

| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| --- | --- | --- |
| NAME: Hyra Cayambas | DATE PERFORMED: 11/06 | /50 |
| Section: IDC1 | DATE SUBMITTED: 11/06 |

# SYSADM1 – Kerberos Basics

Research Activity

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

Kerberos is a network authentication protocol whose function is to provide secure authentication for users and services in a network. It’s mainly used to prevent unauthorized access and to ensure secure communication over untrusted networks.

1. What are the main components of Kerberos?

The main components of Kerberos are:

* **Key Distribution Center**: core server that securely stores keys and manages authentication by issuing tickets to verify identities.
* **Authentication Server**: part of the KDC that verifies users' credentials and provides a Ticket Granting Ticket to access other services.
* **Ticket Granting Server**: part of the KDC, it issues service-specific tickets based on the TGT, allowing users to access desired network services.
* **Kerberos Database**: stores user and service credentials, like encrypted passwords, to facilitate secure authentication.

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

A ticket is an encrypted token that verifies the identity of a user or service. It enables secure, password-free authentication after the initial login, reducing the need for repeated password submissions.

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

A Kerberos realm is an administrative domain within the Kerberos environment defined by the KDC. It groups resources and users under a single authentication domain to streamline security management.

1. How does Kerberos authenticate a user?

Kerberos authenticates users through a series of exchanges involving the KDC, AS, and TGS, which work together to validate the user's identity and issue tickets for secure access. The entire process can look like this:

1. **Initial Login Request**: The user logs in to their device and requests authentication to access network resources.
2. **Authentication Server (AS) Request**: The user’s device sends an authentication request to the AS. This request includes the user's ID, encrypted with their password.
3. **AS Issues Ticket Granting Ticket (TGT)**: The AS decrypts the request using the user’s password stored in the Kerberos Database. If it matches, the AS issues a TGT, which is encrypted and can only be decrypted by the TGS. The TGT includes the user’s session key and an expiration time.
4. **TGT Sent to User**: The TGT is sent back to the user’s device. From now on, this ticket will serve as proof of identity without needing to enter a password again.
5. **Service Request with TGT**: When the user tries to access a specific service, they send the TGT to the Ticket Granting Server (TGS) along with a request for a service ticket.
6. **TGS Issues Service Ticket**: The TGS verifies the TGT, and if valid, issues a Service Ticket specific to the requested service. This ticket contains a session key for the user and the service.
7. **Accessing the Service**: The user’s device sends the Service Ticket to the desired service, which decrypts it using its own key. If the ticket is valid, the service grants access.
8. What does each component (KDC, TGS, AS) contribute to the authentication process?

* KDC: The central authority that holds keys for users and services.
* AS: Validates the user's identity and issues an initial Ticket Granting Ticket (TGT).
* TGS: Issues service-specific tickets based on the TGT, allowing access to requested services.

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

A ticket reduces the need for users to enter passwords repeatedly, minimizing the risk of password exposure. It also allows secure, session-based authentication through temporary tokens, enhancing security over repeated password logins.