|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: BUSONGAN, DEMIRAYE-ANNE | DATE PERFORMED: 06 OCTO 2024 | /50 |
| Section: IDC1 | DATE SUBMITTED: 06 OCTO 2024 |

# SYSADM1 – Kerberos Basics

Research Activity

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 between clients and services over untrusted networks, such as the internet. It was developed in the 1980s at Massachusetts Institute of Technology (MIT) as part of Project Athena and aims to solve the problem of securely authenticating users and services without transmitting passwords in clear text (Loshin & Cobb, 2021).

Kerberos is used primarily to enhance security in network environments by preventing eavesdropping and mitigating replay attacks. One of its key benefits is encryption, where it utilizes symmetric encryption (shared secret keys) to secure communication, ensuring that sensitive information like passwords is never transmitted in plain text across the network. Another important feature is mutual authentication, where both the client and the server authenticate each other, providing assurance that the client is communicating with the correct service and the service is interacting with an authenticated client. This mutual verification helps prevent impersonation attacks. Kerberos also supports Single Sign-On (SSO), allowing users to authenticate once and gain access to multiple services without needing to re-enter credentials, simplifying the user experience and improving security by reducing password fatigue. Finally, secure communication is guaranteed by Kerberos through the use of encrypted tickets issued by the Key Distribution Center (KDC). These tickets ensure that identity assertions are made using trusted third-party verification, thus reducing the risk of unauthorized access and ensuring the integrity of data transmitted over potentially untrusted networks (Loshin & Cobb, 2021).

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

According to Loshin & Cobb, (2021), the main components of Kerberos are as follows:

1. Key Distribution Center(KDC)  
   Known as the main authority in Kerberos which has two parts; the Authentication Server(AS) which verifies and gives a Ticketing Grant Ticket(TGT) and Ticketing Granting Server(TGS) which gives out service tickets that let the user access specific services.
2. Client  
   The user or application that wants to access a service. It communicates with the KDC to get tickets, which are then used to authenticate to services.
3. Service  
   The resource (like a file or database) the client wants to access. It checks the service ticket from the client to allow access.
4. Ticket  
   The keys that prove the client’s identity. Tickets have two types; Ticket Granting Ticket (TGT) which is given by the AS to request other tickets and Service Ticket that is provided by the TGS to access specific services.
5. Secret Keys  
   Used to encrypt and decrypt tickets, ensuring only authorized parties can access the tickets or services.
6. Time Synchronization  
   Ensures that all systems have matching clocks. This prevents tickets from being used at the wrong time or being replayed maliciously.

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

The main components of Kerberos, based on the information from the provided TechTarget article, are:

Key Distribution Center (KDC): A central authority that manages authentication and ticketing. It is divided into two parts:

Authentication Server (AS): Authenticates the user's identity and issues a Ticket Granting Ticket (TGT).

Ticket Granting Server (TGS): Issues service tickets based on the TGT when the client needs to access a specific service.

Client: The entity (user or application) that wants to access a service and seeks authentication through Kerberos.

Service: The resource or application the client wants to access (e.g., file servers, database services). The service validates the service tickets provided by clients.

Ticket: A cryptographically protected credential that allows users to authenticate to services without re-entering passwords. It includes the user's identity and the time period for which access is allowed.

Secret Keys: These are used for encrypting and decrypting communication, ensuring the security of ticket exchanges.

Time Synchronization: Kerberos requires that all participants have synchronized clocks to prevent the replay of expired tickets.

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

According to Loshin & Cobb, (2021), a "ticket" is a secure, cryptographic credential used to verify a user's identity and grant access to services within a network. There are two primary types of tickets: the Ticket Granting Ticket (TGT) and the Service Ticket. The TGT is issued by the Authentication Server after a user successfully logs in, allowing them to request additional service tickets without having to re-enter their password. When the user needs access to a specific service, the Ticket Granting Server issues a Service Ticket, which authenticates the user to that service.

Tickets play a critical role in enhancing both security and usability. By eliminating the need to send passwords over the network, Kerberos reduces the risk of passwords being intercepted by attackers. Additionally, because tickets are time-limited, they minimize the chances of attackers using a stolen ticket in replay attacks. This system also improves user experience by allowing users to authenticate once and then access multiple services without needing to repeatedly enter their credentials.

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

A Kerberos realm is an administrative area where Kerberos authentication is managed, usually corresponding to an organization or a group of trusted systems. It sets the boundaries for how authentication works within a network (Loshin & Cobb, 2021).

.

The main purpose of a realm is to organize and control the authentication process. It ensures that all systems within the realm trust the same authentication server (called the Key Distribution Center or KDC) and follow the same security rules. Realms can also be linked for cross-realm authentication, allowing users to access services in other realms, but this requires a trust relationship between them (Loshin & Cobb, 2021).

.

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

According to Loshin & Cobb, (2021), Kerberos authenticates a user through a ticket-based system. Here’s a simplified breakdown of how Kerberos authentication works:

1. Authentication Request: The client sends a request to the Kerberos Authentication Server (AS) to begin the process. The request is in plaintext, as no sensitive information is included. The AS checks if the client exists in its database and retrieves the client's private key.
2. Authentication Response: If the client is found, the AS sends back a Ticket Granting Ticket (TGT) and a session key. If not, the authentication process stops.
3. Service Ticket Request: After receiving the TGT, the client sends it to the Ticket Granting Server (TGS) to request access to a specific service.
4. Service Ticket Response: If the TGS verifies the client, it sends back a service ticket, encrypted with a session key that is shared between the client and the service. This ticket proves the client's identity to the service.
5. Application Server Request: The client uses the service ticket to request access to the application server.
6. Application Server Response: The application server checks the service ticket. If valid, it grants access and may also send back a Kerberos authentication to confirm its identity to the client.

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

According to Varonis, (2022),

1. Key Distribution Center (KDC): The KDC is the central authority responsible for managing authentication within a Kerberos realm. It oversees the entire authentication process and the distribution of tickets. The KDC contains both the Authentication Server (AS) and the Ticket Granting Server (TGS), which work together to authenticate users and issue the necessary tickets for accessing services.
2. Authentication Server (AS): The AS is the first component that the client interacts with during authentication. When a client attempts to authenticate, the AS checks the client’s credentials (typically the username and password). If the credentials are valid, the AS issues a Ticket Granting Ticket (TGT), which allows the client to request service tickets without needing to re-enter their password.
3. Ticket Granting Server (TGS): Once the client has a valid TGT from the AS, it sends the TGT to the TGS to request access to a specific service. The TGS verifies the TGT's validity and, if everything checks out, issues a service ticket. This ticket is used by the client to authenticate itself to a service (e.g., a file server or email server), allowing the client to access the requested resource.

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

A ticket improves security compared to repeated password logins in several ways:

1. No Password Transmission: After the initial login, Kerberos uses encrypted tickets instead of passwords for further communication. This reduces the risk of passwords being intercepted.
2. Time-limited Validity: Tickets are only valid for a limited time. If a ticket is stolen, it can only be used for a short period, limiting the potential harm.
3. Prevents Replay Attacks: Tickets are encrypted and contain timestamps, making it difficult for attackers to reuse them to gain unauthorized access.
4. Single Sign-On (SSO): Once logged in, the user only needs the TGT to access multiple services without re-entering their password, reducing security risks and improving convenience.

REFERENCE:

Simplilearn. (2024, July 2). *What is Kerberos? How does Kerberos work: Everything you need to know*. Simplilearn.com. https://www.simplilearn.com/what-is-kerberos-article

Loshin, P., & Cobb, M. (2021, September 15). Kerberos. Security. <https://www.techtarget.com/searchsecurity/definition/Kerberos#:~:text=Kerberos%20is%20a%20protocol%20for,network%2C%20such%20as%20the%20internet>.

Varonis retrieve on November 6, 2024 from https://www.varonis.com/blog/kerberos-authentication-explained