smartlearn
virtual learning. real success.

159: DIRECTORYSERVICES KONFIGURIEREN UND IN BETRIEB NEHMEN

M159 LB1

Claude Fankhauser

Name	Vladan Marlon Vranjes	**Datum**	04.09.2024
Prüfung	M159 LB1	**Durchführung**	
159 Modulprüfung LB1 2024	**Punkte Total**	23/ 36 Punkte	**Note**
4.2			

Rahmenbedingungen

- Prüfungszeit: 50 Minuten
- Berechnung der Note: Punkte * 5 / Maximale Punktzahl + 1

Es dürfen keine schriftlichen Unterlagen benützt werden ausser einer persönlichen, selber erstellten zweiseitige Zusammenfassung (1 A4 Seite doppelseitig bedruckt oder 2 A4 Seiten einseitig bedruckt).

- Jegliche Arten von Prüfungen oder Musterlösungen auf der Zusammenfassung sind nicht erlaubt.
- Der Einsatz jeglicher elektronischen Hilfsmittel ist nicht erlaubt.
- Jeglicher Informationsaustausch mit anderen Lernenden ist nicht erlaubt
- Die Nutzung des Internets ist nicht erlaubt
- Nichtbeachten dieser Regelungen wird mit der Note 1 sanktioniert.
- Es werden nur leserliche Antworten bewertet.
- Es gelten die Weisungen zur Leistungsbeurteilung Informatik EFZ der gibb.

Grundbegriffe

Stimmen folgende Aussagen

Aussagen

A)

Bei assymetrischer Verschlüsselung ist der Schlüssel bei der Verschlüsselung und der Entschlüsselung derselbe.

B)

Kerberus verwendet assymetrische Verschlüsselung

Wählen Sie eine Möglichkeit ✅ 2 / 2 Punkte

- [x] Aussage A ist **wahr** / Aussage B ist **wahr**
- [ ] Aussage A ist **wahr** / Aussage B ist **wahr**
- [ ] Aussage A ist **wahr** / Aussage B ist **wahr**
- [ ] Aussage A ist **wahr** / Aussage B ist **wahr**

Aussagen

A)

Bei der symmetrischen Verschlüsselung kommt ein public Key zur Anwendung

B)

Bei der symmetrischen Verschlüsselung kennen der Sender und der Empfänger den Schlüssel

Wählen Sie eine Möglichkeit ✅ 2 / 2 Punkte

- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☒ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**

Single Sign on

Was versteht man unter Single Sign On? Erklären Sie kurz. ❌ 1 / 2 Punkte

Beim erstmaligen Login werden die Daten gespeichert und man mu

Feedback der Lehrperson

"die Daten gespeichert" - Username und Passwort?

Linux Authentication

Wie heisst das Subsystem einer Linuxinstallation, das sich um verschiedene Aspekte der Authentizierung kümmert?
Nennen Sie die Abkürzung und deren Beduetung.

Antwort ✗ 0 / 2 Punkte

LDAP (lightweigt Directory Access protocol), dieses ist ein Protokol

Feedback der Lehrperson

PAM - Pluggable Authentication Modules

Kerberos

Stimmen folgende Aussagen

Aussagen

A)

Das Kerberos Protokoll schützt recht gut vor Man-in-the-middle Attacken, da das Passwort nie über das Netz übertragen wird.

B)

In einem Keytab-File werden temporäre Sessionkeys gespeichert.

Wählen Sie eine Möglichkeit ✅ 2 / 2 Punkte

- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☒ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**
- ☐ Aussage A ist **wahr** / Aussage B ist **wahr**

Credential Cache

Wie nennt man die Einträge allgemein, welche in einem Credential Cache gespeichert werden?

Antwort 2 / 2 Punkte

Credentials

Feedback der Lehrperson

In Kerberos werden die Einträge, die im **Credential Cache** (auch **Ticket Cache** genannt) gespeichert sind, allgemein als **Credentials** bezeichnet. Diese Credentials enthalten in der Regel folgende Informationen:

1. **Ticket-Granting Ticket (TGT)**: Das Hauptticket, das für die Authentifizierung bei anderen Diensten verwendet wird.
2. **Service Tickets**: Tickets, die spezifisch für den Zugang zu bestimmten Diensten sind.

Diese Credentials bestehen aus einer Kombination von Kerberos-Tickets und den zugehörigen Schlüsseln (Session Keys), die für die Authentifizierung bei verschiedenen Diensten im Netzwerk benötigt werden.

Kerberberos CLI

Mit welchem Befehl können Sie sich den Credential Cache anzeigen lassen?

Single-Choice 2 / 2 Punkte

- [ ] ls
- [ ] kadmin
- [x] klist

  Richtig
- [ ] list_cache
- [ ] kvno
- [ ] list_princs

TGS

Wer stellt das TGT aus? Wählen Sie die beste Antwort.

Single-Choice 2 / 2 Punkte

- [ ] Application Service
- [ ] TGS
- [x] AS

  Richtig
- [ ] Principal
- [ ] AS_REQ

verschiedene Principals

Was ist der Unterschied zwischen einem Client-Principal-Namen und einem Service-Principal-Namen in der Kerberos-Authentisierung? Geben Sie jeweils ein Beispiel.

Antwort ✗ 1 / 4 Punkte

Die Ansprechweise ist anders im Kadmin drin

Client: username@REALM.COM Service@REALM.COM

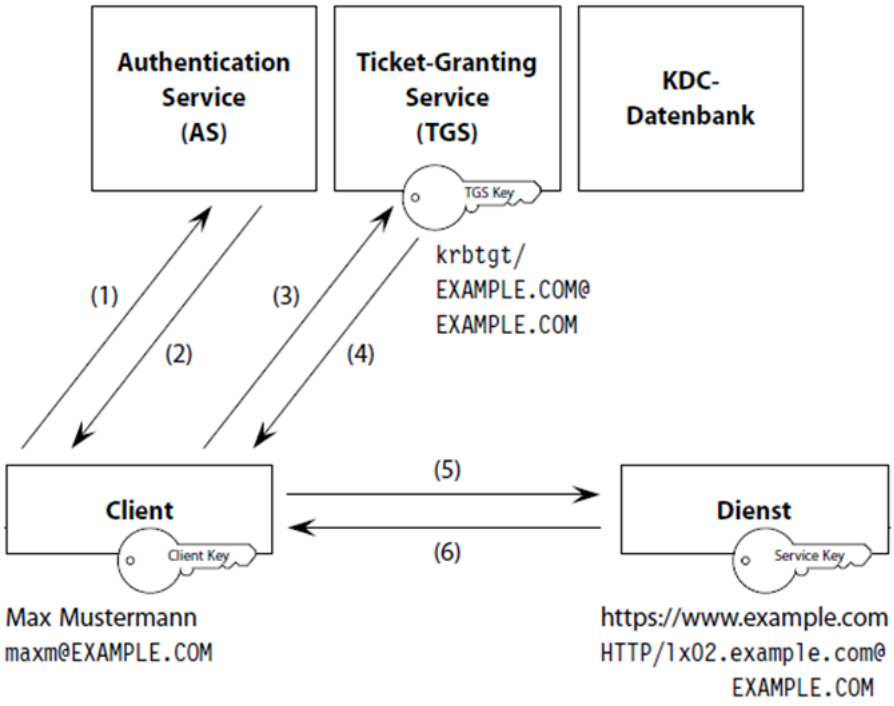
Feedback der Lehrperson

Der Client-Principal-Namen wird für die Identität des Clients verwendet und der Service-Principal-Namen wird für die Identität des Services verwendet.

Der Client-Principal-Name ist mit dem Benutzernamen und dem Realmnamen (grossgeschrieben) aufgebaut. Zwischen den beiden Namen steht ein @ um diese zu trennen. Bsp. max@EXAMPLE.COM

Der Service-Principal-Name ist mit dem Service-Namen/Realmnamen und nocheinmals mit dem Realmnamen(grossgeschrieben) erstellt. Zwischen diesen Namen ist wieder ein @ für die Trennung. Bsp. HTTP/lx02.example.com@EXAMPLE.COM

Kerberos Reihenfolge



Hier sind die sechs Schritte, wie im Bild oben dargestellt. Diese sind jedoch in der falschen Reihenfolge. Ordne sie richtig an.

Reihenfolge

4 / 6 Punkte

3 Richtig	Ein Benutzer oder Dienst fragt beim Ticket Granting Server (TGS) ein Service Ticket an und reicht das erhaltene Ticket Granting Ticket (TGT) ein.
2 Richtig	Der Authentication Server (AS) überprüft die Identität und erstellt ein Ticket Granting Ticket (TGT) mit einem verschlüsselten Session Key.
5 Lösung 6	Der Benutzer oder Dienst übermittelt das Service Ticket und den Zeitstempel an den Dienst, der das Ticket entschlüsselt und die Zugangsdaten prüft.
4 Richtig	Der Ticket Granting Server (TGS) entschlüsselt das erhaltene TGT und erstellt ein Service Ticket, wenn die Authentifizierung erfolgreich ist.
1 Richtig	Der Benutzer oder Dienst sendet eine Anfrage mit Benutzernamen und möglicherweise Passwort an den Authentication Server (AS).
6 Lösung 5	Ein Service Ticket wird ausgestellt und enthält Benutzerinformationen, Dienstname, Zeitbegrenzung und Sitzungsschlüssel.

REALM

Welches ist das REALM dieses Principels? 2 / 2 Punkte
nfs/server.example.com@EXAMPLE.COM

EXAMPLE.COM

Lösung

EXAMPLE.COM

Kerberus Details

a) Wozu muss der KDC den Langzeitschlüssels des Clients kennen?
b) In welcher Phases des Kerberusauthentizierungsprozesses setzt der diesen ein?
c) Was verschlüsselt er damit?
Beantworten Sie jede Frage und geben Sie je eine kurze Erklärung.

Antwort a) ✗ 0 / 1 Punkte

Damit er überprüfen kann ob die einkommenden Werte der Anfrag

Feedback der Lehrperson

a) Der KDC muss den Langzeitschlüssel des Clients kennen, um das TGT sicher zu verschlüsseln und sicherzustellen, dass nur der authentifizierte Client in der Lage ist, das TGT zu verwenden.

Antwort b) ✗ 0 / 1 Punkte

AS_REP, schritt 2

Antwort c) ✗ 0 / 1 Punkte

Session key, exp time, TGS Service Name

Kerberus Details 2

a) Wie kann ein Service den mit dem Service Session Key verschlüsselten Teil des Application Server Requests (AP_REQ 5) entschlüsseln?
b) Wie kommt der Service zum entsprechenden Key?
c) Wer kennt diesen Key auch noch?

Antwort a) ✗ 0 / 1 Punkte

Indem er auch den Langzeitschlüssel des KDC kennt

Antwort b) ✗ 0 / 1 Punkte

Dies wird vom Client mitgesendet

Antwort c) ✓ 1 / 1 Punkte

KDC, TGS & Service

Kerberos Detail 3

Im Netzwerk Ihres Unternehmens hat der KDC eine Panne und ist temporär nicht erreichbar.
Beschreiben Sie die Auswirkungen.
- Was funktioniert noch? Wie lange?
- Was funktioniert nicht mehr?

Antwort 2 / 2 Punkte

> Die Clients die bereits Authentisiert sind funktionieren dank des SSOs noch weiterhin bis sie die Verbindung abbrechen. Sobald