FRAGEN

1.

Damit ein Client einen Service in einem Netzwerk aufrufen kann,

sind 6 Aufrufe (3x REQuests, 3x REPlies) notwendig.

Beschreiben Sie diese 6 Messages in der beiliegenden Excel-Tabelle **M159-Teil1\_AB01-Kerberos-Messages&Keys.xlsx**.

Studieren Sie dazu Kapitel 3 des Skriptes und verwenden Sie die Erklärungen des zweistufigen Kerberos-Verfahren. Verwenden sie auch das Dokument M159\_Kerberos\_ZusatzKap3.docx. Im Internet gibt es weitere Dokumente.

2.

Jeder Request oder Reply wird in Form von Tickets oder Keys in Datenpaketen übermittelt. Diese sind jeweils mit einem entsprechenden

Schlüssel verschlüsselt. Welches Datenpaket ist mit welchem Schlüssel verschlüsselt und welcher Instanz ist der jeweilige Schlüssel bekannt ? Notieren Sie dies ebenfalls in der Tabelle **M159-Teil1\_AB01-Kerberos-Messages&Keys.xlsx.**

3.

Was würde passieren, wenn der private Schlüssel des KDC bekannt wäre ?

4. Warum kann der Client das TGT nicht entschlüsseln ? Der Client hat also

ein Ticket, das er nicht lesen kann? Was würde passieren bzw. welche Gefahr würde

entstehen, wenn er dies könnte?

5. Warum kann der Client das Server-Ticket nicht entschlüsseln ? Warum muss er das auch gar nicht können, um auf den Dienst zuzugreifen?

Die Lösung zur Aufgabe kann bei der Lehrperson bezogen werden.