Blatt zum Selbststudium 2 – Netze

- Kommunikation im VPN -

Hinweis: Führen Sie diese Übung bitte **nicht** im Hochschulnetz durch. Bearbeiten Sie die Aufgaben entweder zu Hause oder nutzen Sie bei Bedarf zum Beispiel ein Mobilfunk-Tethering oder *eduroam*. Zu diesem Übungsblatt ist kein Präsenztermin geplant.

Aufgabe 1: Klartext-Übertragung
Nachdem Sie mit einem passenden Netzwerk verbunden sind (sieshe Hinweis oben) öffnen Sie bitte Wireshark. Anschließend beginnen Sie eine Aufzeichnung über Ihr WLAN- oder Ethernet-Interface und rufen Sie im Browser die Seite http://netze-demo.itsec-workshop.de auf (Zugangsdaten: `netze` / `g3h31m`).
Beantworten Sie folgende Fragen:

1. Was können Sie bei der Übertragung in Wireshark beobachten?
2. Wer könnte Zugriff auf die übertragenen Daten erhalten?
3. Welche Art von IP-Adresse wird auf der Webseite angezeigt?
4. Wie können Sie den Weg der Pakete im Internet ermitteln?
5. Ist dieser Zugriffsschutz Ihrer Meinung nach ausreichend?

Aufgabe 2: Verschlüsselte Übertragung
Richten Sie nun eine VPN-Verbindung zum Fachbereich ein. Nutzen Sie hierfür die Anleitung im Fachbereichs-FAQ (https://faq.infcs.de/vpn; Anmeldung erforderlich). Führen Sie den Netzwerkschnitt weiterhin mit Wireshark fort (schneiden Sie auf demselben Interface wie in Aufgabe 1 mit) und rufen Sie die zuvor erwähnte URL noch einmal auf. Untersuchen Sie dabei:

1. Welche Veränderungen sehen Sie gegenüber der Aufzeichnung ohne VPN?
2. Welche Art von IP-Adresse wird jetzt auf der Webseite angezeigt?
3. Wie sicher ist nun die Verbindung, und vor wem ist sie geschützt?
4. Welche potenziellen Probleme bestehen bei dieser Methode der Transportsicherung?
5. Prüfen Sie die Routing-Tabelle Ihres Systems vor und nach dem Aufbau der VPN-Verbindung. Welche Routen wurden hinzugefügt oder angepasst und warum?
6. Welche Vor- und Nachteile hat diese VPN-Lösung im Vergleich zu einer reinen TLS-Verschlüsselung?

Aufgabe 3: Overhead abschätzen

Führen Sie einmal `ping` mit einer festen Paketgröße ohne VPN aus und wiederholen Sie den Versuch mit angeschaltetem VPN. Ein Beispielaufruf in Linux könnte folgendermaßen aussehen

```
ping -c 1 -M do -s 1000 194.95.66.251
```

(`-c 1` für eine einmalige Anfrage, `-M do` setzt das *Don't-Fragment*-Flag und `-s 1000` legt die Nutzdatenmenge fest). Schauen Sie sich sowohl die Klartext- als auch VPN-Pakete in Wireshark genauer an.

1. Welcher Overhead (zusätzlich zur Payload) fällt beim Klartextpaket an?
2. Wie verändern sich die Paketgrößen beim VPN-Einsatz? Versuchen Sie dabei ein verschlüsseltes Paket Ihrem Ping-Versuch zuzuordnen.
3. Wie wirkt sich dies auf die maximal mögliche Nutzdatenrate aus? Nehmen Sie an, es sei eine ideale 100~MBit/s Verbindung gegeben.
4. **Bonus:** Schätzen Sie ab, wie sich der Overhead bei einer Kapselung innerhalb von TCP verhalten würde und welchen Einfluss das auf die mögliche Nutzdatenrate hätte.

Viel Spaß und Erfolg!