UNIVERSITY OF Baguio SCHOOL OF INFORMATION AND TECHNOLOGY		
NAME: De Leon, Arjay V.	DATE PERFORMED: 11/06/24	
Section: IDC - 1	DATE SUBMITTED: 11/06//24	/50

SYSADM1 – Kerberos Basics

Research Activity

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

- According to Tech Target kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos support is built into all major computer operating systems, including Microsoft Windows, Apple macOS, FreeBSD and Linux.
- The original objective of Kerberos was to provide a way for users of the MIT network to securely authenticate themselves to the systems they needed to use. It also enabled those users to be authorized to access those systems. At that time, networked systems typically authenticated users with a user ID and password combination. Systems routinely transmitted passwords "in the clear," meaning unencrypted. Attackers with access to the network could easily eavesdrop on network transmissions, intercept user IDs and passwords, and then attempt to access systems for which they were not authorized

2. What are the main components of Kerberos?

The primary components of the Kerberos protocol include:

Key Distribution Center (KDC): This is the central component of Kerberos, responsible for managing authentication and issuing tickets. The KDC has two main subcomponents:

- **Authentication Server (AS):** This server authenticates users and issues Ticket Granting Tickets (TGTs) after verifying their credentials.
- **Ticket Granting Service (TGS):** After obtaining a TGT, users can request service tickets from the TGS to access specific services within the network 1.

Kerberos Database: This database maintains records for each principal (user or service) in the Kerberos realm. It stores essential information such as user credentials and service keys, which are used during the authentication process 2.

Principals: These are the entities (users or services) that are authenticated within the Kerberos system. Each principal has a unique identifier, typically formatted as primary/instance@REALM, which helps in distinguishing between different users and services.

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

   A ticket is a digital credential that allows a user or service to authenticate themselves to other services within a network. There are two primary types of tickets in Kerberos:

   Ticket Granting Ticket (TGT): This is issued by the Authentication Server (AS) after a user successfully logs in. The TGT serves as proof that the user has been authenticated and can be used to request additional tickets for accessing specific services.
   Service Ticket: This is obtained from the Ticket Granting Service (TGS) using the TGT. The service ticket allows the user to access a particular service within the network.

   Importance of ticket:

   Kerberos offers secure authentication through encrypted tickets, allowing users to log in once and obtain multiple service tickets without re-entering credentials. These tickets are time-stamped, reducing the risk of unauthorized access and reducing the risk of replay attacks, as they are time-limited and expire after a limited time.

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

- A Kerberos realm is a logical network that defines a group of systems that share a common Kerberos authentication service, typically managed by a master Key Distribution Center (KDC)

  Purpose of realm:

- A realm allows centralized authentication for all users and services within a network, simplifying the process. It operates independently, reducing unauthorized access. Domain mapping organizes realms within a larger network, making management easier. Kerberos supports inter-realm trust, allowing cross-realm authentication while maintaining security boundaries. This simplifies the authentication process for all principals.

5. How does Kerberos authenticate a user?

- This multi-step authentication process ensures mutual authentication, where both the user and the service verify each other's identities. It also enhances security by avoiding the transmission of passwords over the network, relying instead on encrypted tickets that are time-limited and specific to each session

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

- Key Distribution Center (KDC):

    - The KDC is the central authority in the Kerberos protocol, responsible for managing authentication and issuing tickets. It acts as a trusted third party that facilitates secure communication between users and services.
    - The KDC contains two subcomponents: the AS and the TGS. It maintains a database of user credentials and service keys, which are essential for verifying identities and issuing tickets.
- Authentication Server (AS):
    - The AS is the first point of contact for users seeking authentication. When a user logs in, the AS verifies their credentials (username and password) and, upon successful verification, issues a Ticket Granting Ticket (TGT).
    - The TGT serves as proof of the user's identity and allows them to request service tickets without needing to re-enter their credentials. This process enhances security by minimizing the exposure of sensitive information, such as passwords.
- Ticket Granting Service (TGS):
    - The TGS is responsible for issuing service tickets based on the TGT provided by the AS. When a user wants to access a specific service, they present their TGT to the TGS, which verifies it and issues a service ticket for the requested service.
    - The service ticket contains the necessary information for the user to authenticate with the service, including a session key that allows secure communication between the user and the service.
-

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

- Kerberos is a secure authentication system that uses a unique Ticket Granting Ticket (TGT) to limit password exposure and ensures mutual authentication between users and services. The TGT is encrypted and unique to each session, preventing easy decryption. It also provides time-limited access, reducing the opportunity for attackers to exploit compromised tickets. Kerberos also protects against replay attacks by using unique session keys and timestamps. The system's centralization through the Key Distribution Center (KDC) allows for better monitoring and control over authentication processes, enabling easier detection and response to potential security threats.