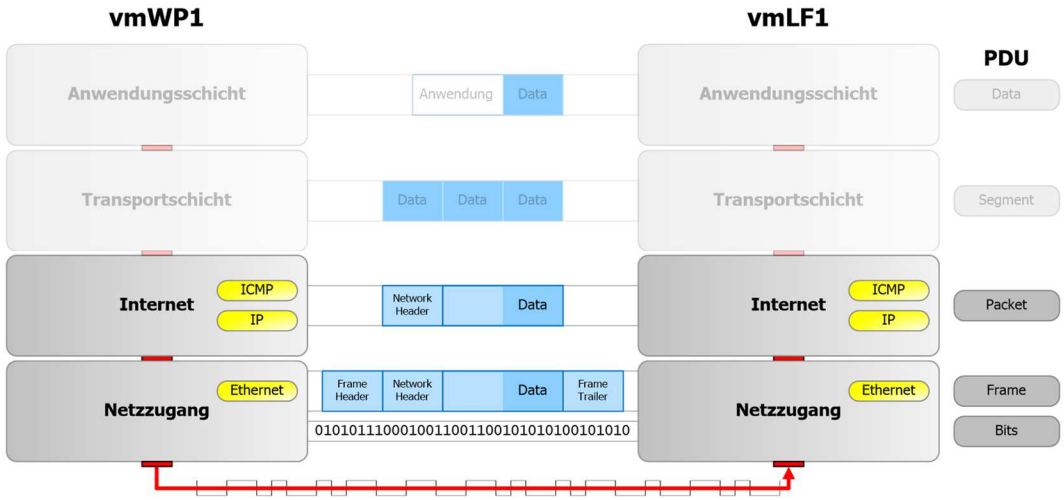
# Protokollanalyse - Workshop

Das bereitgestellte Übungsszenario bietet uns nun gute Möglichkeiten die wichtigsten Handgriffe im Umgang mit den Analysewerkzeugen *WireShark*, *tshark* und *tcpdump*. Mit der gleichzeitigen Darstellung der jeweiligen Auswertungsabläufe im TCP/IP-Kommunikationsmodell gewähren uns diese Tools einen ersten Einblick in die Tiefen des TCP/IP-Datenstroms.

**Ping Auswertungen anzeigen**

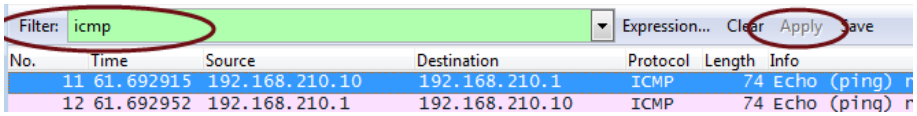
| | |
|---|---|
| **Ablauf** | **Szenario**<br>Auf dem Windows-PC wird die Firewall *vmLF1* auf der Schnittstelle *green0* „angepingt".<br><br>**Erfassen und Auswerten**<br>Auf der *vmLF1* wird der Datenverkehr mit **`tcpdump`** erfasst und angezeigt. Auf der Windowsmaschine *vmWP1* wird der Datenverkehr auf *eth0* mit **`tshark`** erfasst und angezeigt. |
| **TCP/IP-Modell** |  |

| Schritt | Maschine | Aktion |
|---|---|---|
| 1 | *vmLF1*<br>Konsole 1 | `root@vmLF1:~# tcpdump -i green0` |
| 2 | *vmWP1*<br>CMD-Fenster 1 | `C:\>tshark -i 1` |
| 3 | *vmWP1*<br>CMD-Fenster 2 | `C:\>ping -n 10 192.168.210.1` |
| 4 | *vmLF1*<br>*vmWP1* | Aufzeichnung mit `Ctrl+C` abbrechen |

| | | |
|---|---|---|
| **Fragen** | Welche Protokolle werden vom `ping`-Befehl benutzt? | - ICMP, IP, Ethernet |
| | Wie sieht ein ICMP-Request auf der Senderseite aus? | 192.168.210.10 -> 192.168.210.1 ICMP 74 Echo (ping) request |
| | Welche PDU's sind beim `ping` beteiligt? | - Paket, Frame, Bit |
| | Was zeigt `tshark` anders an als `tcpdump`? | - id bei tshark hexadezimal, bei tcpsump dezimal<br>- ttl wird nur bei tshark angezeigt<br>- Länge wird nur bei tcpdump angezeigt<br>- tcpdump zeigt Namen an, tshark IP |
| | Welchen Unterschied sehen Sie beim **`ttl`**? | - ICMP-request hat 128<br>- ICMP-replay hat 64 |

**Ping Auswertungen speichern und anzeigen.** Eine reine Bildschirmauswertung macht meistens wenig Sinn, aus diesem Grund speichern wir die nächste Auswertung in einem zu WireShark kompatiblen File ab.

| | |
|---|---|
| **Ablauf** | **Szenario**<br>Auf dem Windows-PC wird die Firewall *vmLF1* auf der Schnittstelle *green0* „angepingt".<br><br>**Erfassen und Auswerten**<br>Auf der *vmLF1* wird der Datenverkehr mit **`tcpdump`** erfasst und gespeichert. Die Daten werden anschliessend auf den *vmWP1* kopiert und mit *WireShark* angezeigt . Auf der Windowsmaschine *vmWP1* wird der Datenverkehr auf *eth0* mit **`tshark`** erfasst, gespeichert und mit *WireShark* angezeigt. |
| **TCP/IP-Modell** | **siehe Modell auf Seite 1** |

| Schritt | Maschine | Aktion |
|---|---|---|
| 1 | *vmLF1*<br>Konsole 1 | `root@vmLF1:~# tcpdump -i green0 -s 65535 -w /tmp/wp1-ping-lf1-r.pcap` |
| 2 | *vmWP1*<br>CMD-Fenster 1 | `C:\>tshark -i 1 -w \capdat\wp1-ping-lf1-s.pcap` |
| 3 | *vmWP1*<br>CMD-Fenster 2 | `C:\>ping -n 10 192.168.210.1` |
| 4 | *vmLF1*<br>*vmWP1* | Aufzeichnung mit `Ctrl+C` abbrechen, jedoch Fenster nicht schliessen. |
| 5 | *vmWP1* | Aufzeichnung von *vmLF1* mit *pscp.exe* ins Verzeichnis `C:\capdat` kopieren (siehe Seite 5). |
| 6 | *vmWP1* | `vmWP1-ping-vmlf1-r.pcap` und `vmWP1-ping-vmlf1-s.pcap` je mit *WireShark* öffnen und vergleichen. |
| 7 | *vmWP1* | Setzen Sie je den Display-Filter `icmp` in die Filtereingabe und drücken Sie `Apply`.<br>  |

| | | |
|---|---|---|
| **Fragen** | Welchen Unterschied sehen Sie in den zwei Auswertungen? | keine, es sind die gleichen ICMP Pakete |
| | Was ist die Konsequenz aus der ersten Frage? | Es spielt keine Rolle an welchem Endpunkt die Aufzeichnung gemacht wird wenn die überwachten Geräte im gleichen Netz sind. |
| | Was bewirkt der ICMP-Filter? | Es werden nur die ICMP-Pakete angezeigt? |
| | Was passiert, wenn Sie den Display-Filter `icmp.type == 0` eingeben? | Es werden nur die ICMP-Replys angezeigt. |
| | Wie lautet der Display-Filter für die ICMP-Requests? | icmp.type == 8 |
| | In welchem Bereich finden Sie den ICMP-Type? Benutzen Sie die Beschreibung der verschiedenen WireShark-Ausgabefenster im **Anhang A**. | Paketdetail, Abschnitt Internet Control Message Protocol (Type 8 request, Type 0 reply). |
| | Was wird ausgegeben mit dem Filter `ip.dst == 192.168.210.1`? | Nur die Pakete welche für vmLF1 bestimmt sind, in unserem Fall die ICMP-Request. |
| | Wie könnte der Filter aussehen, wenn Sie nur die ausgehenden Pakete von *vmWP1* sehen möchten? | ip.src == 192.168.210.10 |
| | Der Ping-Befehl schickt per Default 32 Byte Daten. Wie findet man diese Daten und wie sehen sie aus? | Im Unterabschnitt Data des Internet Control Message Protocol und zwar wiederholt die Kleinbuchstaben a..w. |
| | Wo können Sie die Laufzeit zwischen einem ICMP-Request und einem ICMP-Reply herauslesen? | Die Time-Differenz zwischen ICMP-Request und ICMP-Reply. |
| | Ergänzen Sie gemäss **Anhang B** die Paketliste mit einem neuen Feld *Delta-Time*. Stimmt die *DeltaTime*-Angabe mit der Ausgabe Zeitangabe im CMD-Fenster 2 von *vmWP1*? | ja |