➢ Module 1

Configuring Authentication using Kerberos Protocol

Module Objectives

- Understanding Kerberos Authentication Protocol.
- Setup KDC Admin Server.
- Configuring Client for Kerberos Authentication.

Lesson One

- Understanding Kerberos Authentication Protocol.

What is Kerberos Protocol ?

- Kerberos is a network authentication protocol created by MIT.
- It uses symmetric-key cryptography to authenticate users to network services so the passwords are never actually sent over the network.
- The authentication mechanism will be done through Tickets.
- The KDC Server (Key Distribution Center) will be responsible for giving the users that Tickets , so it is an SSO System.
- It has its own Database to store passwords of all users ,
- It does not store user information (Shell , Home Directory …etc.) like LDAP , Kerberos Provides Authentication Process.

Terms

- Realm :

The Administrative Domain and it is written as Upper-Case like (EXAMPLE.COM)

- Principle :

An Entry in the authentication DB of Kerberos like (nfs/nfs.example.com)

- KDC (Key Distribution Center) :

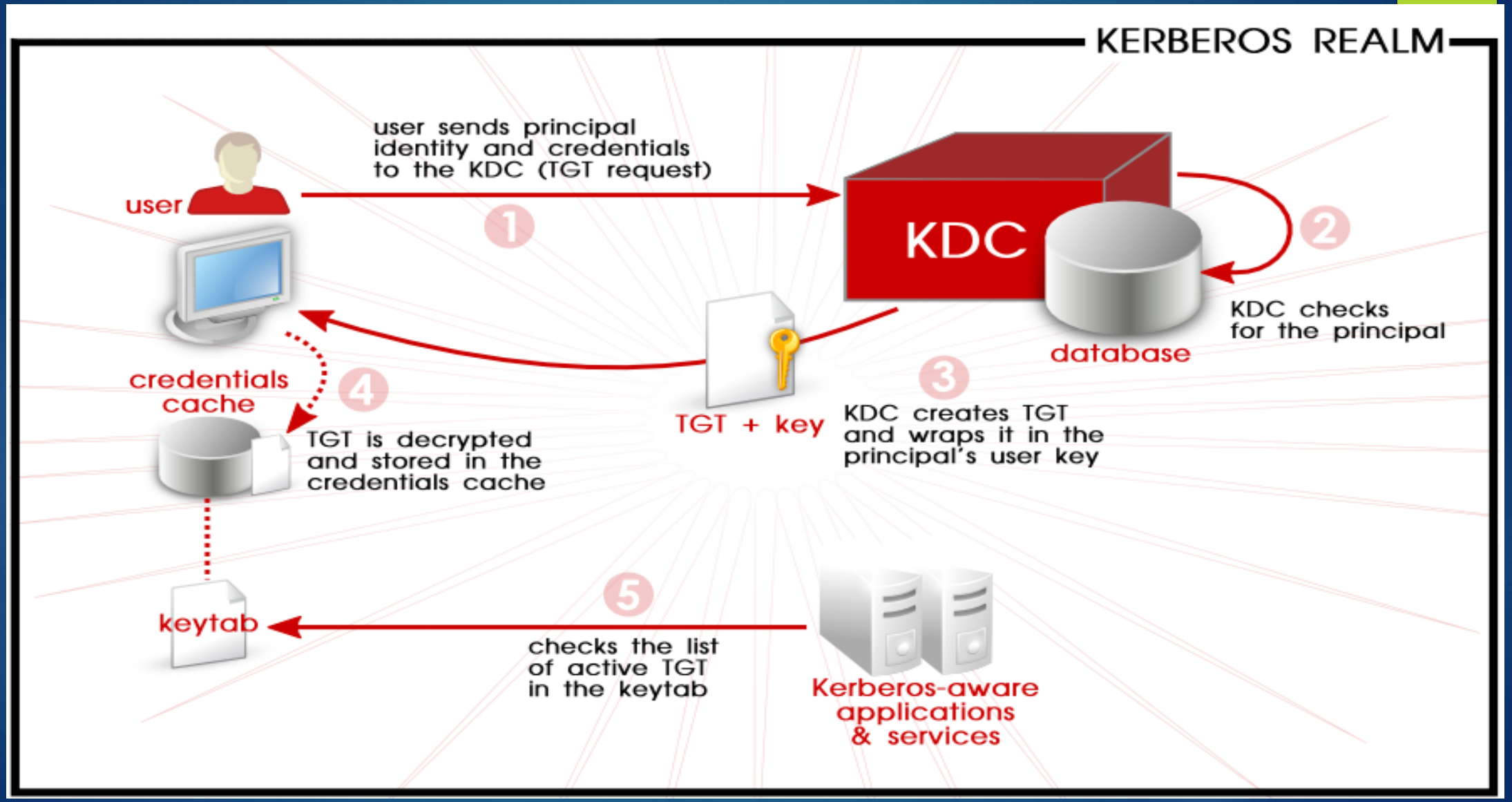
KDC Server has 3 Components :

1. DB : to host all Principles Information.
2. Auth Server : to Initialize the Authentication Process.
3. TGS : (Ticket Granting Ticket)To generate encrypted keys and to be sent to the user.

- Ticket :

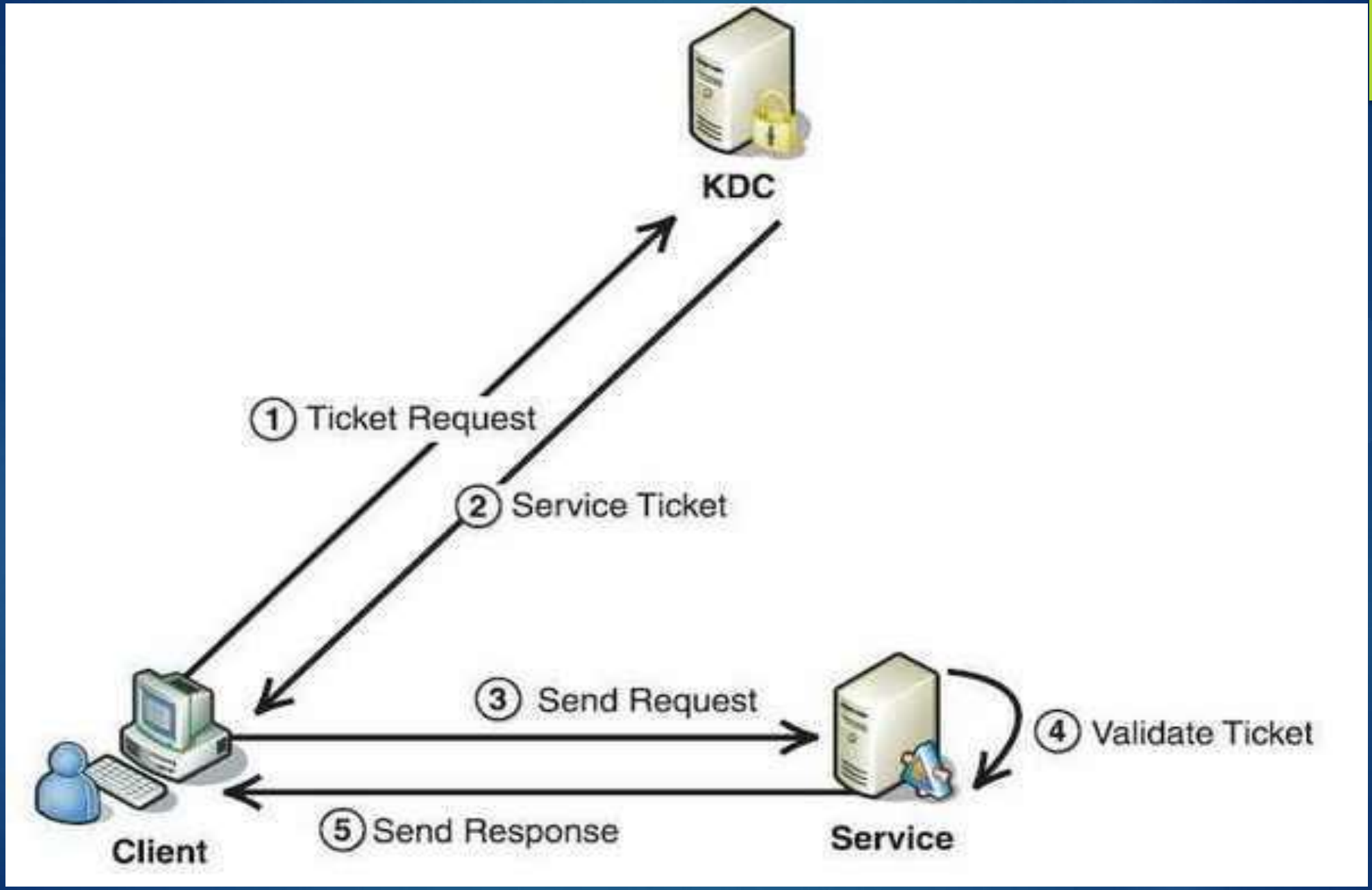
The Client gets this Ticket from the KDC and presents it to the Network Service to Access.

Authentication Process



Authentication Process

1. Client wants to Access Network Service like (NFS).
2. Client will request TGS (Ticket Granting Session) from the KDC Server.
3. KDC Server will Grant the user Encrypted TGT (Ticket Granting Ticket).
4. Client will Present this TGT to the Network Service.
5. Network Service will Verify the User's Ticket.
6. Now the Client can Access the Network Service Normally.


KDC
1 Ticket Request
2 Service Ticket
3 Send Request
4 Validate Ticket
5 Send Response
Client
Service

Setting up KDC Admin Server

- Update the CentOS 7

```
# yum update –y &&  reboot
```

- Install the Required Packages

```
# yum install –y krb5-server krb5-workstation
```

- Open the Below Files and replace “example.com”with your domain and REALM

```
# /etc/krb5.conf
# /var/kerberos/krb5kdc/kadm5.acl
# /var/kerberos/krb5kdc/kdc.conf
```

- Create Kerberos database with master password

```
# kdb5_util create –s –r EXAMPLE.COM
```

- Restart the Service

```
# systemctl restart krb5kdc kadmin
# systemctl enable krb5kdc kadmin
```

- Allow Kerberos on the firewall

```
# firewall-cmd --permanent --add-service=Kerberos
# firewall-cmd –permanent –add-port=749/udp
# firewall-cmd –reload
```

- Create the principals

```
# kadmin.local
```