You are called to investigate a possible break-in on an Ubuntu Linux box. The log file storing ssh login information is of interest. The following is a snippet of the file auth.log. The complete file is available in your Blackboard group directory.  Move it to /home/alice/<company\_name>\_auth.log

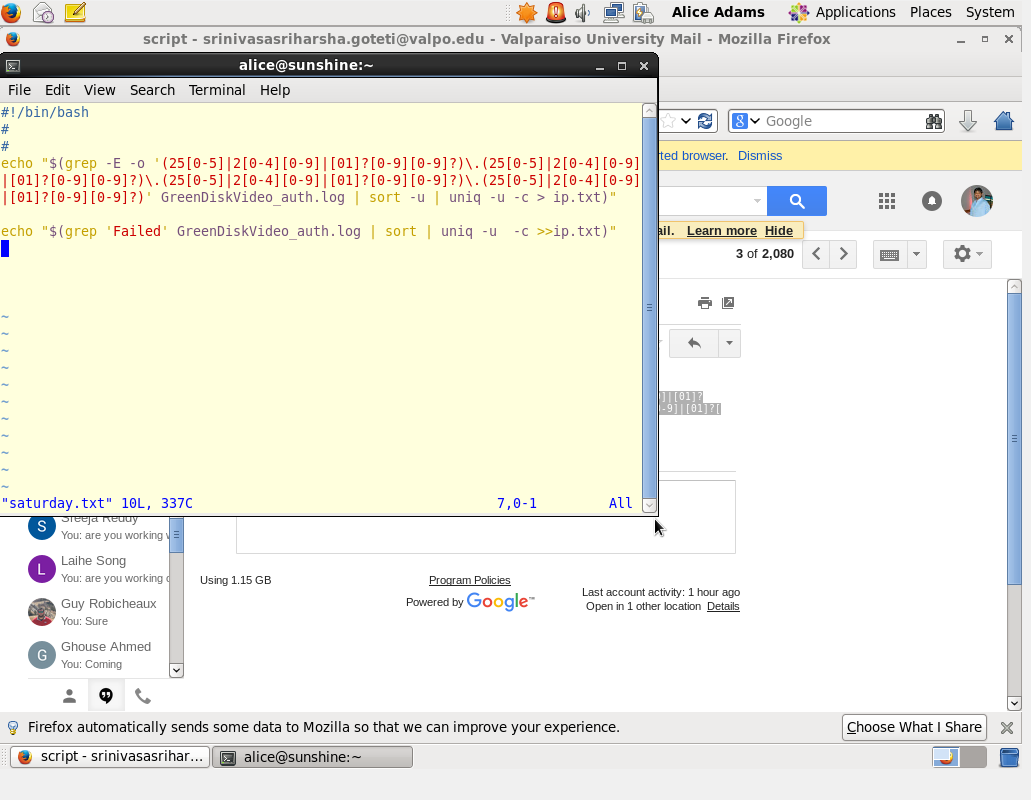
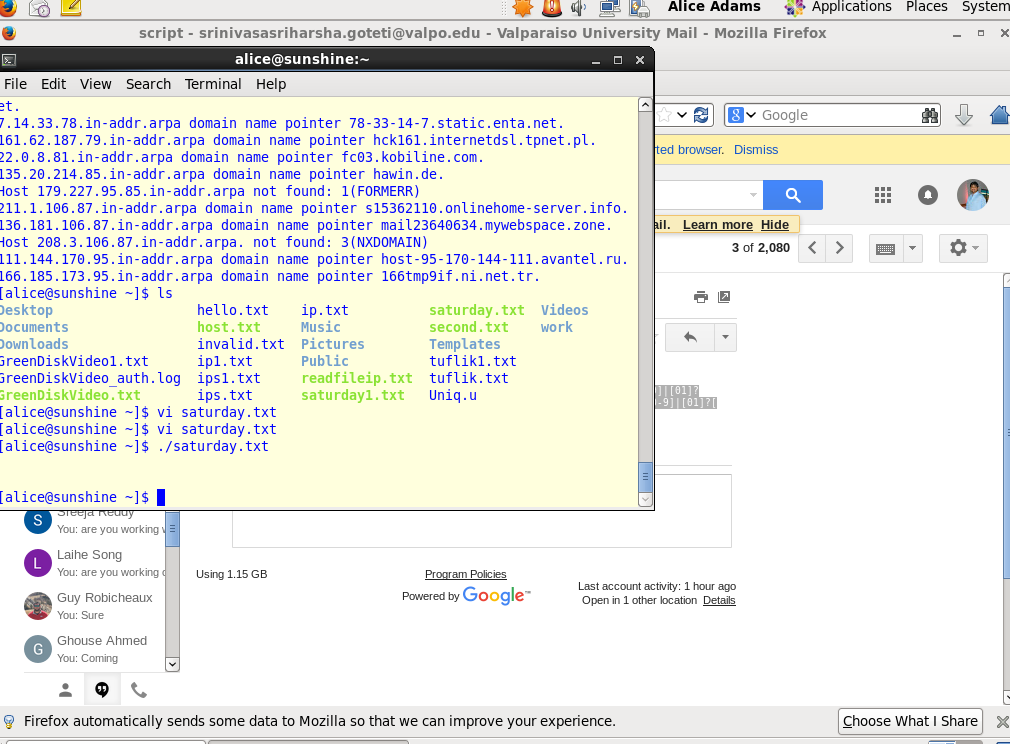
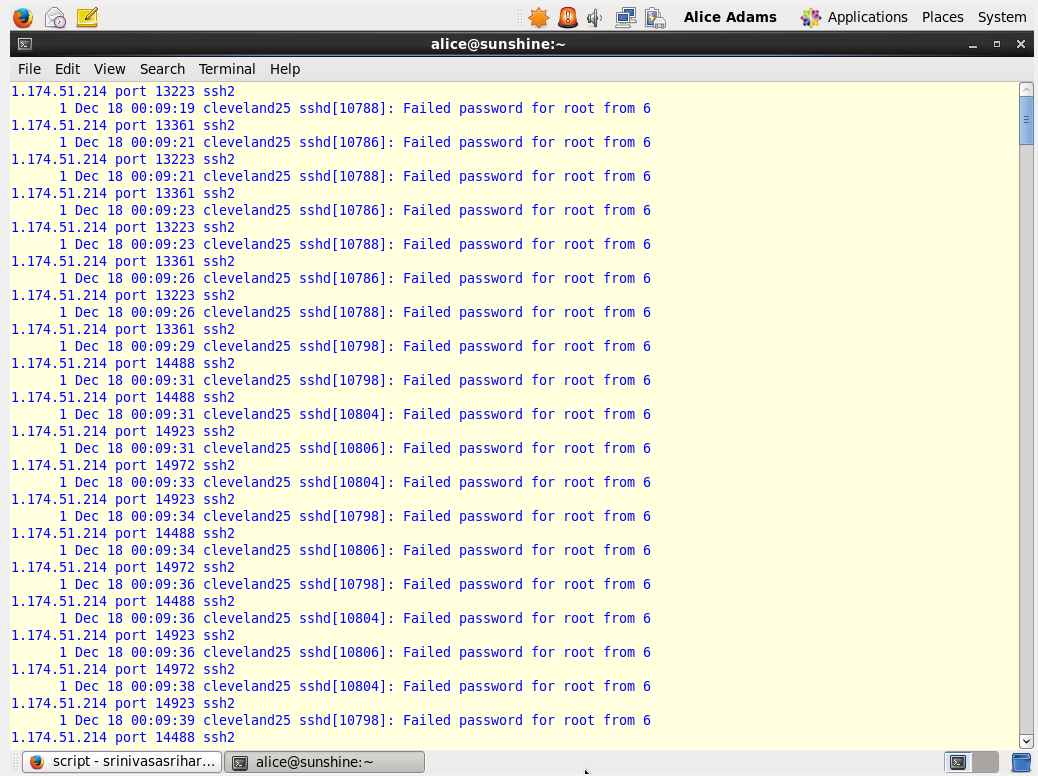
1. Investigate the log file you were given.

Below is the screenshot pasted for creating a file of authentication file, and then we had reviewed that log file , where we can infer many things in terms of observation from the log file. Here are some of the file.   
  
 1. A malicious script is trying to connect to the server using a rhost where a remote application is trying to help to get it to server.

2. The same ip is trying to connect to get connected to the server, where this ip is been used from HongKong, and we had identified this from <https://www.ultratools.com/tools/ipWhoisLookupResult> and so for this we can also make this ip blocked using server iptables and try to block the ip address.   
  
3. Error is regarding with uid > 1000 is missed when logging as a root.  
  
4. Password and username provided is given wrong.  
  
5. Script was given to get access even by different ports and make as access as root.

* 1. Create a script that displays the IP addresses (without duplicates) of all servers that tried to login and failed to login as the user ‘root’ along with the number of times each server attempted to log in. Sort the results by the number of failed logins.  Display the script on your screen, then run it, and investigate of the output.  Take a screenshot of script, run line, and output on the same screen (or showing that the screen continues).

1. Create a script which displays all of the account names and that were tried that do not exist on this server (Hint: look for the phrase ‘Failed password for invalid user’) and the IP address that attempt came from. Sort the list alphabetically and do not include duplicate lines. Display the script on your screen, then run it, and investigate of the output.  Take a screenshot of script, run line, and output on the same screen (or showing that the screen continues).

1. Create a script that will read a file (ip.txt) containing a list of IPs and try to resolve the Fully Qualified Domain Name (FQDN) with the `host` command. The FQDN is the human mnemonic version of the IP address, such as www.google.com or my.usf.edu. The script should store the IP and FQDN (or ‘UNKNOWN’ if the IP cannot be resolved), one set per line, comma-separated, to a file named <your company name>.txt.  Display the script on your screen, then run it, and investigate of the output.  Take a screenshot of script, run line, and output on the same screen (or showing that the screen continues).