Übung 2 Migena Gelaj- 1634641

Aufgabe 2.

Traceroute ist ein Netzwerkprotokoll, das verwendet wird, um den Weg eines Datenpakets von einem Quellsystem zu einem Zielsystem zu verfolgen. Es funktioniert, indem es Pakete mit einer Time-to-Live(TTL) von 1 bis n sendet und die Antworten von jedem Router aufzeichnet, den das Paket durchläuft. Die TTL wird bei jedem Hop dekrementiert, und wenn sie 0 erreicht, bevor das Ziel erreicht wird, sendet der Router eine ICMP-Nachricht „Time Exceeded“ an das Quellsystem. Die Nachricht enthält Informationen über den Knotenpunkt, der das Paket verworfen hat. Traceroute wiederholt diesen Vorgang, wobei es jedes Mal die TTL um 1 erhöht, bis das Ziel erreicht ist. Wenn wir beispielsweise Traceroute verwenden, um den Weg zur ANU von unserem Computer aus zu verfolgen, würde der Befehl folgendermaßen aussehen:

1 192.168.1.1 (192.168.1.1) 1.000 ms 2.000 ms 3.000 ms

2 10.0.0.1 (10.0.0.1) 5.000 ms 6.000 ms 7.000 ms

3 200.1.1.1 (200.1.1.1) 10.000 ms 11.000 ms 12.000 ms

4 168.12.1.1 (168.12.1.1) 15.000 ms 16.000 ms 17.000 ms

5 130.34.56.78 (130.34.56.78) 20.000 ms 21.000 ms 22.000 ms

6 10.10.10.1 (10.10.10.1) 25.000 ms 26.000 ms 27.000 ms

7 anu.edu.au (130.34.56.1) 30.000 ms 31.000 ms 32.000 ms

Jede Zeile in der Ausgabe stellt einen Hop auf dem Weg zum Ziel dar. Die erste Zahl in jeder Zeile ist die Hop-Nummer. Die zweite Zahl ist die IP-Adresse des Routers, der den Hop verarbeitet hat.Die dritte,vierte und fünfte Zahl sind die Round-Trip-Zeiten(RTTs) für die Pakete, die an diesen Router gesendet wurden. Die RTT ist die Zeit, die ein Paket benötigt, um zur Router zu gelangen und eine Antwort zu erhalten.

Die Ausgabe zeigt, dass das Paket sieben Hops durchlaufen muste, um die ANU zu erreichen. Der erste Hop war zu unserem lokalen Router, der zweite Hop war zu unserem ISP-Router,der dritter Hop war zu einem Router im Backbone-Netzwerk unseres ISPs, der vierte Hop war zu einem Router im australischen Internet, der sechste Hop war zu einem Router im ANU-Netzwerk, und der siebte Hop war zum ANU-Webserver.

Die RTTs für die Hops variieren.Dies liegt daran,dass die Entfernung zwischen den Routern und die Auslastung der Netzwerke unterschiedlich sind.Die RTTs zum ANU-

Webserver sind relative niedrig, da sich die ANU in Australien befindet und unser Computer wahrscheinlich über ein Hochgeschwindigkeits-Internetverbindung verfügt.

Traceroute ist ein nützliches Tool zur Fehlerbehebung von Netzwerkproblemen. Es kann verwendet werden,um zu identifizieren, welcher Router auf dem Weg zu einem Zielsystem ein Problem verursacht. Es kann auch verwendet werden,um die Route eines Datenpakets zu verfolgen und zu sehen, wie lange es dauert, um verschiedene Router zu erreichen.

Aufgabe 3.

In der Regel ist der UDP-Scan deutlich schneller als der TCP-Scan.

Gründe:

- **UDP ist verbindungslos :** UDP-Pakete werden einfach an den Zielport gesendet, ohne auf eine Antowrt zu warten. Dies führt zu einem schnelleren Scan, da Nmap nicht auf Antworten von jedem Port warten muss.
- **TCP ist verbindungsorientiert:** Bei TCP wird eine Verbindung zwischen dem Client und dem Server hergestellt, bevor Daten übertragen werden können.Dies erfordert einen Drei-Wege-Handshake, der den Scan verlangsamt.
- **Reaktionsrate:** Generell reagieren UDP-Dienste oft nicht dafür ausgelegt sind,unaufgeforderte Pakete zu empfangen.

Möglichkeiten zur Beschleunigung :

- **Paralleles Scannen:** Nmap kann mehrere Ports gleichzeitig scannen.
- **Scan-Techniken:** Nmap bietet verschiedene Scan-Techniken, die für bestimmte Situationen optimiert sind.Beispielsweise kann der -sU -f-Scan UDP-Ports Schneller scannen, indem er nur SYN-Pakete sendet.
- **Zielfilterung** : Begrenzen wir den Scan auf eine bestimmte Subnetzgruppe oder IP-Adressliste, um die Anzahl der zu scannenden Ziele zu reduzieren.