

Modul 15

1. Erforschung von UDP:

- Tauche ein in die Welt von UDP, einem 'Best-Effort'-Übertragungssystem. Entdecke, warum UDP für Anwendungen wie Streaming-Audio und VoIP bevorzugt wird. Finde heraus, wie UDP-Pakete ihren Weg durch die Datenwolken nehmen und warum Verluste manchmal unvermeidlich sind.

A: UDP (User Datagram Protocol) braucht anders als bei TCP keine Bestätigung vom Zielsystem und wird von Programmen benutzt die keine große Latenz wollen und es nicht schlimm ist wenn ein paar Datenpakete verloren gehen. Datenpakete verloren, weil die Pakete jeweils verschiedene Wege durchs Internet durchlaufen. Manche Wege sind Optimal und so kann es zu Datenpaketverlusten kommen.

2. Das Geheimnis der TCP-Sequenznummern:

- Ergründe die Welt von TCP, wo jedes Paket eine Sequenznummer hat. Verstehe, wie TCP Nachrichten in Segmente aufteilt und sie mit Sequenznummern versieht. Erfahre, warum TCP eine zuverlässige Zustellung sicherstellt, indem es verlorene Segmente erkennt und erneut sendet.

A: Bei TCP(Transmission Control Protocol) wird jede Übertragung von Datenpaketen über eine Bestätigung aller angekommenen Segmente in Form von Sequenznummer versehen. Dies bedeutet das Client und Server dauert im Austausch sind ob alle Datenpakete angekommen sind oder

nicht. Es wird erst mit weiteren Datenpaketen fortgefahren wenn alle Segmente fehlerfrei übertragen wurden. Programme nutzen TCP die es sich nicht leisten können das Datenpakete verloren gehen.

3. Die Rolle der Portnummern:

- Entdecke die Bedeutung von Portnummern, die Protokolle und Dienste identifizieren. Lerne die Kategorien von Ports kennen, von Well-Known Ports bis zu Private Ports. Verstehe, wie Portnummern in jeder Nachricht die Konversation zwischen Client und Server verfolgen.

A: Wenn ein Datenpaket über TCP oder UDP übertragen wird, werden die Protokolle und die Dienste mit bestimmten Portnummer identifiziert. Dies ist dafür da damit jede Konversation zwischen Server und Client übersichtlich überwacht werden kann, sodass mehrere Dienste/Protokolle gleichzeitig auf dem Server oder Client laufen kann. Jede Nachricht die ein Sender sendet beinhaltet ein Quell- und Ziel-port.

4. ICANN und die Verwaltung von Ports:

- Erfahre mehr über die Organisation ICANN, die Ports in drei Kategorien verwaltet. Erkenne, wie Well-Known Ports, Registered Ports und Private Ports unterschiedliche Funktionen und Anwendungen haben.

A: "Well Known Ports" sind die gewöhnlichen Ports die von den meisten Protokollen/Dienste verwendet werden. Bereich ist 1 - 1023.

"Registered Ports" sind Ports die jeweils als Quell oder Ziel Port verwendet werden kann. Bereich ist 1024 - 49151.

"Private Ports" sind Ports meistens verwendet als Quellport. Bereich ist 49152 - 65535.

5. Die Welt der aktiven TCP-Verbindungen:

- Achte auf unerklärte TCP-Verbindungen, die mögliche Sicherheitsrisiken darstellen können. Nutze das Netzwerkdienstprogramm Netstat, um aktive TCP-Verbindungen zu überprüfen. Verstehe, wie Netstat Protokolle, lokale und fremde Adressen sowie den Verbindungsstatus auflistet.

A: "Netstat" zeigt die alle aktiven Verbindungen auf dem eigenen Rechner. Dies ist besonders wichtig wenn man sich fragt warum man einen gewissen Port nicht verwenden kann und dann sieht das dieser schon in Nutzung ist. Außerdem kann dies auch als Übersicht genutzt werden um zu sehen ob fremde aktive Verbindungen zum eigenen Rechner bestehen.