PART I - LINUX AUDITING SYSTEM

Step 1 & 2

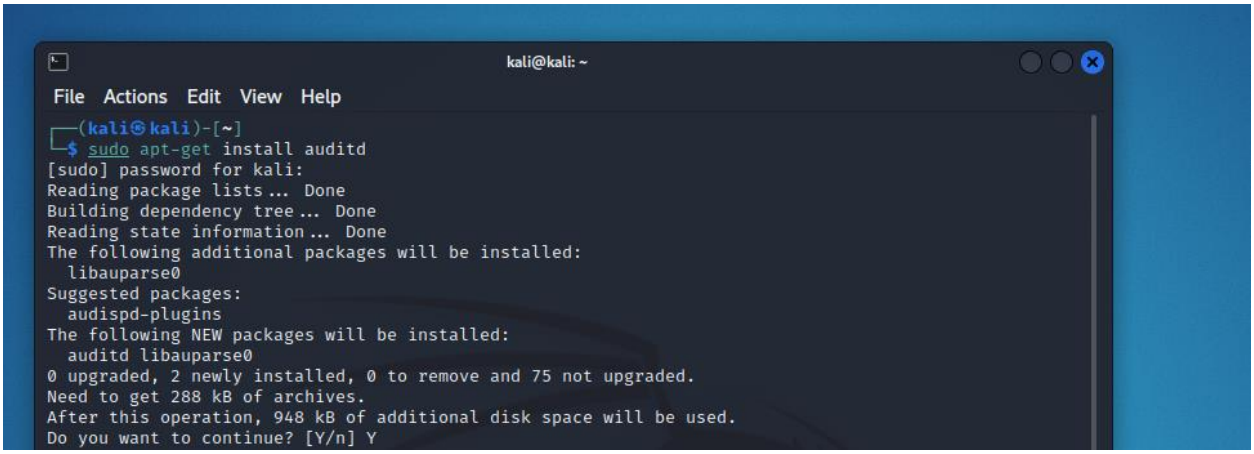
Linux audit system is a process that tells you about what is going on the system in great detail. This would eventually help in building up the security of the system and hardening the device.

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

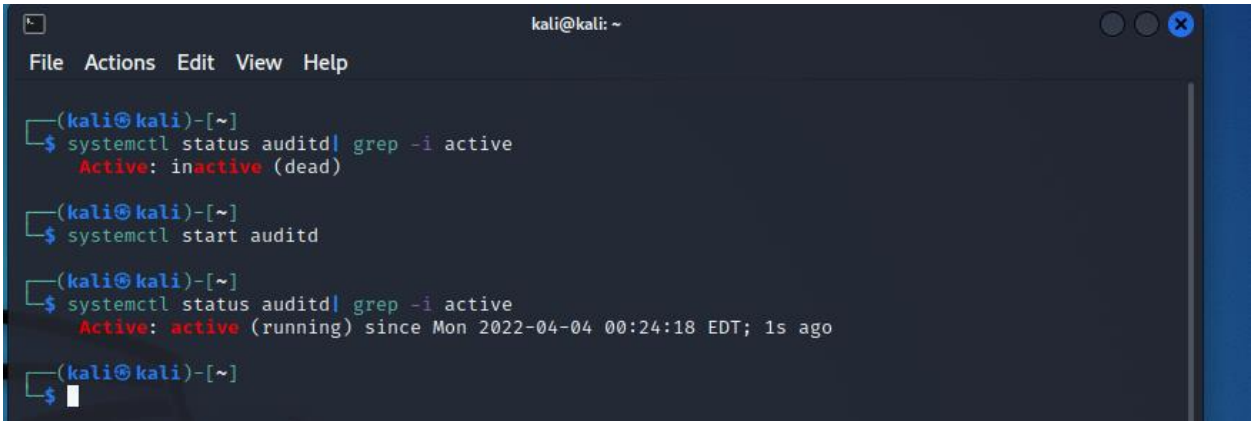
Here in kali linux we have a tool called **auditd** that is capable of provide ever single detail.

Step 3

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

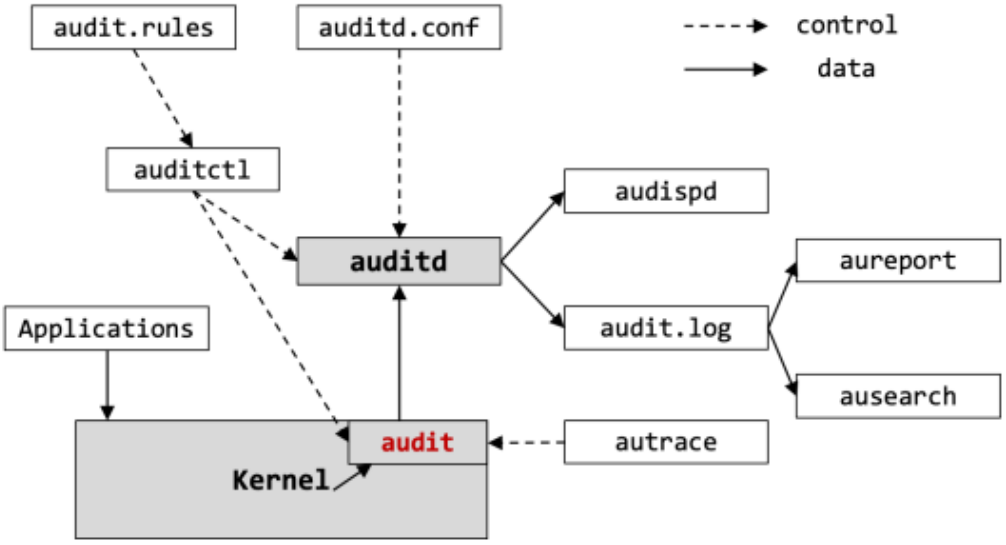


After installing it we are going to **enable** the service.

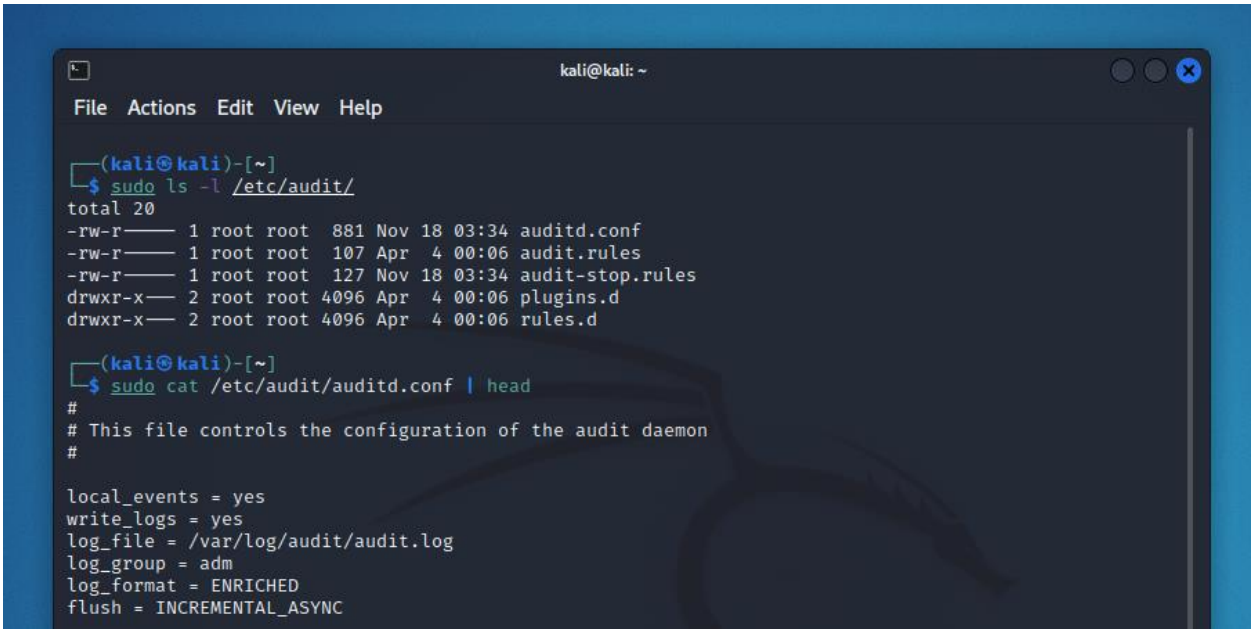


Step 4

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**.

```
┌──(kali㉿kali)-[~]
└─$ sudo auditctl -s
enabled 0
failure 1
pid 0
rate_limit 0
backlog_limit 64
lost 0
backlog 0
backlog_wait_time 15000
backlog_wait_time_actual 0
loginuid_immutable 0 unlocked
```

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.

```
┌──(kali㉿kali)-[~]
└─$ sudo auditctl -e 1
enabled 1
failure 1
pid 6694
rate_limit 0
backlog_limit 8192
lost 0
backlog 3
backlog_wait_time 60000
backlog_wait_time_actual 0

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/audit/audit.log | grep -i syscall | head -n 1
type=SYSCALL msg=audit(1649046258.088:19): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7f
d01a6cd0 a2=3c a3=0 items=0 ppid=6693 pid=6694 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 e
d=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditd" exe="/usr/sbin/auditd" subj==unconfined
ey=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSU
="root" EGID="root" SGID="root" FSGID="root"
```

Step 7

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

```
┌──(kali㉿kali)-[~]
└─$ sudo aureport

Summary Report
======================
Range of time in logs: 04/04/2022 00:24:18.092 - 04/04/2022 00:26:12.525
Selected time for report: 04/04/2022 00:24:18 - 04/04/2022 00:26:12.525
Number of changes in configuration: 5
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 3
Number of terminals: 6
Number of host names: 1
Number of executables: 5
Number of commands: 4
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 8
Number of events: 31
```

Step 8 -- More functionalities

For generating a report related to authentication and attempted login

Authentication --> "**aureport -au**"

Attempted login --> "**aureport -l**"

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo aureport -au
[sudo] password for kali:

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 04/04/2022 00:28:14 root ? /dev/pts/1 /usr/bin/su yes 62
2. 04/04/2022 00:28:21 kali ? /dev/pts/2 /usr/bin/su yes 70
3. 04/04/2022 00:28:44 kali ? /dev/pts/2 /usr/bin/sudo yes 74

┌──(kali㉿kali)-[~]
└─$ sudo aureport -l

Login Report
============================================
# date time auid host term exe success event
============================================
<no events of interest were found>
```

Failed

To see and capture failed events we use "**aureport –failed**"

```
┌──(kali㉿kali)-[~]
└─$ sudo aureport --failed

Failed Summary Report
═══════════════════════
Range of time in logs: 04/04/2022 00:24:18.092 - 04/04/2022 00:29:16.861
Selected time for report: 04/04/2022 00:24:18 - 04/04/2022 00:29:16.861
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 0
Number of terminals: 0
Number of host names: 0
Number of executables: 0
Number of commands: 0
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 0
Number of events: 0
```

Success

To see and capture success events we use "**aureport –success**"

```
┌──(kali㉿kali)-[~]
└─$ sudo aureport --success

Success Summary Report
═══════════════════════
Range of time in logs: 04/04/2022 00:24:18.092 - 04/04/2022 00:30:04.449
Selected time for report: 04/04/2022 00:24:18 - 04/04/2022 00:30:04.449
Number of changes in configuration: 5
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 3
Number of failed authentications: 0
Number of users: 3
Number of terminals: 10
Number of host names: 1
Number of executables: 6
Number of commands: 4
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 17
Number of events: 80
```

Summary

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

```
┌──(kali㉿kali)-[~]
└─$ sudo aureport -u --summary

User Summary Report
═══════════════════════════
total  auid
═══════════════════════════
70  1000
11  -1
5  0
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo aureport -e -i --summary

Event Summary Report
═══════════════════════
total  type
═══════════════════════
15  USER_ACCT
15  USER_START
12  CRED_REFR
12  USER_CMD
10  CRED_DISP
10  USER_END
5  CONFIG_CHANGE
3  USER_AUTH
3  CRED_ACQ
2  SERVICE_START
2  SYSCALL
1  LOGIN
1  SERVICE_STOP
1  DAEMON_START

┌──(kali㉿kali)-[~]
└─$ sudo aureport -e -ts yesterday -te now | head

Event Report
═══════════════════════════════
# date time event type auid success
═══════════════════════════════
1. 04/04/2022 00:24:18 3405 DAEMON_START -1 yes
2. 04/04/2022 00:24:18 19 SYSCALL -1 yes
3. 04/04/2022 00:24:18 20 CONFIG_CHANGE -1 yes
4. 04/04/2022 00:24:18 21 CONFIG_CHANGE -1 yes
5. 04/04/2022 00:24:18 22 CONFIG_CHANGE -1 yes
```

Process report

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

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo aureport -p | head

Process ID Report
═══════════════════════════════════════
# date time pid exe syscall auid event
═══════════════════════════════════════
1. 04/04/2022 00:24:18 6694 ? 0 -1 3405
2. 04/04/2022 00:24:18 6694 /usr/sbin/auditd 44 -1 19
3. 04/04/2022 00:24:18 6694 /usr/sbin/auditd 44 -1 20
4. 04/04/2022 00:24:18 6707 /usr/sbin/auditctl 44 -1 21
5. 04/04/2022 00:24:18 6707 /usr/sbin/auditctl 44 -1 22

┌──(kali㉿kali)-[~]
└─$ sudo aureport -s | head

Syscall Report
═══════════════════════════════════════
# date time syscall pid comm auid event
═══════════════════════════════════════
1. 04/04/2022 00:24:18 44 6694 auditd -1 19
2. 04/04/2022 00:24:18 44 6694 auditd -1 20
3. 04/04/2022 00:24:18 44 6707 auditctl -1 21
4. 04/04/2022 00:24:18 44 6707 auditctl -1 22
5. 04/04/2022 00:24:18 44 6707 auditctl -1 23
```

Step 9

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

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),2
9(audio),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),122(bluetooth),134(scanner),143(
kaboxer)

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -ui 1000 | head
────
time->Mon Apr  4 00:25:04 2022
type=USER_ACCT msg=audit(1649046304.719:31): pid=6907 uid=1000 auid=1000 ses=2 subj==unconfined ms
g='op=PAM:accounting grantors=pam_permit acct="kali" exe="/usr/bin/sudo" hostname=? addr=? termina
l=/dev/pts/0 res=success'
────
time->Mon Apr  4 00:25:04 2022
type=USER_CMD msg=audit(1649046304.719:32): pid=6907 uid=1000 auid=1000 ses=2 subj==unconfined msg
='cwd="/home/kali" cmd=617564697463746C202D652031 exe="/usr/bin/sudo" terminal=pts/0 res=success'
────
time->Mon Apr  4 00:25:04 2022
type=CRED_REFR msg=audit(1649046304.719:33): pid=6907 uid=1000 auid=1000 ses=2 subj==unconfined ms
g='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/
dev/pts/0 res=success'
────
```

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.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -D
No rules

┌──(kali㉿kali)-[~]
└─$ sudo autrace /usr/bin/less
Waiting to execute: /usr/bin/less
Missing filename ("less --help" for help)
Cleaning up...
Trace complete. You can locate the records with 'ausearch -i -p 11118'

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -i -p 11118
----
type=PROCTITLE msg=audit(04/04/2022 00:39:43.694:166) : proctitle=autrace /usr/bin/less
type=SYSCALL msg=audit(04/04/2022 00:39:43.694:166) : arch=x86_64 syscall=close success=yes exit=0
 a0=0x4 a1=0x0 a2=0x0 a3=0x7fbd5fd4aa10 items=0 ppid=11116 pid=11118 auid=kali uid=root gid=root e
uid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts3 ses=2 comm=autrace exe=/usr/
sbin/autrace subj=unconfined key=(null)
----
type=PROCTITLE msg=audit(04/04/2022 00:39:43.694:168) : proctitle=autrace /usr/bin/less
type=PATH msg=audit(04/04/2022 00:39:43.694:168) : item=0 name= inode=6 dev=00:15 mode=character,6
20 ouid=root ogid=tty rdev=88:03 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_f
rootid=0
type=CWD msg=audit(04/04/2022 00:39:43.694:168) : cwd=/home/kali
type=SYSCALL msg=audit(04/04/2022 00:39:43.694:168) : arch=x86_64 syscall=newfstatat success=yes e
xit=0 a0=0x1 a1=0x7fbd5fedd75a a2=0x7ffd78cc33f0 a3=0x1000 items=1 ppid=11116 pid=11118 auid=kali
uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts3 ses=2 com
m=autrace exe=/usr/sbin/autrace subj=unconfined key=(null)
----
type=PROCTITLE msg=audit(04/04/2022 00:39:43.694:169) : proctitle=autrace /usr/bin/less
type=SYSCALL msg=audit(04/04/2022 00:39:43.694:169) : arch=x86_64 syscall=write success=yes exit=3
4 a0=0x1 a1=0x5569e3c1d4c0 a2=0x22 a3=0x7fbd5fed6fc0 items=0 ppid=11116 pid=11118 auid=kali uid=ro
ot gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts3 ses=2 comm=autr
ace exe=/usr/sbin/autrace subj=unconfined key=(null)
----
type=PROCTITLE msg=audit(04/04/2022 00:39:43.694:170) : proctitle=autrace /usr/bin/less
```

PART II - LINUX AUDITING SYSTEM

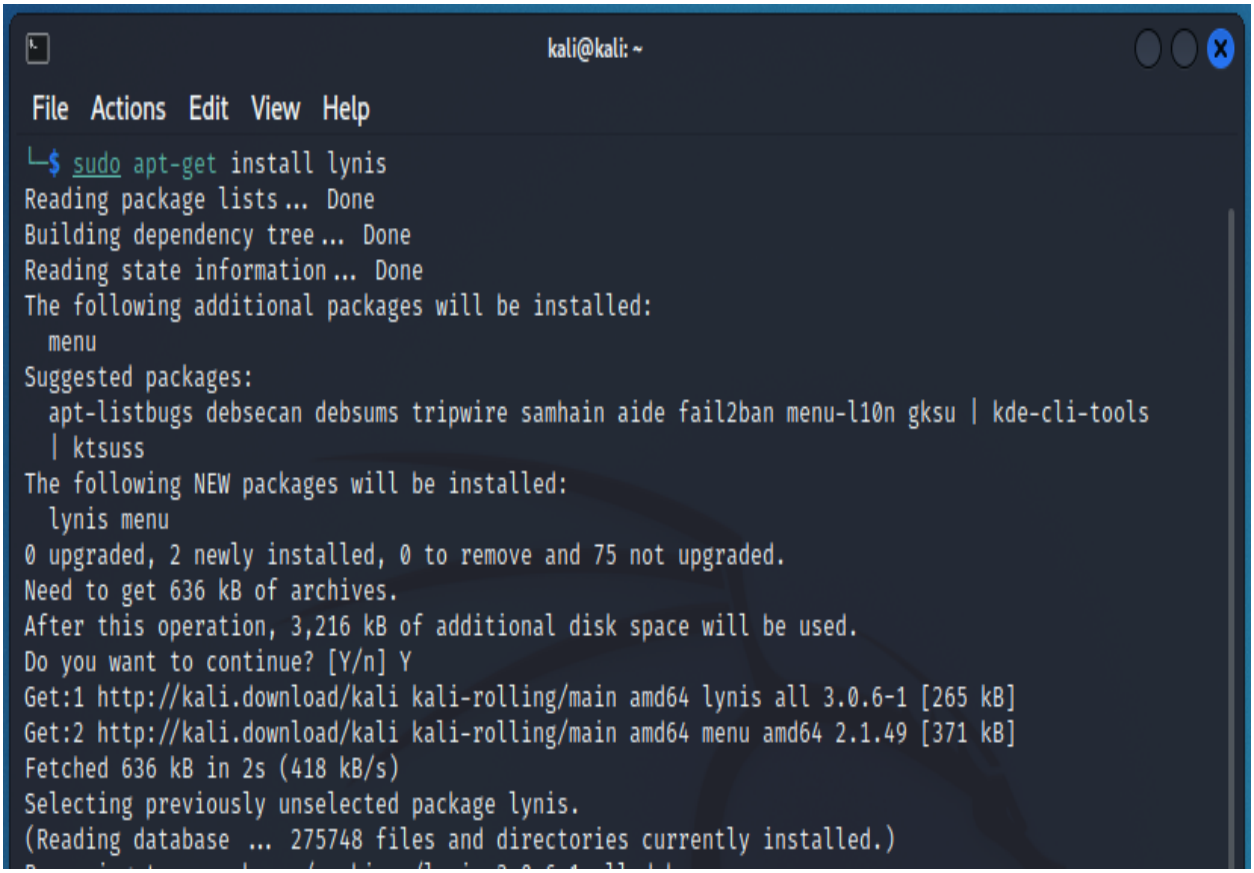
Step 11 & 12 & 13 & 14

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**"

```
┌──(kali㉿kali)-[~]
└─$ lynis show commands

Commands:
lynis audit
lynis configure
lynis generate
lynis show
lynis update
lynis upload-only


┌──(kali㉿kali)-[~]
└─$ lynis show settings
# Colored screen output
colors=1

# Compressed uploads
compressed-uploads=0

# Use non-zero exit code if one or more warnings were found
error-on-warnings=0

# Language
language=en

# License key
license-key=[not configured]

# Logging of tests that have a different OS
log-tests-incorrect-os=1

# Machine role (personal, workstation or server)
machine-role=server

# Pause between tests (in seconds)
pause-between-tests=0
```

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"**

```
┌──(kali㉿kali)-[~]
└─$ sudo lynis audit system

[ Lynis 3.0.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------------
  Program version:           3.0.6
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  Rolling release
  Kernel version:            5.14.0
  Hardware platform:         x86_64
  Hostname:                  kali
  ---------------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
```

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>"**

```
  [WARNING]: Test DEB-0001 had a long execution: 11.439912 seconds

      - libpam-tmpdir                                         [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:

  [WARNING]: Test DEB-0280 had a long execution: 16.657506 seconds

  - Software:
    - apt-listbugs                                            [ Not Installed ]
    - apt-listchanges                                         [ Not Installed ]
    - needrestart                                             [ Not Installed ]
    - fail2ban                                                [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ NONE ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 19 running services
```

```
    - Unique group names                                      [ OK ]
  - Password file consistency                                 [ OK ]
  - Password hashing methods                                  [ OK ]
  - Checking password hashing rounds                          [ DISABLED ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ NOT ENABLED ]
  - Sudoers file(s)                                           [ FOUND ]
    - Permissions for directory: /etc/sudoers.d               [ WARNING ]
    - Permissions for: /etc/sudoers                           [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root         [ OK ]
    - Permissions for: /etc/sudoers.d/README                  [ OK ]
  - PAM password strength tools                               [ SUGGESTION ]
  - PAM configuration files (pam.conf)                        [ FOUND ]
  - PAM configuration files (pam.d)                           [ FOUND ]
  - PAM modules                                               [ FOUND ]
  - LDAP module in PAM                                        [ NOT FOUND ]
  - Accounts without expire date                              [ SUGGESTION ]
  - Accounts without password                                 [ OK ]
  - Locked accounts                                           [ OK ]
  - Checking user password aging (minimum)                    [ DISABLED ]
  - User password aging (maximum)                             [ DISABLED ]
  - Checking expired passwords                                [ OK ]
  - Checking Linux single user mode authentication            [ OK ]
  - Determining default umask
    - umask (/etc/profile)                                    [ NOT FOUND ]
    - umask (/etc/login.defs)                                 [ SUGGESTION ]
  - LDAP authentication support                               [ NOT ENABLED ]
  - Logging failed login attempts                             [ ENABLED ]
```

Step 19 & 20

To increase our security we install the recommended softwares

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install libpam-tmpdir
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  libpam-tmpdir
0 upgraded, 1 newly installed, 0 to remove and 715 not upgraded.
Need to get 11.9 kB of archives.
After this operation, 54.3 kB of additional disk space will be used.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install apt-listbugs
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  ruby2.7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libruby3.0 metasploit-framework ruby ruby-debian ruby-domain-name ruby-gettext ruby-http-cookie
  ruby-httpclient ruby-locale ruby-soap4r ruby-sqlite3 ruby-text ruby-unf ruby-unf-ext ruby-unicode
  ruby-xmlparser ruby3.0
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install apt-listchanges
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  ruby2.7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python3-debconf
Suggested packages:
  default-mta | mail-transport-agent
The following NEW packages will be installed:
  apt-listchanges python3-debconf
0 upgraded, 2 newly installed, 0 to remove and 713 not upgraded.
Need to get 137 kB of archives.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install needrestart
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  ruby2.7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libapt-pkg-perl libcommon-sense-perl libcrypt-ssleay-perl libdbi-perl libfcgi-perl
  libfile-fcntllock-perl libhtml-parser-perl libintl-perl libintl-xs-perl libjson-xs-perl
  liblist-moreutils-xs-perl liblocale-gettext-perl libmodule-find-perl libmodule-scandeps-perl
  libnet-dbus-perl libnet-dns-sec-perl libnet-libidn-perl libnet-ssleay-perl libperl5.34
  libproc-processtable-perl libsocket6-perl libsort-naturally-perl libterm-readkey-perl
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install fail2ban
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  ruby2.7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python3-systemd
Suggested packages:
  mailx monit
The following NEW packages will be installed:
```

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.

```
┌──(root💀kali)-[/home/kali]
└─# sudo lynis audit system

[ Lynis 3.0.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
```

```
      - libpam-tmpdir                                         [ Installed and Enabled ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                            [ Installed and enabled for apt ]
    - apt-listchanges                                         [ Installed and enabled for apt ]
    - needrestart                                             [ Installed ]
    - fail2ban                                                [ Installed with jail.conf ]
]
```

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.