Saim Ghafoor (10-11-2022)

Course Title: Secure Systems Administration

Assignment No.: 1

Submission deadline: 11th December 2022

Marks: 30

Instructions:

1. Please avoid plagiarised content and copying. Zero marks will be given to copied content from others.
2. Upload your assignments solution to blackboard before the deadline.
3. Please provide your answers in the order given below.
4. You can use either fedora or ubuntu. Just mention at the beginning of the document, which one you are using with the version.
5. For the explanation, where needed, provide a to-the-point answer.
6. Save and name your files as ASSIGNMENT_ID_Surname_Initials.ext
7. Include brief text where necessary to explain the steps and also include the screenshots to show the commands and the output.

Description:

The main objective of this assignment is to familiarise students with some basic steps of monitoring the Linux system and the use of scripts with some commands. It includes handling the start-up program, looking at the log files, writing a script, and displaying its output. In scripts, you can use all commands and use them according to your system administration need. Another objective of this assignment is to make you familiarise yourself with virtualization platform installation, configuration, and management. This assignment also includes the installation of a server on a Linux environment, typically on a virtualized platform (like a cloud).

Deliverables and requirements:

A report in PDF format in which all questions should be answered in the given order. There is no word limit for the report but do not unnecessarily extend your answers. Try to provide to-the-point answers. You can use your own template for this report with into page containing name, id, assignment, module, etc. Each question should start from a new page. The report must include step-by-step configuration steps and screenshots for installation related questions like question 3 and 4. For script-based questions script should be included in the report with description and explanation of commands used.

----------*----------

Saim Ghafoor (10-11-2022)

Question 1: (Marks 10)

a. Locate the folder for start-up scripts in Linux. Name those folders and briefly describe for what purpose each folder/s can be used. (2)
b. Describe Samba Server and its uses. (2)
c. Install and configure Samba Server to share a folder and access it from the same and a remote host. See at the bottom for links for basic installation and configuration. (6)

Question 2: (Marks 10)

a. Locate the folder for logs in Linux (show path using commands and the GUI screenshots for logs folder). (1)
b. Which folders or types of files exist inside the logs folder in Linux? Name and briefly describe. (2)
c. What different commands or ways can be used to filter the log entries? Name and describe at least four commands. (2)
d. Write a script to filter the authentication failure including wrong password, SSH, and sudo attempts from the log file, and then save only failure entries to a new file. Use logs of today or yesterday entries. For this, you need to locate first, where such entries are saved in the Linux log folder. You also need to intentionally enter wrong login passwords to create such entries. (3)
e. Find a way to alert the system administrator for such entries. Implementation here is not required for this part but you should know what different ways exist to alert the system administrator. (2)

Question 3: (10 marks)

a. Set up an Apache webserver within Fedora/Ubuntu. Show all the steps with screenshots and descriptions. (6)
b. What different ways can be used to secure the webserver? (4)

**** Links for Question 1b and 1c

https://ubuntu.com/tutorials/install-and-configure-samba#1-overview

https://ubuntu.com/server/docs/samba-introduction