Linux Forensics

Part I - Linux Auditing System

**Step 1 & 2**

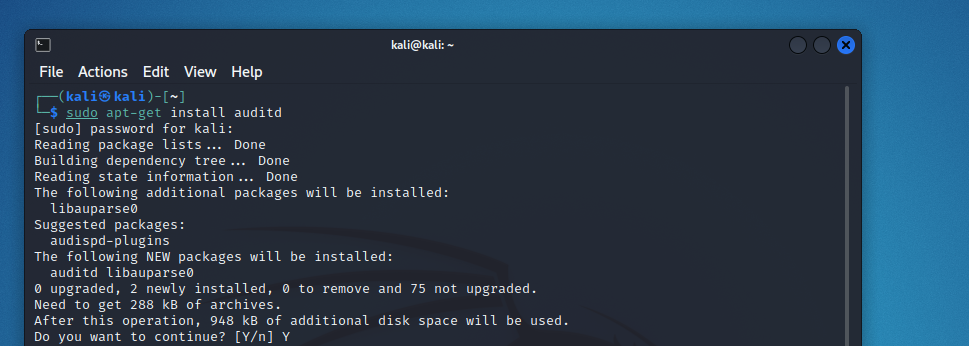
Linux audit system is a process that tells you about what is going on the system in great detail. This would eventually help in building up the security of the system and hardening the device.

Operating systems should provide auditing capabilities to conform with strands of protection profiles.

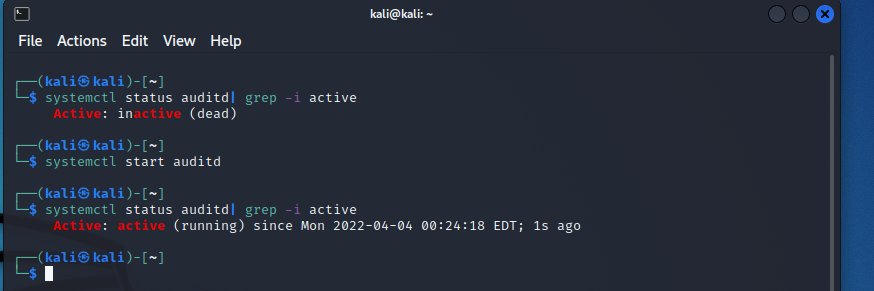
Here in kali linux we have a tool called **auditd** that is capable of provide ever single detail.

**Step 3**

First of all, we will install **auditd** tool,

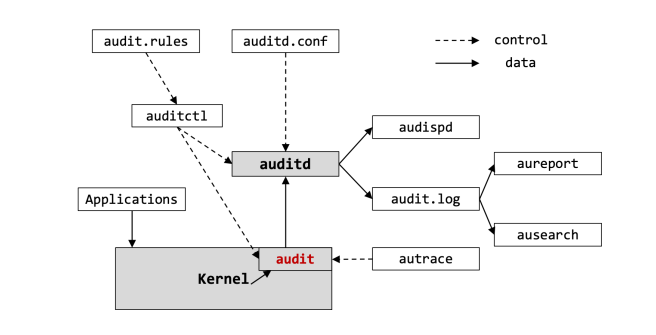


After installing it we are going to **enable** the service.



**Step 4**

**Auditd** tool is Linux auditing system that works over Linux kernel and here is its full diagram.



**The service running at the background writes messages in the log file (/var/log/audit/audit.log). These functions are controlled by a file /etc/audit/auditd.conf.**

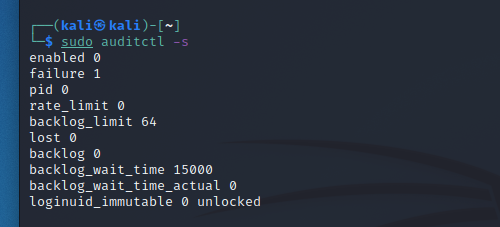


**Step 5**

Utilities in auditd tool:

* **Auditd**: controlled by /etc/audit/auditd.conf file
* **Auditctl**: It controls audit system.
* **Aureport**: This utility allows user to generate reports out of audit log file.
* **Ausearch**: This utility is used to search the audit log file for particular events.
* **Audispd**: Dispatcher service can be used to relay event notifications.
* **Autrace**: This utility is used to trace particular processes. The output of autrace is logged in audit log file.

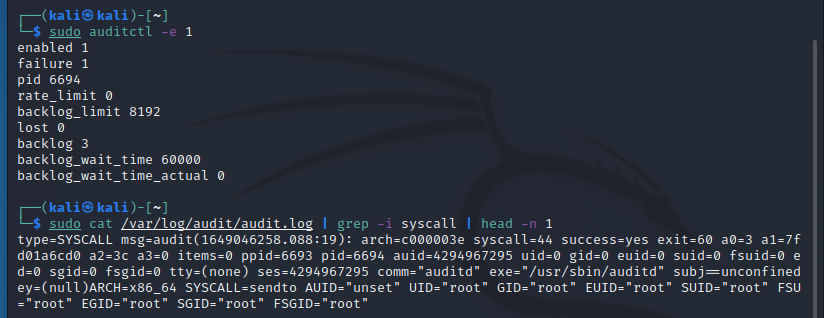
Here we are going to list query that can be controlled by **Auditctl**.



**Step 6**

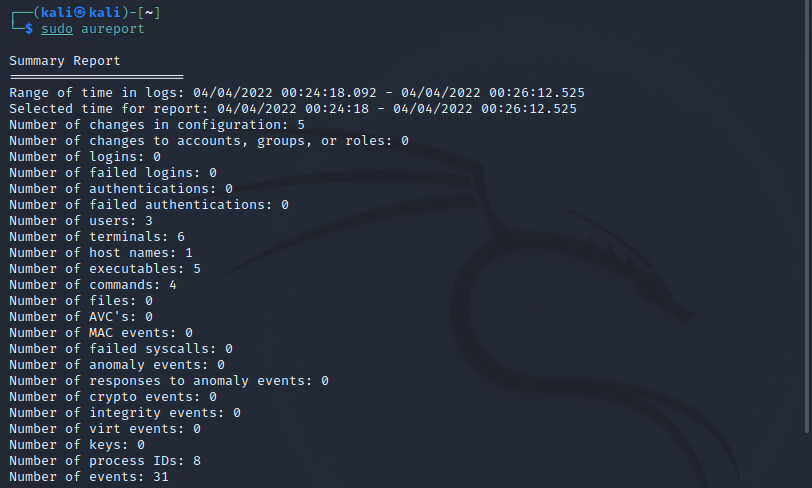
As the **enabled** is marked ‘**0**’ so we are going to change it to ‘**1**’ and this is done using Auditctl.

After that we will display one audit event.



**Step 7**

Aureport are used to create custom reports that are very helpful as there are many different functionalities.

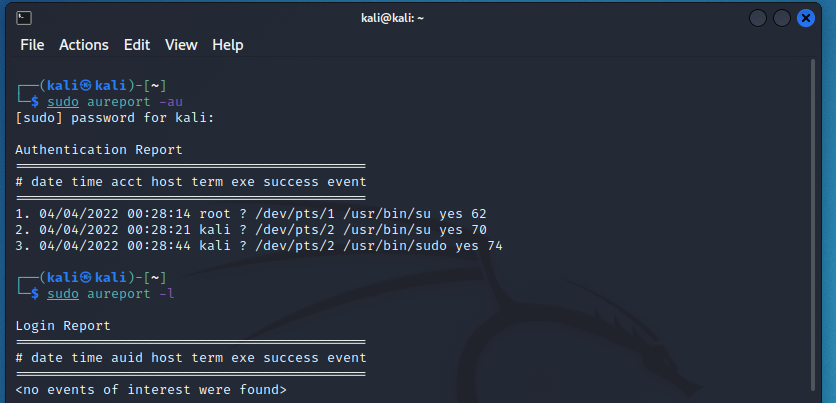


**Step 8 -- More functionalities**

For generating a report related to authentication and attempted login

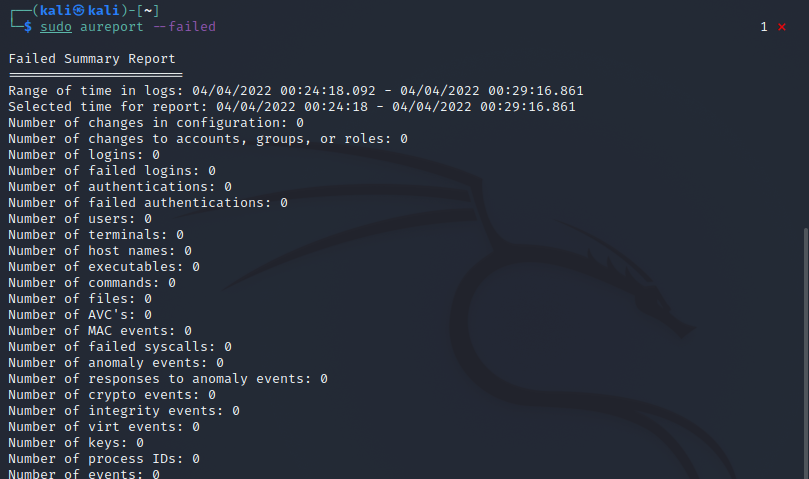
Authentication --> “**aureport -au**”

Attempted login --> “**aureport -l**”



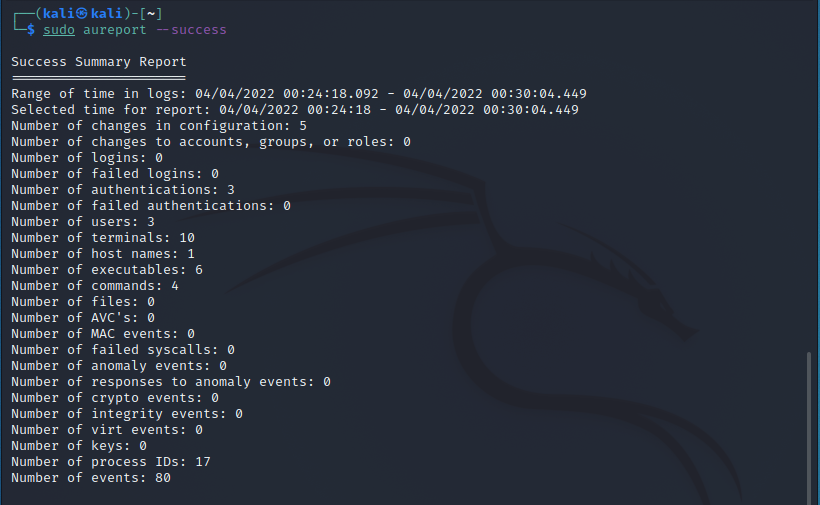
**Failed**

To see and capture failed events we use “**aureport –failed**”



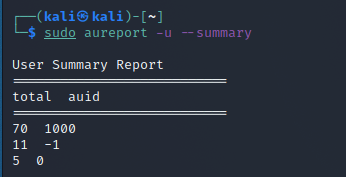
**Success**

To see and capture success events we use “**aureport –success**”

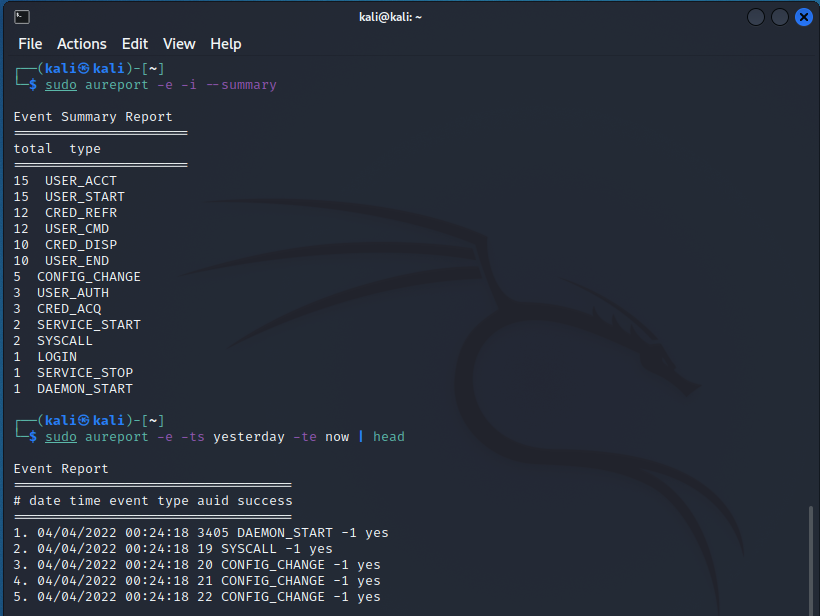


**Summary**

To list the summary of all the users “**aureport -u –summary**”

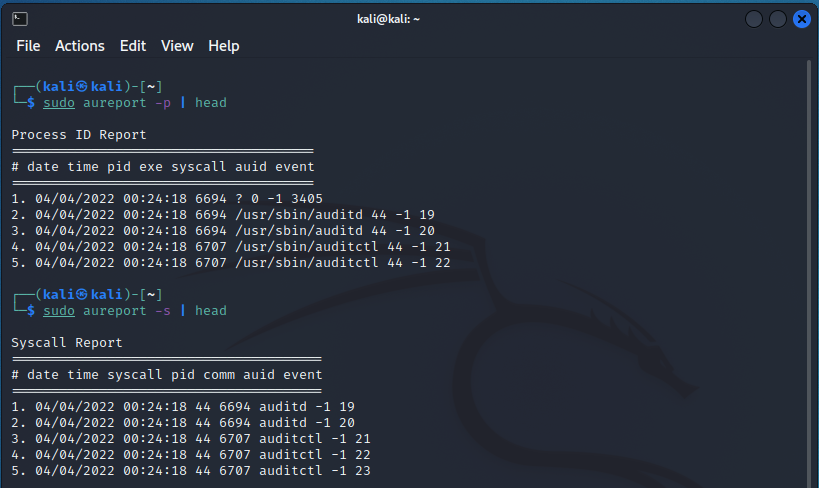


To get the summary of all the events “**aureport -e -I –summary**”



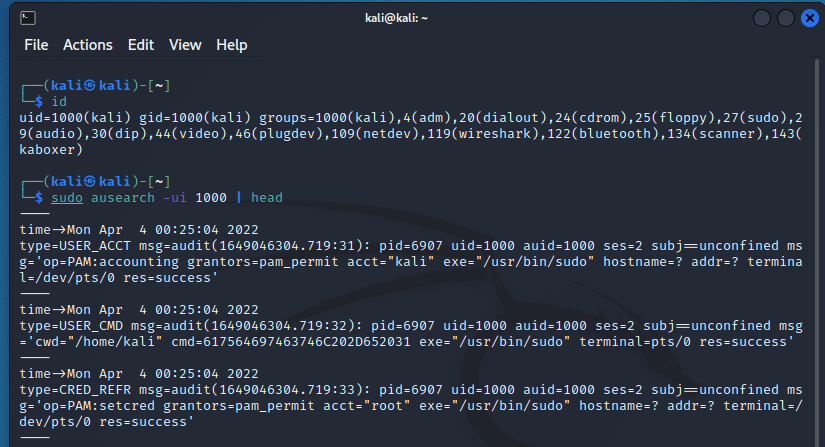
**Process report**

If you want to generate report related to processes “**aureport -p | head**”



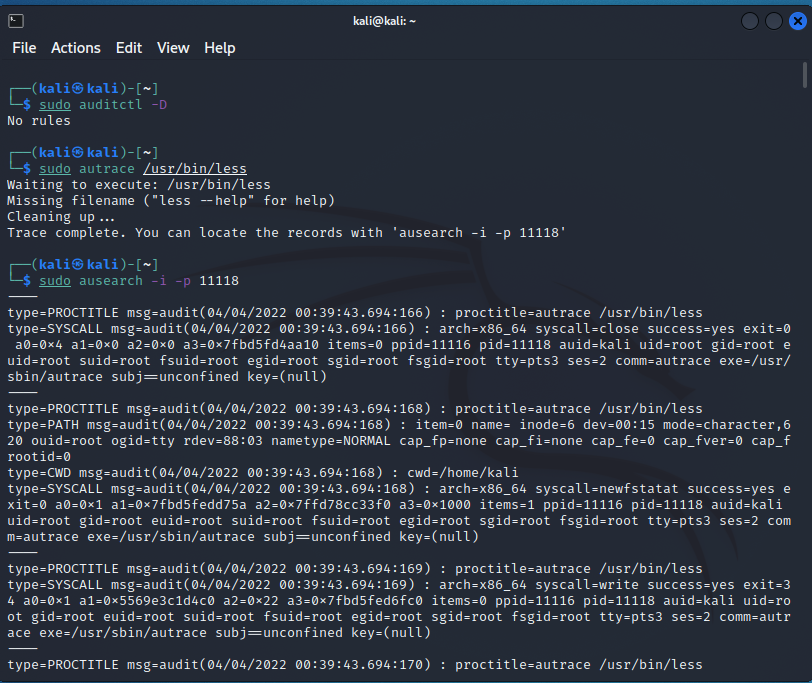
**Step 9**

To list out all of the queries **ausearch** is used:



**Step 10**

**Autrace** is used here to trace the binary of less command and search for all the events related to it that are captured in the specific process.



Part II - Linux Auditing System

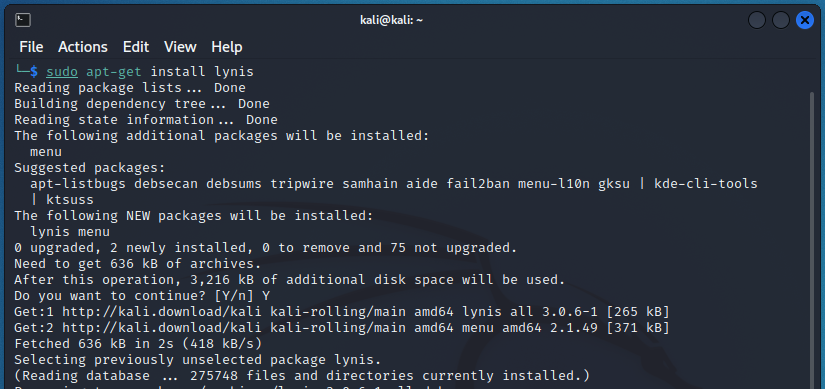
**Step 11 & 12 & 13 & 14**

Lynis is a multiplatform (**linux, macOS and windows**) security auditing tool.

**It is used for:**

* **Penetration Testing**
* **Vulnerability Detection**
* **Security Auditing**
* **System hardening**
* **Compliance Testing**

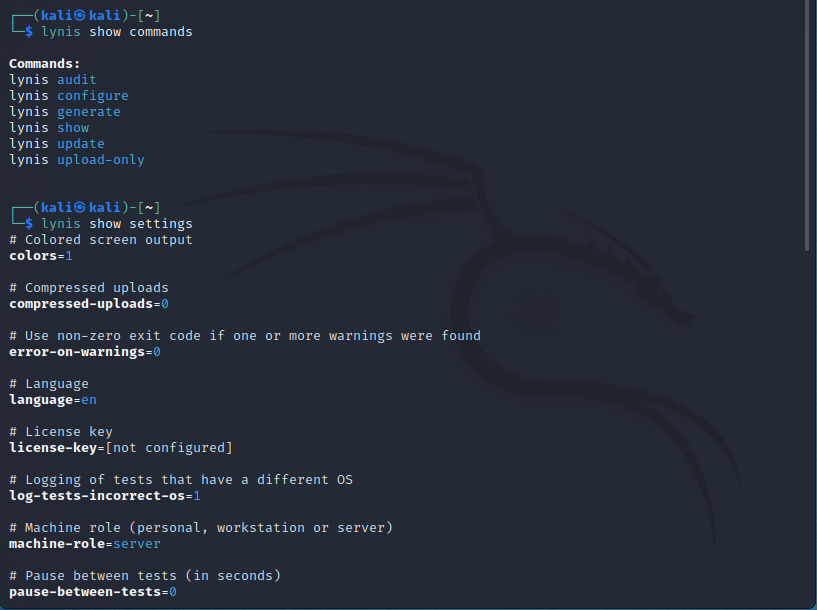
Now we are going to install lynis using “**sudo apt-get install lynis**”



**Step 15 & 16**

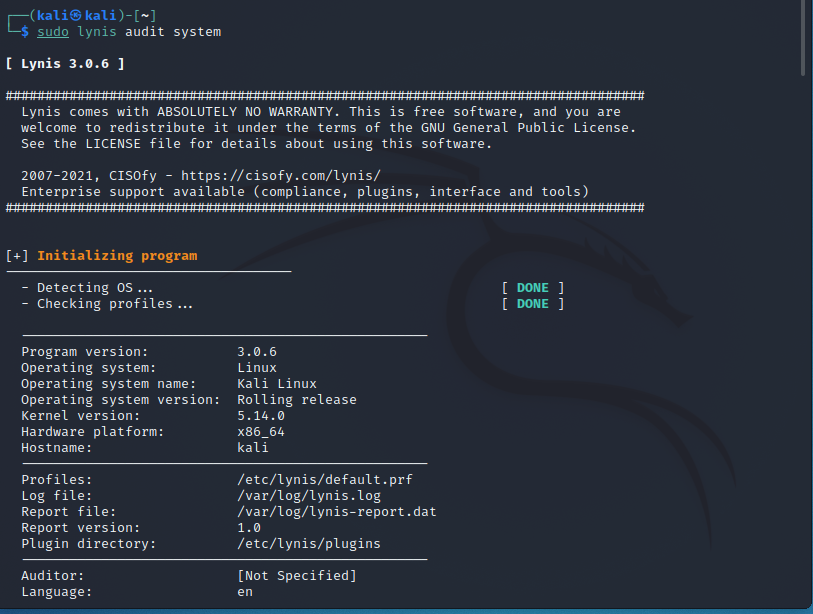
Here we are using command “**lynis show command**” to list down all of the sub-commands that are going to be used for auditing.

To see configuration of this tool we use “**lynis show setting**”



**Step 17**

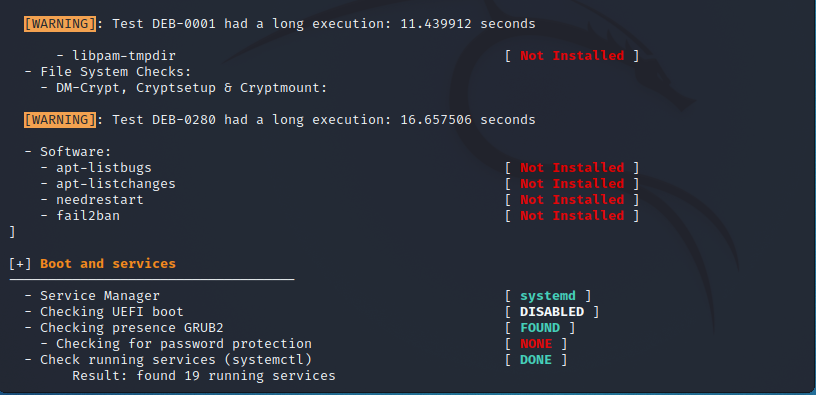
Now to perform security auditing of the system we use “**sudo lynis audit system**” and the audit will be stored in **“/var/log/lynix.log”**

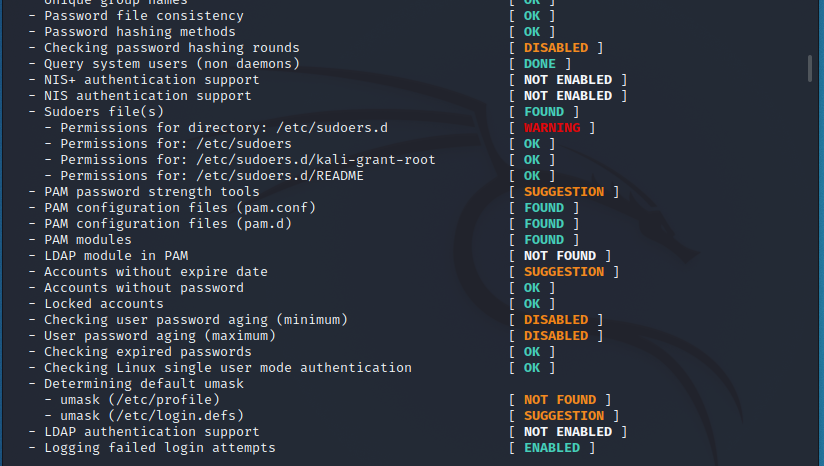


**Step 18**

Here we are given warning and Suggestions to install the packages to harden the security

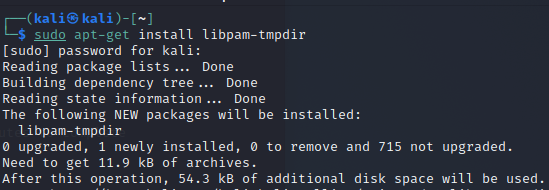
To check more details, we use **“sudo lynis show details <ID>”**

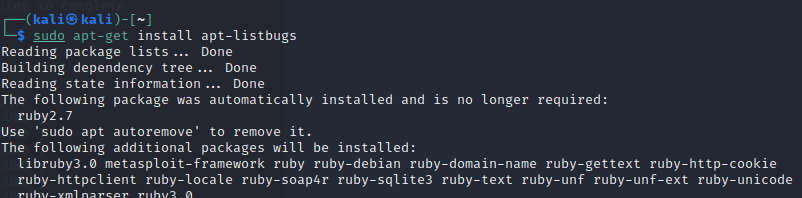


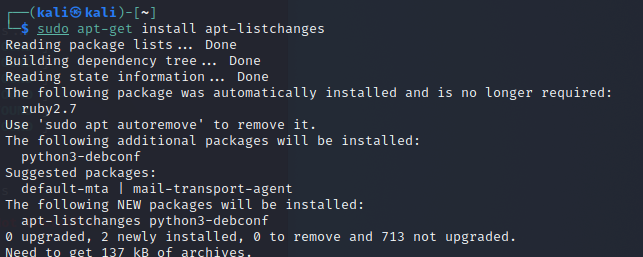


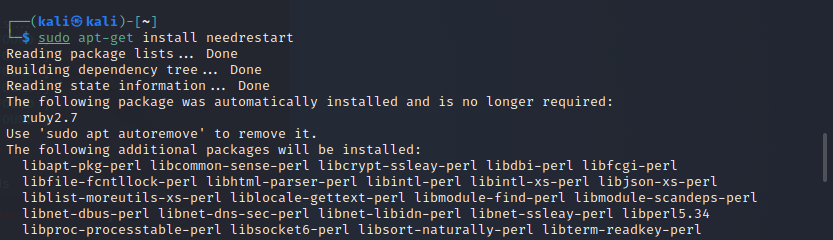
**Step 19 & 20**

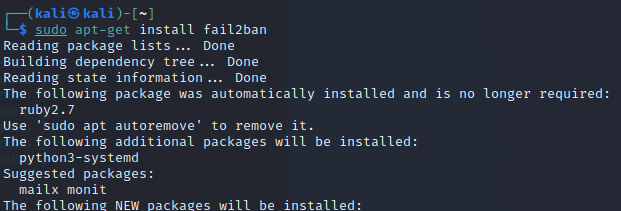
To increase our security we install the recommended softwares





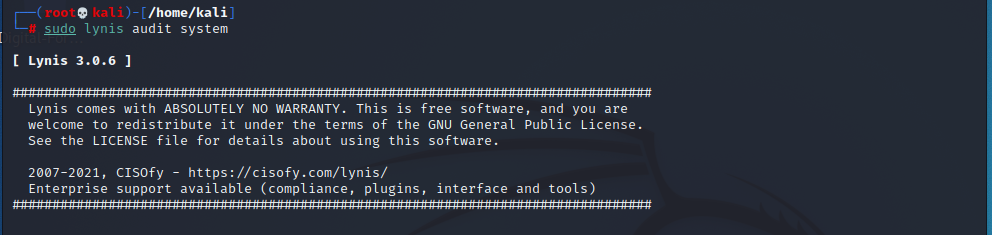


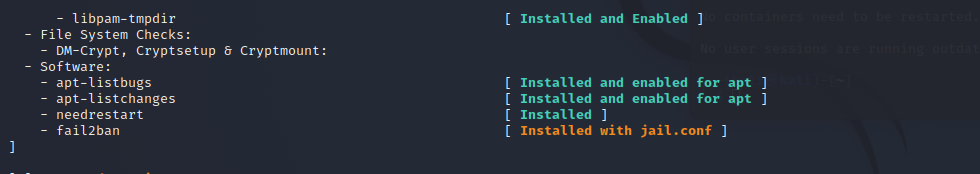




**Step 21**

Now let’s see if we did it correctly and yes here, we are with perfectly installed packages and we don’t see any warning.





SUMMARY

This lab was all about learning **Linux Auditing System** and the usage of two main tools “**auditd**” and “**lynis**”, which are the fundamental tools for auditing.

First section of this lab teaches us about audit, in which we have covered the installation and activation of this tool. After that we saw the auditd.conf file which controls auditing functionality. We have also seen where are the default logs stored. Further more we dig into this tool and saw all the utilities such as auditctl, aureport, ausearch and autrace.

Second section of this lab teaches us about lynis, in which we have covered the installation and activation of the tool. After that we saw the sub-commands of lynis. We did the auditing of out system and found out some Warnings and then fix those warning. After that we ran lynis again and confirmed that our warnings are removed.