Secure Systems Administration CA

# Question 1:

1a. The Etc Directory contains a lot of files. One of those files is init.d, init.d is where all scripts are located inside of the linux system, this is also where you find scripts for changing the runlevel that are called through links from one of the sub-directories.

Text

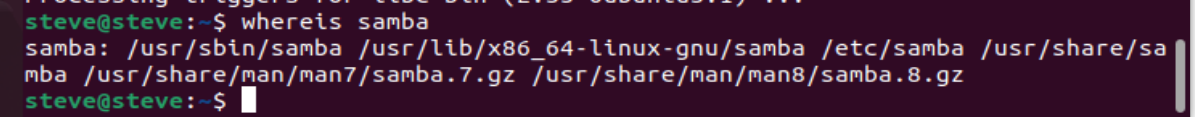
Description automatically generated

Text

Description automatically generated

1b. Samba is a crucial component in integrating Linux as well as Unix servers and desktops into Active Directory settings, it may act as a domain controller or as a standard domain member.

1c. Samba has been installed



­

Samba server setup with shared files

Graphical user interface, text, application

Description automatically generated

# Question 2:

A.

A screenshot of a computer

Description automatically generated

2b. The types of files that exist inside the logs folder of Linux are all plain text files. These are the Linux logs for everything such as system logs, kernel logs, boot process log, Apache, MySQL, etc etc.

An example would be the kernel log, once the system powers on the system logs information about the kernel ring buffer which gives us information on hardware drivers, kernel information and status during the bootup of the system and more.

2c.

The 4 different types of filters that I would use to filter through the log files:

**Grep** – command that helps you get specific keywords that can lead you to messages in the logfile that can help you find a certain string or files depending on the regular expression pattern.

**Awk** – Awk is probably one if not the best commands in Linux, Awk is a scripting language and is used to select particular records in a file and performs operations upon them. Awk is also used to alter data and can be used to process a log file by searching through it.

**Regex** - To filter logs, you may use regular expressions, often known as regex. Regex can help you filter your logs so that you only see what you want to see from the log message. Regex also allows you to write a phrase of your choice. This is useful when dealing with a log file that contains more complex filtering. Regex although is quite useful it can be made even more effective when it is paired with the powerful Linux tool Grep that has been previously mentioned above when used for searching text files.

**Heads or tails? Flip a coin** – Although this title Is just a playful joke Heads and Tails are 2 different and quite useful commands that are regularly used in Linux. Heads are tails although on the other side of the coin both pretty much do the exact same thing, the only difference is Heads prints out the first few numbers of lines by default and Tails prints out the last few lines of by default of a certain file then terminates, Heads and the command Tails print roughly 10 lines of the file each.

# Question 3:

1a.

For Question 3 we will be setting up an Apache Webserver, first we’re going to start off by updating the system repository to get the last version of Apache by opening up the terminal and using the command displayed below.



In the next step we’ll be installing Apache2 which will be used for our Webserver by running the command displayed in the image below.



To make sure the package installed successfully, and we have the latest version we will run the command apache2 -version which will give us the version and date of last install.

A screenshot of a computer

Description automatically generated with medium confidence

Next, we’ll open certain ports in our system, so we are able to access Apache from outside to do so we need to first give the Apache profile access to change ports on the network to enable network activity on port 80. First, we list the types of profile, then we give Apache permission through the sudo ufw allow ‘Apache’ command and then check its state by doing sudo ufw status as seen below

Text

Description automatically generated

Text

Description automatically generated

Now that we have given Apache permission we’re going to verify that the Apache service is operational by running the command seen below, as we can see the Apache service is up and running.

Text

Description automatically generated

Creating directory for domain



Changing directory ownership



Giving necessary permissions



Creating the sample page and adding a small amount of html to the index file.



Text

Description automatically generated

Creating new virtual host file



Please ignore the “SeverAlias” it was fixed later on.

Text

Description automatically generated

Creating the virtual hosts config file

Text

Description automatically generated

Disablin the 000 default config that comes with the default virtual server  


Restarting apache to active the new config

  
adding servername to new server conf file to prevent any errors



Enables configurations servername



Text

Description automatically generated

Now your web server is ready to serve in the domain you provided.

3b.

What different ways can be used to secure the webserver? Personally I would disable the SS directive also known as the Server-Status directive as it contains a lot off direct list Information such as uptime, local, http requests and client ip addresses which can be used to craft an attack against the webserver by a hacker.

You should also disable any type of unused modules and only keep the required modules needed, having unceccesary and unused modules in a server can lead to many security issues as they’re 1. Not being monitored and 2. Leaving more open weaknesses in the server that can be attacked.

And probably one of the most important security pieces that should be apart of your server is well, logging, enabling logging is probably one of the most useful features that you can probably have on well, anything. Logging provides detailed information about client requests and activity on your web server, due to this you can see why it would be usefuul when investigating particular issuees when it comes to monitoring your webserver.