Advanced Linux User!

Day5_LinuxRUN.md

by Nathan Hailu

Last time Topics

ከዜሮ መጀመር ሁሌም ከባድ ነው

- o ገንዘብ በባንክ ውስጥ
- o ችሎታ(skill)
- o ተከታዮች

ለዚያም ነው ብዙ ሰዎች የሚያቆሙት ፣ በፍጥነት ስኬታማ መሆን ይፈልጋሉ ፣ ግን ስኬት ቀርፋፋ ሂደት ነው ፣ እና ማቆም አያፋጥነውም።

On today's class

- Further on User management
- Linux File Ownership + Permissions
- Software Installation
- Script Installation
- Package Installation Common errors

Some advanced user commands

- To change password of user
  - `sudo passwd username`
- To change user id
  - `sudo usermod -u new_id username`
- To Delete User
  - `sudo userdel -r username`
- To Change users on terminal
  - su - username

```
┌──(rexder㉿HunterMachine)-[~]
└─$ sudo passwd nathan
[sudo] password for rexder:
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(rexder㉿HunterMachine)-[~]
└─$ id nathan
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)

┌──(rexder㉿HunterMachine)-[~]
└─$ sudo usermod -u 1293 nathan

┌──(rexder㉿HunterMachine)-[~]
└─$ id nathan
uid=1293(nathan) gid=1001(nathan) groups=1001(nathan)
```

```
┌──(rexder㉿HunterMachine)-[~]
└─$ id
uid=1000(rexder) gid=1000(rexder) groups=1000(rexder),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),117(bluetooth),121(wireshark),130(lpadmin),136(scanner),150(kaboxer)

┌──(rexder㉿HunterMachine)-[~]
└─$ su - geeztech
Password:
┌──(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(geeztech㉿HunterMachine)-[~]
└─$ id
uid=1001(geeztech) gid=1001(geeztech) groups=1001(geeztech)
```

```
┌──(rexder㉿HunterMachine)-[~]
└─$ id nathan
uid=1293(nathan) gid=1001(nathan) groups=1001(nathan)

┌──(rexder㉿HunterMachine)-[~]
└─$ sudo userdel -r nathan
userdel: nathan mail spool (/var/mail/nathan) not found

┌──(rexder㉿HunterMachine)-[~]
└─$ id nathan
id: 'nathan': no such user
```

Continue.....

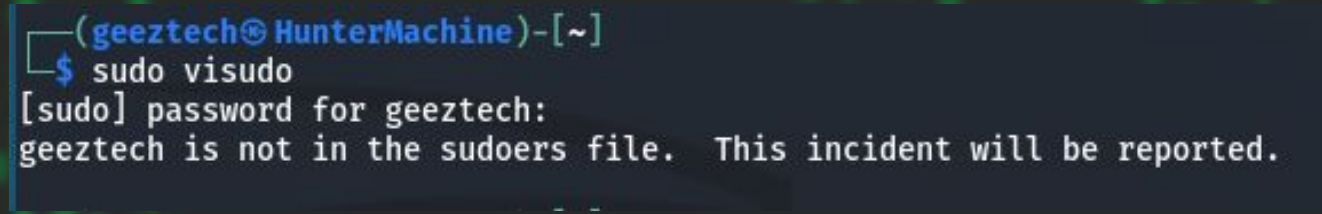
- **sudo mkhomedir_helper <your username>**
  - is used to create a home directory for a specified user in Linux, typically when the user is being added to the system without an existing home directory.
- **sudo usermod <your username> -s /bin/<shell>**
  - changes the default login shell for the specified user to the specified shell (e.g., /bin/bash, /bin/zsh).

Some advanced group commands

- Create a New Group (if not already created):
  - sudo groupadd <groupname>
- Add Users to the Group:
  - sudo usermod -aG <groupname> <username>
- Verify the User's Group Membership:
  - groups <username>
- Remove User from the Group:
  - sudo gpasswd -d <username> <groupname>
  - Verify the User's Group Membership:
    - groups <username>

Sudoers file

- The sudoers file is **a file Linux and Unix administrators use to allocate system rights to system users**
- The user you created doesn't have power to use **sudo** as the original one.
- This is Because it is not Added in the sudoers file (የSudoዎች file)
- To access this file
  - sudo visudo



Cont...

The 1st appearance when you open the sudoers file

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

Cont...

You can add the User you need to have access to the sudoers file, so he can use the sudo command.

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
geeztech ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
~
```

Then after the user can use sudo command

```
┌──(geeztech㉿HunterMachine)-[~]
└─$ sudo visudo
[sudo] password for geeztech:
visudo: /etc/sudoers.tmp unchanged
```

Linux File permission

- Every file on linux have their own
  - Owner
  - Permissions
- There is 5 main parts on the listing
  - Permission
  - Owners
  - Date
  - Size
  - filename

```
┌──(rexder㉿HunterMachine)-[~]
└─$ ls -l
total 48
-rw-r--r-- 1 rexder rexder   47 Dec 19 11:43 Day3_MoreLinux.md
drwxr-xr-x 2 rexder rexder 4096 Dec 16 02:32 Desktop
drwxr-xr-x 2 rexder rexder 4096 Dec 16 07:32 Documents
drwxr-xr-x 2 rexder rexder 4096 Dec 16 05:00 Downloads
drwxr-xr-x 2 rexder rexder 4096 Dec 16 12:27 gtst
drwxr-xr-x 2 rexder rexder 4096 Dec 16 12:59 linux
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Music
drwxr-xr-x 2 rexder rexder 4096 Dec 16 07:32 Pictures
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Public
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Templates
-rw-r--r-- 1 rexder rexder 1302 Dec 19 11:51 testing.txt
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Videos
```

Ownership

- Ownership is the owner of the file
- This have 2 kinds
  - User
  - Group
- To change the owner of file you can use the command
  - `chown user:group filename`

USER **GROUP**

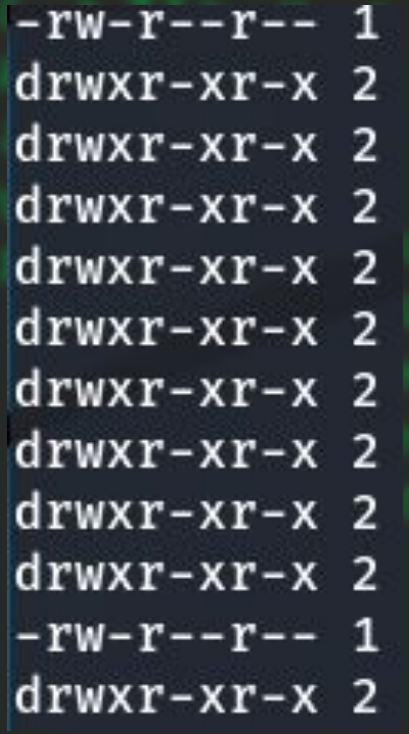
rexder rexder

```
┌──(rexder㉿HunterMachine)-[~]
└─$ sudo chown root Day4.md

┌──(rexder㉿HunterMachine)-[~]
└─$ ls -l
total 48
-rw-r--r-- 1 rexder rexder   47 Dec 19 11:43 Day3_MoreLinux.md
-rw-r--r-- 1 root   rexder    0 Dec 19 12:14 Day4.md
drwxr-xr-x 2 rexder rexder 4096 Dec 16 02:32 Desktop
drwxr-xr-x 2 rexder rexder 4096 Dec 16 07:32 Documents
drwxr-xr-x 2 rexder rexder 4096 Dec 16 05:00 Downloads
drwxr-xr-x 2 rexder rexder 4096 Dec 16 12:27 gtst
drwxr-xr-x 2 rexder rexder 4096 Dec 16 12:59 linux
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Music
drwxr-xr-x 2 rexder rexder 4096 Dec 16 07:32 Pictures
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Public
drwxr-xr-x 2 rexder rexder 4096 Dec  6 03:03 Templates
-rw-r--r-- 1 rexder rexder 1302 Dec 19 11:51 testing.txt
```

Permission

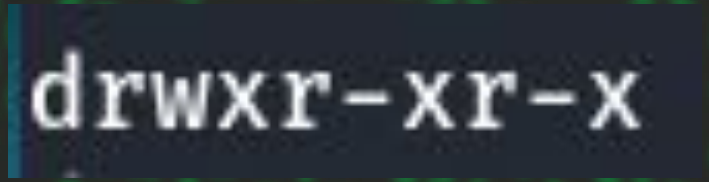
- There are 3 types of permissions
  - Read (r)
  - Write (w)
  - Execute (x)
- The folders and files are differ with the ‘d’ and ‘-’ on the beginning of the permission.



Cont...

- There still the permission have three parts.
  - user -group-other
- User (u) => power of user defined on the the ownership
- Group (g) => power of group defined on the the ownership
- Other (o) => power of other users.
- All (a) => power of all which can be found in the 3 above owners
- Command to change permission of file
  - chmod <option> filename

User -group -other




```
┌──(rexder㉿HunterMachine)-[~]
└─$ ls -l day4
-rw-r--r-- 1 rexder rexder 0 Dec 19 12:19 day4

┌──(rexder㉿HunterMachine)-[~]
└─$ chmod +x day4

┌──(rexder㉿HunterMachine)-[~]
└─$ ls -l day4
-rwxr-xr-x 1 rexder rexder 0 Dec 19 12:19 day4
```

CHMOD command

- This command helps to change file permission.
- Those file permissions are read,write & execute.
- Each of the permission have a number representations.
  - Read -> 4 - r
  - Write -> 2 - w
  - Execute -> 1 - x
- Syntax
  - chmod <parameter> filename

Cont...

+ Is giving the permission
- Is taking / removing " "

- The parameter can be in numbers and symbols

A) Parameters in symbol
   - chmod a+x filename -> adding execute permission for all (chmod +x filename)
   - chmod u+x filename -> adding execute permission for user
   - chmod g+x filename -> adding execute permission for group
   - chmod o+x filename -> adding execute permission for other
   - chmod -x filename -> removing execute permission for all
   - chmod a+rwx , u-rw , g-x , o-xw filename -> gives rwx for all and removes something from all

B) Parameters in Number

- chmod 621 filename -> 6 for user, 2 for group, 1 for other (6 = 4+2), 6 =r w
- chmod 777 filename -> 7 for users, 7 for group , 7 for others (7 =4+2+1), 7 = rwx

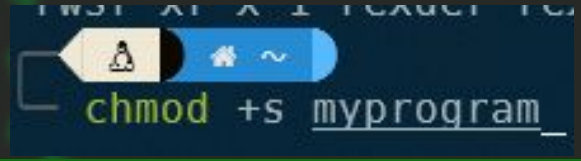
Breaktime

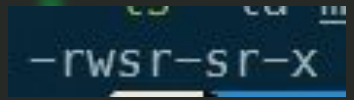
20 MIN

1. Create file called “Perm.txt” and give the following permission to it `--w-r----x`
2. What is the equivalent of 631 permission in symbolic?
3. What is the equivalent of 200 permission in symbolic?
4. What is the numeric equivalent of `-rwxrw-rw-`
5. Create a user called gtst & test with password 123456
6. Change the file user owner of Perm.txt to gtst and the group owner to root
7. Change the user password of gtst to “pass123”
8. Change the user id of ‘gtst’ to 1923
9. Delete the user ‘test’

Special File Permissions

- There are another 3 special permissions, you may encounter on your pentest Journey.
- They are
  - SUID bits(s) - set user ID bit - add 4 infront of our numeric value -> 4000
  - SGID bits(s) - set group ID bit - add 2 infront of our numeric value -> 2777
  - Sticky bits(t) - set other ID bit - add 1 in front of our numeric value -> 1602
- These are permissions like the execute(x), but they will set the execute permission t**o the user who settled them**.
- Example: if Mr. a add suid bit to a program then any user can execute the program with permission of Mr. a
  - Meaning if root add suid bit on some program. Then any user got that program they can run it as root without any sudo password





Example

- This is A computer Program Written in C, We will See SUID bit Powerfulness with this Program.
- This Program will try to open `/etc/shadow` and if the permission is Correct it will respond "Successfully opened /etc/shadow file!". But if the permission does not meet it will responded with "Unable to open /etc/shadow"

```c
#include <stdio.h>
#include <stdlib.h>

int main() {
    FILE *fp = fopen("/etc/shadow", "r");
    if (fp == NULL) {
        perror("Unable to open /etc/shadow");
        return EXIT_FAILURE;
    }
    printf("Successfully opened /etc/shadow file!\n");
    fclose(fp);
    return EXIT_SUCCESS;
}
```

```
~/GTSTv1 > $ ls -la readergtst
-rwxrwxr-x 1 rexder rexder 16112 Nov  8 11:44 readergtst*
~/GTSTv1 > $ ./readergtst
Unable to open /etc/shadow: Permission denied
```

why?

Cont...

- After changing the Owner of the Binary/Program, Still is not running.

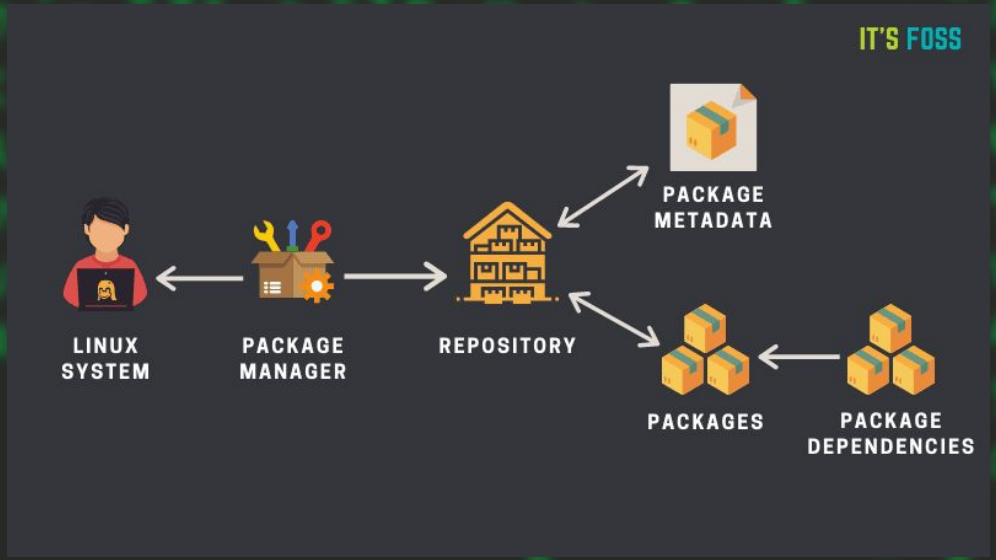
```
~/GTSTv1 > $ sudo chown root:root readergtst
[sudo] password for rexder:
~/GTSTv1 > $ ls -la readergtst
-rwxrwxr-x 1 root root 16112 Nov  8 11:44 readergtst*
~/GTSTv1 > $ ./readergtst
Unable to open /etc/shadow: Permission denied
```

```
~/GTSTv1 > $ sudo chmod u+s readergtst
~/GTSTv1 > $ ls -la readergtst
-rwsrwxr-x 1 root root 16112 Nov  8 11:44 readergtst*
~/GTSTv1 > $ ./readergtst
Successfully opened /etc/shadow file!
```

- Here it Comes the interesting part. **Now, the owner of the file is root. So if the root user set a SUID bit on the program that means, we can run it with the File Owner's Privilege and Permission.**

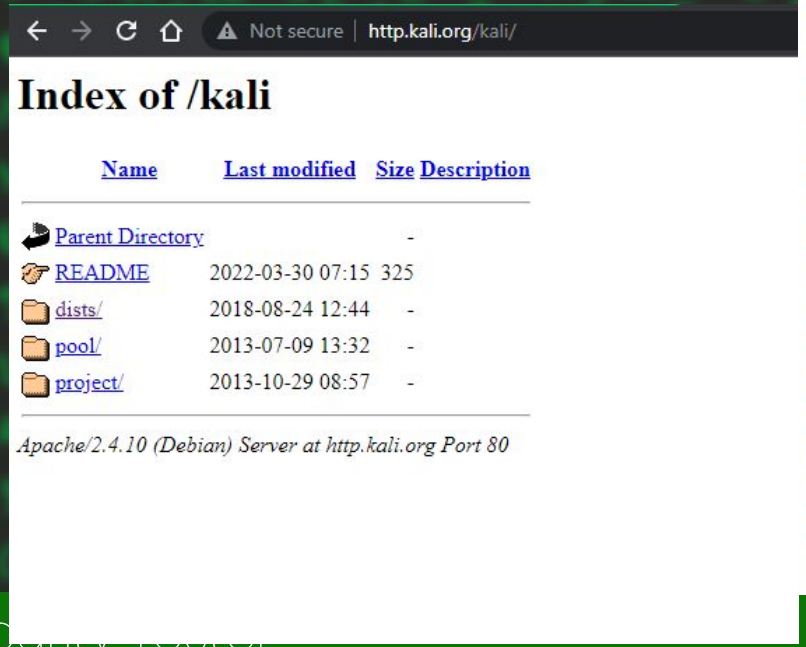
Package installation on linux

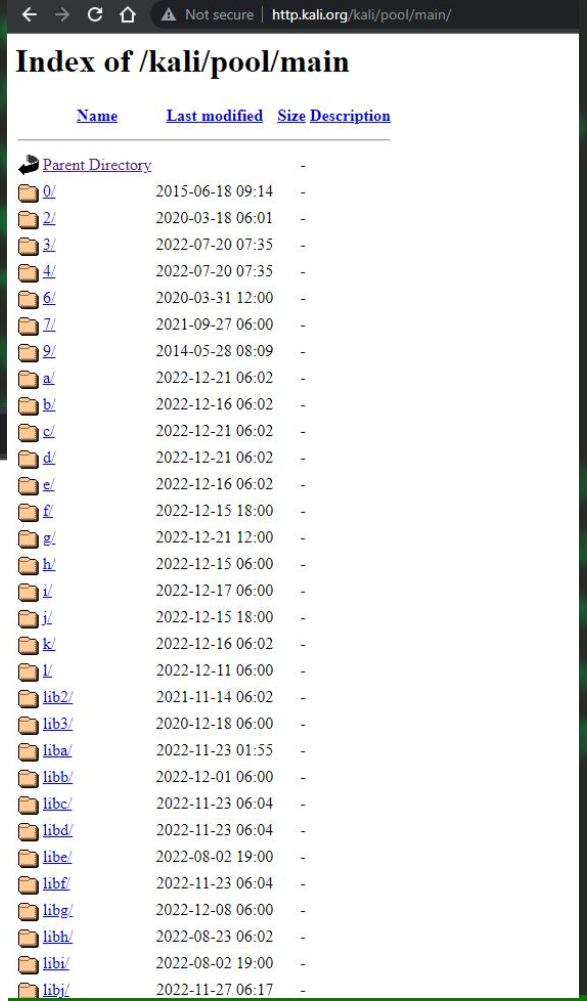
- ON linux to install softwares you use package managers.
  - Ex: apt,pacman,pkg,...
- We will use debian package manager.
- On debian the package manager i called ‘APT’ also there is called ‘dpkg’
- Package managers are **a free-software user interface that work with an online server to handle the installation and removal of software on Debian, and Debian-based Linux distributions**.



The repository

This is the site/server kali use to upload the packages





Advanced package tool / apt /

- Apt is **a free-software user interface that work with an online server to handle the installation and removal of software on Debian, and Debian-based Linux distributions**.used for online and offline purpose.
- The old ‘apt’ used as ‘apt-get’
- Syntax
  - `sudo apt update`
  - `sudo apt search <softwarename>`
  - `sudo apt install <softwarename>`
  - `sudo apt remove <softwarename>`
  - `sudo apt upgrade`
  - `sudo apt purge <softwarename>`

```
APT(8)                                APT                                APT(8)

NAME
       apt - command-line interface

SYNOPSIS
       apt [-h] [-o=config_string] [-c=config_file] [-t=target_release]
           [-a=architecture] {list | search | show | update |
           install pkg [{=pkg_version_number | /target_release}]...  |
           remove pkg...  | upgrade | full-upgrade | edit-sources |
           {-v | --version} | {-h | --help}}

DESCRIPTION
       apt provides a high-level commandline interface for the package
       management system. It is intended as an end user interface and enables
       some options better suited for interactive usage by default compared to
       more specialized APT tools like apt-get(8) and apt-cache(8).

       Much like apt itself, its manpage is intended as an end user interface
       and as such only mentions the most used commands and options partly to
       not duplicate information in multiple places and partly to avoid
       overwhelming readers with a cornucopia of options and details.

       update (apt-get(8))
           update is used to download package information from all configured
           sources. Other commands operate on this data to e.g. perform
           package upgrades or search in and display details about all
           packages available for installation.

 page apt(8) line 1 (press h for help or q to quit)
```

Package dependencies

- A software can be built based on another program called ‘modules’
- SO, a program to work properly, the dependencies have to be installed successfully.
- Those package managers install the software+dependencies.

example:

```
┌──(rexder㉿HunterMachine)-[~]
└─$ sudo apt install terminator
[sudo] password for rexder:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apg faraday-client gir1.2-accountsservice-1.0 gir1.2-clutter-gst-3.0
  gir1.2-gck-1 gir1.2-gcr-3 gir1.2-gdm-1.0 gir1.2-geoclue-2.0 gir1.2-gmenu-3.0
  gir1.2-gnomebluetooth-1.0 gir1.2-graphene-1.0 gir1.2-gtkclutter-1.0
  gir1.2-gweather-3.0 gir1.2-malcontent-0 gir1.2-nma-1.0 gir1.2-polkit-1.0
  gir1.2-rsvg-2.0 gir1.2-upowerglib-1.0 gnome-control-center-data
  gnome-session-bin gnome-session-common gnome-settings-daemon-common
  gnome-shell-common gstreamer1.0-pipewire libarmadillo10 libcharls2
  libcolord-gtk1 libdap27 libdapclient6v5 libedata-cal-2.0-1 libepsilon1
  libextutils-pkgconfig-perl libflatpak0 libgdal28 libgdm1 libgeoclue-2-0
  libgeocode-glib0 libgeos-3.9.1 libges-1.0-0 libgnome-menu-3-0 libgsound0
  libgweather-3-16 libgweather-common libmalcontent-ui-0-0 libmozjs-78-0
  libnetcdf18 libnss-myhostname libostree-1-1 libpython3.9-dev libqhull8.0
  librygel-core-2.6-2 librygel-db-2.6-2 librygel-renderer-2.6-2
  librygel-server-2.6-2 libtbb2 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 libyara4
  malcontent malcontent-gui mutter-common odbcinst odbcinst1debian2
  python-mpltoolkits.basemap-data python3-deprecation python3-llvmlite
  python3-pyproj python3-pyshp python3.9-dev realmd rygel switcheroo-control
  xwayland
Use 'sudo apt autoremove' to remove them.
```

Common Linux Repository Errors

1. **Could not get lock /var/lib/apt/lists/lock**
   - This Occurs when You run 2 different apt's or if there is another apt process running on Background, for this you can simply solve it by restarting your PC of closing the another apt process

```
~ > $ sudo apt install evolution
[sudo] password for rexder:
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 799328 (apt)
```

Common Linux Repository Errors

2. Could not open lock /var/lib/dpkg/lock-frontend
   - This Occurs when you forget to run apt with root user aka ‘sudo’

```
~/GTSTv1 > $ apt install evolution
Error: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
Error: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
```

Common Linux Repository Errors

```
~/GTSTv1 > $ sudo apt install dex2jr
Error: Unable to locate package dex2jr
```

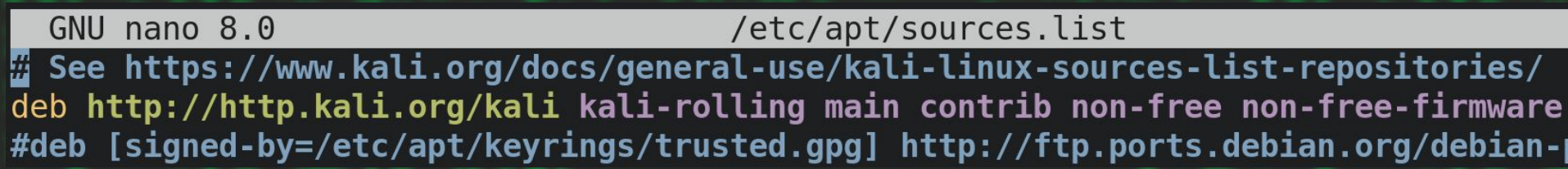
3. Unable to locate package
   - This Occurs when you Miss spell the program name.

```
~/GTSTv1 > $ sudo apt install dex2jar
dex2jar is already the newest version (2.1~nightly-28-0kali2).
The following packages were automatically installed and are no longer required
  libdrm-nouveau2:i386 libu2f-udev
Use 'sudo apt autoremove' to remove them.
```

Common Linux Repository Errors

4. The repository 'http://http.kali.org/kali kali-rolling Release' does not have a Release file.

   - This Occurs when There is a problem on the Repository Configuration. Sometimes the link might be broken.



   - You have to put the correct link "**deb http://http.kali.org/kali kali-rolling main contrib non-free**", this might differ based on the Distro so you can search the repository link on google or chatGPT

For more...

- Don’t close apt while installation
- Repository errors, if this happened you can fix it using
  - `sudo apt edit-sources`

→ **For those kinds of errors what you have to do is google/youtube { detail we will see this while we learn Footprinting }**

Dpkg / Debian package manager /

- Dpkg is an offline package managing program.
- Packages on debian have an extension ".deb"
- Syntax
  - `sudo dpkg -i <packagename>`
  - `sudo dpkg -r <packagename>`
  - `sudo dpkg -P <packagename>`

Let's get our hand dirty

1. Update your system repository
2. Search for package called 'cmatrix'
3. Install 'cmatrix'
4. Remove 'cmatrix'

Class is over

- DO the notes on github
- Install some program and practice