**1. Directory Services verstehen:** Definition: Ein Directory Service (Verzeichnisdienst) verwaltet die Objekte in einem Rechnernetzwerk, wie Benutzer, Rechner, Drucker, etc. Dieser Service basiert häufig auf der X.500-Spezifikation, und der Zugriff erfolgt meist über LDAP (Lightweight Directory Access Protocol).

Beispielkomponenten: Active Directory Domain Services (ADDS) von Microsoft.

**2. Kerberos in einer Microsoft ADDS-Infrastruktur:** Kerberos in ADDS: In Microsoft-Umgebungen wird Kerberos v5 als primärer Authentifizierungsdienst verwendet, vorallem ab Windows 2000 mit Active Directory.

**3. Authentisierung vs. Autorisierung:**

Authentisierung: Der Prozess, durch den die Identität eines Benutzers überprüft wird, z. B. durch Eingabe von Benutzername und Passwort.

Autorisierung: Bestimmt, welche Rechte ein authentifizierter Benutzer auf Ressourcen im Netzwerk hat, z. B. Lese- oder Schreibzugriff auf Dateien.

**4. Rolle von Kerberos in Directory Services:** Kerberos als Authentisierungsdienst: Kerberos sorgt dafür, dass Benutzer und Server ihre Identität nachweisen können, ohne Passwörter über das Netzwerk zu senden.

**5. Begriffe innerhalb von Kerberos:**

**KDC (Key Distribution Center)**: Vertrauenswürdiger Dienst, der die Authentifizierung zwischen Client und Server vermittelt.

**Realm**: Eine administrative Einheit innerhalb einer Kerberos-Umgebung, vergleichbar mit einer Domain.

**Principals**: Eindeutige Identitäten in Kerberos, z.B. Benutzer oder Dienste.

**Tickets**: Zeitlich begrenzte Zugriffsrechte, die von Kerberos vergeben werden.

**TGT (Ticket Granting Ticket)**: Ermöglicht das Anfordern von weiteren Tickets.

**Session Tickets**: Ermöglichen den Zugriff auf spezifische Dienste.

**Mutual Authentication**: Beide Seiten (Client und Server) authentifizieren sich gegenseitig.

**PAM (Pluggable Authentication Modules)** ist ein flexibles System zur Integration verschiedener Authentifizierungsmethoden in Anwendungen und Diensten unter Unix/Linux.

**6. Komponenten einer Kerberos-Infrastruktur:**

KDC: Bestehend aus Authentication Service (AS) und Ticket Granting Service (TGS).

Tickets: TGT (Ticket Granting Ticket) und Service Tickets für den Zugriff auf Dienste.

**7. Netzwerkdienste und Kerberos:** Integration am Beispiel von sshd: Der Prozess der Authentifizierung mittels Kerberos für Dienste wie SSH wird im zweistufigen Kerberos-Verfahren beschrieben, wo ein TGT verwendet wird, um ein Service-Ticket für den sshd-Dienst zu erhalten.

**8. SSO und Kerberos:**Single Sign-On (SSO): Kerberos ermöglicht SSO, indem ein Benutzer sich einmal authentifiziert und Zugriff auf verschiedene Dienste erhält, ohne erneut das Passwort eingeben zu müssen.

**9. Speicherung der Kerberos-Daten:** Speicherorte: Die Kerberos-Datenbank speichert Principals und ihre Schlüssel, normalerweise auf dem KDC. In produktiven Umgebungen kann LDAP verwendet werden.

**10. Das Kerberos-Protokoll:**Ablauf bei der Anmeldung: Wenn ein Benutzer sich bei einem Kerberos-geschützten Dienst anmeldet, durchläuft er mehrere Schritte, um ein TGT zu erhalten und anschließend damit Service-Tickets zu bekommen.

Bedeutung von Schlüsseln: Temporäre Schlüssel (Session Keys) werden zur Authentifizierung verwendet, während Langzeitschlüssel sicher auf dem KDC gespeichert werden.

**11. Kerberos Wichtige Schlüssel:**

Service Key: Ein langfristiger Schlüssel, den ein Dienst für die Entschlüsselung von Service-Tickets verwendet.

Service Session Key: Ein temporärer Schlüssel, der zwischen Client und Dienst für eine Sitzung verwendet wird.

**12. Administration von Kerberos:**Verwaltungskommandos: Befehle wie kinit, klist, und kadmin werden zur Administration von Kerberos verwendet, z. B. um Tickets abzurufen oder Principals zu verwalten.

**13. Kerberos-Administrationsservice:**Notwendige Ressourcen: Um einen Kerberos-Administrationsservice zu betreiben, wird ein korrekt konfigurierter KDC benötigt, der die Kerberos-Datenbank verwaltet.

**14. Unterschiede und Bestandteile von LDAP und X.500:** LDAP vs. X.500: LDAP ist ein Protokoll, das den Zugriff auf Verzeichnisdienste wie X.500-basierten Verzeichnissen ermöglicht. Objekte im LDAP werden hierarchisch im Directory Information Tree (DIT) gespeichert.

**TGT =** Wohnungsschlüssel (Ticket Granting Ticket) (Bekommt der User nach der Authentifizierung bei KDC)

**ST =** Türenschlüssel (Session Ticket) (Bekommt der User vom TGT) (Bei Ablauf neues Ticket von TGT)

**Betriebssystem-Verwaltung und Dienste:**

**sudo apt:** Wird verwendet, um das Betriebssystem und installierte Pakete zu aktualisieren.

1. Problem: Du möchtest sicherstellen, dass alle Pakete auf dem neuesten Stand sind und Sicherheitsupdates angewendet wurden.
2. Beispiel: sudo apt update && sudo apt upgrade

**ntpdate**: Dient zur Zeitsynchronisation mit einem NTP-Server.

1. Problem: Wenn die Systemzeit nicht synchron ist, was in Kerberos-Umgebungen zu Authentifizierungsproblemen führen kann.
2. Beispiel: sudo ntpdate ntp.server.com

**systemctl**: Wird verwendet, um Dienste zu starten, stoppen oder neu zu starten.

* Problem: Ein Dienst wie DNS oder Kerberos muss neu gestartet oder überprüft werden.
* Beispiel: sudo systemctl restart dns-server

**Kerberos-spezifische Befehle: Diese Befehle werden für den CC (Credential Cache) gebraucht:**

**kinit**: Fordert ein Kerberos-Ticket (TGT) vom KDC an. (Kann auch für einen anderen Benutzer ein Ticket anfordern)

* Problem: Ein Benutzer muss sich im Netzwerk authentifizieren, um Zugriff auf Dienste zu erhalten.
* Beispiel: kinit username@REALM

**klist**: Zeigt die aktuell gespeicherten Kerberos-Tickets an.

* Problem: Du möchtest überprüfen, ob der Benutzer über gültige Tickets verfügt oder welche Tickets aktuell im Credential Cache gespeichert sind.
* Beispiel: klist

**kvno**: Gibt die Version eines Service-Tickets zurück. / Bewirkt zusätzlichen Eintrag im CC (Service Tickets (Allgemein: TGT). Unter Linux im TMP Verzeichnis)

* Problem: Überprüfen, welche Version eines Tickets verwendet wird, oft zur Fehlerbehebung oder zur Sicherstellung der richtigen Ticketnutzung.
* Beispiel: kvno service\_name

**kpasswd**: Ändert das Kerberos-Passwort.

* Problem: Ein Benutzer muss sein Passwort in der Kerberos-Datenbank ändern.
* Beispiel: kpasswd

**kdestroy**: Zerstört alle im Credential Cache gespeicherten Kerberos-Tickets.

* Problem: Es ist notwendig, die Authentifizierungsinformationen eines Benutzers zu entfernen, zum Beispiel bei einem Abmeldeprozess.
* Beispiel: kdestroy

**kadmin.local**: Verwaltung von Kerberos-Principals direkt auf dem KDC.

* Problem: Administrieren der Kerberos-Datenbank, z. B. Hinzufügen oder Entfernen von Benutzern (Principals).
* Beispiele:
  + addprinc username@REALM - Hinzufügen eines neuen Principals.
  + delprinc username@REALM - Löschen eines Principals.
  + ktadd username@REALM - Hinzufügen eines Principals zur Keytab-Datei.
  + getprinc username@REALM - Anzeigen der Informationen eines Principals.

**LDAP-spezifische Befehle:**

**ldapsearch**: Suchen nach LDAP-Daten.

* Problem: Du musst Informationen über LDAP-Objekte abfragen, z. B. Benutzer oder Gruppen.
* Beispiel: ldapsearch -x -h vmKDC -b dc=example,dc=com '(cn=Erika\*)'

**ldapmodify**: Änderungen an LDAP-Daten vornehmen.

* Problem: Es ist notwendig, Attribute von LDAP-Objekten zu ändern, z. B. eine neue E-Mail-Adresse hinzufügen.
* Beispiel: ldapmodify -x -D cn=admin,dc=example,dc=com -w 'passwort' -f datei.ldif

**ldapadd**: Hinzufügen neuer LDAP-Objekte.

* Problem: Ein neues Objekt, wie ein Benutzer oder eine Gruppe, muss zum LDAP-Verzeichnis hinzugefügt werden.
* Beispiel: ldapadd -x -D cn=admin,dc=example,dc=com -w 'passwort' -f new\_user.ldif

**ldapdelete**: Löschen von LDAP-Objekten.

* Problem: Ein existierendes Objekt muss aus dem LDAP-Verzeichnis entfernt werden.
* Beispiel: ldapdelete -x -D cn=admin,dc=example,dc=com -w 'passwort' "cn=Erika Musterfrau,ou=people,dc=example,dc=com"

Einstufiges Kerberos-Verfahren:

AS-REQ: Client sendet Anfrage an KDC für Dienst-Ticket.

AS-REP: KDC erstellt Session Key und Dienst-Ticket, verschlüsselt für Client und Dienst. Entschlüsselung: Client entschlüsselt Session Key.

AP-REQ: Client sendet Ticket und Authenticator an Dienst. (Client

Überprüfung: Dienst entschlüsselt Ticket, prüft Authenticator, authentifiziert Client.

Zweistufiges Kerberos-Verfahren:

AS-REQ: Client fordert TGT vom KDC an. (Client -> KDC (AS))

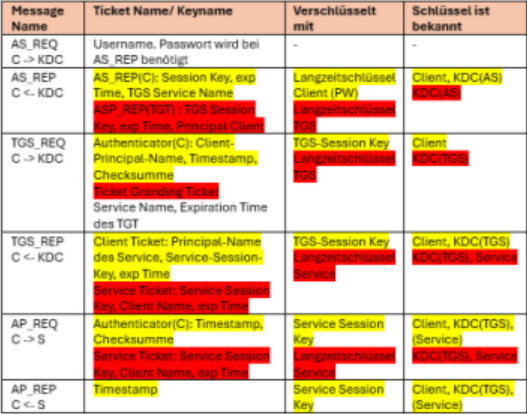
AS-REP: KDC gibt TGT und TGS-Session Key an Client zurück. (KDC (AS) -> Client)

TGS-REQ: Client fordert Service-Ticket vom TGS mit TGT und Authenticator an. (Client -> KDC (TGS))

TGS-REP: TGS erstellt Service-Ticket und Authenticator der verschlüsselt ist für Client und Dienst. (KDC (TGS) -> Client)

AP-REQ: Client sendet Service-Ticket und Authenticator an Dienst. (Client -> Server/Service)

AP-REP: Optional, Dienst sendet Authentifizierungsantwort zurück, bestätigt Legitimität. (Server/Service -> Client)



Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Kinit maxm

(AAA) Authentification-Authorization-Accounting

AS = Authentication Server -> sends TGT to client, client with TGT goes to TGS, TGS give the client an ST key

DN (LDAP) = Distinguished Name

Description entschlüsseln:

Echo <description> | base64 -d

LDAP Syntax: & (Und), ! (nicht), | (oder), suchfilter immer in runden klammern

**ldapsearch -x -h vmKDC -b dc=example,dc=com '(&(objectClass=person)(seeAlso=\*))' cn**

-D = Angabe Benutzer für suche, -w passwort in konsole, -W angabe Passwort interaktiv, -y passwortfile

-x = simple bind (anmeldedaten)

-b = suchbasis

-h = Angabe Hostname

Ou = organisational unit

Dc = Domain component

Listprincs -> Angelegten Principal anzeigen lassen



**1. Integration von Kerberos mit Netzwerkdiensten (am Beispiel von sshd)**

**Erklärung:** Kerberos kann verwendet werden, um Netzwerkdienste wie SSH zu authentifizieren. Dies erfolgt durch das zweistufige Kerberos-Verfahren, bei dem der Benutzer zunächst ein Ticket Granting Ticket (TGT) vom Key Distribution Center (KDC) anfordert. Mit diesem TGT kann der Benutzer dann ein Service-Ticket für den spezifischen Dienst, z. B. sshd, erhalten.

**Beispiel:**

1. Der Benutzer gibt kinit ein, um ein TGT zu erhalten.
2. Danach authentifiziert sich der Benutzer mit ssh user@hostname, wobei ein Service-Ticket für sshd angefordert wird.
3. Der SSH-Dienst überprüft das Ticket und gewährt den Zugriff, ohne dass der Benutzer erneut ein Passwort eingeben muss.

**Befehl:** ssh -K user@hostname

Dieser Befehl nutzt das Kerberos-Ticket für die SSH-Anmeldung.

**2. Kerberos-Protokoll und Schlüsselaustausch**

**Erklärung:** Kerberos verwendet zwei Arten von Schlüsseln:

* **Langzeitschlüssel (Long-Term Keys):** Diese sind in der KDC-Datenbank gespeichert und werden zur Verschlüsselung von Tickets verwendet.
* **Temporäre Schlüssel (Session Keys):** Diese werden bei jeder Authentifizierungssitzung erzeugt und zwischen dem Client und dem Dienst ausgetauscht.

**Beispiel:**

1. Der Client fordert ein TGT an, das mit dem Langzeitschlüssel des Clients verschlüsselt ist.
2. Mit dem TGT wird ein Session Key erzeugt, der für die Dauer der Sitzung gilt und für die sichere Kommunikation zwischen dem Client und dem Dienst verwendet wird.

**Befehl:** klist

**3. Unterschiede zwischen LDAP und X.500 sowie LDAP-Suche**

**Erklärung:**

* **X.500:** Ein Standard für Verzeichnisdienste, auf dem LDAP basiert. Es beschreibt ein Verzeichnis, das hierarchisch aufgebaut ist und Informationen über Benutzer, Geräte, etc. speichert.
* **LDAP (Lightweight Directory Access Protocol):** Ein Protokoll zum Zugriff auf X.500-Verzeichnisdienste. Es ermöglicht die Abfrage und Modifikation von Informationen in einem Verzeichnis.

**Beispiel:** Ein Benutzer sucht nach allen Einträgen, deren Name mit "Erika" beginnt:

**Befehl:** ldapsearch -x -h ldap.example.com -b dc=example,dc=com '(cn=Erika\*)'

**4. Single Sign-On (SSO) und Mechanismen**

**Erklärung:** SSO ermöglicht es Benutzern, sich einmal anzumelden und dann auf mehrere Dienste zuzugreifen, ohne erneut ein Passwort eingeben zu müssen. Dies wird durch das Kerberos-Protokoll ermöglicht, indem nach der ersten Anmeldung alle weiteren Authentifizierungen mit Tickets (TGT und Service-Tickets) durchgeführt werden.

**Beispiel:** Ein Benutzer meldet sich an seinem Arbeitsplatzrechner an und erhält ein TGT. Anschließend kann er ohne weitere Passwortabfrage auf Netzwerkressourcen wie Drucker oder Dateiserver zugreifen.

**Befehl**: klist -A

Überprüfung des TGT für SSO

**5. Speicherorte von Kerberos-Daten**

**Erklärung:** Kerberos-Daten, wie Principals und Schlüssel, werden hauptsächlich in der KDC-Datenbank gespeichert. Diese kann lokal auf dem KDC oder in einem LDAP-Verzeichnis gespeichert werden. Zusätzlich können Keytabs (Dateien, die verschlüsselte Schlüssel enthalten) verwendet werden, um Dienste ohne Passwort zu authentifizieren.

**Beispiel:**

* **Keytab Speicherort:** /etc/krb5.keytab
* **KDC-Datenbank:** Wird typischerweise auf dem KDC-Server selbst gespeichert.

**Befehl**: ktutil

# Verwaltung von Keytabs

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte BeschreibungEin Bild, das Diagramm, Reihe, Entwurf, Text enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Diagramm, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung

**AES (Advanced Encryption Standard)** ist ein symmetrisches Verschlüsselungsverfahren, das weltweit als Standard für die sichere Verschlüsselung von Daten verwendet wird. AES verschlüsselt Datenblöcke mit einer festen Größe von 128 Bits, wobei es verschiedene Schlüssellängen unterstützt: 128, 192 oder 256 Bits. Es wird oft in verschiedenen sicherheitskritischen Anwendungen, wie z.B. in der Datenverschlüsselung für Kerberos, verwendet, um die Vertraulichkeit und Integrität von Informationen zu gewährleisten.

Der Dienst entschlüsselt zuerst das Service Ticket, um den Session Key und die Identität des Clients zu erhalten. Danach wird der Authenticator entschlüsselt, um die Legitimität des Clients zu überprüfen.

TGT enthält im wesentlichen nur Session Key mit Namen des Clients

TGT (Session key), TGS gibt Service Ticket mit authenticator (verschüsselt mit session key)

Kerberos verwendet symmetrische Verschlüsselung und shared Secrets (gemeinsame geheime Schlüssel) für die Authentifizierung

Ein **Silver Ticket** ist ein gefälschtes Service Ticket (ST) in einem Kerberos-Netzwerk. Angreifer, die den Passwort-Hash eines Dienstkontos (z.B. eines Computer-Accounts) erlangen, können ein Silver Ticket erzeugen, das ihnen Zugang zu einem bestimmten Dienst verschafft, ohne den KDC um ein legitimes Ticket zu bitten. Da das Ticket nicht vom KDC ausgestellt wurde, bleibt dieser Angriff oft unentdeckt, was ihn besonders gefährlich macht.

1. User Principal
   1. Benutzer
   2. Beispiel: username@REALM
2. Service Principal
   1. Dienst, der in einem Netzwerk lauft
   2. service/hostname@REALM
3. Host Principal
   1. Stellt Host oder Server dar
   2. host/hostname@REALM
4. KDC Principal
   1. Repräsentier KDC selbst
   2. krbtgt/REALM@REALM
5. Cross-Realm Principal
   1. Authentifizierung zwischen verschiedenen Kerberos-Realms
   2. krbtgt/REALM-B@REALM-A

**KDC Abkürzung:**

* **Worum geht es:** Bedeutung von KDC in einem Kerberos-Netz.
* **Antwort:** Key Distribution Center.

**Rolle des KDC:**

* **Worum geht es:** Funktion des KDC im Kerberos-Netz.
* **Antwort:** Trusted Third Party.

**KDC-Komponente in Windows-Netzwerk:**

* **Worum geht es:** Entsprechung des KDC in Windows.
* **Antwort:** Domain Controller (DC).

**Zuständigkeit des KDC:**

* **Worum geht es:** Aufgaben des KDC.
* **Antwort:** Vergabe von TGTs und Service Tickets.

**Kerberos’ 3 Köpfe:**

* **Worum geht es:** Symbolik der 3 Köpfe von Kerberos.
* **Antwort:** Client, Server, KDC.

**Bezeichnung von Objekten:**

* **Worum geht es:** Namen von Client und Server im Kerberos-Netz.
* **Antwort:** Principals.

**Verwaltungseinheit im Kerberos-Netz:**

* **Worum geht es:** Äquivalent zur Domain in Windows.
* **Antwort:** Realm.

**Schwächstes Glied im Kerberos-Netzwerk:**

* **Worum geht es:** Sicherheitsrisiko im Kerberos-System.
* **Antwort:** Sicherheit des KDC.

**Maßnahmen zur Schwachstellenbekämpfung:**

* **Worum geht es:** Schritte zur Sicherung des KDC.
* **Antwort:** Sicherheitsupdates, Zugriffsbeschränkungen, Verschlüsselung.

**Verschlüsselungsprotokoll Kerberos v5:**

* **Worum geht es:** Verwendetes Verschlüsselungsprotokoll.
* **Antwort:** AES (Advanced Encryption Standard).

**Verschlüsselungsart:**

* **Worum geht es:** Symmetrische oder asymmetrische Verschlüsselung.
* **Antwort:** Symmetrisch.

**Silver Ticket:**

* **Worum geht es:** Gefälschtes Ticket im Kerberos-Kontext.
* **Antwort:** Service Ticket.

**Voraussetzungen für Silver Ticket-Angriff:**

* **Worum geht es:** Notwendige Kenntnisse für den Angriff.
* **Antwort:** Service Principal Key.

**Manipulationsschritt:**

* **Worum geht es:** Zeitpunkt der Manipulation im Kerberos-Ablauf.
* **Antwort:** Schritt 5 (AP\_REQ).

**Tickets im Kerberos-Protokoll:**

* **Worum geht es:** Arten von Tickets.
* **Antwort:** Ticket Granting Ticket (TGT) und Service Ticket.

**Manipulation mit KDC-Langzeitschlüssel:**

* **Worum geht es:** Was mit dem Langzeitschlüssel gemacht werden kann.
* **Antwort:** Gefälschte TGTs erstellen.

**Erste Kontrolle bei Problemen:**

* **Worum geht es:** Erste Maßnahme bei Authentifizierungsproblemen.
* **Antwort:** Uhrzeitsynchronisierung zwischen Clients und KDC prüfen.