|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Dale Matthew R. Boquiren | 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 security protocol that acts as a gateway between users and the internet, helping to protect private networks from cyber attackers. Serving as an "intermediary," it operates between end-users and the websites they access online. Kerberos is primarily used to authenticate entities requesting access to network resources, making it particularly valuable in large networks to enable single sign-on (SSO) functionality. The protocol is also the default authentication method in many widely used network systems.

1. What are the main components of Kerberos?

* Authentication Server (AS):   
  - The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
* Database:   
  - The Authentication Server verifies the access rights of users in the database.
* Ticket Granting Server (TGS):   
  - The Ticket Granting Server issues the ticket for the Server

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

* Kerberos credentials, or "tickets," are electronic data used to verify your identity. These tickets may be stored in a file or exist solely in memory. The first ticket you receive is the ticket-granting ticket, which allows you to request additional tickets for accessing specific resources. Tickets are important because it provides mutual authentication, allowing nodes to prove their identity to one another in a secure manner.

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

* A Kerberos realm is a collection of principals that defines an administrative domain or sphere, where a unified security policy is typically enforced. Each realm must have a master Kerberos server, but it can also include one or more optional slave servers for added support. Kerberos realms are logical groupings of resources and identities that utilize the Kerberos protocol. A realm is essentially the "home" of your Kerberos identity and serves as your entry point to the network resources managed by Kerberos. In Windows systems, these realms are referred to as domains.

1. How does Kerberos authenticate a user?

* Kerberos authenticates a user through a ticket-based process that allows secure access across multiple network resources. First, the user submits their credentials to the Authentication Server (AS), which verifies them and issues a Ticket-Granting Ticket (TGT). The TGT, encrypted for security, allows the user to request specific service tickets from the Ticket-Granting Server (TGS) without re-entering credentials. When the user requests access to a resource, they present the service ticket, which the resource validates to grant access. This process, supporting single sign-on (SSO), enables seamless, secure access across a network.

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

* The KDC checks the user's TGT and confirms their authorization for the requested service. The TGS then provides a valid session key for the service, which the client forwards to the service as proof of access. The service then grants access to the user.

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

* Kerberos tickets enhance security by eliminating the need to repeatedly transmit passwords, reducing the risk of interception. After an initial login, a Ticket-Granting Ticket (TGT) is issued, which is used to request service-specific tickets. These tickets are encrypted, time-limited, and unique to each service, preventing unauthorized access and replay attacks, while keeping credentials secure.