Hacker Script

09.04.2018

By
Kune Mohith & Chakrapani
3rd-CSE.

Github Link:

The Github link is here. Please give a star and show like towards the repository. Pull requests are always welcomed.

Overview:

The script developed is useful for automating some tasks done by a Hacker. Even normal users without any idea of hacking can also use it. Most of the sensitive details are automated through this script and the user no need to bother about those implementations.

Goals:

1. Detecting the Mac-addresses around the script user (in an optimal range) without going into all the raw details.
2. To fake Mac-addresses.
3. Detect devices that are connected to current network.
4. To know all the details of connected devices.
5. Downloading

Specifications:

A debian distribution with packages:

- nmap
- netdiscover
- aircrack-ng
- macchanger

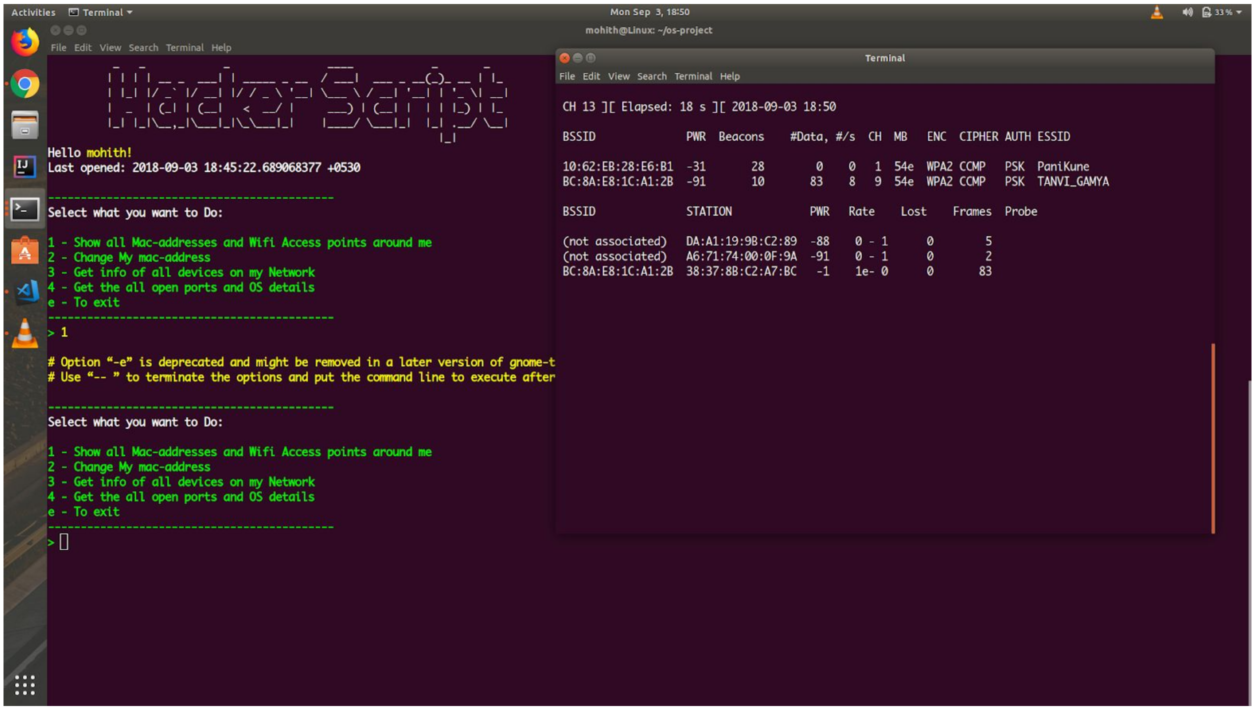
Disclaimer:

This script is only for Educational purposes. We are not responsible for any illegal usage .Any actions and or activities related to the material contained within this Document is solely your responsibility.

Functions

I. Get to know all mac-address and Wifi access points around you:

This functions helps the hacker to know the mac-addresses of the devices around him, on which wifi is turned on. The range is dependent on the strength of the Wifi card present in the Computer. This helps the hacker to performs attacks like DDOS, Mac-spoof etc., and saves a lot of time


Activities
Terminal
Mon Sep 3, 18:50
33 %
mohith@Linux: ~/os-project
File Edit View Search Terminal Help
Terminal
File Edit View Search Terminal Help

```
 _   _            _               ____            _       _
| | | | __ _  ___| | _____ _ __  / ___|  ___ _ __(_)_ __ | |_
| |_| |/ _` |/ __| |/ / _ \ '__| \___ \ / __| '__| | '_ \| __|
|  _  | (_| | (__|   <  __/ |     ___) | (__| |  | | |_) | |_
|_| |_|\__,_|\___|_|\_\___|_|    |____/ \___|_|  |_| .__/ \__|
                                                   |_|
Hello mohith!
Last opened: 2018-09-03 18:45:22.689068377 +0530

---------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
---------------------------------------------
> 1

# Option “-e” is deprecated and might be removed in a later version of gnome-t
# Use “-- ” to terminate the options and put the command line to execute after

---------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
---------------------------------------------
> 
```

```
CH 13 ][ Elapsed: 18 s ][ 2018-09-03 18:50

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:62:EB:28:E6:B1  -31       28        0    0   1  54e  WPA2 CCMP   PSK  PaniKune
BC:8A:E8:1C:A1:2B  -91       10       83    8   9  54e  WPA2 CCMP   PSK  TANVI_GAMYA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   DA:A1:19:9B:C2:89  -88    0 - 1      0        5
(not associated)   A6:71:74:00:0F:9A  -91    0 - 1      0        2
BC:8A:E8:1C:A1:2B  38:37:8B:C2:A7:BC   -1    1e- 0      0       83
```

The common useful terms here are:

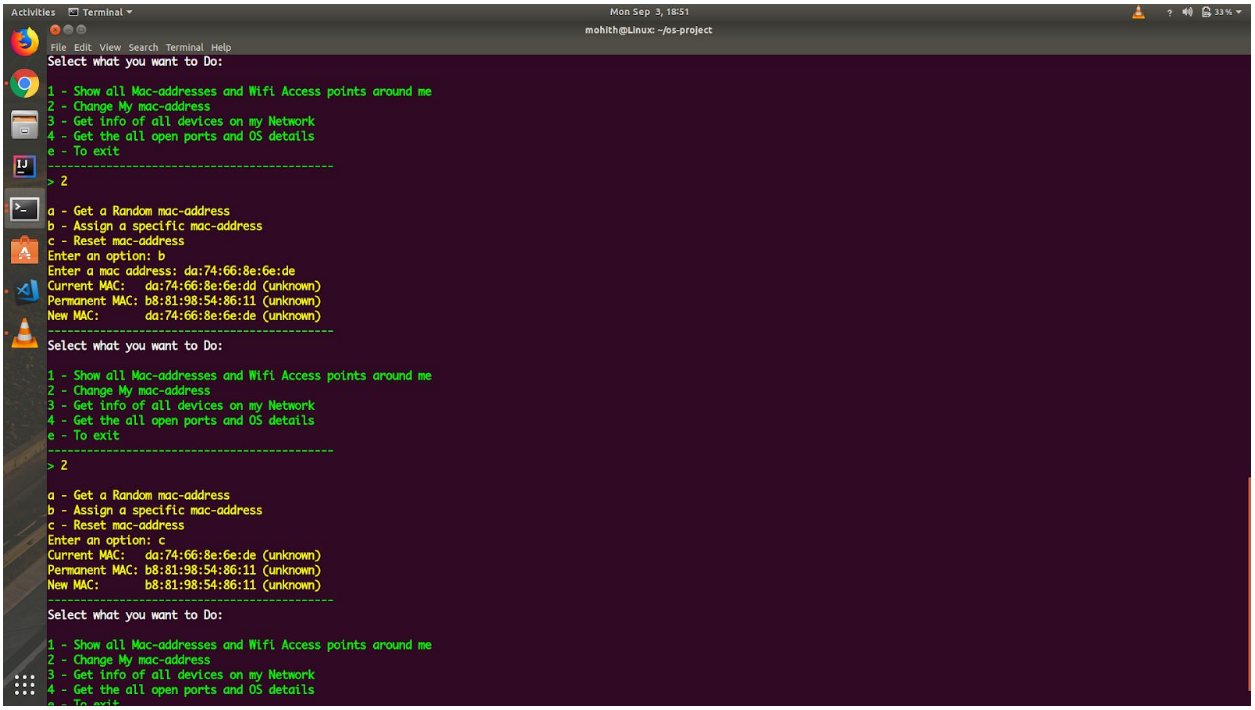
1) BSSID: It is the MAC (Medium Access Control) address of the AP (Access Point).
2) CH: Channel in which the scan is going on. Although it may be unclear, but this script assumes a user having no hacking knowledge.
3) STATION: It the Mac address of the devices around the user.

During this command Wifi mode is changed to “monitor mode”. The “airmon-ng” command uses the wireless interface to fetch all the mac-address. During this we will no longer be connected to the internet (except if we have LAN, since it uses only wireless interface).

NOTE: Don’t forget to press CTRL+C to stop the new opened terminal. Else it will cause the wireless interface to stay in monitor mode.

II. Change My Mac-Address:

This function helps the user to temporarily change the mac-address. The user can spoof the mac-address by changing to another one nearby him. This allows to access other network, even if he doesn't belong though that network.


Activities
Terminal
Mon Sep 3, 18:51
33 %
mohith@Linux: ~/os-project
File Edit View Search Terminal Help

```
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
--------------------------------------------
> 2

a - Get a Random mac-address
b - Assign a specific mac-address
c - Reset mac-address
Enter an option: b
Enter a mac address: da:74:66:8e:6e:de
Current MAC:   da:74:66:8e:6e:dd (unknown)
Permanent MAC: b8:81:98:54:86:11 (unknown)
New MAC:       da:74:66:8e:6e:de (unknown)
--------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
--------------------------------------------
> 2

a - Get a Random mac-address
b - Assign a specific mac-address
c - Reset mac-address
Enter an option: c
Current MAC:   da:74:66:8e:6e:de (unknown)
Permanent MAC: b8:81:98:54:86:11 (unknown)
New MAC:       b8:81:98:54:86:11 (unknown)
--------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
```

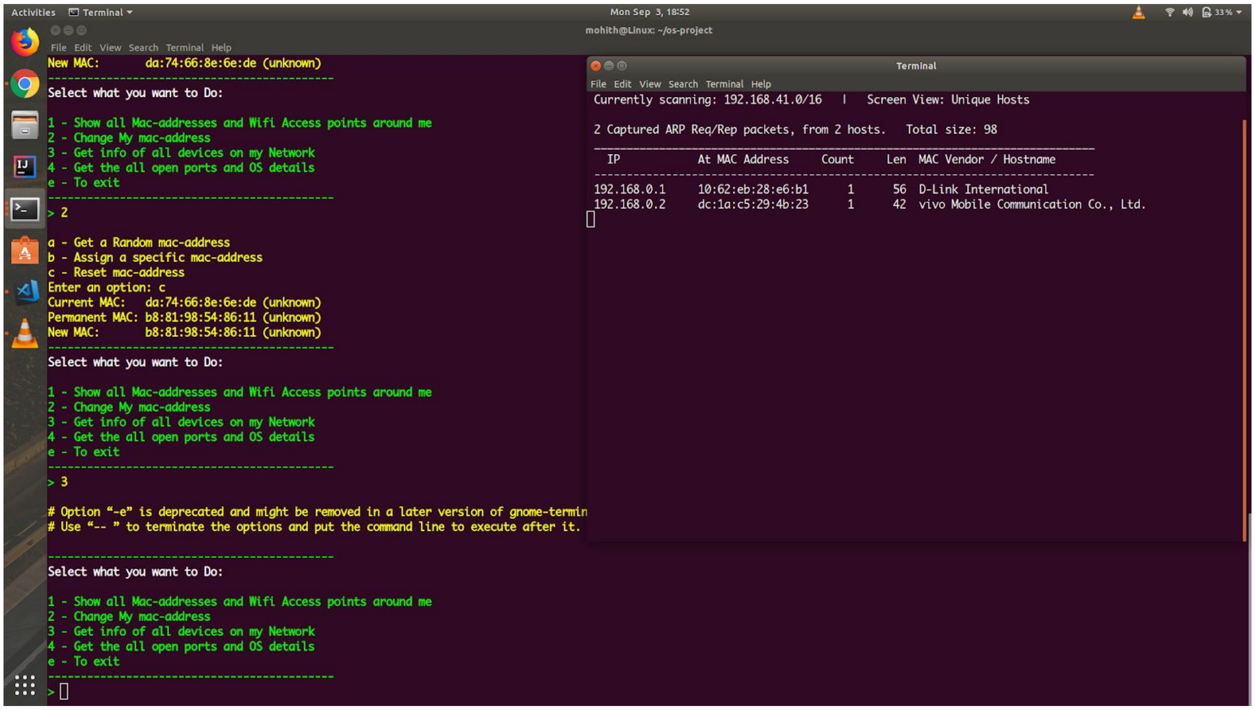
This function allows users to:

1) Get a random mac-address
2) Switch to a different mac-address
3) Reset mac-address

NOTE: If we change mac-address we no longer be able to connect to the previously connected network. Moreover its just a virtual mac-address on top of the hardware. And it is not possible to change mac-address permanently.

III. Get to know all devices connected to current network:

This function helps user to know which devices are connected to current network.


Activities
Terminal
Mon Sep 3, 18:52
mohith@Linux: ~/os-project
File Edit View Search Terminal Help
Terminal
File Edit View Search Terminal Help

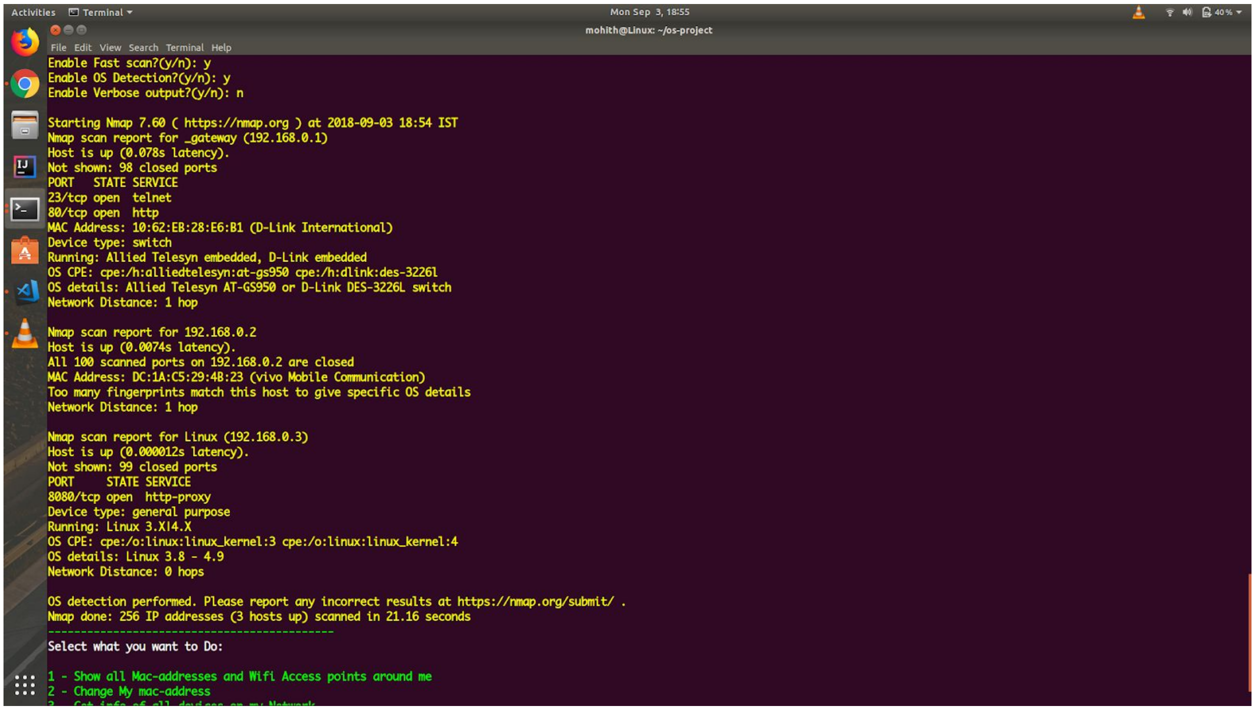
```
New MAC:       da:74:66:8e:6e:de (unknown)
--------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
--------------------------------------------
> 2

a - Get a Random mac-address
b - Assign a specific mac-address
c - Reset mac-address
Enter an option: c
Current MAC:   da:74:66:8e:6e:de (unknown)
Permanent MAC: b8:81:98:54:86:11 (unknown)
New MAC:       b8:81:98:54:86:11 (unknown)
--------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
--------------------------------------------
> 3

# Option “-e” is deprecated and might be removed in a later version of gnome-termin
# Use “-- ” to terminate the options and put the command line to execute after it.

--------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
4 - Get the all open ports and OS details
e - To exit
--------------------------------------------
> 
```

```
 Currently scanning: 192.168.41.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 98
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     10:62:eb:28:e6:b1      1      56  D-Link International
 192.168.0.2     dc:1a:c5:29:4b:23      1      42  vivo Mobile Communication Co., Ltd.
```

This function uses “netdiscover” tool and the function detects the user’s current network automatically and runs this tool. This opens a new live window showing all devices with their mac-address and device names.

IV. Get to know all devices connected to current network:

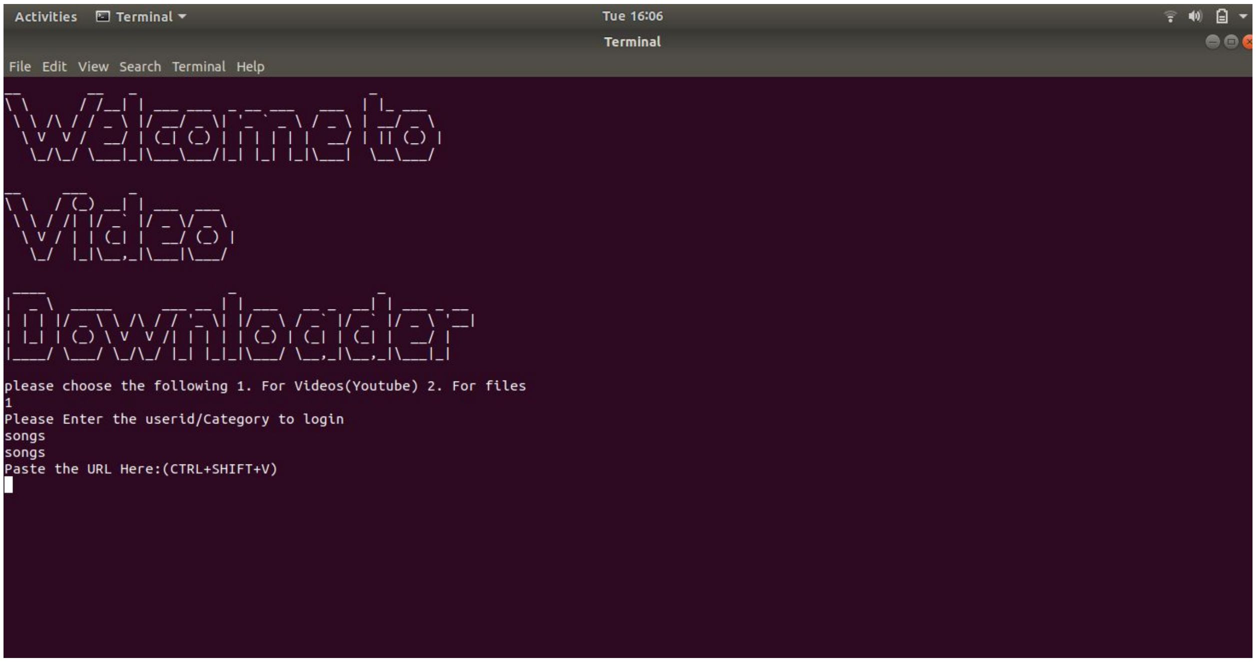
This function uses “nmap” tool to perform all types of scans on the hosts(devices) present on the current network. This indeed allows user to know which OS is running on the other host. This script also performs scans to check which ports are open on others hosts.


Activities
Terminal
Mon Sep 3, 18:55
mohith@Linux: ~/os-project
File Edit View Search Terminal Help

```
Enable Fast scan?(y/n): y
Enable OS Detection?(y/n): y
Enable Verbose output?(y/n): n

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-03 18:54 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.078s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: 10:62:EB:28:E6:B1 (D-Link International)
Device type: switch
Running: Allied Telesyn embedded, D-Link embedded
OS CPE: cpe:/h:alliedtelesyn:at-gs950 cpe:/h:dlink:des-3226l
OS details: Allied Telesyn AT-GS950 or D-Link DES-3226L switch
Network Distance: 1 hop

Nmap scan report for 192.168.0.2
Host is up (0.0074s latency).
All 100 scanned ports on 192.168.0.2 are closed
MAC Address: DC:1A:C5:29:4B:23 (vivo Mobile Communication)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for Linux (192.168.0.3)
Host is up (0.000012s latency).
Not shown: 99 closed ports
PORT     STATE SERVICE
8080/tcp open  http-proxy
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.9
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 21.16 seconds
---------------------------------------------
Select what you want to Do:

1 - Show all Mac-addresses and Wifi Access points around me
2 - Change My mac-address
3 - Get info of all devices on my Network
```

V. It is time to Download Some stuff from Youtube:

When the mac-address is obtained we can access the wifi by changing our mac-address. We just need the URL of the video to download it.



```
__        __   _                            _        
\ \      / /__| | ___ ___  _ __ ___   ___  | |_ ___  
 \ \ /\ / / _ \ |/ __/ _ \| '_ ` _ \ / _ \ | __/ _ \ 
  \ V  V /  __/ | (_| (_) | | | | | |  __/ | || (_) |
   \_/\_/ \___|_|\___\___/|_| |_| |_|\___|  \__\___/ 

__     ___     _            
\ \   / (_) __| | ___  ___  
 \ \ / /| |/ _` |/ _ \/ _ \ 
  \ V / | | (_| |  __/ (_) |
   \_/  |_|\__,_|\___|\___/ 

 ____                      _                 _           
|  _ \  _____      ___ __ | | ___   __ _  __| | ___ _ __ 
| | | |/ _ \ \ /\ / / '_ \| |/ _ \ / _` |/ _` |/ _ \ '__|
| |_| | (_) \ V  V /| | | | | (_) | (_| | (_| |  __/ |   
|____/ \___/ \_/\_/ |_| |_|_|\___/ \__,_|\__,_|\___|_|   
please choose the following 1. For Videos(Youtube) 2. For files
1
Please Enter the userid/Category to login
songs
songs
Paste the URL Here:(CTRL+SHIFT+V)
```