Admirer

IP: 10.10.10.187

Nmap

```
# nmap -sC -sV -p21,22,80,4242 10.10.10.187
```

Total scan time was 24.09 s. The 22 and 80 ports are open. The 21 and 4242 ports are closed. I ran a deeper scan on these specifically: `nmap -sC -sV -p21,22,80,4242 -T5 10.10.10.187`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 19:46 EDT
Nmap scan report for 10.10.10.187
Host is up (0.0386s latency).

PORT     STATE SERVICE VERSION
21/tcp   closed ftp
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:dd:a5:bd:b3:7b:8b:bd:2f:ff:cf:f6:a9:f2:fa:f2 (RSA)
|   256 d7:6f:64:f8:fb:c2:19:3f:2a:ed:d8:ad:d8:11:f1:6e (ECDSA)
|   256 09:d5:c2:04:95:1a:90:f9:60:7b:6b:d1:a0:a6:56:86 (ED25519)
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir/
|_http-server-header: Apache/2.4.25 (Debian)
4242/tcp closed vrml-multi-use

Service Info: Host: admirer.htb; OS: Linux; CPU: Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
```

Of course we can't just go to `admirer.htb`. So we'll add it to `/etc/hosts`. Port 21 is closed, so we can't do anything with `ftp`. Port 22 is `OpenSSH 7.4`, so there doesn't seem to be any `ssh` exploits. Port 80 is `Apache 2.4.25`. Port 4242 is closed.

Port 80 Website

Let's look at the main page's source, nothing too interesting. Looked at all the `.js` files, and downloaded all images and stuff (`wget -r -np -k -p http://admirer.htb`). Nothing. **Nmap** told us **robots.txt** exists, so let's go look there:

robots.txt

```
User-agent: *
# Directories
Disallow: /admin-dir/
# Files
Disallow: /assets/
# Paths (clean URLs)
Disallow: /admin/
Disallow: /assets/admin/
Disallow: /assets/admin-lte/
Disallow: /assets/bootstrap/
Disallow: /assets/dist/
Disallow: /assets/plugins/
Disallow: /assets/plugins/bootstrap-wysihtml5/
Disallow: /assets/plugins/ckeditor/
Disallow: /assets/plugins/datepicker/
Disallow: /assets/plugins/datetime-picker/
Disallow: /assets/plugins/fastclick/
Disallow: /assets/plugins/fileupload/
Disallow: /assets/plugins/fullcalendar/
Disallow: /assets/plugins/jquery-ui/
Disallow: /assets/plugins/jvectormap/
Disallow: /assets/plugins/slimscroll/
Disallow: /assets/plugins/timepicker/
Disallow: /assets/plugins/timepicker-addon/
Disallow: /assets/plugins/timepicker-addon-lang/
Disallow: /assets/plugins/timepicker-addon-sliderAccess/
Disallow: /assets/plugins/timepicker-addon-timeformat/
Disallow: /assets/plugins/timepicker-addon-timezone/
Disallow: /assets/plugins/timepicker-addon-validation/
Disallow: /assets/plugins/timepicker-addon-year/
Disallow: /assets/plugins/timepicker-addon-yearAndMonth/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDay/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHour/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinute/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecondAndDecisecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecondAndDecisecondAndDecisecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecondAndDecisecondAndDecisecondAndDecisecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecondAndDecisecondAndDecisecondAndDecisecondAndDecisecond/
Disallow: /assets/plugins/timepicker-addon-yearAndMonthAndDayAndHourAndMinuteAndSecondAndMillisecondAndMicrosecondAndNanosecondAndPicosecondAndFemtosecondAndAttosecondAndZeptosecondAndYoctosecondAndNonosecondAndDecis
```