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 (Npcap). 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.

Q01 *Was ist die Aufgabe der Npcap-Library?*

"packet capture and transmission library" d.h. es zeichnet die einzelnen Datenpakete im Netzwerk auf (und könnte auch welche senden)

Q02 *Nehmen Sie an, die Aufzeichnung im Wireshark sei gestartet, aber es werden offensichtlich falsche (oder gar keine) Pakete angezeigt. Was könnte der Grund sein?*

Falsche Netzwerkschnittstelle ausgewählt, falsche Filter gewählt, Firewall oder Sicherheitssoftware blockiert den Zugriff, etc.

Q03 *Das Wireshark Fenster besteht aus 3 Teilen. Wie werden diese bezeichnet und was ist deren Zweck?*

Oben: **Packet List Pane (Paketliste)**

Mitte: **Packet Details Pane (Paketdetails)**

Unten: **Packet Bytes Pane (Paketbytes)**

Q04 *Wozu dienen im Wireshark die Coloring Rules?*

Hervorhebung relevanter Pakete, Schnelle Fehlererkennung, Verbesserte Lesbarkeit

Demonstrieren Sie das installierten Wireshark auf Ihrem Laptop.

3 Aufbau der Versuchsanordnung

Die Versuchsanordnung soll gemäss Abbildung 1 aufgebaut werden.

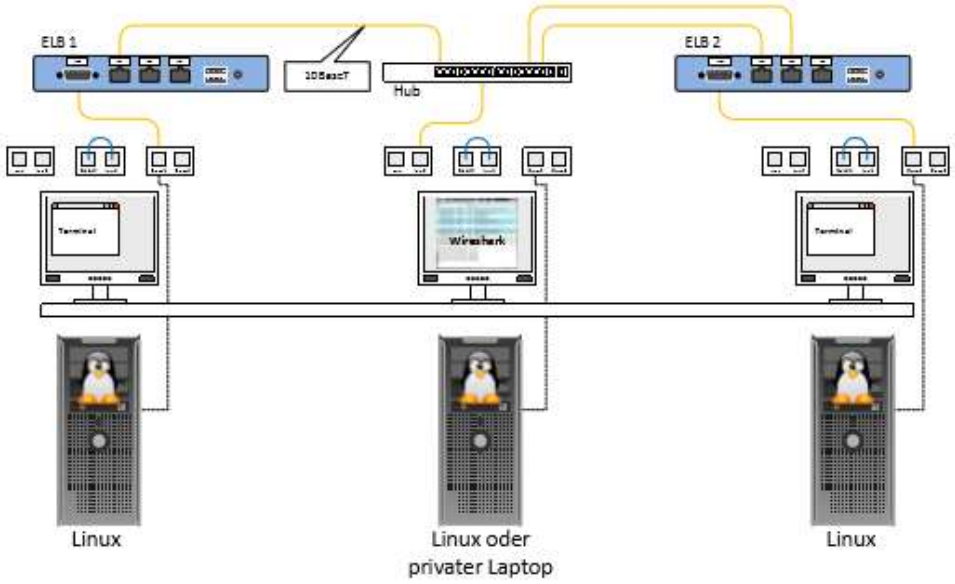

Abbildung 1 - Versuchsaufbau

- Falls nötig, verbinden Sie alle Rechner mit dem ZHAW-Netz. Verbinden Sie dazu jeweils an den Arbeitsplätzen die Dosen ZHAW und lan1 miteinander (kurzes blaues 10BaseT Kabel).
- Starten Sie alle Rechner mit Linux

Statt des mittleren Rechners können Sie mit einem Ethernet-Kabel vom Hub auch einen oder mehrere private Laptops anschliessen, auf denen Sie Wireshark installiert haben.

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

Verbinden Sie **die ELB 1** mit dem Laborrechner links und **die ELB 2** mit dem Laborrechner rechts.

- Starten Sie auf den Laborrechnern das Programm PuTTY (**Menu > Internet > PuTTY SSH Client**), wählen Sie die Schnittstelle **COM1** aus, laden die dessen Config (**Load,** (Serial Verbindung mit Speed 115'200 via COM1 oder COM2)) und öffnen Sie die Verbindung (**Open**).
- Nachdem das Linux auf der ELB hochgefahren ist, wechseln Sie ins Verzeichnis von Praktikum 1.

```
cd /ktlabor/protokoll-analyzer
```

- 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 der ELB 1** das Programm `messung1` (Verzeichnis `/ktlabor/protokoll-analyzer`). Dieses Programm sendet 100'000 Pakete auf Ihr Versuchsnetz.
  `./messung1`
- Starten Sie auf dem mittleren Rechner oder dem/den privaten Laptop/s in Wireshark die Aufzeichnung. Die Messung dauert ca. 13 Sekunden.
- Nachdem `messung1` beendet ist, stoppen Sie die Aufzeichnung im Wireshark.
  Schauen Sie sich anschliessend in den Statistik-Menüs die verschiedenen Informationen an und beantworten Sie die folgenden Fragen:

Q05 *Wie gross ist der maximale Datendurchsatz im LAN (Bit/sec)?*

8.6 MBit/s

Q06 *Wie gross ist der durchschnittliche Datendurchsatz im LAN (Bit/sec)?*
Drücken Sie dazu ev. die "Refresh"-Taste, damit sicher alle gemessenen Daten geladen werden.

5.5 kBit/s

Q07 *Welches Protokoll (TCP, UDP, ICMP oder ARP) sendet prozentual am meisten Daten?*

TCP (34.1%)

4.2 Statistische Auswertungen des Netzwerkverkehrs (*Monitor*)

- Starten Sie **auf der ELB 1** das Programm `messung2` (2'000 Pakete) und zeichnen Sie diese auf.
  `./messung2`
- Warten Sie, bis das Programm `messung2` abgeschlossen wurde und stoppen Sie die Aufzeichnung.
- Schauen Sie sich die Informationen in den verschiedenen Windows an.

Q08 *Welche IP-Adresse sendet am meisten Pakete und wie gross ist sein Anteil (in %)?*

160.85.17.10 (55%)

- Starten Sie eine neue Aufzeichnung und starten Sie **auf der ELB 2** einen ping der Grösse 1'000 Bytes an die Adresse 160.85.17.10

  ELB2: `ping 160.85.17.10 -s 1000 -c 5`

Betrachten Sie die verschiedenen Layer im mittleren Protokoll-Window
und die Position der entsprechenden Header im Daten-Window (unten).

Q09 *Eruieren Sie die Grössen der Header von Ethernet (Layer2), IP (Layer 3).*

IP: 20 Bytes
Ethernet: 14 Bytes

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.

Alternativ kann unter dem Menü **Edit > Find Packet...** unter dem Display Filter eine zusätzliche Zeile eingeblendet werden, welche 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 ☺.

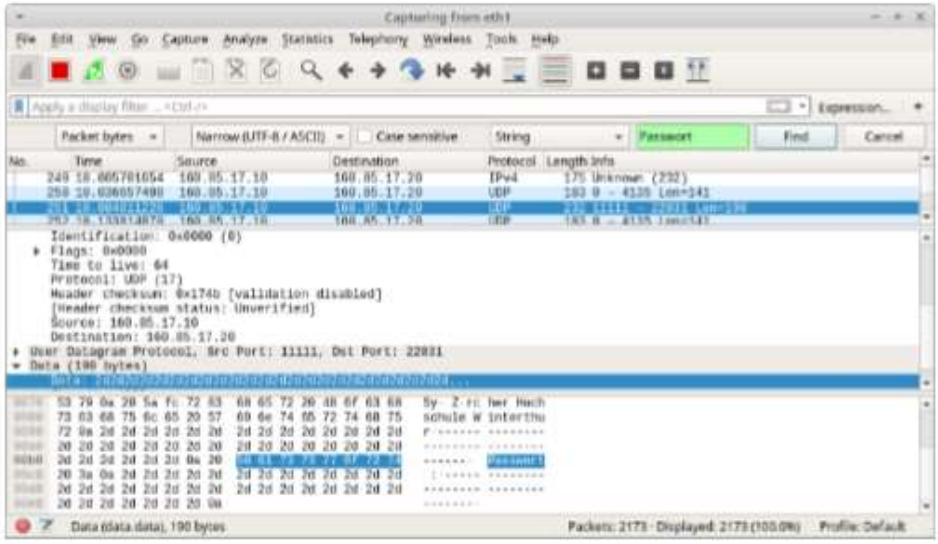

Abbildung 2

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"`

Q10 *Wie heisst das Passwort (Hinweis: Textinfos finden Sie am besten im Hex-Window)?*

Passwort: kommunation

- 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` (2'000 Pakete).
  `./benutzer`

Q11 *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`

Q12 *Wie heisst die Geheimzahl?*

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.

Q13 *Authentisieren Sie sich mit dem gefundenen Benutzernamen und dem Passwort.*

✓

Zeigen Sie die Resultate dem Laborbetreuer.

6 Optionale Aufgaben zur Vertiefung

- Öffnen Sie **Capture -> Options** und wählen Sie das Interface lan1, 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"
```

dann werden die entsprechenden Pakete als farblich hervorgehobene Kurven angezeigt.