# Overview

## Goals

Installation and configuration of Kerberos and LDAP servers. The servers will be

used to authenticate users to your CentOS VM.

## Deliverables

* Lab Report including the following
  + Information section at beginning of the lab
  + Description of the lab steps completed and the results
  + Any errors you encountered and the steps you took to resolve them
  + Any mistakes found or corrections made to the lab steps
  + Answers to the questions posed at the end of this lab
  + Appendix A: Properly titled “LDAP Search”
    - Pasted text representing the output of the following command from your Debian VM:  
      ldapsearch –xWD cn=admin,dc=**LAST\_NAME**,dc=hades,dc=lab –b dc=example,dc=hades,dc=lab “(uid=**NEWUSER**)”
  + Appendix B: Properly titled “CentOS krb5.conf”
    - Pasted contents of */etc/krb5.conf* (From CentOS)

## Information

The IP addresses, networks, and sub domains used throughout this lab document are for example only. Fill out the table below and refer to it when following this lab’s directions.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Description*** | ***Formula*** | ***Used in Lab*** | ***Answer*** |
| Assigned Subnet Number | *n* | - |  |
| Your Last Name | *<last\_name>* | LAST\_NAME |  |
| Debian VM IP | 172.16.*n*.10 | DEBIAN\_IP |  |
| CentOS VM IP | 172.16.*n.*50 | CENTOS\_IP |  |
| Subzone | *<last\_name>*.hades.lab | SUBZONE |  |
| Kerberos Realm | *LAST\_NAME*.HADES.LAB | REALM |  |
| LDAP base | dc=*<last\_name>*,dc=hades,dc=lab | LDAP\_BASE |  |
| New User | - | NEWUSER |  |

Note: By convention the REALM is UPPER CASE, so use an UPPER CASE name for your REALM. Use lower case for the new user.

Transfer these key names from your DNS lab

| ***Key Name*** | ***Used in Lab*** | ***File Name*** |
| --- | --- | --- |
| Zone Signing Key | ZONE\_SIGNING\_KEY |  |
| Key Signing Key | KEY\_SIGNING\_KEY |  |

# Update Network Configuration

Kerberos, like many services is very sensitive to your network configuration. Follow these steps to ensure that your network configuration will play well with Kerberos. These steps require that your DNS server from the last lab is operating correctly.

## Debian VM

1. Verify your Debian VM’s hostname is ‘debian’
   1. hostname –s
      1. Should output ‘debian’
      2. If not, run
         1. echo “debian” > /etc/hostname
2. Update */etc/hosts*
   1. Remove line that starts with 127.0.1.1 (use a comment to do it)
   2. Replace with line below (substitute your Debian IP)

**DEBIAN\_IP** debian.**SUBZONE** debian

1. Update */etc/resolv.conf* to use your DNS server

domain **SUBZONE**

search **SUBZONE**

nameserver **DEBIAN\_IP**

1. Reboot your Debian VM
2. Check your fully qualified domain name
   1. hostname –f
   2. Should include your subzone (e.g. debian.**SUBZONE**)

## CentOS VM

1. Edit /etc/sysconfig/network
   1. Set HOSTNAME variable to your fully qualified domain name (e.g. centos.**SUBZONE**)
2. Update /etc/resolv.conf to use your DNS server

domain **SUBZONE**

search **SUBZONE**

nameserver **DEBIAN\_IP**

1. Reboot your CentOS VM
2. Check your fully qualified domain name
   1. hostname –f
   2. Should include your subzone (e.g. centos.**SUBZONE**)

# Update DNS to support Kerberos (Debian VM)

1. Update your DNS zone (/var/cache/bind/db.**SUBZONE**)
   1. Do not forget to update the zone’s serial number

; Kerberos Configuration

kerberos IN CNAME debian

\_kerberos IN TXT "**REALM**"

\_kerberos.\_udp IN SRV 0 0 88 debian

\_kerberos-master.\_udp IN SRV 0 0 88 debian

\_kerberos-adm.\_tcp IN SRV 0 0 749 debian

\_kpasswd.\_udp IN SRV 0 0 464 debian

1. Update zone’s DNSSEC information
   1. **Remember to run this command in /etc/bind/keys/:**dnssec-signzone -r /dev/urandom -k **KEY\_SIGNING\_KEY** -o **SUBZONE** -t –A /var/cache/bind/db.**SUBZONE** **ZONE\_SIGNING\_KEY**
2. Reload DNS server
   1. rndc reload
3. Verify DNS configuration
   1. dig -t TXT \_kerberos.**SUBZONE**

# Install Kerberos (Debian VM)

**NOTE** – You will need to install and configure Kerberos from the console on the Debian VM. Installing Kerberos through an SSH connection does not always create the proper files.

**WARNING** – Use a new username for this lab as opposed to the name of your user account on your VMs. If you use the same username, bad things will happen.

1. Install Kerberos client and server using aptitude
   1. aptitude –R install krb5-admin-server krb5-config krb5-kdc krb5-user libpam-krb5
   2. The installation will ask ‘Kerberos server for your realm and possibly more. Leave the default answer (blank?) as it should be detected from DNS.
   3. If you need to start over:
      1. aptitude purge krb5-admin-server krb5-config krb5-kdc krb5-user libpam-krb5
      * Be sure the folder /var/lib/krb5kdc is removed, if not, manually delete it
      * Then start at beginning
2. Initialize the Kerberos database
   1. The password you create in this step is used to encrypt the Kerberos database. It should be a very safe password and kept in a secure location. It will almost never be required but is very useful for disaster recovery
   2. kdb5\_util create –s
      1. If the above command does not work try: krb5\_newrealm
   3. This step can only be run once. Purge all the Kerberos packages and start over if you need to redo this step
3. Configure ACLs for kadmin
   1. This step is specific to MIT’s implementation
   2. Create the file /etc/krb5kdc/kadm5.acl and add the following lines
   3. This allows any admin instance to manage Kerberos.

\*/admin@**REALM** \*

1. Start Kerberos’s KDC and admin server
   1. /etc/init.d/krb5-kdc start
   2. /etc/init.d/krb5-admin-server start
2. Create a Kerberos account using kadmin.local
   1. kadmin.local should only be used when first initializing Kerberos. All subsequent management should be done through kadmin
   2. Your Kerberos principle should be different from your UNIX username.
   3. You need to create an admin instance as well

# **kadmin.local**

Authenticating as principal root/admin@**REALM** with password.

kadmin.local: **addprinc *NEWUSER***

Enter password for principal “**NEWUSER**@**REALM**”:

Re-enter password for principal “**NEWUSER**@**REALM**”:

kadmin.local: **addprinc *NEWUSER*/admin**

Enter password for principal “**NEWUSER**/admin@**REALM**”:

Re-enter password for principal “**NEWUSER**/admin@**REALM**”:

Kadmin.local: **quit**

1. Verify that you can get tokens using your Kerberos principal
   1. kinit **NEWUSER**
   2. klist

# Install OpenLDAP (Debian VM)

1. Install LDAP packages
   1. aptitude –R install ldap-utils libsasl2-modules libsasl2-modules-gssapi-mit sasl2-bin slapd
   2. The password you set in this step is for the LDAP admin user
   3. You can purge these packages same as you purged the Kerberos packages if you need to start over
2. Create a LDIF file to initialize the database.
   1. Name the file init.ldif (this file can be located in any directory, but the home directory would be nice)

dn: ou=People,dc=**LAST\_NAME**,dc=hades,dc=lab

objectClass: top

objectClass: organizationalUnit

ou: People

dn: ou=Group,dc=**LAST\_NAME**,dc=hades,dc=lab

objectClass: top

objectClass: organizationalUnit

ou: Group

1. Load the LDIF file into the LDAP server
   1. ldapadd –xWD cn=admin,dc=**LAST\_NAME**,dc=hades,dc=lab –f init.ldif
   2. Use the password you set in Step 1 above
2. Create a LDIF file to add yourself to the database
   1. Name it user.ldif
   2. Your userid must match the Kerberos principal you created earlier

dn: uid=**NEWUSER**,ou=People,dc=**LAST\_NAME**,dc=hades,dc=lab

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: top

objectClass: person

uid: **NEWUSER**

sn: Watson

givenName: Prof

cn: Prof Watson

mail: jwatso8@uncc.edu

telephoneNumber: +1.704.555.5757

userPassword: {SASL}**NEWUSER**@**REALM**

shadowLastChange: 13977

shadowMax: 99999

shadowWarning: 7

loginShell: /bin/bash

uidNumber: 1000

gidNumber: 1000

homeDirectory: /home/**NEWUSER**

gecos: Prof Watson

dn: cn=**NEWUSER**,ou=Group,dc=**LAST\_NAME**,dc=hades,dc=lab

objectClass: posixGroup

objectClass: top

cn: **NEWUSER**

userPassword: {crypt}x

gidNumber: 1000

1. Load the LDIF file into the LDAP server
   1. ldapadd –xWD cn=admin,dc=**LAST\_NAME**,dc=hades,dc=lab –f user.ldif
   2. Use the password you set in Step 1 above
2. Verify the LDIF file loaded correctly
   1. ldapsearch –xWD cn=admin,dc=**LAST\_NAME**,dc=hades,dc=lab –b dc=**LAST\_NAME**,dc=hades,dc=lab “(uid=**NEWUSER**)”

# Client Configuration (CentOS)

1. Edit /etc/krb5.conf
   1. This only shows what you need to change, leave in all other lines

[libdefaults]

default\_realm = **REALM**

[realms]

**REALM** = {

kdc = kerberos.**SUBZONE**:88

admin\_server = kerberos.**SUBZONE**:749

default\_domain = **SUBZONE**

[domain\_realm]

.**SUBZONE** = **REALM**

**SUBZONE** = **REALM**

1. Edit /etc/ldap.conf

host **DEBIAN\_IP**

base dc=**LAST\_NAME**,dc=hades,dc=lab

1. Edit /etc/nsswitch.conf

passwd: files ldap

shadow: files ldap

group: files ldap

1. Test configuration
   1. kinit **NEWUSER**
      1. Should ask for your password and return
   2. klist
      1. Should show you Kerberos 5 tickets (no Kerberos 4 tickets)
   3. getent passwd **NEWUSER**
      1. Should return your user account from LDAP. If it is blank or your UID does not match, something went wrong. Check the log files for any errors
2. Run ‘system-config-authentication’
   1. This utility modifies PAM for you.
   2. Under the User Information tab, enable LDAP Support
   3. Under the Authentication tab, enable Kerberos
   4. Under the Options tab, enable ‘Create home directories on the first login’
3. Log out of CentOS system (if logout doesn't work, you may need to reboot)
4. Log in to your CentOS system using your Kerberos username and password
   1. You should be presented with a desktop for your Kerberos user

# Questions

1. What does kdb5\_util's '-s' option do? Explain in your own words why is this important?
2. This lab completely ignores encryption for LDAP. In your lab report, explain why this is a bad idea.