|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Paul Raynee D. Andres | DATE PERFORMED: 11/06/2024 | /50 |
| Section: IDC1 | DATE SUBMITTED: 11/06/2024 |

# SYSADM1 – Kerberos Basics

Research Activity

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

Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos support is built in to all major computer operating systems, including Microsoft Windows, Apple macOS, FreeBSD and Linux.

Kerberos is used to authenticate entities requesting access to network resources, especially in large networks to support SSO. The protocol is used by default in many widely used networking systems. Some systems in which Kerberos support is incorporated or available include the following:

* Amazon Web Services Apple macOS
* Google Cloud
* Hewlett Packard Unix
* IBM Advanced Interactive eXecutive
* Microsoft Azure
* Microsoft Windows Server and AD
* Oracle Solaris
* Red Hat Linux
* FreeBSD
* OpenBSD

1. **What are the main components of Kerberos?**

The main components of the Kerberos protocol include:

**Client (User or Service):**

The entity requesting access to a network resource (e.g., a user, application, or device). The client initiates the authentication process to prove its identity.

**Server (Service):**

The resource or service that the client wants to access. The server checks whether the client has a valid ticket before granting access.

**Key Distribution Center (KDC):**

A trusted entity responsible for managing authentication. The KDC is made up of two primary components:

**Authentication Server (AS):** Authenticates users and issues Ticket Granting Tickets (TGTs).

**Ticket Granting Server (TGS):** Issues service-specific tickets after the client presents a valid TGT.

Tickets:

Securely encrypted data structures that contain authentication information. They are used to grant access to services without needing to repeatedly transmit sensitive information like passwords.

**Database of Secrets:**

A storage area on the KDC containing secret keys for all users and services within the Kerberos realm.

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

A ticket in Kerberos is an encrypted data structure used to prove a user's identity to a service without needing to transmit a password over the network.

**Importance of a Ticket:**

**Authentication without Repeated Passwords:** After initial authentication, the user doesn't need to send their password repeatedly. Instead, they use a ticket issued by the KDC, which contains encrypted authentication data.

**Security:** Tickets are encrypted using a secret key, ensuring that sensitive information (like passwords) is not exposed on the network.

**Access Control:** The ticket is time-stamped and valid for a specific period, which helps prevent replay attacks and ensures timely access.

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

A Kerberos realm is a logical network or domain managed by a Kerberos authentication system. It defines the boundaries within which Kerberos tickets and credentials are valid.

**Purpose of a Kerberos Realm:**

**Namespace for Authentication:** A realm represents a security boundary where users, services, and authentication mechanisms are centrally managed.

**Cross-realm Authentication:** A realm can trust other realms, enabling users to authenticate across different domains (for example, different Kerberos realms for different organizations or geographical locations).

**Security Context:** A realm can be thought of as a network segment that shares the same authentication policies and key distribution infrastructure.

1. **How does Kerberos authenticate a user?**

Kerberos authenticates a user using a Ticket Granting Ticket (TGT), which allows the user to access services without needing to repeatedly enter their password. The general authentication flow is:

**1. User Request (Initial Login):**

The user enters their username and password into the client system.

**2. Authentication Server (AS) Request:**

The client sends a request to the Authentication Server (AS) on the KDC, asking for a Ticket Granting Ticket (TGT). This request includes the username, and the password is used to derive a secret key.

**3. AS Verifies Credentials:**

The AS checks the password against the database of secrets. If the password is correct, the AS generates a TGT and sends it back to the client. The TGT is encrypted with the KDC's secret key.

**4. Client Requests Service Ticket:**

To access a specific service, the client sends the TGT to the Ticket Granting Server (TGS) and requests a service ticket for the desired resource (e.g., file server, database).

**5. TGS Issues Service Ticket:**

The TGS verifies the TGT and, if valid, issues a service-specific ticket that allows the user to access the requested service.

**6. Access Granted:**

The client presents the service ticket to the server (e.g., file server). If the ticket is valid, the server grants access to the requested resource.

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

**1.** **Key Distribution Center (KDC):**

The central trusted authority that issues and manages authentication tickets.

**The KDC is composed of two parts:**

* **Authentication Server (AS):** Verifies user credentials when they first log in (e.g., password validation).Issues the Ticket Granting Ticket (TGT), which can be used to request access to other services.
* **Ticket Granting Server (TGS):** Validates the TGT presented by the client and issues service-specific tickets. Ensures that the user is authorized to access the requested service by issuing the appropriate service ticket.

**2. Client (User or Service):**

Initiates authentication and requests tickets to access services.

Uses the TGT to request service-specific tickets from the TGS.

**3. Server (Service):**

The service being accessed. The server verifies the service ticket presented by the client and grants access if the ticket is valid.

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

Tickets enhance security over repeated password logins in several ways:

**Reduced Exposure of Passwords:**

Instead of sending passwords across the network each time the user tries to access a resource, Kerberos uses tickets that are encrypted and do not expose the password in transit.

**Prevents Replay Attacks:**

Tickets are time-stamped and have a limited validity period, making it difficult for attackers to reuse them later. Once a ticket expires, it is no longer valid.

**Mutual Authentication:**

Kerberos ensures both the client and the server authenticate each other. This reduces the risk of man-in-the-middle attacks, where an attacker might intercept or impersonate a party in the authentication process.

**One-Time Authentication:**

Once a user authenticates and receives a TGT, they can access multiple services without having to re-enter their password or expose their credentials. This reduces the attack surface by minimizing the number of times the password is used.

**Strong Encryption:**

Kerberos uses strong encryption algorithms to protect the tickets, ensuring that even if a ticket is intercepted, it cannot easily be decrypted by an attacker without the appropriate secret key.