Week #6 – LDAP

Overview of the week's objectives

If you manage a large corporate network that has several hundred or thousands of machines, you will quickly realize how much duplication of effort is involved with normal administrative tasks.

Routine operations like changing passwords, canceling accounts, and modifying groups become time-consuming if repeated on individual machines. Centralizing user and authentication information can solve these issues.

Lightweight Directory Access Protocol (LDAP) is a set of protocols that has become the Internet standard for accessing information directories. LDAP and directory services allow administrators the capability to decentralize information in a secure and reliable manner.

This lesson will introduce the student to the terminology and basic skill sets required to administer both and LDAP components.

Please refer to "Week #2's Overview PDF" and to "ALL PREVIOUS WEEK's OVERVIEWS" for details / advice relating to, or concerning, each of the tasks detailed in the remainder of this overview. You are responsible for recommendations or instructions noted in them!

TODO List

Please refer to all previous "Week's Overview PDFs" for details / advice about each of the tasks detailed in the remainder of this overview. While we focus on instructions specific to this week's material herein, previous instructions still apply.

Learning Activity			**Time in hours**		**Points**
			Expected	**Spent**	
Reading Assignments	O4L4	Online Module Guides &Videos	2		
Practice Assignments	O4L4-PA	Working on PAs & Participating to PA forums	1		
	W6-PA	Working on PAs & Participating to PA forums	8		
Graded Assignments	W6-GQ	Taking Graded Quiz	1		2
		Participating to Discussion forums			1
			12		**3**

Task #1 – Reading Assignments

You will find one "online module guide" document in this week's folder per module.

Refer to all previous "Week's Overview PDFs" for detailed instructions on how to use online module guides, practice quizzes and our support forum while working on this task.

Task #2 – Practice Assignments

Refer to "ALL PREVIOUS WEEK's Overview PDF" files for detailed instructions applying to all Practice Assignments.

These activities were designed to help you think critically about the topics covered in this lesson and to assess whether your knowledge and application of the content meets the stated objectives. You will need to research each topic and complete the assignment as instructed. Do not rely only on the contents of this lesson or on Wikipedia to complete these assignments.

PA #1 : Lab – Activity (C4L4A1)

1) Create a fresh Ubuntu 10.4 or above virtual machine install. (Verify that your Ubuntu distro is 10.4 or later.)

2) Download and run nmap against your fresh Ubuntu virtual machine. Note all ports that are open.

3) Download and install slapd, apt-get ldap-utils, migrationtools and phpldapadmin.

4) Open a terminal editor of your choice and copy and paste the following script, save it as script.sh (script obtained from: http://albanianwizard.org/ubuntu-10-0-4-lucid-lynx-ldap-configuration-the-working-how-to.albanianwizard)

```
#!/bin/sh
passwd =pleaseeditme
dc1 =pleaseeditme
dc2 =pleaseeditme
hash_pw = ` slappasswd -s $passwd`
tmpdir = / tmp
#-------------------------------------------------------------#
ldapadd -Y EXTERNAL -H ldapi: /// -f / etc / ldap / schema / cosine.ldif
ldapadd -Y EXTERNAL -H ldapi: /// -f / etc / ldap / schema / inetorgperson.ldif
ldapadd -Y EXTERNAL -H ldapi: /// -f / etc / ldap / schema / nis.ldif
ldapadd -Y EXTERNAL -H ldapi: /// -f / etc / ldap / schema / misc.ldif
#————————————————————————-#
# database.ldif
#————————————————————————-#
cat << EOF > $tmpdir/ database.ldif
# Load dynamic backend modules
dn: cn =module {0} , cn =config
objectClass: olcModuleList
```

```
cn: module {0}
olcModulePath: / usr / lib / ldap
olcModuleLoad: {0} back_hdb
# Create directory database
dn: olcDatabase = {1} hdb, cn =config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1} hdb
olcDbDirectory: / var / lib / ldap
olcSuffix: dc = $dc1 , dc = $dc2
olcRootDN: cn =admin, dc = $dc1 , dc = $dc2
olcRootPW: $hash_pw
olcAccess: {0} to attrs =userPassword,shadowLastChange by dn =
"cn=admin,dc=$dc1,dc=$dc2" write by anonymous auth by self write by * none
olcAccess: {1} to dn.base= "" by * read
olcAccess: {2} to * by dn = "cn=admin,dc=$dc1,dc=$dc2" write by * read
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcDbConfig: {0} set_cachesize 0 2097152 0
olcDbConfig: {1} set_lk_max_objects 1500
olcDbConfig: {2} set_lk_max_locks 1500
olcDbConfig: {3} set_lk_max_lockers 1500
olcDbIndex: uid pres,eq
olcDbIndex: cn,sn,mail pres,eq,approx,sub
olcDbIndex: objectClass eq
###################################
# Modifications
###################################
dn: cn =config
changetype: modify
dn: olcDatabase = { - 1} frontend, cn =config
changetype: modify
delete: olcAccess
dn: olcDatabase = {0} config, cn =config
changetype: modify
add: olcRootDN
olcRootDN: cn =admin, cn =config
dn: olcDatabase = {0} config, cn =config
changetype: modify
add: olcRootPW
olcRootPW: $hash_pw
dn: olcDatabase = {0} config, cn =config
changetype: modify
delete: olcAccess
EOF
sudo ldapadd -Y EXTERNAL -H ldapi: /// -f $tmpdir/ database.ldif
#####################################
# Mini DIT
#####################################
cat << EOF > $tmpdir/ dit.ldif
# Tree root
dn: dc = $dc1 , dc = $dc2
objectClass: dcObject
objectclass: organization
o: $dc1 . $dc2
dc : $dc1
description: Tree root
# Populating
dn: cn =admin, dc = $dc1 , dc = $dc2
```

```
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
userPassword: $hash_pw
description: LDAP administrator
dn: cn =aw, dc = $dc1 , dc = $dc2
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: aw
userPassword: $hash_pw
description: LDAP aw
dn: ou =people, dc = $dc1 , dc = $dc2
ou: people
objectClass: organizationalUnit
objectClass: top
dn: ou = groups , dc = $dc1 , dc = $dc2
ou: groups
objectClass: organizationalUnit
objectClass: top
dn: ou =addressbook, dc = $dc1 , dc = $dc2
ou: addressbook
objectClass: top
objectClass: organizationalUnit
#Adding user
dn: uid =ldap1, ou =people, dc = $dc1 , dc = $dc2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ldap1
sn: Asdasd
givenName: ldap1
cn: ldap1 Asdasd
displayName: ldap1 asdasd
uidNumber: 1002
gidNumber: 1000
userPassword: $hash_pw
gecos: ldap1 asdasd
loginShell: / bin /bash
homeDirectory: / home / ldap1
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: aw @$dc1 . $dc2
postalCode: 31000
l: Mysity
o: $dc1
mobile: + 33 (0)6 22 22 22 22 22
homePhone: + 33 (0)5 33 22 33 22
title: System Administrator
postalAddress:
initials: LP
EOF
sudo ldapadd -x -D cn =admin, dc = $dc1 , dc = $dc2 -W -f $tmpdir/ dit.ldif
```

6) Edit the script at the top where it says **pleaseeditme**. I suggest you use **example** and **com** as your dc’s

7) Save your script and run it using $sh script.sh

8) Use the command **ldapsearch -D cn=admin,dc=yourhost,dc=yourdomain -W -x -b dc=yourhost,dc=yourdomain** to test your system.

9) Run nmap against your local host and note the open ports. What has changed? What port(s) was opened as part of the LDAP installation? How do the services provided on these ports compare to that on a Microsoft machine?

Submit your responses to item 9 to your instructor along with screenshots verifying you followed the included instructions.

You will find the following videos useful:

- Albanian Wizard
- Installing slapd
- Migration tools
- phpldapadmin

PA #2 : Lab – Setup LDAP and phpldapadmin (C4L4A2)

Use LDAP and phpldapadmin to setup a contact management system that maintains the following information:

- First Name
- Last Name
- Phone Number
- ID Number
- Email address

Create an LDIF file to import the following information in to your LDAP server…

- First Name: Bob
- Last Name: Jones
- Phone Number: 407-555-1212
- ID Number: 515
- Email Address: BJones@example.com

Take screenshots of your listing and activities and submit to your instructor showing details of your work.

If you make a mistake setting up LDAP, create and run this script: (also from albanianwizard.org)

```
#!/bin/sh
aptitude purge slapd ldap-utils
cat /dev/null &gt; /var/log/debug
rm /var/lib/ldap/*
rm -rf /etc/ldap
apt-get install slapd ldap-utils
```

Task #3 – Use the "Support forum"

Refer to all previous "Week's Overview PDFs" for detailed instructions applying to all discussion forums assignments.

PA #3 : Forum – Databases and Directory (C4L4F1)

Research and discuss what databases and directory services have in common and where they are different. Discuss how these items affect businesses in general and create two example scenarios where your team might choose a database over a directory or vice versa.

Post two comments or respond to two of your colleagues. Your responses should be comprehensive.

Upload this file using standard naming convention of: firstname_lastname_course5_lesson8_lab2.gpg to receive credit.

PA#4 : Forum – Choosing Directory or Database (C4L4F2)

You are the residential expert on LDAP at XYZ Products, Inc. Your boss asks you to create a LDAP-based service to manage inventory including invoicing, accounts receivable, accounts payable, vendor information, client information, sales information, and inventory management.

How would you answer and explain whether or not using LDAP is the correct service? If LDAP is not the correct service, what might you suggest instead? Justify your answer.

PA #5 : Forum – Security of LDAP (C4L4F3)

Research the additional security benefits of LDAP and discuss the various options offered. Are some security options more preferred than others? Discuss whether additional security options are more beneficial to smaller companies or larger companies (or both).

PA #6 : Forum – LDAP in Education (C4L4F4)

The company you work for creates different IT solutions for a wide variety of businesses. They have been contacted by the local school administrators requesting a solution for tracking and maintaining student grades. This system would only include entering and storing homework and grade card entries.

Discuss if you would and how you could implement LDAP for this purpose.

PA #7 : Forum – Comparison of LDAP and Active Directory (C4L4F3)

Discuss and compare the similarities and differences between LDAP and Microsoft Active Directory.

Do either of them have an advantage in the world of IT? Is there one that you prefer over the other? Justify your responses.

PA #8 : Forum – Microsoft Active Directory (C4L4F6)

Research and discuss the requirements for setting up Microsoft Active Directory. Include which Microsoft operating systems support Active Directory services and include the cost of the OS in your analysis.

How does the Microsoft cost compare to an Ubuntu alternative? Prepare a two-page memo to your instructor outlining the information and cost factors.

Task #4 – Graded quizzes

Refer to all previous "Week's Overview PDFs" and "ALL PREVIOUS WEEK's Overview PDF" for detailed instructions applying to all graded quizzes.