Secure Systems Administration Assignment

Daniel Gallagher

L00158616

[L00158616@atu.ie](mailto:L00158616@atu.ie)

11th December 2022

I am using ubuntu version 22.04.1 LTS for the Assignment.

**Question 1**

**A.**



Text

Description automatically generated

• The start-up scripts are in the /etc/init.d directory.

Text

Description automatically generated

**/etc/init.d/apache2** – It can be used to start, stop, and restart the Apache server, as well as to configure various aspects of the server's behaviour.

**/etc/init.d/cron** – It can be used to start, stop, and restart the cron daemon, as well as to configure how the daemon behaves.

**/etc/init.d/rsync -** It can be used to start, stop, and restart the rsync service, as well as to configure how the service behaves.

**/etc/init.d/ufw -** It can be used to start, stop, and restart the ufw service, as well as to enable or disable specific firewall rules.

**/etc/init.d/acpid** - It can be used to start, stop, and restart the acpid daemon, as well as to configure how the daemon behaves.

**B.**

**Describing the Samba Server**

**•** Samba is an open-source implementation of the SMB/CIFS network protocol, which allows Linux and other Unix-like operating systems to share files, printers, and other resources with Windows-based systems. It provides access to shared resources over the network using the SMB/CIFS protocol.

**Its Uses**

• Samba can be used in a variety of ways, including to provide file and printer sharing services on a network, to allow Linux systems to access resources on a Windows-based network, or to enable Linux systems to participate in a Windows domain.

• The Samba server can also be configured to act as a domain controller for a Windows domain, allowing Linux systems to be managed and authenticated in the same way as Windows systems.

**C.**

**Installing Samba**



Text

Description automatically generated

**•** To install Samba, I ran the sudo apt update command and the sudo apt install samba command.

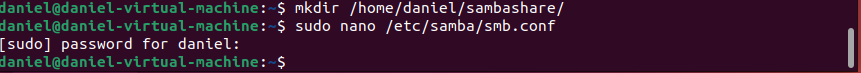


**•**  I checked if the installation was successful by running the command whereis samba.

**Setting up Samba**



**•** I created a new folder called sambashare in my home directory.

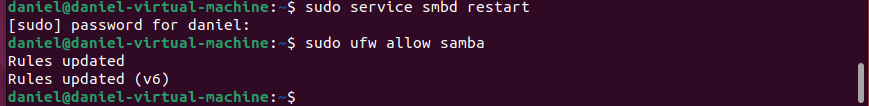


• to add the new directory as a share, I edit the configuration file for samba /etc/samba/smb.conf

Graphical user interface, text

Description automatically generated

• the image above shows configuration for the new share which has a path with the directory of my share, a read only to modify the contents of the share folder and a browsable which will allow file managers to list the share under Network.



**•** Saving and restarting Samba for the new share to take effect and updating the firewall rules to allow samba traffic.

**Setting up a User Account and Connecting to Share**

A picture containing text

Description automatically generated

• Setting up a samba password for my user account



Graphical user interface, text, application, email

Description automatically generated

• Connecting to Share.

**Question 2**

**A.**

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

**B.**

**•** The logs foldercontains log files that record important events and messages from the operating system and various applications.

Some examples of log files you will find in the log’s directory include:

**auth.log -** This file contains log messages related to authentication, such as when users log in and out of the system, and when authentication failures occur.

**syslog** - This file contains system-wide log messages, including information about the kernel, system services, and other system-level components.

**mail.log -** This file contains log messages related to the mail system, including information about incoming and outgoing messages, as well as any errors or warnings that occur during the mail process.

**dmesg -** This file contains log messages generated by the kernel, including information about hardware devices and drivers that are loaded during the boot process.

**C.**

**grep -** you could use the grep command to search for log entries that contain a specific keyword, or that were generated by a specific application.

**awk** - you could use the awk command to extract the timestamp, severity level, and message text from each log entry, and then to sort or filter the entries based on those values.

**tac –** you could use the tac command if you want to view the most recent log entries without having to scroll to the end of the file.

**sed** – you could use sed to allow you to manipulate log entries in various ways, such as by replacing specific words or phrases, or by deleting certain lines or entries.

**D.**

Text

Description automatically generated

**E.**

Text

Description automatically generated

**Question 3**

**A.**

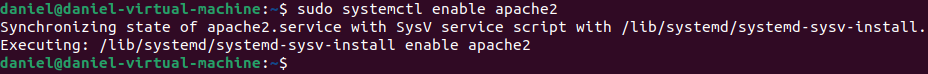
Text

Description automatically generated

**•** I used the sudo apt-get install apache2 command to install Apache**.**



**•** I used the sudo systemctl start apche2 command to start the Apache service.



• I used the sudo systemctl enable apache2 command so that Apache automatically starts when the system boots up.

Graphical user interface, text, application, Word

Description automatically generated

• Verifying that Apache is running by visiting <http://localhost> in Firefox and it shows the Apache default page.

Text

Description automatically generated

• To allow incoming traffic to my Apache server, I adjusted my firewall settings and used sudo ufw allow http command and the sudo ufw allow https command to allow HTTP and HTTPS traffic.

**B.**

The different ways that can be used to secure an Apache webserver are:

**1.** Is to configure the Apache webserver to use SSL/TLS encryption to secure communication between the server and clients.

**2.** Is to restrict access to the server by blocking unnecessary ports and using a firewall.

**3.** Is to enable the Apache webserver’s built-in security features, such as mod security and mod evasive.

**4.** Is to keep the Apache webserver and the operating system up to date with the latest security patches.

**5.** Is to Implement a backup and a disaster recovery plan to ensure that you can recover from any security breaches or other disasters

**6.** Is to use intrusion detection and prevention systems to monitor for and protect against malicious activity.