This element of the assignment should be done after engaging in the discussion of the authentication log.

We will start with three elements of a security architecture for your server. Before doing so **make sure you have a password that is complex**. Many experts suggest pass phrases because they are typically longer and easier to remember. Adding numbers and replacing letters with special character increasing the defense against a brute force attack as well as dictionary attacks (two forms of attack that you should know and understand).

A brute force attack attempts to use all possible combinations of characters (tokens) in guessing a user id or password. A dictionary attach uses a collection of common userids or passwords in an attempt to login to the system. In 2019 a successful attack on the VMWare lab was probably a dictionary attack. The attacker successfully guessed a user name of "test" with a very common password that was used by one of the students in testing procedures to add new user accounts for a lab assignment (Lab Assignment 2).

If you have not chosen a complex password, please learn how to change your password and do so.

The elements of security we are calling for currently are:

1. If you haven't done so already, automatically install all updates to your system. You can configure automatic updates by following the steps in the article [How to enable automatic security updates for Ubuntu Server - TechRepublic](https://www.techrepublic.com/article/how-to-enable-automatic-security-updates-for-ubuntu-server/). This link takes you to an article in one of the more reliable UBUNTU documentation sites.
2. The fail2ban utility monitors server log files for intrusion attempts and other suspicious activity. After a predefined number of failures from a host, fail2ban blocks the offending IP address automatically for a specific duration. Install fail2bn by following the steps in this article <https://www.a2hosting.com/kb/security/hardening-a-server-with-fail2ban>. The article explains how to configure fail2ban. For now, the default configuration should be sufficient. This lab assignment asks you to examine the authentication log. **You should examine the log before installing fail2ban.**If you are curious to see what fail2ban does, you can examine the authentication log again after a couple of days after installing fail2ban and consider the differences. You can also use the *iptables* command documented in the article to see what *ip addresses* have been banned. After installing this utility, be careful because login failures can lead to your IP address being banned.
3. Next you will add an auditing capability to UBUNTU. (If you would like to learn more, see <https://linuxhint.com/auditd_linux_tutorial/>) AuditD is a component the Linux Auditing System. AuditD operates as a audit daemon. A daemon is a service that runs in the background looking for some sort of triggering event and then taking action. In Linux, the letter ‘d’ attached at the end of the application service to designate it as a background service operating as a daemon. The purpose of AuditD is to collect and write log files to the disk as a background service. Like most services it is configurable through a configuration file. It also operates by a set of rules that are found in a separate file. The files used for rules and logs are configurable items (configuration items). For our purposes we will use the default configuration and default rules. To install and start the audit services issue these commands:
   * *sudo apt-get install auditd audispd-plugins*
   * *service auditd start*
4. In this step you will be adding additional external monitoring to the virtual server. One of the primary tools used to understand the behavior of systems and services is logging. The logs are reviewed to detect cybersecurity problems. We are using a common commercial tool named s*plunk* to do security monitoring in a Security Operations Center (SOC). There is a "universal forwarder" that must be installed on your server. It can forward any logs created. It can be configured to monitor and send specific logs to a *splunk* server (Splunk Enterprise) that we have set up in the SOC. Splunk Enterprise has various tools including a log parser to ensure readability. The data forwarded to the splunk server will be monitored by a student working in a Security Operations Center (SOC). The SOC can implement rules that raise alerts. We are using our installation of *splunk* as a Security Information and Event Management (SIEM) tool in the SOC. S*plunk*is one of the most commonly used SIEM tools. To set up *splunk*forwarding of critical logs there is a complex process described in the following. It begins with downloading the forwarder that collects and sends logs.
   * In your server copy and execute this long command:
     + wget -O splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 'https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'
     + wget is a utility to download files/software from an Internet server. The first argument is the name of the file (“splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb“) and the second is the URL-location “https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb”)
   * After the download we install the package using the dpkg package manager. dpkg is the package manager for Debian based Linux systems. Issue this command: *sudo dpkg -i <insert the .deb-filename here>* (HINT: typing “splunkforwarder” and hitting tab key should auto-complete to the full file name
   * Enter the command “sudo chown -R splunk:splunk /opt/splunkforwarder/”
   * To ensure that the forwarder is restarted if the system is rebooted, issue the command: “sudo /opt/splunkforwarder/bin/splunk enable boot-start” (HINT: the tab key can auto-complete names for you).
   * You will be asked to agree to the software license terms which will display many screens worth of information. This will probably come as a surprise. After moving through the many screens of this long agreement, eventually you will be asked to agree. Follow the prompt to agree.
   * After agreeing to the license, you will be asked to create a Splunk administrator username and password for yourself. **Make sure that you remember this username and password.** You now have many usernames and passwords. Be sure to keep them organized.
   * We now want to start the service. Enter the command: *sudo /opt/splunkforwarder/bin/splunk start*
   * Tell the forwarder where to send logs. We have a server located in our lab that can accept the forwarded records. It has an IP address of 134.48.13.244 and it is listening for records on port 9997. Enter the command “*sudo /opt/splunkforwarder/bin/splunk add forward-server 134.48.13.244:9997”* using the splunk administrator credentials that you created.
   * You will be forwarding several logs that we can use to spot suspicious behavior. You will tell the forwarder what logs to forward and how to treat them on the receiving side and then, because these are configuration items, you will restart the service. Restarting a service after doing configuration is a common activity that you should learn to expect. Three of the logs we forward are automatically maintained by UBUNTU. The fourth is the audit.log that you created in a prior step (installing AuditD). Initiate collecting the four logs (system.log, auth.log, dpkg.log, and audit.log)
     1. *sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/syslog -index main -sourcetype Systemlogs*
        + *this log contains many entries reflecting system operations*
     2. *sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index main -sourcetype Authlog*
        + *this log contains information about all login attempts*
     3. *sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/dpkg.log -index main -sourcetype dpkglogs*
        + *this log contains information about software installations using the standard package manager (dpkg)*
     4. *sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/audit/audit.log -index main -sourcetype Auditlog*
        + *by default, this log contains information about events, changes to auditd, all authentication events, changes to sensitive data such as passwords, and incoming and outgoing information to and from the server.*
     + *sudo /opt/splunkforwarder/bin/splunk restart*
       - *The customary restart of the service after changing the configuration*

All these items should be documented in your lab report for this assignment.