ST2412

Linux Administration and Security
Assignment (CA1 – Part 1)

Applied Research on Common Administrative/Security Operations for Oracle Linux

(Due date/time: 9:00 pm, 5 Jan 2024 (Friday))

Overview

You have just been attached to ABC Company for your internship program. On your first day of work, Harry, your company supervisor, give you the first internship assignment, to evaluate the level of your Linux knowledge and skills.

He asks you (and the other interns) to choose **one task each** from the below list.

1. Working out a solution on grub password and root password recovery.

2. Implement a simple web site to allow **remote** users to update the web content via ftp.

3. Implement a reverse proxy for a vsftpd service.

4. Implement a security measure to prevent brute force attack on a web site (using standard user authentication) with fail2ban.

5. Demonstrate how to use LVM to create a file system that span over 2 hard disk devices.

6. Apply one of the built-in features of the Apache 2 web server to enable personal web pages for selected users. For the selected users, this feature will allow them to publish web content at their home directory.

All the above should be targeted to work on an Oracle Linux 8 system.
You need to do some applied research to find useful and relevant references to complete the task you have selected to work on.

Your Tasks

Work in groups of maximum 4 students:

1. Write a technical report/guide (you may write in point form or use screenshots, similar to the style of your ST2412 Practical Guide) to demonstrate the steps to resolve the problem/to implement the prototype listed above.
   List down the references you have gathered to assist you on completing the task.
   List down any assumptions you/your team made about the task you are working on.

2. You are required to create a demonstration video (a screencast) and upload it to YouTube (as unlisted video) to prove that your solution/implementation is working. The duration of the video is expected to be about 7 to 10 minutes.

3. Complete the formative peer assessment and rate your group members.

Further Details on these six tasks

1. Grub password recovery:

Assume that you have lost the root password (and there is no sudo user available) and the Grub menu is also protected by an unknown password. You need to find a solution to gain access to the system and reset both of the root and Grub menu passwords.

Back in your year 1 LAS module at DISM, you have learned how to recover the Root access from an Oracle Linux system, but that technique cannot apply as the Grub menu is now locked by an unknown password.

There are many references on this topic at YouTube. Once you find the correct reference, this task may be considered as the easiest task among all the choices.

Unlike other tasks, once you have reset these two passwords and able to login to the system as root, your task is completed. Therefore, your YouTube video have to cover the actual process / procedures of the recovery.

2. Updating web site content via ftp:

This is a common practice that remote web content designers are using ftp to upload newer versions of the web page to the server.
Usually, a remote web content designer will set up a local web server at his own system to test out his newly designed web page(s). Once the page(s) have been tested in the local web server, he will upload the new page(s) to the actual web server via ftp.

In this assignment, you do not need to implement a real web site. A couple of sample / dummy web pages will be good enough to prove your implementation.

Search relevant resources on how to configure httpd and vsftpd services, and integrate both of them to work together.

For the YouTube video, you need to demonstrate how users use the ftp connections to update the web pages and prove that by showing the updated web content.

3. Reverse Proxy on vsftpd:

Reverse Proxy can serve as an additional layer of security measure to protect a public facing service. In this task, you will hide a public facing vsftpd service behind a reverse proxy.

Search relevant resources on how to configure a reverse proxy for an httpd service, and implement the reverse proxy for the vsftpd service.

Please take note that, the vsftpd runs on ftp protocol which utilizes multiple and dynamic ports. It is fairly difficult to configure it to run behind a reverse proxy server.

For the YouTube video, you need to demonstrate how users use access the ftp connections (with file upload and download operations) via a reverse proxy server.

4. Fail2ban for httpd/web page authentication:

Fail2ban is a utility to detect fail attempts of authentications and it can prevent brute force attack by blocking the clients which triggers the fail attempts. In this task, you need to implement fail2ban to protect your web page(s) from the brute force attack.
Search relevant resources on how to implement user authentication for web page login and fail2ban to protect the sshd access, and implement the fail2ban for the web page login.

For the YouTube video, you need to demonstrate the actual effect of how the fail2ban detect and block the user browsing to the web page after a few attempts of login with incorrect credential.

5. Large file system that span over multiple disks

For this task, you can use VMware Workstation to add in a couple of additional virtual disks to your demo VM and using LVM to configure them to complete this task. This is considered to be an easier one among all the choices.

For the YouTube video, you need to prove you have completed the task by examining and show the list of block devices, file systems, physical volume, volume group and logical volume.

6. Implement personal web site for local users

Back in your DISM year 1 FOC module, you have learned the basic setup of the Apache server 2. However, the LAS lessons did not cover this. Now it the time for you to explore this. This task may take you a while to do some research. Once you find the correct reference, this task may be considered as the easiest task among all the choices.

For the YouTube video, you need to prove you have completed the task by creating a few personal web pages with different user accounts.

Marking Scheme

	Written Report	**Marks**
1	Report Structure & Completeness Proper report layout. • Provide sufficient background, overview for the prerequisite of the proposed solution/implementation. • Provide **strong support of Sources of information.**	10%
2	Readability & Correctness • Proper **stepwise breakdown of the solution.** • Content Clarity. • Using illustrations / diagrams effectively. • Correctness.	30%
	YouTube Video	
3	Quality • Smoothness of the demonstration flow. • Interesting and engaging. • Using screencast, caption / sound / video editing techniques effectively. • Pace and duration.	20%

4	Effectiveness and correctness • Proper introduction • Clearly showing the key steps/operations of the solution. • Closely corresponding to the written reports. • Easy to follow and apply the solution.	30%
	Formative Peer Assessment	
5	• Rate your group members • Provide constructive feedback • Strengths & Weaknesses • Contribution and Proactiveness	10%
	Total	100%

Deliverables & Due Date

- A written report.
- Completed Formative Peer Assessment
- Include the link to Youtube in the report

You may upload the report to Brightspace by

9:00 pm, 5 Jan 2024 (Friday)

Take note of the "**SOC – Policy on Late Submission of Assignments**". 50 marks will be deducted for every working day late submission. Assignments will not be accepted after more than 2 working days after the due date.

~ The End ~