Avenger's Blog

Nmap

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-05 08:25 CDT
Nmap scan report for 10.10.169.216
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp
                   vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
    2048 ac:2c:20:2e:5f:3c:df:bb:b4:5b:62:19:93:ba:15:06 (RSA)
    256 ac:04:2e:3d:35:f1:7e:8a:24:3e:e2:c0:55:96:d9:a6 (ECDSA)
256 a2:33:4a:f7:df:34:b3:cb:52:75:91:38:e7:68:24:7d (ED25519)
80/tcp open http
                   Node.js Express framework
http-title: Avengers! Assemble!
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=7/5%OT=21%CT=1%CU=37733%PV=Y%DS=4%DC=T%G=Y%TM=60E30880
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)SEQ(
OS:SP=102%GCD=2%ISR=105%TI=Z%CI=Z%TS=A)OPS(01=M506ST11NW7%02=M506ST11NW7%03
OS:=M506NNT11NW7%04=M506ST11NW7%05=M506ST11NW7%06=M506ST11)WIN(W1=68DF%W2=6
OS:8DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M506NNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel
TRACEROUTE (using port 993/tcp)
HOP RTT
             ADDRESS
   57.10 ms 10.6.0.1
   ... 3
2
   125.74 ms 10.10.169.216
OS and Service detection performed. Please report any incorrect results at
```

https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 31.55 seconds

Flag 1

The web-page displays blog comments from users. Inspecting the page with developer tools gives us our first flag.



I also noticed the rocket user mentioned helping reset groot's password.



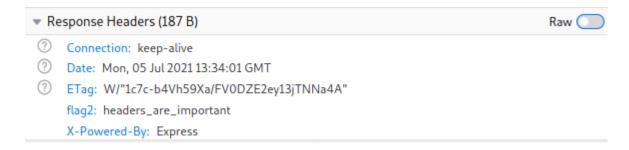
Rocket

Groot asks if someone can reset his password. He said the last one he can remember is iamgroot?

Lets take note of this and move on.

Flag 2

We need to investigate the response headers of the page to obtain the second flag. We can use the developer tools again and look for the request within the network tab.



We can also view them raw.



Flag 3

Now we move onto to he FTP service. We can try logging in with the credentials we found on the blog for groot.

```
root kali)-[~/thm/rooms/avengers]

# ftp 10.10.169.216

Connected to 10.10.169.216.

220 (vsFTPd 3.0.3)

Name (10.10.169.216:root): groot

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp>

■
```

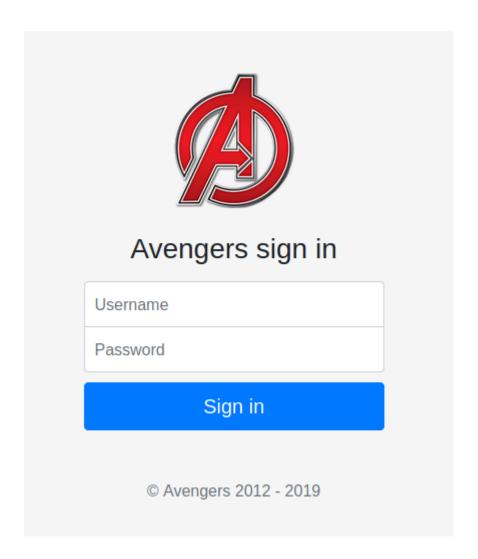
Move into the files directory and download the flag.

Flag 4

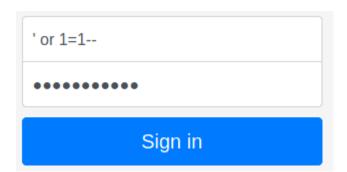
Now we will use gobuster to brute-force directories on the blog.

```
2021/07/05 08:46:20 Starting gobuster in directory enumeration mode
/img
                       (Status: 301) [Size: 173] [--> /img/]
                      (Status: 302) [Size: 23] [--> /]
/home
                      (Status: 302) [Size: 23] [--> /]
/Home
                      (Status: 301) [Size: 179] [--> /assets/]
/assets
                      (Status: 200) [Size: 1409]
/portal
                      (Status: 301) [Size: 173] [--> /css/]
/css
 js
                       (Status: 301) [Size: 171] [--> /js/]
 logout
                       (Status: 302) [Size: 29] [--> /portal]
```

We find the portal directory which contains the login page.



You can bypass authentication by using SQL injection. Enter ' or 1=1 -- in both the Username and Password Fields.



Once logged in, view the source of the page to count the number of lines of code to complete the challenge.

Flag 5

The Jarvis web page lets us run commands on the machine. Try running a few commands to read the flag.

You will not be able to use "cat" to read the file. Instead try using less

Command results

avengers flag5.txt d335e2d13f36558ba1e67969a1718af7

Welcome to the Javis Development Environment. We can directly interactive with Jarvis using the command line..

Command

cd ../; ls; less flag5.txt