Unix for Telecommunications

Portfolio Task – P-Project-LDAP

Pass/Credit/Distinction/High Distinction Level Task

I. Introduction

This is the major project task in your Unit and should take most of the semester to complete. In this task you will be required to design and deploy a network-based service using existing tools, and to develop and integrate a user interface to your system. The particular task required for this project revolves around deploying a networked user account authentication service with support for scripted maintenance. Details on the task can be found in this task sheet.

II. Purpose

To gain and/or enhance the following practical skills:

- Design and construct unfamiliar network services
- Synthesise knowledge gained throughout the Unit to create a systems solution
- Professional documentation of process and usage of your system

III. Scenario

The corporation in which you work has grown to the point where the number of computers, servers and corresponding computer accounts has become unmanageable. Too much time is spent by IT Support Staff to manually manage systems. In order to simplify both administration and to minimise problems such as updating passwords, they have decided to centralise the user account/password database such that all systems within the corporation use the same account/password details. The advantages include only having to remember one password and that changing a password results in an instantaneous update across all machines.

To accomplish this task, you have been assigned to deploy and configure an LDAP server to store the account/password details for the corporation and to develop a simple set of instructions to configure other machines to make use of this LDAP database. Your project is due the night of the last project presentation session (Portfolio task **C-Presentation**) in week 12.

A. Required Background Knowledge

You are required to perform research into the following topics:

- **LDAP** – How does LDAP function in general terms, and gain an understanding of the primary purposes through which it can be deployed. What are the advantages/disadvantages of LDAP systesms, particularly for authentication purposes.
- **OpenLDAP** – You will deploying OpenLDAP (http://www.openldap.org) to build your solution
- **PAM** – Pluggable Authentication Module (PAM) should be used to manage authentication and access to your Unix system. Consider how to combine this with LDAP
- **NSS** – Name Service Switch (NSS) should be used to provide user account information to your Unix systems. Consider how to combine this with LDAP
- **CLI and CGI Scripting** – Understand the options available for you to automate the process of managing your system

B. Deployment Considerations

You will be required to build, test, and deploy your system as follows:

- **Server** – Install and configure your LDAP server on your highest numbered rule host
- **Client** – Install and configure your client (remote access) on your middle numbered rule host

Note: *If you are unsure which RULE hosts you must implement your system on, ask your laboratory or tutorial supervisor.*

IV. Assessment

This section highlights the absolute requirements to achieve the nominated grade for this task

Note: *It is **NOT** required to configure an encrypted LDAP service (ldaps) for this assessment. If you are unsure as to why you don't need encryption for an authentication service, I encourage you to discuss it in the forums.*

A. Pass

In order to receive a **Pass** for this Portfolio Task, you must at a minimum successfully complete all of the following requirements.

1) LDAP Server is configured to automatically run at system boot
2) LDAP Server is correctly configured to accept requests from the Swinburne network (`136.186.0.0/16`)
3) LDAP Server is responding to authentication requests from a remote computer
4) LDAP Server is responding to account information queries from a remote computer
5) Client host is properly configured to authenticate against the LDAP server
6) Able to login to Client host using ssh and a user account only available on the LDAP Server
7) Files on the Client host owned by an LDAP user are identified as such by the filesystem (eg. `ls -l`)
8) Server Configuration Documentation – A complete list of the location and names of all configuration files you edited on the server. Also details of at least two user accounts (usernames and passwords) configured in your LDAP server
9) User Documentation – Step-by-step instructions on how `root` can add/remove user accounts from the LDAP server

B. Credit

In order to receive a **Credit** for this Portfolio Task, you must at a minimum successfully complete all of the following requirements.

1) All **Pass** requirements
2) Server host is properly configured to use itself as an LDAP authentication server
3) Able to login to Server host using ssh and a user account only available on the LDAP Server
4) Files on the Server host owned by an LDAP user are identified as such by the filesystem (eg. `ls -l`)
5) Client Configuration Documentation – Step-by-step instructions on how `root` can configure a third FreeBSD workstation to authenticate against your LDAP server. This should include:
   - List of all software to install
   - Software installation instructions and procedure
   - Configuration file changes to be made
6) Password change instructions – Step-by-step instructions how `root` can change a user's password

C. Distinction

In order to receive a **Distinction** for this Portfolio Task, you must at a minimum successfully complete all of the following requirements.

1) All **Credit** requirements
2) When the LDAP server starts/re-starts, it launches with no delays or any other warnings/errors
3) Password change instructions – Step-by-step instructions how a user can change their own password
4) A web-based or CLI solution is provided to add and delete user accounts

D. High Distinction

In order to receive a **High Distinction** for this Portfolio Task, you must at a minimum successfully complete all of the following requirements.

1) All **Distinction** requirements
2) A web-based or CLI solution to edit user account details including passwords
3) A web-based or CLI solution is provided to allow users to change their own passwords
4) Use your imagination for other features you may want to add to your system. One example might be scripting to automate installation of a new FreeBSD client host
   Note: *Completing the minimal set of requirements will only guarantee you a minimal **High Distinction** result*

V. Self Assessment

Below are the steps we will take when assessing your system. This is a complete set of tests that will confirm functionality of all level tasks, it is up to you to determine whether you meet your target result.

A. LDAP Server

From your rule host:

- Check that `slapd` was automatically started
- Check that startup occured without any delay or any other warnings/errors
- Examine your configuration files to ensure you have correctly secured your database
- Confirm that **all** LDAP user accounts do **NOT** exist in the passwd file
- Run `getent` to retrieve user information

From a desktop computer

- Probe your LDAP server to ensure that queries work from another Swinburne machine
- Perform an LDAP query to extract user account information
- **ssh** into your server using an LDAP account with the provided password
- Create a file owned by an LDAP user and check ownership is correctly reported via `ls -l`

B. LDAP Client

- Check that `slapd` is **NOT** running
- Examine your configuration files to ensure client is configured to use your LDAP server host
- Confirm that **all** LDAP user accounts do **NOT** exist in the passwd file
- Run `getent` to retrieve user information

From a desktop computer

- **ssh** into your client using an LDAP account with the provided password
- Create a file owned by an LDAP user and check ownership is correctly reported via `ls -l`

C. Other Tasks

Other tasks we will perform to verify functionality include:

- An LDAP user will be created, tested, and deleted
- A third machine will be built to authenticate against your LDAP server
- The password for one user will be modified
- An attempt to change the password of the other user should fail

D. Implemented code

The code will be examined to see how it works and whether it has been properly structured and commented

E. Documentation

The documentation will be checked to ensure that it is complete (*all required documentation has been submitted*) and is correct (*the nominated instructions work as provided*)

VI. Assessment

For task **C-Project-LDAP**, you will be graded to a **Pass**, **Credit**, **Distinction** or **High Distinction** level as per the requirements listed above.

A. High Distinction Assessment

A Project graded at a **High Distinction** level will also be given a score based on the overall quality of the solution and any extra features you have decided to implement. Students will be given a score of **HD1** (meets minimum HD requirements), **HD2** (*Excellent work, cool new features, well implemented*), or **HD3** (*Did you hire a professional to build this*!!!). If a student is eligible for a **HD** result on their Portfolio, this result will be used as partial input to determine the student final score between **80HD** and **100HD**.

VII. Submission

The due date for completion of the project is **11:00pm** on the night of the **final** project presentation session in **Week 12**.

You must upload your documentation and select the Ready for Feedback option in your Doubtfire portfolio by the due date. Once this is done, your RULE hosts will be disabled until marking is complete.

A. Completion of task in Doubtfire

Your Doubtfire result will be updated once your RULE host has been assessed.