|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: PEDRO, FLEX D. | DATE PERFORMED:11-06-24 | /50 |
| Section:IDC1 | DATE SUBMITTED: 11-06-24 |

# SYSADM1 – Kerberos Basics

Research Activity

1. What is Kerberos, and why is it used?

Kerberos is a network authentication protocol designed to provide secure authentication for users and services over an insecure network. It uses secret-key cryptography to ensure that both the user's identity and the integrity of the communication are protected. Kerberos is primarily used to enable secure single sign-on (SSO) capabilities, allowing users to authenticate once and gain access to multiple services without needing to re-enter their credentials.

1. What are the main components of Kerberos?

**Key Distribution Center (KDC)** - The central authority that manages authentication and ticket granting.

**Authentication Service (AS)** - A part of the KDC that verifies user credentials and issues the initial ticket.

**Ticket Granting Service (TGS)** - Another part of the KDC that issues service tickets for accessing specific services.

**Client** - The user or application requesting access to a service.

**Server** - The service that the client wants to access, which relies on Kerberos for authentication.

1. What is a "ticket" in Kerberos, and why is it important?

A "ticket" in Kerberos is a time-limited credential that allows a user to access a specific service without needing to provide their password again. It contains information such as the user's identity, the service being accessed, and a session key for encrypting communication. Tickets are important because they help to minimize the number of times a user's password is transmitted over the network, reducing the risk of interception and replay attacks.

1. What is a Kerberos "realm," and what is its purpose?

A Kerberos "realm" is a logical network that defines the administrative boundaries for Kerberos authentication. It consists of a KDC and the users and services within its domain. The purpose of a realm is to manage authentication policies, user identities, and ticket issuance within that specific domain, allowing for organized management of security credentials and services.

1. How does Kerberos authenticate a user?

1. **Initial Request** - The user sends a request to the AS for a ticket.

2. **Credential Verification** - The AS verifies the user's credentials (usually a password).

3. **Ticket Granting** - If the credentials are valid, the AS issues a Ticket Granting Ticket (TGT) encrypted with the user's password.

4. **Service Request** - The user presents the TGT to the TGS to request access to a specific service.

5. **Service Ticket Issuance** - The TGS verifies the TGT and issues a service ticket for the requested service.

6. A**ccessing the Service** - The user presents the service ticket to the server, which verifies it and grants access.

1. What does each component (KDC, TGS, AS) contribute to the authentication process?

**KDC (Key Distribution Center)** - Acts as the central authority for managing authentication and issuing tickets. It contains both the AS and TGS.

**AS (Authentication Service)** - Responsible for verifying the user's identity and issuing the initial Ticket Granting Ticket (TGT).

**TGS (Ticket Granting Service)** - Issues service tickets based on the TGT, allowing the user to access specific services securely.

1. How does a ticket improve security compared to repeated password logins?

**Reduced Password Exposure** - Since users only enter their password once to obtain a TGT, the risk of password interception during transmission is minimized.

**Limited Lifetime** - Tickets are time-limited, reducing the window of opportunity for attackers to misuse them.

**Session Keys** - Tickets include session keys that encrypt communications between the client and server, providing confidentiality and integrity.

**Replay Attack Prevention** - Each ticket is unique and tied to a specific session, making it difficult for attackers to reuse intercepted credentials.