!(ip.proto == 17)”;`** es gibt aber auch die Kurzform: „**`!udp”`**

  Wie heisst das Passwort (Hinweis: Textinfos finden Sie am besten im Hex-Window)?

kommunikation

- Ein Benutzername ist in einem TCP-Paket versteckt. Starten Sie eine neue Aufzeichnung im Wireshark und starten Sie auf der ELB 1 das Programm **`benutzer`** (2000 Pakete).
  `./benutzer`
- Versuchen Sie den Benutzernamen durch Kombination von Filtern herauszufinden.

Benutzername: student

5.3 Hardware-Filter und Quick-Filter

- Eine Geheimzahl ist in einem IP-Paket versteckt. Dieses IP-Paket enthält ein UDP-Protokoll mit der Zeichenfolge „**`Geheimzahl`**“.
- Starten Sie eine neue Aufnahme via *Capture -> Options* und geben Sie dort im Dialog bereits einen passenden Filter ein.
- Starten Sie auf der ELB 1 das Programm **`adresse`** (1500 Pakete).
  `./adresse`

Wie heisst die Geheimzahl?

160.85.17.30

Haben Sie alle drei Angaben gefunden?

- Starten Sie auf der ELB 1 eine Telnet-Verbindung zu der gefundenen Geheimzahl.
  `telnet` ***`geheimzahl`***
- Sie erhalten eine Linux Information. Authentisieren Sie sich mit dem gefundenen Benutzernamen und dem Passwort.

Zeigen Sie die Resultate dem Laborbetreuer.

6 Weitere Aufgaben

- Öffnen Sie Capture -> Options und wählen Sie das Interface eth0, das am ZHAW Netz angeschlossen ist.
- Starten Sie eine Aufzeichnung und erzeugen Sie etwas Netzverkehr: z.B. Surfen auf verschiedenen Websites, Youtube, Email-Versand, Videochat etc.
- Stoppen Sie die Aufzeichnung.
- Gehen Sie nun in das Menü Statistics -> Protocol Hierarchy. Dort sehen Sie die Verteilung des gesamten aufgezeichneten Verkehrs auf die verschiedenen Protokolle und deren Schachtelung.
- Gehen Sie nun in das Menü Statistics -> IO Graph. Sie sollten nun eine graphische Darstellung des Netzwerksverkehrs über die Zeit sehen. Wenn Sie Filter eintragen, wie:

```
tcp
udp
ip.src_host contains "zhaw"
```

werden die entsprechenden Pakete als farblich hervorgehobene Kurven angezeigt.