|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Hyra Cayambas | DATE PERFORMED: 11/13 | /50 |
| Section: IDC1 | DATE SUBMITTED: 11/13 |

# SYSADM1 – Kerberos Lab Activity: A step-by-step Guide

**Objective:**

Set up a basic Kerberos authentication system to understand how Kerberos manages secure logins through ticket-based access.

**Setup Requirements:**

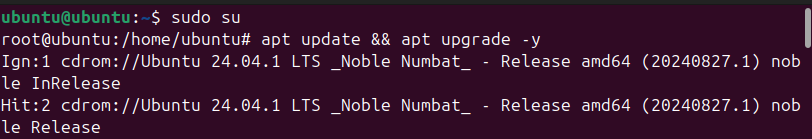
* Two VMs in Oracle VM, both running a Linux distribution like Ubuntu or CentOS.
* VM1: Kerberos Server
* VM2: Kerberos Client

**Step 1: Initial Setup and Package Installation**

1. **Update Packages on Both VMs:**
   * Open a terminal on each VM and run:

*bash*

*sudo apt update && sudo apt upgrade -y*

**

*A computer screen shot of a program

Description automatically generated*

1. **Install Kerberos Server Packages on VM1 (Kerberos Server):**
   * In VM1, install the Kerberos Key Distribution Center (KDC) and admin server:

*bash*

*sudo apt install krb5-kdc krb5-admin-server -y*

*A black background with white text

Description automatically generated*

*A screenshot of a computer

Description automatically generated*

1. **Install Kerberos Client Package on VM2 (Kerberos Client):**
   * In VM2, install the Kerberos client software:

*bash*

*sudo apt install krb5-user -y*

*A screenshot of a computer

Description automatically generated*

* + During installation, when prompted, enter the Kerberos realm you plan to set up, e.g., MYLAB.LOCAL.

**Step 2: Configure the Kerberos Server (VM1)**

1. **Edit the Kerberos Configuration File:**
   * Open /etc/krb5.conf for editing:

*bash*

*sudo nano /etc/krb5.conf*

* + Set the realm as MYLAB.LOCAL. You should also specify the KDC and admin server as VM1’s hostname or IP address:

ini

[libdefaults]

default\_realm = MYLAB.LOCAL

[realms]

MYLAB.LOCAL = {

kdc = <VM1\_IP\_or\_hostname>

admin\_server = <VM1\_IP\_or\_hostname>

}

A screenshot of a computer program

Description automatically generated

* + Save and close the file (Ctrl+X, then Y, and Enter to confirm).

1. **Initialize the Kerberos Database:**
   * Create the database for the Kerberos realm:

*bash*

*sudo krb5\_newrealm*

*A screenshot of a computer

Description automatically generated*

* + You will be prompted to set a password for the Kerberos database.

1. **Start and Enable the Kerberos Services:**
   * Start the KDC and admin server, and ensure they start automatically on boot:

*bash*

*sudo systemctl start krb5-kdc*

*sudo systemctl start krb5-admin-server*

*sudo systemctl enable krb5-kdc*

*sudo systemctl enable krb5-admin-server*

*A screen shot of a computer

Description automatically generated*

**Step 3: Set Up a Kerberos User Principal**

1. **Create a New User Principal:**
   * Run the following command to create a test user in the Kerberos realm:

*bash*

*sudo kadmin.local -q "addprinc* [*testuser@MYLAB.LOCAL*](mailto:testuser@MYLAB.LOCAL)*"*

*A screen shot of a computer code

Description automatically generated*

* + Set a password for testuser.

1. **Verify the User Principal:**
   * To confirm the principal is created, list all principals:

*bash*

*sudo kadmin.local -q "listprincs"*

A screenshot of a computer

Description automatically generated

**Step 4: Configure the Kerberos Client (VM2)**

1. **Edit the Kerberos Configuration File on VM2:**
   * Open /etc/krb5.conf for editing on VM2:

*bash*

*sudo nano /etc/krb5.conf*

*A screenshot of a computer program

Description automatically generated*

* + Set the default realm to MYLAB.LOCAL and point to the KDC and admin server on VM1. The configuration should match what you set on VM1.

**Step 5: Test Kerberos Authentication**

1. **Request a Kerberos Ticket for the User on VM2:**
   * In the terminal on VM2, request a ticket for testuser:

*bash*

*kinit* [*testuser@MYLAB.LOCAL*](mailto:testuser@MYLAB.LOCAL)

*A close up of white text

Description automatically generated*

* + Enter the password you set for testuser.

1. **Verify the Ticket:**
   * Check if the ticket was issued by listing active Kerberos tickets:

*bash*

*list*

*A computer screen with white text

Description automatically generated*

* + You should see details about the ticket, such as the principal and expiration time, confirming successful Kerberos authentication.

HANDSHAKE BETWEEN VMS:

A screenshot of a computer

Description automatically generated